

**IN THE SUPERIOR COURT FOR THE DISTRICT OF COLUMBIA  
CIVIL DIVISION**

MUSLIM ADVOCATES,

*Plaintiff,*

v.

MARK ZUCKERBERG, *et al.*,

*Defendants.*

**Case No.: 2021 CA 001114 B**

Judge Anthony C. Epstein

**Exhibit A**

IN THE SUPERIOR COURT FOR THE DISTRICT OF COLUMBIA  
CIVIL DIVISION

MUSLIM ADVOCATES,

*Plaintiff,*

v.

MARK ZUCKERBERG, *et al.*,

*Defendants.*

Case No. 2021 CA 001114 B

**DECLARATION OF STEPHANIE R. CORREA**

STEPHANIE R. CORREA, being duly sworn, deposes and says:

1. I am a Supervising Staff Attorney at Muslim Advocates.
2. I am familiar with this matter based upon a review of the file maintained by Muslim Advocates.
3. I submit this declaration, along with the accompanying exhibits, in support of Plaintiff's Opposition to Defendants' Special Motion to Dismiss, based on my organizational knowledge.

**Muslim Advocates (hereinafter "MA")**

4. MA is a public interest, nonprofit organization based in the District of Columbia. Annexed hereto as Exhibit 1 is a true and accurate copy of MA's 501(c)(3) Certificate.
5. MA is a national civil rights organization committed to ensuring that American Muslims have expert representation so that all people, including American Muslims, may live free from hate and discrimination. Annexed hereto as Exhibit 3 is a true and accurate copy of MA's Mission Statement and History. (<https://muslimadvocates.org/about/#OurMission>).

## Individual Defendants

6. Mark Zuckerberg (“Defendant Zuckerberg”) is the Founder, Chairman and Chief Executive Officer of Facebook, Inc. Annexed hereto as Exhibit 4 is a true and accurate copy of Defendant Zuckerberg’s Facebook Profile. Defendant Zuckerberg plays a central role in marketing Facebook’s services. *See Mark Zuckerberg Reveals the Future of Facebook at F8 Event*, <https://www.youtube.com/watch?v=LY6zxU1f92Y&t=1283s>. Annexed hereto as Exhibit 13 is a true and accurate copy of Elizabeth Culliford, Munsif Vengattil, and Sheila Dang’s article published by Reuters, *Facebook takes on Clubhouse, unveils upcoming audio products*, on April 19, 2021, describing Defendant Zuckerberg promoting a new Facebook feature. (<https://www.reuters.com/technology/facebook-announces-new-audio-product-2021-04-19/>).

7. Sheryl K. Sandberg (“Defendant Sandberg”) is the Chief Operating Officer of Facebook, Inc. Annexed hereto as Exhibit 5 is a true and accurate copy of Defendant Sandberg’s Facebook Profile. Sandberg frequently communicates with the public about Facebook’s services. Annexed hereto as Exhibit 14 is a true and accurate copy of Christine Lagorio-Chafkin’s article published by Inc., *Facebook’s Sheryl Sandberg Breaks Silence about Business Practices, Outage*, reporting on Sandberg’s praise for Facebook at the 2021 Inc. 5000 Vision Conference. <https://www.inc.com/christine-lagorio-chafkin/facebook-sheryl-sandberg-mark-zuckerberg-outage-small-business.html>. Annexed hereto as Exhibit 15 is a true and accurate copy of Abigail Freeman’s article published by Forbes, *Sheryl Sandberg on Facebook’s Role in Small Business Support and Voter Registration During the Pandemic*, on September 28, 2020, describing Sandberg’s address at Forbes’ Small Business Summit to promote Facebook’s services. (<https://www.forbes.com/sites/abigailfreeman/2020/09/28/sheryl-sandberg-on-facebooks-role-in-small-business-support-and-voter-registration-during-the-pandemic/?sh=288d2f3a2bfb>).

8. Joel Kaplan (“Defendant Kaplan”) is the Vice President for Global Policy of Facebook, Inc., and he is responsible for managing the company’s global public policy strategy. Annexed hereto as Exhibit 6 is a true and accurate copy of Joel Kaplan’s Professional Background from the Bush Center. (<https://www.bushcenter.org/people/joel-kaplan.html>).

9. Kevin J. Martin (“Defendant Martin”) is the head of Facebook’s Global Economic Policy Team and formally served as the Vice President of Facebook’s U.S. Public Policy at Facebook. Annexed hereto as Exhibit 7 is a true and accurate copy of Kevin J. Martin’s Professional Background from the World Economic Forum. (<https://www.weforum.org/people/kevin-j-martin>).

**Defendant Facebook, Inc.<sup>1</sup>**

***Influence***

10. Facebook pays law firms and lobbyists in the District of Columbia to influence federal government and national leaders. Annexed hereto as Exhibit 8 is a true and accurate copy of Lauren Feiner’s article published on CNBC.com, *Facebook Spent More On Lobbying Than Any Other Big Tech Company in 2020*, on January 22, 2021. (<https://www.cnbc.com/2021/01/22/facebook-spent-more-on-lobbying-than-any-other-big-tech-company-in-2020.html>).

11. Facebook is a product which advertises itself as allowing families, friends and communities to remain connected. Annexed hereto as Exhibit 61 is a true and accurate copy of Facebook App’s Description. (<https://about.facebook.com/technologies/facebook-app/>).

---

<sup>1</sup> Subsequent to the Defendants’ joint filings on September 17, 2021, the Defendant company rebranded and changed its name to Meta. However, for the sake of this Opposition, Plaintiff will continue referring to the Defendant company as “Facebook.”

### *Users*

12. Facebook has billions of users around the world and nearly 60% of the United States' population uses Facebook's services amounting to approximately 200 million U.S. users. Annexed hereto as Exhibit 9 is a true and accurate excerpt from Facebook's 10-K Tax Form for Fiscal Year Ending in December 2020 at P. 52 (<https://d18rn0p25nwr6d.cloudfront.net/CIK-0001326801/4dd7fa7f-1a51-4ed9-b9df-7f42cc3321eb.pdf>); Annexed hereto as Exhibit 10 is a true and accurate copy of Statista Research Department's *Most popular social networks worldwide as of October 2021*, which shows the amount of Facebook users. (<https://www.statista.com/statistics/268136/top-15-countries-based-on-number-of-facebook-users/>).

### *Facebook's Terms of Service*

13. Annexed hereto as Exhibit 11 is a true and accurate copy of Facebook's Terms of Service as of August 9, 2021 which describes the terms that a user agrees to when using Facebook's products and services. The Terms include, but are not limited to, agreeing to abide by Facebook's Community Standards and allowing Facebook to collect user data. (<https://perma.cc/M659-BCZV>).

14. Annexed hereto as Exhibit 12 is a true and accurate copy of David Nield's article published in Wired, *All the Ways Facebook Tracks You—And How to Limit It*, on January 12, 2020. The article highlights Facebook's tracking efforts and how Facebook is given permission to collect user data whenever a user logs on to the platform. (<https://www.wired.com/story/ways-facebook-tracks-you-limit-it/>).

### *Facebook's Community Standards*

15. Annexed hereto as Exhibit 16 is a true and accurate copy of Facebook's current Community Standards, which prohibit the following conduct or content on the company's platform: Hate Speech, Violent and Graphic Content, Violence and

Incitement, Dangerous Individuals and Organizations, Coordinating Harm and Publicizing Crime, n Bullying and Harassment

***Facebook's Business Model***

16. Annexed hereto as Exhibit 9 is a true and accurate excerpt from Facebook's 2020 Form 10-K (pp 1-27; 50-53), which sets forth that substantially all of Facebook's revenue is generated by third-party advertising, thus any decreases in user engagement would adversely affect Facebook's revenue. Ex. 9 at 10. Moreover, in it, Facebook acknowledges that "[t]he size of our user base and our users' level of engagement are critical to our success. Our financial performance has been and will continue to be significantly determined by our success in adding, retaining, and engaging active users of our products, particularly for Facebook." *Id.* at 15. In this disclosure, Facebook further asserts: "If we are unable to maintain or increase our user base and user engagement, our revenue and financial results may be adversely affected. Any decrease in user retention, growth, or engagement could render our products less attractive to users, marketers, and developers, which is likely to have a material and adverse impact on our revenue, business, financial condition, and results of operations. If our active user growth rate continues to slow, we will become increasingly dependent on our ability to maintain or increase levels of user engagement and monetization in order to drive revenue growth." *Id.* at 11.

17. Annexed hereto as Exhibit 53 is a true and accurate copy of Robert J. Shapiro's article published on Washington Monthly, *What Your Data is Really Worth to Facebook*, in July/August 2019, "conservatively estimating that tech companies 'earned an average of \$202 per American internet user' in 2018 from "scoop[ing] up, analyz[ing], and sell[ing] our personal information." (<https://washingtonmonthly.com/magazine/july-august-2019/what-your-data-is-really-worth-to-facebook/>).

18. Annexed hereto as Exhibit 78 is a true and accurate copy description of how Facebook uses look alike audiences to assist with its business model, stating “A lookalike audience is a way your ads can reach new people who are likely to be interested in your business because they share similar characteristics to your existing customers.” In addition, Facebook sets forth that “our system leverages information such as demographics, interests and behaviors from your source audience.” (<https://www.facebook.com/business/help/164749007013531?id=401668390442328>).

19. Annexed hereto as Exhibit 19 is a true and accurate copy of Lake Munn’s article published in Humanities and Social Sciences Communications, Vol. 7, *Angry by Design: Toxic Communication and Technical Architectures* in 2020 which found that an internal research team in 2018 found that Facebook was “feeding people ‘more and more divisive content in an effort to gain user attention and increase time on the platform.’ However, Facebook management ignored these findings and shelved the research.” (<https://www.nature.com/articles/s41599-020-00550-7>).

20. Annexed hereto as Exhibit 81 is a true and accurate copy of Len Sherman’s article published in Forbes, *Why Facebook Will Never Change Its Business Model*, on April 16, 2018, asserting that Facebook is free to users because “the price advertisers are willing to pay Facebook to invade users’ privacy is vastly greater than the price most consumers would be willing to pay Facebook to protect their privacy.” (<https://www.forbes.com/sites/lensherman/2018/04/16/why-facebook-will-never-change-its-business-model/?sh=6ca7113f64a7>).

***Facebook’s Enforcement of its Community Standards and Content Moderation***

21. Annexed hereto as Exhibit 20 is a true and accurate copy of Andy Serwer and Max Zahn’s article published on Yahoo Finance, *Facebook’s Zuckerberg and Sandberg Are This Involved with the Company’s Content Issues*, on September 9, 2010, which discusses how Defendant Sandberg and Defendant Zuckerberg are closely involved with Facebook’s promulgation and implementation of Facebook’s Community Standards. ([tinyurl.com/ija5cxv7](http://tinyurl.com/ija5cxv7)).

22. Annexed hereto as Exhibit 54 is a true and accurate copy of Elizabeth Dwoskin, Tory Newmyer and Shibani Mahtani’s article published by the Washington Post, *The case against Mark Zuckerberg: Insiders say Facebook’s CEO chose growth over safety*, on October 25, 2021, discussing Defendant Zuckerberg’s deep involvement in content moderation as a force for growth at the expense of stated policies and values.

[\(https://www.washingtonpost.com/technology/2021/10/25/mark-zuckerberg-facebook-whistleblower/\)](https://www.washingtonpost.com/technology/2021/10/25/mark-zuckerberg-facebook-whistleblower/)

23. Annexed hereto as Exhibit 21 is a true and accurate copy of Ryan Mac and Craig Silverman’s article published on BuzzFeed News, *How Facebook Was Easy on Alex Jones and other Right-Wing Figures*, on February 22, 2021, discussing Defendant Zuckerberg’s and Defendant Kaplan’s changes to content moderation policies to allow misinformation and hate to remain on Facebook’s platform, which sets forth: “Internal documents obtained by BuzzFeed News and interviews with 14 current and former employees show how the company’s policy team — guided by Joel Kaplan, the vice president of global public policy, and Zuckerberg’s whims — has exerted outsize influence while obstructing content moderation decisions, stymieing product rollouts, and intervening on behalf of popular conservative figures who have violated Facebook’s rules.” (<https://www.buzzfeednews.com/article/ryanmac/mark-zuckerberg-joel-kaplan-facebook-alex-jones>).

24. Facebook’s 2020 10-K SEC filing, Ex. 9, sets forth that Defendant Zuckerberg “has control over key decision making as a result of his control of a majority of the voting power” and that “regulatory or legislative actions affecting the manner in which we display content to our users or obtain consent to various practices, or otherwise relating to content that is made able to our products, could adversely affect our financial results.” Exhibit 9 at pp. 8, 25.

25. Annexed hereto as Exhibit 2 is a true and accurate copy of Jeff Horwitz’s article published in the Wall Street Journal, *Facebook Says Its Rule Apply to All. Company Documents Reveal a Secrete Elite That’s Exempt*, on September 13, 2021, which highlights that Facebook has exempted “elite” users from enforcement of Facebook’s Community Standards. (<https://www.wsj.com/articles/facebook-files-xcheck-zuckerberg-elite-rules-11631541353>).

26. Annexed hereto as Exhibit 80 is a true and accurate copy of a letter from John Tye and Andrew Bakaj to SEC Office of the Whistleblower, which sets forth that Facebook mislead investors and the public about equal enforcement of its terms given that high-profile users are ‘whitelisted’ under its ‘XCheck’ program. (A set of whistleblower complaints are available at <https://www.cbsnews.com/news/facebook-whistleblower-sec-complaint-60-minutes-2021-10-04/>).

27. Annexed hereto as Exhibit 64 is a true and accurate copy of Tim De Chant’s article published on Ars Technica, *Facebook AI Moderators Confused Videos of Mass Shootings and Car Washes*, on October 19, 2021, reporting that “Facebook made it a goal to “reduce \$ cost of total hate review capacity by 15% . . . .” (<https://arstechnica.com/tech-policy/2021/10/facebook-ai-moderator-confused-videos-of-mass-shootings-and-car-washes/>).

28. Annexed hereto as Exhibit 70 is a true and accurate copy of David Ingram, Olivia Solon, Brandy Zadrozny, and Cyrus Farivar’s article published on NBC News, *The Facebook Papers: Documents Reveal Internal Fury and Dissent Over the Site’s Policies*, on October 25, 2021, reporting that internal Facebook documents reveal “the company’s automated systems deleted only about 2 percent of hate speech as of 2019 and, as of this year, less than 1 percent of content trying to incite violence.” (<https://www.nbcnews.com/tech/tech-news/facebook-whistleblower-documents-detail-deep-look-facebook-rcna3580>)

29. Annexed hereto as Exhibit 17 is a true and accurate copy of a letter from John Tye and Andrew Bajak to the SEC Office of the Whistleblower regarding “Facebook misled investors

and the public about the negative consequences of its algorithms, which claim to prioritize 'meaningful social interactions' ... but which actually promote virality of polarizing information and hate speech.” Moreover, this document asserts that research “has shown how outrage and misinformation are more likely to be viral.” (A set of whistleblower complaints are available at <https://www.cbsnews.com/news/facebook-whistleblower-sec-complaint-60-minutes-2021-10-04/>).

30. Annexed hereto as Exhibit 63 is a true and accurate copy of a letter from John Tye and Andrew Bajak to the SEC Office of the Whistleblower, which sets forth that Facebook misled investors and the public about removing hate speech when internal records show as little as 3-5% of hate speech is removed. (A set of Whistleblower Complaints related to Frances Haugen are available at <https://www.cbsnews.com/news/facebook-whistleblower-sec-complaint-60-minutes-2021-10-04/>).

31. Annexed hereto as Exhibit 18 is a true and accurate copy of Deepa Seetharaman, Jeff Horowitz and Justin Scheck’s article published in the Wall Street Journal, *Facebook Says AI Will Clean Up the Platform. Its Own Engineers Have Doubts*, on October 17, 2021, noting that Facebook only removes 3% to 5% of hate speech on its platform. (<https://www.wsj.com/articles/facebook-ai-enforce-rules-engineers-doubtful-artificial-intelligence-11634338184>).

***Facebook’s Billions of Dollars in Revenue and Profits Reported for 2018 and 2019***

32. Annexed hereto as Exhibit 22 is a true and accurate excerpt from Facebook’s Form 10-K for Fiscal Year Ending in December 31, 2018, p. 15.

(<https://www.sec.gov/Archives/edgar/data/1326801/000132680119000009/fb-12312018x10k.htm>)

33. Annexed hereto as Exhibit 23 is a true and accurate excerpt of Facebook’s Form 10-K for Fiscal Year Ending in December 31, 2019 reporting Facebook’s revenue and profits,

p.44. (<https://www.sec.gov/Archives/edgar/data/1326801/000132680120000013/fb-12312019x10k.htm>).

*Facebook Executives Congressional Testimonies & Involvement*

**Defendant Zuckerberg**

34. Annexed hereto as Exhibit 25 is a true and accurate excerpt of Mark Zuckerberg's Testimony before the Senate Commerce and Judiciary Committees on April 10, 2018, where he represented that: "when content gets flagged to us . . . if it violates our policies then we take it down." The full testimony can be found at: (<https://www.govinfo.gov/content/pkg/CHRG-115shrg37801/html/CHRG-115shrg37801.htm>).

35. Annexed hereto as Exhibit 26 is a true and accurate excerpt of Mark Zuckerberg's Testimony before the House Energy and Commerce Committee on April 11, 2018, where he further stated on Page 67, "We do not allow hate groups on Facebook overall. So, if there is a group that their primary purpose or a large part of what they do is spreading hate, we will ban them from the platform overall." He added that when it comes to ads that violate Facebook's policies, if the ads "are flagged for us we will review and take [them] down if they violate our policies[.]" The full testimony can be found at (<https://www.govinfo.gov/content/pkg/CHRG-115hrg30956/pdf/CHRG-115hrg30956.pdf>).

36. Annexed hereto as Exhibit 27 is a true and accurate excerpt of Mark Zuckerberg's June 8, 2019 responses to questions for the record from the Senate Commerce Committee, in which he told the Committee: "Our Community Standards and Ads Policies outline the content that is not allowed on the platform, such as hate speech, fake accounts, and praise, support, or representation of terrorism/terrorists. When we find things that violate these Standards, we remove them." He added that "[c]ontent that violates our Community Standards is removed when [Facebook is] made aware of it," and that Facebook "remove[s] content that violates [its] policies,

regardless of who posted the content.” The full responses can be found at:

(<https://www.judiciary.senate.gov/imo/media/doc/Zuckerberg%20Responses%20to%20Judiciary%20Committee%20QFRs.pdf>).

### **Defendant Sandberg**

37. Annexed hereto as Exhibit 28 is a true and accurate excerpt from Sheryl Sandberg’s statement during the Senate Intelligence Committee’s Open Hearing on Foreign Influence Operations’ Use of Social Media Platforms on September 5, 2018 where she made the following assurances, “Senators, let me be clear. We are more determined than our opponents, and we will keep fighting. When bad actors try to use our site, we will block them. When content violates our policies, we will take it down.” The full testimony can be found at

(<https://www.govinfo.gov/content/pkg/CHRG-115shrg31350/html/CHRG-115shrg31350.htm>)

### **Nathaniel Gleicher, Facebook’s Head of Cyber Security Policy**

38. Mr. Gleicher’s testimony to Congress again affirms Facebook’s commitment to not allow content on Facebook to remain which violates its Community Standards. Annexed hereto as Exhibit 29 is a true and accurate excerpt from Nathaniel Gleicher’s testimony before the House Intelligence Committee on June 18, 2020. The full testimony can be found at

(<https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=110805>); Annexed hereto as

Exhibit 30 is a true and accurate excerpt from Nathaniel Gleicher’s Testimony before the House Committee on Oversight and Reform, Subcommittee on National Security on May 22, 2019. The full testimony can be found at ([https://www.govinfo.gov/content/pkg/CHRG-](https://www.govinfo.gov/content/pkg/CHRG-116hhr36662/pdf/CHRG-116hhr36662.pdf)

[116hhr36662/pdf/CHRG-116hhr36662.pdf](https://www.govinfo.gov/content/pkg/CHRG-116hhr36662/pdf/CHRG-116hhr36662.pdf)); Annexed hereto as Exhibit 31 is a true and

accurate excerpt from Mr. Gleicher’s testimony before the House Committee on Veterans Affairs on November 13, 2019. The full testimony can be found at

<https://docs.house.gov/meetings/VR/VR00/20191113/110183/HHRG-116-VR00-Wstate-GleicherN-20191113.pdf>).

**Monika Bickert, Facebook’s Head of Global Policy Management**

39. Ms. Bickert similarly made representations to Congress similar to her peers regarding Facebook’s efforts to remove content from the platform that violates Facebook’s Community Standards. Annexed hereto as Exhibit 32 is a true and accurate excerpt from Monika Bickert’s testimony before the Senate Committee on Commerce, Science and Transportation on January 17, 2018. The full testimony can be found at

[https://www.commerce.senate.gov/services/files/A9DACCB8-5F07-42A6-B4C3-](https://www.commerce.senate.gov/services/files/A9DACCB8-5F07-42A6-B4C3-20AD0B9BA26D)

[20AD0B9BA26D](https://www.commerce.senate.gov/services/files/A9DACCB8-5F07-42A6-B4C3-20AD0B9BA26D)); Annexed hereto as Exhibit 33 is a true and accurate excerpt from Monika Bickert’s testimony before the Senate Committee on Commerce, Science and Transportation on September 18, 2019. The full testimony can be found at

<https://www.commerce.senate.gov/services/files/53DEE3E9-C1D2-4A00-BFCE-3FC3C3297386>)

**Neil Potts, Vice President of Public Policy**

40. Echoing his peers, Neil Potts provided the following written testimony to the House Committee on the Judiciary on April 9, 2019: “We disallow hate speech because it creates an environment of intimidation and exclusion that limits people’s willingness to communicate and share with one another. In fact, Facebook rejects not just hate speech, but all hateful ideologies. That means that white supremacists are not allowed on our platform under any circumstances, and we have recently announced a ban on white nationalism and white separatism as well. We will therefore now use our Dangerous Organizations policy to remove from our platform praise, support, or representation of white supremacy, as well as of white nationalism or white separatism, because both ideologies are inextricably linked with white supremacy and with violence more generally. We have already banned more than 200 white supremacist groups because of our

Dangerous Organizations policy.” His Congressional testimony further highlighted Facebook’s ban on white nationalists from the platform. *See* (<https://www.c-span.org/video/?459662-1/house-judiciary-committee-holds-hearing-hate-crimes#>) at 32:40- 35:00 and 3:07:00- 3:08:00) The full testimony can be found at (<https://www.judiciary.senate.gov/imo/media/doc/Potts%20Testimony.pdf>).

### **Defendant Kaplan**

41. Annexed hereto as Exhibit 36 is a true and accurate copy of Ethan Wolff-Mann’s article published in Yahoo Finance, *Here’s Who is Sitting Behind Mark Zuckerberg and Why They’re There*, on April 11, 2018, shows that Defendant Kaplan accompanied Defendant Zuckerberg to the House and Senate Hearings in which he testified in April 2018.

42. Annexed hereto as Exhibit 24 is a true and accurate copy of an image taken from Congressional Hearings showing Defendant Kaplan sitting directly behind and staffing Defendant Mark Zuckerberg. Full videos can be found at <https://www.youtube.com/watch?v=BylLTX05jSY>, <https://www.youtube.com/watch?v=h3vkyVC7Qj8> and <https://www.youtube.com/watch?v=B1a5h5KncNM>).

43. Annexed hereto as Exhibit 82 is a true and correct copy of Chris Taylor’s article published by Mashable, *Zuck is a lightweight, and 4 more things we learned about Facebook from ‘An Ugly Truth’*, on July 17, 2021, describing how Joel Kaplan interceded in content moderation policy to create loopholes for certain hate speech and misinformation. (<https://sea.mashable.com/tech/16760/zuck-is-a-lightweight-and-4-more-things-we-learned-about-facebook-from-an-ugly-truth>).

44. Annexed hereto as Exhibit 35 is a true and correct copy of a Noticias Financieras article, *Facebook Papers: 10 shocking revelations from the leaked documents*, published on

October 26, 2021, describing Joel Kaplan's influence in creating exceptions for powerful right-wing figures from content moderation enforcement.

**Defendant Martin**

45. Annexed hereto as Exhibit 2 is a true and accurate copy of Jeff Horwitz's article published in the Wall Street Journal, *Facebook Says Its Rule Apply to All. Company Documents Reveal a Secrete Elite That's Exempt, on September 13, 2021*, which shows an image of Kevin Martin sitting directly behind and staffing Mark Zuckerberg at an October 23, 2019 House Financial Services hearing and being handed a briefing book by Zuckerberg. (<https://www.wsj.com/articles/facebook-files-xcheck-zuckerberg-elite-rules-11631541353>).

46. Annexed hereto as Exhibit 24 is a true and accurate copies of an image taken from the October 23, 2019 House Financial Services hearing in which Kevin Martin sat directly behind and staffed Mark Zuckerberg. A full video can be found at: <https://www.youtube.com/watch?v=B1a5h5KncNM>

***Emails Between MA and Facebook Executives Regarding Facebook's Policies***

47. Facebook Executives represented to MA staff that the company will remove content which violates Facebook's Community Standards when the company is aware of such content. Annexed hereto as Exhibit 38 is a true and accurate copy of Monique Dorsainvil's, Facebook's Public Policy Director email to MA's former Executive Director, Farhana Khera, on May 26, 2019; Annexed hereto as Exhibit 39 is a true and accurate copy of Defendant Sandberg's Email to Ms. Khera on May 1, 2019; Annexed hereto as Exhibit 40 is a true and accurate copy of Defendant Martin's March 17, 2020 Email to Naheed Quereshi.

***Facebook Staff's Representations to the Media Regarding Facebook's Policies***

48. Facebook executives also directly addressed the matter of hate speech and violent content being banned from the platform to the Media. Annexed hereto as Exhibit 41 is a true and

accurate copy of Michael McGowan, Christopher Knaus and Nick Evershed's article published in The Guardian, *Monetising Hate: Covert Enterprise Co-opts Far-Right Facebook Pages to Churn out Anti-Islamic Posts*, on December 5, 2019.

(<https://www.theguardian.com/technology/2019/dec/05/monetising-hate-covert-enterprise-co-opts-far-right-facebook-pages-to-churn-out-anti-islamic-posts>); Annexed hereto as Exhibit 42 is a true

and accurate copy of Alex Hern's article published in The Guardian, *Facebook Leak Underscores Strategy to Operate in Oppressive Regimes*, on March 23, 2021.

(<https://www.theguardian.com/technology/2021/mar/23/facebook-leak-underscore-strategy-operate-repressive-regimes>)

***Facebook's Representations to Other Organizations Regarding Its Policies***

49. Annexed hereto as Exhibit 37 is a true and accurate copy of Mr. Zafar's email to Ms. Khera, Ms. Qureshi, and Ms. Ahussain on December 18, 2018, stating, "As Sheryl Sandberg notes in this Newsroom Post, Facebook is committed to working with leading U.S. civil rights organizations such as Muslim Advocates to strengthen and advance civil rights on our service."

50. Annexed hereto as Exhibit 43 is a true and accurate copy of Michael Edison Hayden's article published in Newsweek, *Facebook Has Failed to Stop Anti-Muslim hate Groups Despite Mark Zuckerberg's Pledge*, on April 20, 2018 highlighting MA's engagement with Facebook. (<https://www.newsweek.com/facebook-anti-muslim-hate-groups-890338>).

51. Annexed hereto as Exhibit 79 is a true and accurate copy of Craig Timberg's article published in the Washington Post, *Civil Rights Leaders Thought They'd Figured Out how to Deal with Facebook*, on October 25, 2019, in which a Facebook spokesperson describes Facebook as a partner to the civil rights community.

(<https://www.washingtonpost.com/technology/2019/10/25/civil-rights-leaders-thought-theyd-figured-out-how-deal-with-facebook-now-they-are-livid/>)

*Facebook Executive's Direct Solicitations to MA*

52. Facebook's executives sought MA's expertise on various occasions. Annexed hereto as Exhibit 44 is a true and accurate copy of Shaarik Zafar's, Facebook's former Special Representatives to the Muslim Communities, email to Ms. Ahussain dated September 16, 2019, in which he solicits Ms. Ahussain's insights on how Facebook can address anti-Muslim stereotypes; Annexed hereto as Exhibit 45 is a true and accurate copy of Facebook's Employee, Georgina Fields', Email to Ms. Ahussain dated September 18, 2019, in which she requests MA's participation in a project to update Facebook's Community Standards; Annexed hereto as Exhibit 46 is a true and accurate copy of Facebook's Employee, Kim Malfacini's, Email to Ms. Ahussain dated December 12, 2019, asking for feedback on how Facebook can improve its Standards related to harassment of public figures; Annexed hereto as Exhibit 47 is a true and accurate copy of Mr. Zafar's December 17, 2019 Email to Ms. Ahussain requesting her input on common words, phrases, and images used in anti-Muslim hate speech for a project updating Facebook's Standards.

53. The Individual Defendants, including Defendant Zuckerberg and Defendant Sandberg also told MA staff they valued Facebook's partnership with MA. Annexed hereto as Exhibit 48 is a true and accurate copy of Linday Elin's, Facebook's Vice President of Public Policy and External Affairs, May 5, 2018 Email to Ms. Khera where Ms. Elin stated "Thanks Farhana, these reflect the points I outlined in my email to you all yesterday. We're on the same page. Let's get started in crafting our next steps on the thread I started. Together, we'll make progress." Annexed hereto as Exhibit 49 is a true and accurate copy of Ms. Dorsainvil's Email to Ms. Khera dated June 30, 2019 where Ms. Dorsainvil stated "Civil rights and liberties issues that have been flagged by third party stakeholders have been an invaluable part of this process. Shaarik [Zafar] shared some of your team's early feedback on the report. As we continue our work to advance and strengthen civil rights on Facebook, we look forward to more dialogue and partnership with

you.”; Annexed hereto as Exhibit 50 is a true and accurate copy of Defendant Zuckerberg’s November 6, 2019 Email to Ms. Khera where he stated, “I’m grateful for your partnership with [Defendant Sandberg] to provide us with guidance and advice, and I plan to stay close to the work to follow our progress.”; and Annexed hereto as Exhibit 51 is a true and accurate copy of Defendant Sandberg’s January 11, 2021 Email to Ms. Khera where she stated: “We are truly grateful for the guidance and insights from you, Naheed [Qureshi], and other civil rights leaders who have played a crucial role in evolving Facebook’s products and policies for the better.”

***Facebook’s Failure to Take Action on Content that Violates Its Community Standards***

54. Annexed hereto as Exhibit 52 is a true and accurate copy of Oliva Solon’s article published on NBC News, *Facebook Ignored Racial Bias Research*, July 23, 2020, which states, “The lack of action on this issue from the management has contributed to a growing sense among some Facebook employees that a small inner circle of senior executives – including Chief Executive Mark Zuckerberg, Chief Operating Officer Sheryl Sandberg, Nick Clegg, Vice president of Global Affairs and Communications, and Joel Kaplan, Vice President of Global Public Policy – are making decisions that run counter to the recommendations of subject matter experts and researchers below them, particularly around hate speech, violence and racial bias, the employees said . . . . [One] engineer . . . accused Zuckerberg of making misleading statements about the company’s handling of hate speech.” (<https://www.nbcnews.com/tech/tech-news/facebook-management-ignored-internal-research-showing-racial-bias-current-former-n1234746>)

**Professor Megan Squire’s Work**

55. Professor Megan Squire’s research and work related to hate groups and violent groups on Facebook has been described in various articles. Annexed hereto as Exhibit 56 is a true and accurate copy of Adam Maida’s article published on Wired, *Meet Antifa’s Secret Weapon Against Far-Right Extremists*, on January 16, 2018. (<https://www.wired.com/story/free-speech-issue->

antifa-data-mining/

***Examples of Facebook's Inaction in Enforcing Its Community Standards Despite Knowledge***

56. Despite knowledge of content that violated Facebook's Community Standard, Facebook did not take any action to enforce them. Annexed hereto as Exhibit 60 is a true and accurate copy of Will Carless and Michael Corey's article published in Reveal News, *American Cops Have Openly Engaged in Islamophobia on Facebook, with no penalties*, on June 27, 2019. (<https://revealnews.org/article/american-cops-have-openly-engaged-in-islamophobia-on-facebook-with-no-penalties/>); Annexed hereto as Exhibit 62 is a true and accurate copy of Melissa Nan Burke's article published in The Detroit News, *Tlaib Not Cowed by 'Hateful' Threats, Behavior* on January 28, 2019, which shows that violent posts directed toward Muslim public figures, including Congressional members, were not removed. (<https://www.detroitnews.com/story/news/politics/2019/01/27/tlaib-death-threats-anti-muslim-slurs/2668471002/>).

57. Annexed hereto as Exhibit 65 is a true and example of Tech Transparency Project's *White Supremacist Groups Are Thriving on Facebook* on May 21, 2020. (<https://www.techtransparencyproject.org/sites/default/files/Facebook-White-Supremacy-Report.pdf>). This report found that Facebook autogenerated Anti-Muslim, White Supremacist pages and altered a nominal amount of hate content.

58. Annexed hereto as Exhibit 67 is a true and accurate copy of Facebook's Civil Rights Audit dated July 8, 2020, which highlighted Facebook's failure to enforce its own Community Standards as against Anti-Muslim threats. (<https://about.fb.com/wp-content/uploads/2020/07/Civil-Rights-Audit-Final-Report.pdf>)

***Facebook's Platform Used to Organize the June 6<sup>th</sup> Capitol Riots***

59. Annexed hereto as Exhibit 68 is a true and accurate copy of Tech Transparency's Project, *Capitol Attack Was Months in the Making on Facebook*, on January 19, 2021.

(<https://www.techtransparencyproject.org/articles/capitol-attack-was-months-making-facebook>)

60. Annexed hereto as Exhibit 69 is a true and accurate copy of Elizabeth Dwoskin's article published on Washington Post, *Facebook's Sandberg Deflected Blame for Capitol Riot, But New Evidence Shows How Platform Played Role*, on January 13, 2021.

61. Annexed hereto as Exhibit 71 is a true and accurate copy of Tech Transparency's *Facebook's Militia Mess*, on March 24, 2021, which shows that there were militia groups and pages still active two months after the January 6 Capitol Riots.

(<https://www.techtransparencyproject.org/articles/facebooks-militia-mess>)

62. Further, studies from the Southern Poverty Law Center reported on Hate Groups, including Anti-Muslim hate groups in the United States, that had content on Facebook that violates Community Standards remained on the platform despite Facebook's knowledge. Annexed hereto as Exhibit 72 is a true and accurate copy of Southern Poverty Law Center's *Hate Map*, which was last accessed on Facebook on August 4, 2021. <https://www.facebook.com/SPLCenter> (last accessed Aug. 4, 2021) (hosting Year In Hate Report as "pinned" item).

***Myanmar***

63. Despite Defendant Zuckerberg's representations to address anti-Muslim hate on Facebook in Myanmar, no action was taken allowing for Anti-Muslim content to remain. Annexed hereto as Exhibit 73 is a true and accurate copy of the United Nations Office of the High

Commissioner for Human Rights, *Myanmar: UN Fact-Finding Mission releases its full account of massive violations by military in Rakhine, Kachin, and Shan States*, United Nations Human Rights Office (Sept. 18, 2018),

(<https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23575>); Annexed

hereto as Exhibit 74 is a true and accurate copy of Steve Stecklow's article published in Reuters, *Why Facebook is Losing the War on Hate Speech in Myanmar, on August 15, 2018.*

(<https://www.reuters.com/investigates/special-report/myanmar-facebook-hate/>).

### ***New Zealand***

64. Facebook allowed the Christchurch, New Zealand mosque massacres to be live streamed and shared multiple times prior to removing it from the platform despite having knowledge of the video. Annexed hereto as Exhibit 75 is a true and accurate copy of Emanuel Stoakes' article published in the Washington Post, *New Zealand mosque attack victims confront gunman in courtroom, on Aug. 24, 2020.*

([https://www.washingtonpost.com/world/asia\\_pacific/brenton-tarrant-sentence-new-zealand-mosque-attack-christchurch/2020/08/23/abd51832-e10c-11ea-82d8-5e55d47e90ca\\_story.html](https://www.washingtonpost.com/world/asia_pacific/brenton-tarrant-sentence-new-zealand-mosque-attack-christchurch/2020/08/23/abd51832-e10c-11ea-82d8-5e55d47e90ca_story.html));

Annexed hereto as Exhibit 76 is a true and accurate copy of Andrew Liptak's article on the Verge, *Facebook says that it removed 1.5 million videos of the New Zealand mass shooting, on March 17, 2019* (<https://www.theverge.com/2019/3/17/18269453/facebook-new-zealand-attack-removed-1-5-million-videos-content-moderation>).

### ***MA's Critique on Facebook***

65. Annexed hereto as Exhibit 77 a true and accurate copy of Muslim Advocates project with the Global Project on Hate and Extremism, *Complicit: The Human Cost of Facebook's Disregard for Muslim Life* on October 20, 2017, which reports on Facebook enabling

Anti-Muslim to remain on the platform without consequence.

[https://muslimadvocates.org/files/Letter\\_19CivilRightsGroupstoFacebook.pdf](https://muslimadvocates.org/files/Letter_19CivilRightsGroupstoFacebook.pdf)

66. Annexed hereto as Exhibit 55 is a true and accurate copy of Muslim Advocate’s article *Facebook Does Not Take Hate Content Seriously* published on June 30, 2019.

67. Annexed hereto as Exhibit 57 is a true and accurate copy of Muslim Advocate’s article *Muslim Advocates Demands that Zuckerberg Address Facebook’s Anti-Muslim Problem* published on October 16, 2019.

68. Annexed hereto as Exhibit 58 is a true and accurate copy of Muslim Advocates and Partner’s Letter to Facebook dated October 30, 2017.

[https://muslimadvocates.org/files/Letter\\_19CivilRightsGroupstoFacebook.pdf](https://muslimadvocates.org/files/Letter_19CivilRightsGroupstoFacebook.pdf)

69. Annexed here to as Exhibit 59 is a true and accurate copy of Muslim Advocates’ *Click Here to End Hate: Anti-Muslim Bigotry Online & How to Take Action* on May 2014.

<https://muslimadvocates.org/wp-content/uploads/Click-Here-to-End-Hate.pdf>

#### **Anti-SLAPP**

70. Annexed hereto as Exhibit 66 is a true and accurate copy of the Committee on Public Safety and the Judiciary Committee Report on Bill 18-893, the “Anti-SLAPP Act of 2010” (Nov. 18, 2010) (including District of Columbia Attorney General Peter J. Nickles letter to Committee on Public Safety & the Judiciary Chairperson Phil Mendelson “register[ing] a preliminary concern” that the anti-SLAPP bill “can be construed to abrogate . . . [and] conflict with the Superior Court’s rules of civil procedure and, consequently, violate section 602(a)(4) of the Home Rule Act . . . .”

I declare under penalty of perjury that the foregoing is accurate to the best of my knowledge.

*Stephanie R. Correa*  
i n t e

Nov. 17, 2021  
te

IN THE SUPERIOR COURT FOR THE DISTRICT OF COLUMBIA  
CIVIL DIVISION

MUSLIM ADVOCATES,

*Plaintiff,*

v.

MARK ZUCKERBERG, *et al.*,

*Defendants.*

Case No. 2021 CA 001114 B

**Exhibit Index**

<b>Exhibit Number</b>	<b>Exhibit Name</b>
Exhibit 1.	Muslim Advocates 501(c)(3) letter
Exhibit 2.	Jeff Horwitz, <i>Facebook Says Its Rule Apply to All. Company Documents Reveal a Secret Elite That's Exempt</i> , Wall Street Journal (Sept. 13, 2021)
Exhibit 3.	Muslim Advocates Mission Statement and History
Exhibit 4.	Zuckerberg Facebook profile
Exhibit 5.	Sandberg Facebook profile
Exhibit 6.	Kaplan professional background from the Bush Center
Exhibit 7.	Martin professional background from the World Economic Forum
Exhibit 8.	Lauren Feiner, <i>Facebook Spent More on Lobbying Than Any Other Big Tech Company in 2020</i> , CNBC.com (Jan. 22, 2021)
Exhibit 9.	Facebook, Inc., <i>Form 10-K for the Fiscal Year Ending December 31, 2020</i>
Exhibit 10.	Statista Research Department's <i>Leading Countries Based on Facebook Audience Size as of October 2021</i> (Nov. 16, 2021)
Exhibit 11.	Facebook Terms of Service
Exhibit 12.	David Nield, <i>All the Ways Facebook Tracks You—and How to Limit It</i> , Wired (Jan. 12, 2020)
Exhibit 13.	Elizabeth Culliford, Munisef Vengattil, & Sheila Dang, <i>Facebook takes on Clubhouse, unveils upcoming audio products</i> , Reuters (Apr. 19, 2021)

- Exhibit 14. Christine Lagorio-Chafkin, *Facebook's Sheryl Sandberg Breaks Silence about Business Practices*, *Outage*, Inc. (Oct. 19, 2021)
- Exhibit 15. Abigail Freeman, *Sheryl Sandberg on Facebook's Role in Small Business Support and Voter Registration During the Pandemic*, *Forbes* (Sept. 28, 2020)
- Exhibit 16. ce t Facebook Community Standards ( )
- Exhibit 17. Supplemental Disclosures of Securities Law Violations by Facebook, Inc.
- Exhibit 18. Deepa Seetharaman, Jeff Horwitz, and Justin Scheck, *Facebook Says AI Will Clean Up the Platform, Its Own Engineers Have Doubts*, *Wall Street Journal* (Oct. 17, 2021)
- Exhibit 19. Lake Munn, *Angry by design: toxic communication and technical architectures*, *Humanities and Social Sciences Communications*, Volume 7, Article 53 (2020)
- Exhibit 20. Andy Serwer and Max Zahn, *Facebook's Zuckerberg and Sandberg are this involved with the company's content issues*, *Yahoo Finance* (Sept. 9, 2019)
- Exhibit 21. Ryan Mac and Craig Silverman, *"Mark Changed the Rules": How Facebook Went Easy on Alex Jones and Other Right-Wing Figures*, *BuzzFeed News* (Feb 22, 2021)
- Exhibit 22. Facebook, Inc., *Form 10-K for the Fiscal Year Ending December 31, 2018*, p.15
- Exhibit 23. Facebook, Inc., *Form 10-K for the Fiscal Year Ending December 31, 2019*, p.44
- Exhibit 24. Copies of images taken from Congressional Hearings showing Defendant Kaplan sitting near Defendant Zuckerberg
- Exhibit 25. Mark Zuckerberg's Testimony before the Senate Commerce and Judiciary Committees on April 10, 2018
- Exhibit 26. Mark Zuckerberg's Testimony before the House Energy and Commerce Committee on April 11, 2018
- Exhibit 27. Mark Zuckerberg's Testimony before the Senate Commerce Committee on June 8, 2018.
- Exhibit 28. Sheryl Sandberg's statement during the Senate's Open Hearing on Foreign Influence Operations' Use of Social Media Platforms before the Select Committee on Intelligence on September 5, 2018
- Exhibit 29. Nathaniel Gleicher's Testimony before the House Intelligence Committee on June 18, 2020
- Exhibit 30. Nathaniel Gleicher's Testimony before the House Committee on Oversight and Reform, Subcommittee on National Security on May 22, 2019

- Exhibit 31. Nathaniel Gleicher’s Testimony before the House Committee on Veterans Affairs on November 13, 2019
- Exhibit 32. Monika Bickert’s Testimony Before the Senate Committee on Commerce, Science, and Transportation on January 17, 2018
- Exhibit 33. Monika Bickert’s Testimony Before the Senate Committee on Commerce, Science, and Transportation on September 18, 2019
- Exhibit 34. Neil Potts’ Testimony before Senate Judiciary Committee Subcommittee on the Constitution on April 10, 2019
- Exhibit 35. *Facebook Papers: 10 shocking revelations from the leaked documents*, Noticias Financieras (Oct. 26, 2021)
- Exhibit 36. Ethan Wolff-Mann, *Here’s Who is Sitting Behind Mark Zuckerberg and Why They’re There*, Yahoo Finance (April 11, 2018)
- Exhibit 37. Shaarik Zafar, Facebook’s U.S. Public Policy Advisor, email to Farhana Khera, Naheed Qureshi, and Madihha Ahussain on December 18, 2018
- Exhibit 38. Monique Dorsainvil, Facebook’s Public Policy Director, email to Muslim Advocates’ former Executive Director, Farhana Khera, on March 26, 2019
- Exhibit 39. Sandberg’s Email to Ms. Khera on May 1, 2019
- Exhibit 40. Martin’s Letter to Ms. Quereshi on March 17, 2020
- Exhibit 41. Michael McGowan, Christopher Knaus and Nick Evershed, *Monetising Hate: Covert Enterprise Co-Opts Far-Right Facebook Pages to Churn out Anti-Islamic Posts*, The Guardian (December 5, 2019)
- Exhibit 42. Alex Hern, *Facebook Leak Underscores Strategy to Operate in Repressive Regimes*, The Guardian (March 23, 2021)
- Exhibit 43. Michael Edison Hayden, *Facebook Has Failed to Stop Anti-Muslim Hate Groups, Despite Mark Zuckerberg Pledge*, Newsweek (April 20, 2018)
- Exhibit 44. Mr. Zafar’s Email to Ms. Ahussain on September 16, 2019
- Exhibit 45. Facebook’s Employee, Georgina Fields’ Email to Ms. Ahussain on September 18, 2019
- Exhibit 46. Facebook’s Employee, Kim Malfacini’s, Email to Ms. Ahussain on December 12, 2019
- Exhibit 47. Mr. Zafar’s Email to Ms. Ahussain on December 17, 2019

- Exhibit 48. Linday Elin, Facebook's Vice President of Public Policy and External Affairs, Email to Ms. Khera on May 5, 2018
- Exhibit 49. Ms. Dorsainvil's Email to Ms. Khera on June 30, 2019
- Exhibit 50. Zuckerberg's Email to Ms. Khera on November 6, 2019
- Exhibit 51. Sandberg's Email to Ms. Khera on January 11, 2021
- Exhibit 52. Oliva Solon, *Facebook Ignored Racial Bias Research, Employees Say*, NBC News, (July 23, 2020)
- Exhibit 53. Robert J. Shapiro, *What Your Data is Really Worth to Facebook*, Washington Monthly (July/Aug. 2019)
- Exhibit 54. Elizabeth Dwoskin, Tory Newmyer, & Shibani Mahtani, *The case against Mark Zuckerberg: Insiders say Facebook's CEO chose growth over safety*, Washington Post (Oct. 25, 2021)
- Exhibit 55. Muslim Advocates' Press Release on June 30, 2019, *Facebook Does Not Take Hate Content Seriously*
- Exhibit 56. Doug Bock Clark, *Meet Antifa's Secret Weapon Against Far-Right Extremists*, Wired (January 16, 2018)
- Exhibit 57. Muslim Advocates' Press Release on October 16, 2019, *Muslim Advocates Demands that Zuckerberg Address Facebook's Anti-Muslim Problem.*
- Exhibit 58. Muslim Advocates and Partners' Letter to Facebook on October 30, 2017.
- Exhibit 59. *Click Here to End Hate: Anti-Muslim Bigotry Online & How to Take Action*, Muslim Advocates (May 2014)
- Exhibit 60. Will Carless and Michael Corey, *American Cops Have Openly Engaged in Islamophobia on Facebook, with no penalties*, Reveal News (June 27, 2019).
- Exhibit 61. Facebook App's Description
- Exhibit 62. Melissa Nan Burke, *Tlaib Not Cowed by 'Hateful' Threats, Behavior*, The Detroit News (January 28, 2019)
- Exhibit 63. Letter from John Tye and Andrew Bakaj to SEC Office of the Whistleblower
- Exhibit 64. Tim De Chant, *Facebook AI Moderators Confused Videos of Mass Shootings and Car Washes*, Ars Technica (October 19, 2021)
- Exhibit 65. *White Supremacist Groups Are Thriving on Facebook*, Tech Transparency Project (May 21, 2020)

- Exhibit 66. Committee on Public Safety and the Judiciary Committee Report on Bill 18-893, the “Anti-SLAPP Act of 2010” (Nov. 18, 2010). Includes District of Columbia Attorney General Peter J. Nickles letter to Committee on Public Safety and the Judiciary Chairperson Phil Mendelson
- Exhibit 67. Facebook’s Civil Rights Audit dated July 8, 2020.
- Exhibit 68. *Capitol Attack Was Months in the Making on Facebook*, Tech Transparency Project (January 19, 2021)
- Exhibit 69. Elizabeth Dwoskin, *Facebook’s Sandberg Deflected Blame for Capitol Riot, But New Evidence Shows How Platform Played Role*, Washington Post (January 13, 2021)
- Exhibit 70. David Ingram, Olivia Solon, Brandy Zadrozny, & Cyrus Farivar, *The Facebook Papers: Documents reveal internal fury and dissent over site’s policies*, NBC News (October 25, 2021)
- Exhibit 71. *Facebook’s Militia Mess*, Tech Transparency Project (March 24, 2021)
- Exhibit 72. *Hate Map*, Southern Poverty Law Center (Aug. 4, 2021)
- Exhibit 73. United Nations Office of the High Commissioner for Human Rights, *Myanmar: UN Fact-Finding Mission releases its full account of massive violations by military in Rakhine, Kachin, and Shan States*, United Nations Human Rights Office (Sept. 18, 2018)
- Exhibit 74. Steve Stecklow, *Why Facebook is Losing the War on Hate Speech in Myanmar*, Reuters (August 15, 2018)
- Exhibit 75. Emanuel Stoakes, *New Zealand mosque attack victims confront gunman in courtroom*, Washington Post (Aug. 24, 2020)
- Exhibit 76. Andrew Liptak, *Facebook says that it removed 1.5 million videos of the New Zealand mass shooting*, The Verge (March 17, 2019)
- Exhibit 77. Muslim Advocates project with the Global Project on Hate and Extremism, *Complicit: The Human Cost of Facebook’s Disregard for Muslim Life* (October 20, 2017)
- Exhibit 78. Description of how Facebook uses look alike audiences to assist with its business model
- Exhibit 79. Craig Timberg, *Civil Rights Leaders Thought They’d Figured Out how to Deal with Facebook*, Washington Post, (October 25, 2019)
- Exhibit 80. Letter from Andrew Bakaj to SEC Office of the Whistleblower

- Exhibit 81. Len Sherman, *Why Facebook Will Never Change Its Business Model*, Forbes (Apr. 16, 2018)
- Exhibit 82. Chris Taylor, *Zuckerberg is a lightweight, and 4 more things we learned about Facebook from 'An Ugly Truth'*, Mashable (July 17, 2021)

# Exhibit 1

INTERNAL REVENUE SERVICE  
P. O. BOX 2508  
CINCINNATI, OH 45201

DEPARTMENT OF THE TREASURY

Date: JAN 13 2006

MUSLIM ADVOCATES  
C/O BARRY J HART  
WINSTON & STRAWN LLP  
1700 K ST NW  
WASHINGTON, DC 20006

Employer Identification Number:  
30-0298794  
DLN:  
17053147028005  
Contact Person:  
JENNIFER NICOLIN ID# 95152  
Contact Telephone Number:  
(877) 829-5500  
Accounting Period Ending:  
December 31  
Public Charity Status:  
IRC 170(b)(1)(A)(vi)  
Form 990 Required:  
Yes  
Effective Date of Exemption:  
February 4, 2005  
Contribution Deductibility:  
Yes  
Advance Ruling Ending Date:  
December 31, 2009

Dear Applicant:

We are pleased to inform you that upon review of your application for tax exempt status we have determined that you are exempt from Federal income tax under section 501(c)(3) of the Internal Revenue Code. Contributions to you are deductible under section 170 of the Code. You are also qualified to receive tax deductible bequests, devises, transfers or gifts under section 2055, 2106 or 2522 of the Code. Because this letter could help resolve any questions regarding your exempt status, you should keep it in your permanent records.

Organizations exempt under section 501(c)(3) of the Code are further classified as either public charities or private foundations. During your advance ruling period, you will be treated as a public charity. Your advance ruling period begins with the effective date of your exemption and ends with advance ruling ending date shown in the heading of the letter.

Shortly before the end of your advance ruling period, we will send you Form 8734, Support Schedule for Advance Ruling Period. You will have 90 days after the end of your advance ruling period to return the completed form. We will then notify you, in writing, about your public charity status.

Please see enclosed Information for Exempt Organizations Under Section 501(c)(3) for some helpful information about your responsibilities as an exempt organization.

Letter 1045 (DO/CG)

MUSLIM ADVOCATES

We have sent a copy of this letter to your representative as indicated in your power of attorney.

Sincerely,

Lois G. Lerner  
Director, Exempt Organizations  
Rulings and Agreements

Enclosures: Information for Organizations Exempt Under Section 501(c)(3)  
Statute Extension

MUSLIM ADVOCATES

INFORMATION FOR ORGANIZATIONS EXEMPT UNDER SECTION 501(c)(3)

WHERE TO GET FORMS AND HELP

Forms and instructions may be obtained by calling toll free 1-800-829-3676, through the Internet Web Site at [www.irs.gov](http://www.irs.gov), and also at local tax assistance centers.

Additional information about any topic discussed below may be obtained through our customer service function by calling toll free 1-877-829-5500 between 8:30 a.m. - 5:30 p.m. Eastern time.

NOTIFY US ON THESE MATTERS

If you change your name, address, purposes, operations or sources of financial support, please inform our TE/GE Customer Account Services Office at the following address: Internal Revenue Service, P.O. Box 2508, Cincinnati, Ohio 45201. If you amend your organizational document or by-laws, or dissolve your organization, provide the Customer Account Services Office with a copy of the amended documents. Please use your employer identification number on all returns you file and in all correspondence with the Internal Revenue Service.

FILING REQUIREMENTS

In your exemption letter we indicated whether you must file Form 990, Return of Organization Exempt From Income Tax. Form 990 (or Form 990-EZ) is filed with the Ogden Submission Processing Center, Ogden UT 84201-0027.

You are required to file a Form 990 only if your gross receipts are normally more than \$25,000.

If your gross receipts are normally between \$25,000 and \$100,000, and your total assets are less than \$250,000, you may file Form 990-EZ. If your gross receipts are over \$100,000, or your total assets are over \$250,000, you must file the complete Form 990. The Form 990 instructions show how to compute your "normal" receipts.

Form 990 Schedule A is required for both Form 990 and Form 990-EZ.

If a return is required, it must be filed by the 15th day of the fifth month after the end of your annual accounting period. There are penalties for failing to timely file a complete return. For additional information on penalties, see Form 990 instructions or call our toll free number.

If your receipts are below \$25,000, and we send you a Form 990 Package, follow the instructions in the package on how to complete the limited return to advise us that you are not required to file.

If your exemption letter states that you are not required to file Form 990, you

MUSLIM ADVOCATES

are exempt from these requirements.

UNRELATED BUSINESS INCOME TAX RETURN

If you receive more than \$1,000 annually in gross receipts from a regular trade or business you may be subject to Unrelated Business Income Tax and required to file Form 990-T, Exempt Organization Business Income Tax Return. There are several exceptions to this tax.

1. Income you receive from the performance of your exempt activity is not unrelated business income.
2. Income from fundraisers conducted by volunteer workers, or where donated merchandise is sold, is not unrelated business income.
3. Income from routine investments such as certificates of deposit, savings accounts, or stock dividends is usually not unrelated business income.

There are special rules for income derived from real estate or other investments purchased with borrowed funds. This income is called "debt financed" income. For additional information regarding unrelated business income tax see Publication 598, Tax on Unrelated Business Income of Exempt Organizations, or call our toll free number shown above.

PUBLIC INSPECTION OF APPLICATION AND INFORMATION RETURN

You are required to make your annual information return, Form 990 or Form 990-EZ, available for public inspection for three years after the later of the due date of the return, or the date the return is filed. You are also required to make available for public inspection your exemption application, any supporting documents, and your exemption letter. Copies of these documents are also required to be provided to any individual upon written or in person request without charge other than reasonable fees for copying and postage. You may fulfill this requirement by placing these documents on the Internet. Penalties may be imposed for failure to comply with these requirements. Additional information is available in Publication 557, Tax-Exempt Status for Your Organization, or you may call our toll free number shown above.

FUNDRAISING

Contributions to you are deductible only to the extent that they are gifts and no consideration is received in return. Depending on the circumstances, ticket purchases and similar payments in conjunction with fundraising events may not qualify as fully deductible contributions.

CONTRIBUTIONS OF \$250 OR MORE

Donors must have written substantiation from the charity for any charitable contribution of \$250 or more. Although it is the donor's responsibility to obtain written substantiation from the charity, you can assist donors by

## MUSLIM ADVOCATES

providing a written statement listing any cash contribution or describing any donated property.

This written statement must be provided at the time of the contribution. There is no prescribed format for the written statement. Letters, postcards and electronic (e-mail) or computer-generated forms are acceptable.

The donor is responsible for the valuation of donated property. However, your written statement must provide a sufficient description to support the donor's contribution. For additional information regarding donor substantiation, see Publication 1771, Charitable Contributions - Substantiation and Disclosure Requirements. For information about the valuation of donated property, see Publication 561, Determining the Value of Donated Property.

### CONTRIBUTIONS OF MORE THAN \$75 AND CHARITY PROVIDES GOODS OR SERVICES

You must provide a written disclosure statement to donors who receive goods or services from you in exchange for contributions in excess of \$75.

Contribution deductions are allowable to donors only to the extent their contributions exceed the value of the goods or services received in exchange. Ticket purchases and similar payments in conjunction with fundraising events may not necessarily qualify as fully deductible contributions, depending on the circumstances. If your organization conducts fundraising events such as benefit dinners, shows, membership drives, etc., where something of value is received, you are required to provide a written statement informing donors of the fair market value of the specific items or services you provided in exchange for contributions of more than \$75.

You should provide the written disclosure statement in advance of any event, determine the fair market value of any benefit received, determine the amount of the contribution that is deductible, and state this information in your fundraising materials such as solicitations, tickets, and receipts. The amount of the contribution that is deductible is limited to the excess of any money (and the value of any property other than money) contributed by the donor less the value of goods or services provided by the charity. Your disclosure statement should be made, no later than, at the time payment is received. Subject to certain exceptions, your disclosure responsibility applies to any fundraising circumstances where each complete payment, including the contribution portion, exceeds \$75. For additional information, see Publication 1771 and Publication 526, Charitable Contributions.

### EXCESS BENEFIT TRANSACTIONS

Excess benefit transactions are governed by section 4958 of the Code. Excess benefit transactions involve situations where a section 501(c)(3) organization provides an unreasonable benefit to a person who is in a position to exercise substantial influence over the organization's affairs. If you believe there may be an excess benefit transaction involving your organization, you should report the transaction on Form 990 or 990-EZ. Additional information can be

## MUSLIM ADVOCATES

found in the instructions for Form 990 and Form 990-EZ, or you may call our toll free number to obtain additional information on how to correct and report this transaction.

## EMPLOYMENT TAXES

If you have employees, you are subject to income tax withholding and the social security taxes imposed under the Federal Insurance Contribution Act (FICA). You are required to withhold Federal income tax from your employee's wages and you are required to pay FICA on each employee who is paid more than \$100 in wages during a calendar year. To know how much income tax to withhold, you should have a Form W-4, Employee's Withholding Allowance Certificate, on file for each employee. Organizations described in section 501(c)(3) of the Code are not required to pay Federal Unemployment Tax (FUTA).

Employment taxes are reported on Form 941, Employer's Quarterly Federal Tax Return. The requirements for withholding, depositing, reporting and paying employment taxes are explained in Circular E, Employer's Tax Guide, (Publication 15), and Employer's Supplemental Tax Guide, (Publication 15-A). These publications explain your tax responsibilities as an employer.

## CHURCHES

Churches may employ both ministers and church workers. Employees of churches or church-controlled organizations are subject to income tax withholding, but may be exempt from FICA taxes. Churches are not required to pay FUTA tax. In addition, although ministers are generally common law employees, they are not treated as employees for employment tax purposes. These special employment tax rules for members of the clergy and religious workers are explained in Publication 517, Social Security and Other Information for Members of the Clergy and Religious Workers. Churches should also consult Publications 15 and 15-A. Publication 1828, Tax Guide for Churches and Religious Organizations, also discusses the various benefits and responsibilities of these organizations under Federal tax law.

## PUBLIC CHARITY STATUS

Every organization that qualifies for tax-exemption as an organization described in section 501(c)(3) is a private foundation unless it falls into one of the categories specifically excluded from the definition of that term [referred to in section 509(a)(1), (2), (3), or (4)]. In effect, the definition divides these organizations into two classes, namely private foundations and public charities.

Public charities are generally those that either have broad public support or actively function in a supporting relationship to those organizations.

Public charities enjoy several advantages over private foundations. There are certain excise taxes that apply to private foundations but not to public charities. A private foundation must also annually file Form 990-PF, Return of Private Foundation, even if it had no revenue or expenses.

MUSLIM ADVOCATES

The Code section under which you are classified as a public charity is shown in the heading of your exemption letter. This determination is based on the information you provided and the request you made on your Form 1023 application. Please refer to Publication 557 for additional information about public charity status.

GRANTS TO INDIVIDUALS

The following information is provided for organizations that make grants to individuals. If you begin an individual grant program that was not described in your exemption application, please inform us about the program.

Funds you distribute to an individual as a grant must be made on a true charitable basis in furtherance of the purposes for which you are organized. Therefore, you should keep adequate records and case histories that demonstrate that grants to individuals serve your charitable purposes. For example, you should be in a position to substantiate the basis for grants awarded to individuals to relieve poverty or under a scholarship or education loan program. Case histories regarding grants to individuals should show names, addresses, purposes of grants, manner of selection, and relationship (if any) to members, officers, trustees, or donors of funds to you.

For more information on the exclusion of scholarships from income by an individual recipient, see Publication 520, Scholarships and Fellowships.

**Part X Public Charity Status (Continued)**

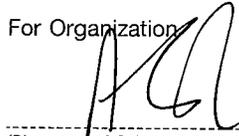
- e 509(a)(4)—an organization organized and operated exclusively for testing for public safety.
- f 509(a)(1) and 170(b)(1)(A)(iv)—an organization operated for the benefit of a college or university that is owned or operated by a governmental unit.
- g 509(a)(1) and 170(b)(1)(A)(vi)—an organization that receives a substantial part of its financial support in the form of contributions from publicly supported organizations, from a governmental unit, or from the general public.
- h 509(a)(2)—an organization that normally receives not more than one-third of its financial support from gross investment income and receives more than one-third of its financial support from contributions, membership fees, and gross receipts from activities related to its exempt functions (subject to certain exceptions).
- i A publicly supported organization, but unsure if it is described in 5g or 5h. The organization would like the IRS to decide the correct status.

6 If you checked box g, h, or i in question 5 above, you must request either an **advance** or a **definitive ruling** by selecting one of the boxes below. Refer to the instructions to determine which type of ruling you are eligible to receive.

- a **Request for Advance Ruling:** By checking this box and signing the consent, pursuant to section 6501(c)(4) of the Code you request an advance ruling and agree to extend the statute of limitations on the assessment of excise tax under section 4940 of the Code. The tax will apply only if you do not establish public support status at the end of the 5-year advance ruling period. The assessment period will be extended for the 5 advance ruling years to 8 years, 4 months, and 15 days beyond the end of the first year. You have the right to refuse or limit the extension to a mutually agreed-upon period of time or issue(s). Publication 1035, *Extending the Tax Assessment Period*, provides a more detailed explanation of your rights and the consequences of the choices you make. You may obtain Publication 1035 free of charge from the IRS web site at [www.irs.gov](http://www.irs.gov) or by calling toll-free 1-800-829-3676. Signing this consent will not deprive you of any appeal rights to which you would otherwise be entitled. If you decide not to extend the statute of limitations, you are not eligible for an advance ruling.

**Consent Fixing Period of Limitations Upon Assessment of Tax Under Section 4940 of the Internal Revenue Code**

For Organization



(Signature of Officer, Director, Trustee, or other authorized official)

Awais Sufi

(Type or print name of signer)

**Chairman, Board of Directors**

(Type or print title or authority of signer)

5/12/05  
(Date)

For Director, Exempt Organizations

By 

JAN 13 2006

Date

- b **Request for Definitive Ruling:** Check this box if you have completed one tax year of at least 8 full months and you are requesting a definitive ruling. To confirm your public support status, answer line 6b(i) if you checked box g in line 5 above. Answer line 6b(ii) if you checked box h in line 5 above. If you checked box i in line 5 above, answer both lines 6b(i) and (ii).

- (i) (a) Enter 2% of line 8, column (e) on Part IX-A. Statement of Revenues and Expenses. \_\_\_\_\_
- (b) Attach a list showing the name and amount contributed by each person, company, or organization whose gifts totaled more than the 2% amount. If the answer is "None," check this box.
- (ii) (a) For each year amounts are included on lines 1, 2, and 9 of Part IX-A. Statement of Revenues and Expenses, attach a list showing the name of and amount received from each **disqualified person**. If the answer is "None," check this box.
- (b) For each year amounts are included on line 9 of Part IX-A. Statement of Revenues and Expenses, attach a list showing the name of and amount received from each payer, other than a disqualified person, whose payments were more than the larger of (1) 1% of line 10, Part IX-A. Statement of Revenues and Expenses, or (2) \$5,000. If the answer is "None," check this box.

- 7 Did you receive any unusual grants during any of the years shown on Part IX-A. Statement of Revenues and Expenses? If "Yes," attach a list including the name of the contributor, the date and amount of the grant, a brief description of the grant, and explain why it is unusual.  Yes  No

# Exhibit 2

# Facebook Says Its Rules Apply to All. Company Documents Reveal a Secret Elite That's Exempt.

A program known as XCheck has given millions of celebrities, politicians and other high-profile users special treatment, a privilege many abuse

By [Jeff Horwitz](#)

Sept. 13, 2021 10:21 am ET

**M**ark Zuckerberg has publicly said Facebook Inc. allows its more than three billion users to speak on equal footing with the elites of politics, culture and journalism, and that its standards of behavior apply to everyone, no matter their status or fame.

In private, the company has built a system that has exempted high-profile users from some or all of its rules, according to company documents reviewed by The Wall Street Journal.

The program, known as “cross check” or “XCheck,” was initially intended as a quality-control measure for actions taken against high-profile accounts, including celebrities, politicians and journalists. Today, it shields millions of VIP users from the company’s normal enforcement process, the documents show. Some users are “whitelisted”—rendered immune from enforcement actions—while others are allowed to post rule-violating material pending Facebook employee reviews that often never come.

---

[A LOOK INSIDE THE FACEBOOK FILES »](#)

---

[Ask your questions now](#)

---

At times, the documents show, XCheck has protected public figures whose posts contain harassment or incitement to violence, violations that would typically lead to sanctions for regular users. In 2019, it allowed international soccer star Neymar to show nude photos of a woman, who had accused him of rape, to tens of millions of his fans before the content

was removed by Facebook. Whitelisted accounts shared inflammatory claims that Facebook's fact checkers deemed false, including that vaccines are deadly, that Hillary Clinton had covered up “pedophile rings,” and that then-President Donald Trump had called all refugees seeking asylum “animals,” according to the documents.

A 2019 internal review of Facebook's whitelisting practices, marked attorney-client privileged, found favoritism to those users to be both widespread and “not publicly defensible.”

“We are not actually doing what we say we do publicly,” said the confidential review. It called the company's actions “a breach of trust” and added: “Unlike the rest of our community, these people can violate our standards without any consequences.”

---

[THE FACEBOOK FILES »](#)

---

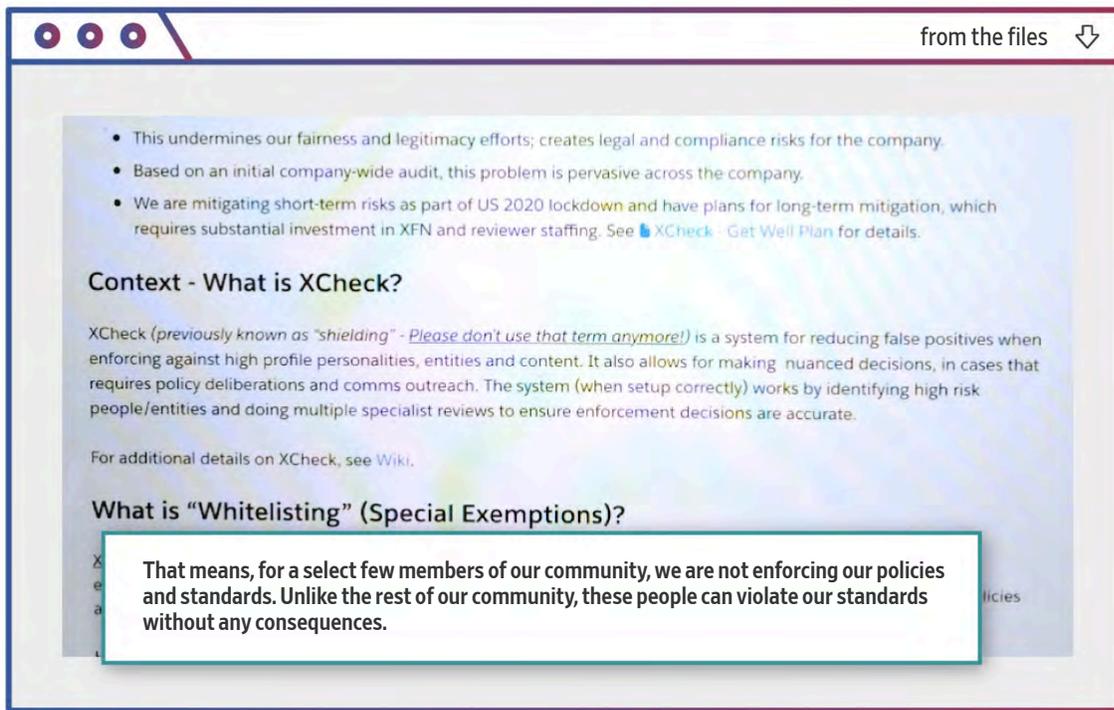
[Facebook Files](#)

[Sign up here](#)

---

Despite attempts to rein it in, XCheck grew to include at least 5.8 million users in 2020, documents show. In its struggle to accurately moderate a torrent of content and avoid negative attention, Facebook created invisible elite tiers within the social network.

In describing the system, Facebook has misled the public and its own Oversight Board, a body that Facebook created to ensure the accountability of the company's enforcement systems.



Source: 2019 Facebook internal review of the XCheck program, marked attorney-client privileged

In June, Facebook told the Oversight Board in writing that its system for high-profile users was used in "a small number of decisions."

In a written statement, Facebook spokesman Andy Stone said criticism of XCheck was fair, but added that the system "was designed for an important reason: to create an additional step so we can accurately enforce policies on content that could require more understanding."



At Facebook's headquarters in Menlo Park, Calif.

PHOTO: IAN BATES FOR THE WALL STREET JOURNAL

He said Facebook has been accurate in its communications to the board and that the company is continuing to work to phase out the practice of whitelisting. “A lot of this internal material is outdated information stitched together to create a narrative that glosses over the most important point: Facebook itself identified the issues with cross check and has been working to address them,” he said.

The documents that describe XCheck are part of an extensive array of internal Facebook communications reviewed by The Wall Street Journal. They show that Facebook knows, in acute detail, that its platforms are riddled with flaws that cause harm, often in ways only the company fully understands.

Moreover, the documents show, Facebook often lacks the will or the ability to address them.

This is the first in a series of articles based on those documents and on interviews with dozens of current and former employees.

At least some of the documents have been turned over to the Securities and Exchange Commission and to Congress by a person seeking federal whistleblower protection, according to people familiar with the matter.

Facebook’s stated ambition has long been to connect people. As it expanded over the past 17 years, from Harvard undergraduates to billions of global users, it struggled with the messy reality of bringing together disparate voices with different motivations—from people wishing each other happy birthday to Mexican drug cartels conducting business on the platform. Those problems increasingly consume the company.

Time and again, the documents show, in the U.S. and overseas, Facebook’s own researchers have identified the platform’s ill effects, in areas including teen mental health, political discourse and human trafficking. Time and again, despite congressional hearings, its own pledges and numerous media exposés, the company didn’t fix them.

Sometimes the company held back for fear of hurting its business. In other cases, Facebook made changes that backfired. Even Mr. Zuckerberg’s pet initiatives have been thwarted by his own systems and algorithms.

The documents include research reports, online employee discussions and drafts of presentations to senior management, including Mr. Zuckerberg. They aren't the result of idle grumbling, but rather the formal work of teams whose job was to examine the social network and figure out how it could improve.

They offer perhaps the clearest picture thus far of how broadly Facebook's problems are known inside the company, up to the CEO himself. And when Facebook speaks publicly about many of these issues, to lawmakers, regulators and, in the case of XCheck, its own Oversight Board, it often provides misleading or partial answers, masking how much it knows.



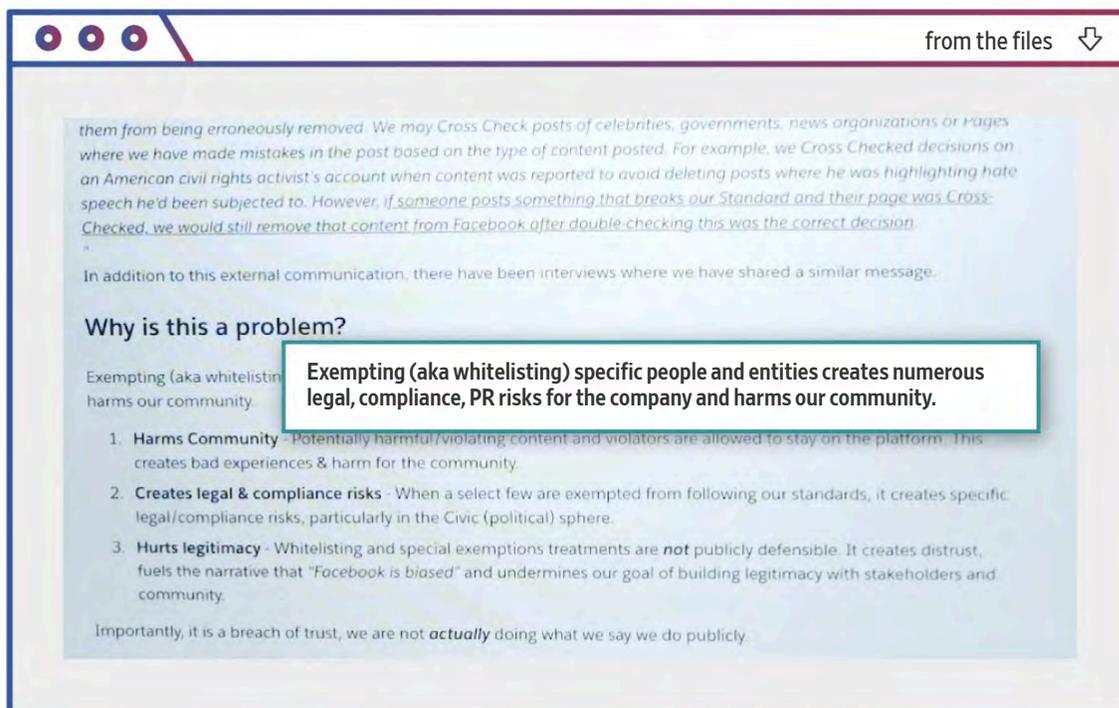
Facebook CEO Mark Zuckerberg, right, at a House Financial Services Committee hearing on Capitol Hill in 2019.

PHOTO: ANDREW HARNIK/ASSOCIATED PRESS

One area in which the company hasn't struggled is profitability. In the past five years, during which it has been under intense scrutiny and roiled by internal debate, Facebook has generated profit of more than \$100 billion. The company is currently valued at more than \$1 trillion.

For ordinary users, Facebook dispenses a kind of rough justice in assessing whether posts meet the company's rules against bullying, sexual content, hate speech and incitement to violence. Sometimes the company's automated systems summarily delete or bury content suspected of rule violations without a human review. At other times, material flagged by

those systems or by users is assessed by content moderators employed by outside companies.



Source: 2019 Facebook internal review of the XCheck program, marked attorney-client privileged

Mr. Zuckerberg estimated in 2018 that Facebook gets 10% of its content removal decisions wrong, and, depending on the enforcement action taken, users might never be told what rule they violated or be given a chance to appeal.

Users designated for XCheck review, however, are treated more deferentially. Facebook designed the system to minimize what its employees have described in the documents as “PR fires”—negative media attention that comes from botched enforcement actions taken against VIPs.

If Facebook’s systems conclude that one of those accounts might have broken its rules, they don’t remove the content—at least not right away, the documents indicate. They route the complaint into a separate system, staffed by better-trained, full-time employees, for additional layers of review.

Most Facebook employees were able to add users into the XCheck system, the documents say, and a 2019 audit found that at least 45 teams around the company were involved in whitelisting. Users aren’t generally told that they have been tagged for special treatment. An internal guide to XCheck eligibility cites qualifications including being “newsworthy,” “influential or popular” or “PR risky.”

Neymar, the Brazilian soccer star whose full name is Neymar da Silva Santos Jr., easily qualified. With more than 150 million followers, Neymar’s account on Instagram, which is owned by Facebook, is one of the most popular in the world.

After a woman accused Neymar of rape in 2019, he posted Facebook and Instagram videos defending himself—and showing viewers his WhatsApp correspondence with his accuser, which included her name and nude photos of her. He accused the woman of extorting him.



Brazilian soccer star Neymar, left, in Rio de Janeiro in 2019.

PHOTO: LEO CORREA/ASSOCIATED PRESS

Facebook’s standard procedure for handling the posting of “nonconsensual intimate imagery” is simple: Delete it. But Neymar was protected by XCheck.

For more than a day, the system blocked Facebook’s moderators from removing the video. An internal review of the incident found that 56 million Facebook and Instagram users saw what Facebook described in a separate document as “revenge porn,” exposing the woman to what an employee referred to in the review as abuse from other users.

“This included the video being reposted more than 6,000 times, bullying and harassment about her character,” the review found.

Facebook’s operational guidelines stipulate that not only should unauthorized nude photos be deleted, but that people who post them should have their accounts deleted.

“After escalating the case to leadership,” the review said, “we decided to leave Neymar’s accounts active, a departure from our usual ‘one strike’ profile disable policy.”

Neymar denied the rape allegation, and no charges were filed against him. The woman was charged by Brazilian authorities with slander, extortion and fraud. The first two charges were dropped, and she was acquitted of the third. A spokesperson for Neymar said the athlete adheres to Facebook's rules and declined to comment further.

The lists of those enrolled in XCheck were "scattered throughout the company, without clear governance or ownership," according to a "Get Well Plan" from last year. "This results in not applying XCheck to those who pose real risks and on the flip-side, applying XCheck to those that do not deserve it (such as abusive accounts, persistent violators). These have created PR fires."

In practice, Facebook appeared more concerned with avoiding gaffes than mitigating high-profile abuse. One Facebook review in 2019 of major XCheck errors showed that of 18 incidents investigated, 16 involved instances where the company erred in actions taken against prominent users.

Four of the 18 touched on inadvertent enforcement actions against content from Mr. Trump and his son, Donald Trump Jr. Other flubbed enforcement actions were taken against the accounts of Sen. Elizabeth Warren, fashion model Sunnaya Nash, and Mr. Zuckerberg himself, whose live-streamed employee Q&A had been suppressed after an algorithm classified it as containing misinformation.

Historically, Facebook contacted some VIP users who violated platform policies and provided a "self-remediation window" of 24 hours to delete violating content on their own before Facebook took it down and applied penalties.

Mr. Stone, the company spokesman, said Facebook has phased out that perk, which was still in place during the 2020 elections. He declined to say when it ended.

At times, pulling content from a VIP's account requires approval from senior executives on the communications and public-policy teams, or even from Mr. Zuckerberg or Chief Operating Officer Sheryl Sandberg, according to people familiar with the matter.

In June 2020, a Trump post came up during a discussion about XCheck's hidden rules that took place on the company's internal communications platform, called Facebook

Workplace. The previous month, Mr. Trump said in a post: “When the looting starts, the shooting starts.”

A Facebook manager noted that an automated system, designed by the company to detect whether a post violates its rules, had scored Mr. Trump’s post 90 out of 100, indicating a high likelihood it violated the platform’s rules.

For a normal user post, such a score would result in the content being removed as soon as a single person reported it to Facebook. Instead, as Mr. Zuckerberg publicly acknowledged last year, he personally made the call to leave the post up. “Making a manual decision like this seems less defensible than algorithmic scoring and actioning,” the manager wrote.

Mr. Trump’s account was covered by XCheck before his two-year suspension from Facebook in June. So too are those belonging to members of his family, Congress and the European Union Parliament, along with mayors, civic activists and dissidents.



Those included in the XCheck program, according to Facebook documents, include, in top row: Neymar, Donald Trump, Donald Trump, Jr. and Mark Zuckerberg, and in bottom row, Elizabeth Warren, Dan Scavino, Candace Owens and Doug the Pug.

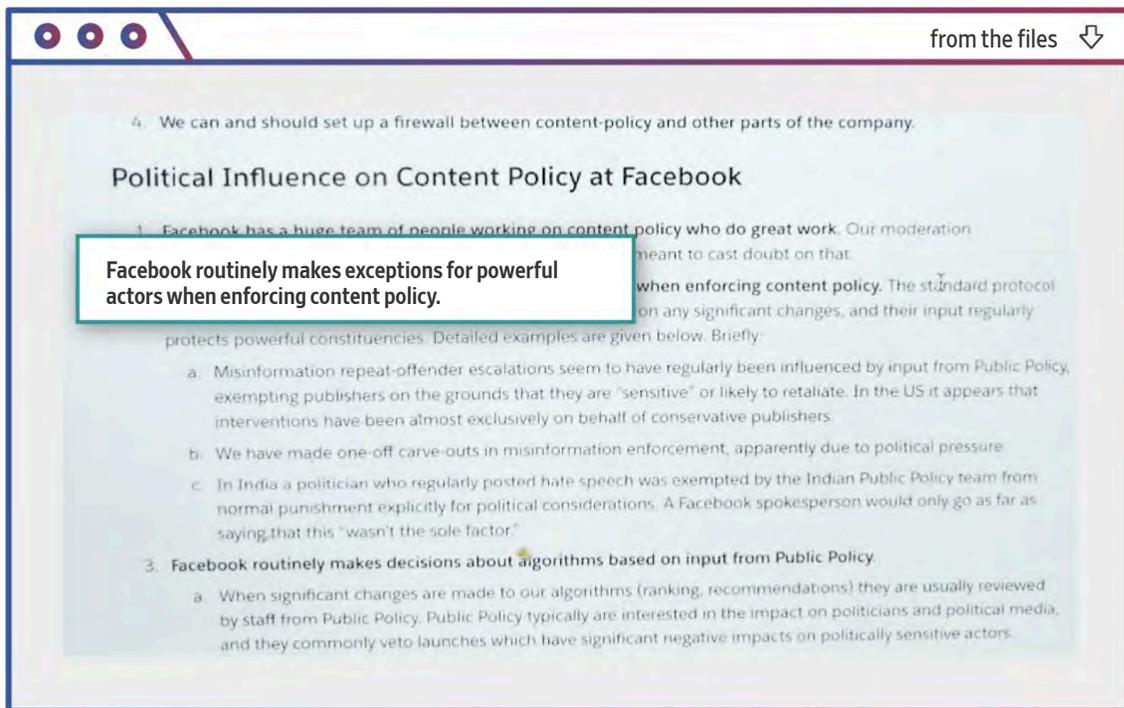
PHOTO: ZUMA PRESS; GETTY IMAGES (3); REUTERS (2); ASSOCIATED PRESS; PRESS POOL

While the program included most government officials, it didn’t include all candidates for public office, at times effectively granting incumbents in elections an advantage over challengers. The discrepancy was most prevalent in state and local races, the documents show, and employees worried Facebook could be subject to accusations of favoritism.

Mr. Stone acknowledged the concern but said the company had worked to address it. “We made multiple efforts to ensure that both in federal and nonfederal races, challengers as well as incumbents were included in the program,” he said.

The program covers pretty much anyone regularly in the media or who has a substantial online following, including film stars, cable talk-show hosts, academics and online

personalities with large followings. On Instagram, XCheck covers accounts for popular animal influencers including “Doug the Pug.”



Source: August 2020 Facebook internal presentation called “Political Influence on Content Policy”

In practice, most of the content flagged by the XCheck system faced no subsequent review, the documents show.

Even when the company does review the material, enforcement delays like the one on Neymar’s posts mean content that should have been prohibited can spread to large audiences. Last year, XCheck allowed posts that violated its rules to be viewed at least 16.4 billion times, before later being removed, according to a summary of the program in late December.

Facebook recognized years ago that the enforcement exemptions granted by its XCheck system were unacceptable, with protections sometimes granted to what it called abusive accounts and persistent violators of the rules, the documents show. Nevertheless, the program expanded over time, with tens of thousands of accounts added just last year.

In addition, Facebook has asked fact-checking partners to retroactively change their findings on posts from high-profile accounts, waived standard punishments for propagating what it classifies as misinformation and even altered planned changes to its algorithms to avoid political fallout.

“Facebook currently has no firewall to insulate content-related decisions from external pressures,” a September 2020 memo by a Facebook senior research scientist states, describing daily interventions in its rule-making and enforcement process by both Facebook’s public-policy team and senior executives.

A December memo from another Facebook data scientist was blunter: “Facebook routinely makes exceptions for powerful actors.”

Mr. Zuckerberg has consistently framed his position on how to moderate controversial content as one of principled neutrality. “We do not want to become the arbiters of truth,” he told Congress in a hearing last year.

Facebook’s special enforcement system for VIP users arose from the fact that its human and automated content-enforcement systems regularly flub calls.

Part of the problem is resources. While Facebook has trumpeted its spending on an army of content moderators, it still isn’t capable of fully processing the torrent of user-generated content on its platforms. Even assuming adequate staffing and a higher accuracy rate, making millions of moderation decisions a day would still involve numerous high-profile calls with the potential for bad PR.

Facebook wanted a system for “reducing false positives and human workload,” according to one internal document. The XCheck system was set up to do that.

To minimize conflict with average users, the company has long kept its notifications of content removals opaque. Users often describe on Facebook, Instagram or rival platforms what they say are removal errors, often accompanied by a screenshot of the notice they receive.

Facebook pays close attention. One internal presentation about the issue last year was titled “Users Retaliating Against Facebook Actions.”

“Literally all I said was happy birthday,” one user posted in response to a botched takedown, according to the presentation.



In response to what the documents describe as chronic underinvestment in moderation efforts, many teams around Facebook chose not to enforce the rules with high-profile accounts at all—the practice referred to as whitelisting. In some instances, whitelist status was granted with little record of who had granted it and why, according to the 2019 audit.

“This problem is pervasive, touching almost every area of the company,” the 2019 review states, citing the audit. It concluded that whitelists “pose numerous legal, compliance, and legitimacy risks for the company and harm to our community.”



Facebook is trying to eliminate the practice of whitelisting, the documents show. Its headquarters in Menlo Park.

PHOTO: IAN BATES FOR THE WALL STREET JOURNAL

A plan to fix the program, described in a document the following year, said that blanket exemptions and posts that were never subsequently reviewed had become the core of the program, meaning most content from XCheck users wasn’t subject to enforcement. “We currently review less than 10% of XChecked content,” the document stated.

Mr. Stone said the company improved that ratio during 2020, though he declined to provide data.

The leeway given to prominent political accounts on misinformation, which the company in 2019 acknowledged in a limited form, baffled some employees responsible for protecting the platforms. High-profile accounts posed greater risks than regular ones, researchers noted, yet were the least policed.

previously reported on the document.

In one instance, political whitelist users were sharing articles from alternative-medicine websites claiming that a Berkeley, Calif., doctor had revealed that chemotherapy doesn't work 97% of the time. Fact-checking organizations have debunked the claims, noting that the science is misrepresented and that the doctor cited in the article died in 1978.

In an internal comment in response to the memo, Samidh Chakrabarti, an executive who headed Facebook's Civic Team, which focuses on political and social discourse on the platform, voiced his discomfort with the exemptions.

"One of the fundamental reasons I joined FB is that I believe in its potential to be a profoundly democratizing force that enables everyone to have an equal civic voice," he wrote. "So having different rules on speech for different people is very troubling to me."

Other employees said the practice was at odds with Facebook's values.

"FB's decision-making on content policy is influenced by political considerations," wrote an economist in the company's data-science division.

"Separate content policy from public policy," recommended Kaushik Iyer, then lead engineer for Facebook's civic integrity team, in a June 2020 memo.





In May, Facebook's Oversight Board upheld the suspension of former President Donald Trump.  
PHOTO: ANDREW HARRER/BLOOMBERG NEWS



# Exhibit 3


[DONATE](https://muslimadvocates.org/donate)
[HTTPS://MUSLIMADVOCATES.ORG/DONATE](https://muslimadvocates.org/donate)
[\(https://muslimadvocates.org/\)](https://muslimadvocates.org/)

# WORKING TO HALT BIGOTRY IN ITS TRACKS

Working in the courts, in the halls of power, and in communities to halt bigotry in its tracks.

[OUR MISSION](#)

[OUR HISTORY](#)

[ANNUAL REPORTS](#)

## OUR MISSION

Muslim Advocates is a national civil rights organization working in the courts, in the halls of power, and in communities to halt bigotry in its tracks. We ensure that American Muslims have a seat at the table with expert representation so that all Americans may live free from hate and discrimination.

## Who We Are

Muslim Advocates provides expert representation in the courts, the policy making process, and in the public dialogue so that American Muslims and all people can live free from discrimination.

We litigate, educate, and advocate to uphold our country's promise of equal treatment under the law for all Americans – and we get results.

We are a big tent organization that recognizes the rich and full diversity of the American Muslim community in race, sex, place of birth, ability, income, education, gender identity, sexual orientation, sect of worship and level of religiosity.

# OUR HISTORY

Muslim Advocates was founded in the aftermath of the passage of the Patriot Act, which led to widespread surveillance and discrimination, to ensure that American Muslims have expert and strategic representation in the courts, the halls of power and communities.

Over a snowy Martin Luther King Day Weekend in 2005, a group of Muslim advocates charted the path for a national civil rights group to take on any civil rights struggle facing the community.

Since then, Muslim Advocates has taken on hate groups, major corporations and White Houses led by both parties to halt bigotry in its tracks and stop discrimination from becoming law.

## Our Partnership with the Dulles Justice Coalition

In November of 2017, Muslim Advocates and the Dulles Justice Coalition (DJC) announced a new partnership to advance civil and human rights.

In this new collaboration, DJC and Muslim Advocates will join forces to defend individuals and communities who are unjustly targeted and to push back against unlawful and discriminatory policies at the federal, state, and local levels. The organizations will work together to develop trainings and resources and to mobilize a rapid-response network of volunteers who are working on issues related to the Muslim ban, immigrants' rights, and other civil rights matters.

## ANNUAL REPORTS

**[2019 Form 990 \(https://muslimadvocates.org/wp-content/uploads/2020/12/MA-2019-Form-990-website.pdf\)](https://muslimadvocates.org/wp-content/uploads/2020/12/MA-2019-Form-990-website.pdf)**

**[2019 Year in Review \(https://muslimadvocates.org/wp-content/uploads/2020/06/MA-2019AccomplishmentsNov-2019.pdf\)](https://muslimadvocates.org/wp-content/uploads/2020/06/MA-2019AccomplishmentsNov-2019.pdf)**

**[2018 Year in Review \(https://muslimadvocates.org/wp-content/uploads/2020/06/MA-2018-Year-in-Review-2018.pdf\)](https://muslimadvocates.org/wp-content/uploads/2020/06/MA-2018-Year-in-Review-2018.pdf)**

**[2018 Form 990 \(https://muslimadvocates.org/wp-content/uploads/2020/04/MA-2018-990.pdf\)](https://muslimadvocates.org/wp-content/uploads/2020/04/MA-2018-990.pdf)**

**[2016 Financial Statements \(https://muslimadvocates.org/wp-content/uploads/2019/02/MA-Financial-Statements-12.31.2016-and-2015-1.pdf\)](https://muslimadvocates.org/wp-content/uploads/2019/02/MA-Financial-Statements-12.31.2016-and-2015-1.pdf)**

**[2016 Form 990 \(https://muslimadvocates.org/wp-content/uploads/2019/02/MA-2016-IRS-Form-990-2016.pdf\)](https://muslimadvocates.org/wp-content/uploads/2019/02/MA-2016-IRS-Form-990-2016.pdf)**

---

**[Public-1.pdf](#)**

**[2014 Annual Report \(https://muslimadvocates.org/2014/12/annual-report-2014/\)](https://muslimadvocates.org/2014/12/annual-report-2014/)**

**[2013 Financial Statements \(https://muslimadvocates.org/wp-content/uploads/2019/02/Muslim-Advocates-Financial-Statements-12.31.2013-and-2012.pdf\)](https://muslimadvocates.org/wp-content/uploads/2019/02/Muslim-Advocates-Financial-Statements-12.31.2013-and-2012.pdf)**

**[2013 Form 990 \(https://muslimadvocates.org/wp-content/uploads/2019/02/MA-2013-990-public-with-CA-forms.pdf\)](https://muslimadvocates.org/wp-content/uploads/2019/02/MA-2013-990-public-with-CA-forms.pdf)**

**[2012 Financial Statements \(https://muslimadvocates.org/wp-content/uploads/2019/02/MA-2012-IRS-Form-990-public.pdf\)](https://muslimadvocates.org/wp-content/uploads/2019/02/MA-2012-IRS-Form-990-public.pdf)**

**[2012 Form 990 \(https://muslimadvocates.org/wp-content/uploads/2019/02/MA-2012-IRS-Form-990-public.pdf\)](https://muslimadvocates.org/wp-content/uploads/2019/02/MA-2012-IRS-Form-990-public.pdf)**

**[2011 Annual Report \(https://muslimadvocates.org/2011/12/annual-report-2011/\)](https://muslimadvocates.org/2011/12/annual-report-2011/)**

**[2010 Annual Report \(https://muslimadvocates.org/2010/12/annual-report-2010/\)](https://muslimadvocates.org/2010/12/annual-report-2010/)**

**[2009 Annual Report \(https://muslimadvocates.org/2009/12/annual-report-2009/\)](https://muslimadvocates.org/2009/12/annual-report-2009/)**

**[2008 Annual Report \(https://muslimadvocates.org/2008/12/annual-report-2008/\)](https://muslimadvocates.org/2008/12/annual-report-2008/)**

## OUR TEAM

Muslim Advocates provides expert representation with the leading civil and human rights attorneys, advocates, and communicators in the field. Learn more about our growing and dynamic team.

**[LEARN MORE \(HTTPS://MUSLIMADVOCATES.ORG/ABOUT/OUR-TEAM/\)](https://muslimadvocates.org/about/our-team/)**

## CAREERS

Muslim Advocates is growing and we need passionate, dedicated individuals to join our team! Do you know someone who might be a match for one of our openings? Could it be you? If so, apply at the job links below.

**[LEARN MORE \(HTTPS://MUSLIMADVOCATES.ORG/ABOUT/CAREERS/\)](https://muslimadvocates.org/about/careers/)**

# SUPPORT THE FIGHT FOR EQUALITY

Muslim Advocates is entirely supported by private donations from people like you. All donations are tax-deductible and zakat-eligible.

**\$25**

**\$50**

**\$100**

**\$500**

**DONATE**  
**(HTTPS://SECURE.EVERYACTION.COM/EGRONOFY3KSZVNSPBJXONA2?AM=50)**



[\(https://muslimadvocates.org/\)](https://muslimadvocates.org/)

## **ISSUES**

**(HTTPS://MUSLIMADVOCATES.ORG/ISSUES/)**

Hate Crimes (<https://muslimadvocates.org/issue/hate-crimes/>).

Muslim Ban (<https://muslimadvocates.org/issue/muslim-ban/>).

Religious Freedom (<https://muslimadvocates.org/issue/religious-freedom/>).

Law Enforcement Bias (<https://muslimadvocates.org/issue/law-enforcement-bias/>).

Fighting Bigotry (<https://muslimadvocates.org/issue/fighting-bigotry/>).

Corporate Accountability (<https://muslimadvocates.org/issue/corporate-accountability/>).

Stopping Discrimination (<https://muslimadvocates.org/issue/stopping-discrimination/>).

## **VISIT THE ACTION CENTER**

**(HTTPS://MUSLIMADVOCATES.ORG/TAKE-ACTION/)**

COVID-19 Response (<https://muslimadvocates.org/issue/covid-19-response/>).

<https://muslimadvocates.org/about/#OurMission>

**DONATE (HTTPS://MUSLIMADVOCATES.ORG/DONATE)**

## **WAYS TO GIVE**

**(HTTPS://MUSLIMADVOCATES.ORG/GIVE/)**

## **ABOUT US**

**(HTTPS://MUSLIMADVOCATES.ORG/ABOUT/)**

Our Team (<https://muslimadvocates.org/about/our-team/>).

Careers (<https://muslimadvocates.org/about/careers/>).

Contact Us (<https://muslimadvocates.org/about/contact/>).

## **REPORT DISCRIMINATION**

**(HTTPS://MUSLIMADVOCATES.ORG/ACTION/REPORT-DISCRIMINATION/)**

[\(https://muslimadvocates.org/issue/coronavirus/\)](https://muslimadvocates.org/issue/coronavirus/)

[Muslim Ban Action Center  
\(https://muslimadvocates.org/muslim-ban/\)](https://muslimadvocates.org/muslim-ban/)

**DEFENDING YOUR RIGHTS**  
**(HTTPS://MUSLIMADVOCATES.ORG/DEFENDING-YOUR-RIGHTS/)**

[Know Your Rights \(https://muslimadvocates.org/defending-your-rights/know-your-rights/\)](https://muslimadvocates.org/defending-your-rights/know-your-rights/)

[Court Cases \(https://muslimadvocates.org/court-cases/\)](https://muslimadvocates.org/court-cases/)

[FOIA Requests \(https://muslimadvocates.org/foia-requests/\)](https://muslimadvocates.org/foia-requests/)

**NEWSROOM**  
**(HTTPS://MUSLIMADVOCATES.ORG/NEWSROOM/)**

**GET IN TOUCH**

Muslim Advocates  
P.O. Box 34440  
Washington, DC 20043

<https://www.facebook.com/muslimadvocates>

[info@muslimadvocates.org](mailto:info@muslimadvocates.org)  
202.897.2622

**SEARCH**

[PRIVACY POLICY \(/PRIVACY-POLICY/\)](/privacy-policy/) | © MUSLIM ADVOCATES

# Exhibit 4



11



# Mark Zuckerberg

Follow

Message

[Posts](#)

[About](#)

[Friends](#)

[Photos](#)

[Videos](#)

[Check-Ins](#)

[More](#) ▾



## Intro

Bringing the world closer together.

Founder and CEO at [Meta](#)

Works at [Chan Zuckerberg Initiative](#)

Studied Computer Science and Psychology at [Harvard University](#)

Lives in [Palo Alto, California](#)

From [Dobbs Ferry, New York](#)

Married to [Priscilla Chan](#)

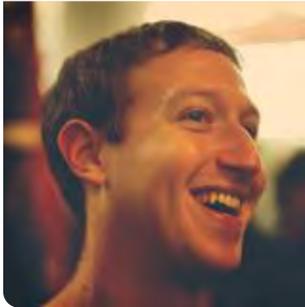
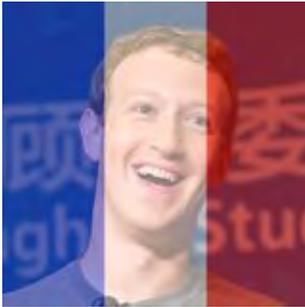




11

### Photos

[See All Photos](#)



### Friends

[See All Friends](#)

### Life Events

[See All](#)



August Was Born



Harvard Degree





11



Privacy · Terms · Advertising · Ad Choices · Cookies · More · Meta © 2021

Posts

Filters



Mark Zuckerberg

2h · 🌐



Meta's Reality Labs team is working on haptic gloves to create a realistic sense of touch in the metaverse. One day you'll be able to feel texture and pressure when you touch virtual objects.



0:02 / 0:43



17K

3.4K Comments 2K Shares

Like

Comment

Share





11



David Michaud · Follow

I'm sorry but... what's the goal of putting yourself in a virtual reality when you already live in the reality? 🤔

Like · Reply · 1h



84

22 Replies

View more comments

1 of 2,997



Mark Zuckerberg

November 11 at 7:18 PM · 🌐



The metaverse is the next frontier in social connection. I talked with Gary Vaynerchuk about what this future will unlock and the technology we need to bring it to life.



40K

7.6K Comments 3.5K Shares

Like

Comment

Share

Most Relevant



Write a comment...



Baraa Habab · Follow

Meta , = Future will coming !! To help a lot of people 🤖



Like · Reply · 4d

44 Replies

View more comments

1 of 6,631



# Exhibit 5



11



# Sheryl Sandberg

Follow

Message

[Posts](#)

[About](#)

[Friends](#)

[Photos](#)

[Videos](#)

[Check-Ins](#)

[More](#) ▾



## Intro



Chief operating officer at Meta



Former Vice President, Online Sales & Operations at Google



Former Consultant at McKinsey & Company



Former India Division Health Team & Research Assistant at World Bank



Studied at Harvard Business School



Studied Economics at Harvard University



Went to North Miami Beach Senior High



Lives in Menlo Park, California





11

 Followed by 2,201,926 people

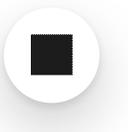


+ 4

Featured

### Photos

[See All Photos](#)





11



## Friends

[See All Friends](#)

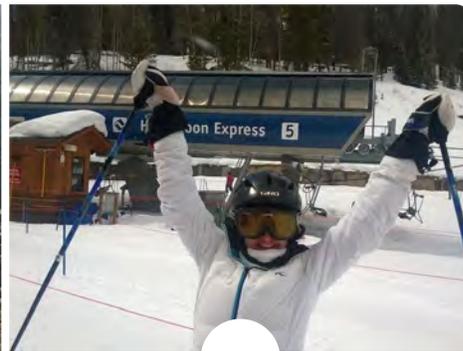
## Life Events

[See All](#)



After flying over it many times but never having the chance to actually go - the Great W...

June 28, 2015



Skied my first black run!

March 24, 2015

[Privacy](#) · [Terms](#) · [Advertising](#) · [Ad Choices](#)  · [Cookies](#) · [More](#) · Meta © 2021

## Posts

 [Filters](#)



**Sheryl Sandberg**

November 12 at 6:11 PM · 



Many of the best ideas at [Meta](#) come from our employees who see a problem and want to do something about it. That's exactly what [Jason Trimiew](#) did. Jason leads our diverse supplier program, and he saw that many diverse small businesses struggle with cash flow problems because they must wait months to get their invoices paid. So, he devised an initiative I'm really proud of – our Invoice Fast Track Program – that helps eligible small businesses in the US get cash immediately fo... [See more](#)



# Exhibit 6

(2)

## GEORGE W. BUSH PRESIDENTIAL CENTER

### ABOUT US

0

Through our three Impact Centers — Domestic Excellence, Global Leadership, and our Engagement Agenda — we focus on developing leaders, advancing policy, and taking action to solve today's most pressing challenges.



Joel Kaplan

---

### *Board of Directors, George W. Bush Presidential Center*

Joel Kaplan is Vice President, Global Public Policy at Facebook. In this role, he manages the company's global public policy strategy, working with governments and non-governmental organizations to foster understanding and support for Facebook's innovative technology. He originally joined Facebook in 2011 as Vice President of US Public Policy, overseeing the company's relationships with policymakers at the federal and state levels.

**Show more (Javascript:void(0):)**

# Exhibit 7

[Join us](#)

## Kevin J. Martin

### Vice-President, Mobile and Global Access Policy, Meta

Kevin Martin is the Vice-President for Mobile and Global Access Policy at Facebook, where he oversees, among others, Facebook's free access program Internet.org. Previously, he served as Chairman (2005-2009) and Commissioner (2001-2005) of the Federal Communications Commission. During his tenure, the FCC adopted a non-binding policy statement on net neutrality which led to the 2010 Open Internet Order. After leaving the FCC he joined the Aspen Institute as a Senior Fellow at the think tank's Communications and Society Program, and later the law firm Squire Patton Boggs LLP as a Partner. He holds a B.A. from the University of North Carolina at Chapel Hill, an M.P.P. from Duke University, and a J.D. from Harvard Law School.



### Subscribe for updates

A weekly update of what's on the Global Agenda

Email address

---

**Follow the World Economic Forum**

# Exhibit 8

BREAKING



WATCH LIVE

TECH

# Facebook spent more on lobbying than any other Big Tech company in 2020

PUBLISHED FRI, JAN 22 2021-11:03 AM EST UPDATED FRI, JAN 22 2021-11:41 AM EST



**Lauren Feiner**  
@LAUREN\_FEINER

WATCH LIVE

## KEY POINTS

Tech companies disclosed their lobbying spending for the fourth quarter of 2020 late Thursday night, revealing big swings in spending from 2019 to 2020.

Facebook spent more than any other Big Tech company in 2020 at \$19.68 million. It increased its lobbying spending by 17.8% versus 2019.

Google notably spent 36.2% less on lobbying in 2020 compared with 2019, totaling \$7.53 million.



MARKETS



CNBC TV



WATCHLIST



MENU

BREAKING



WATCH LIVE



In a year when examining the power of the Big Tech companies became a major theme across the federal government, the top five major players spent millions of dollars lobbying Congress on issues ranging from election integrity to immigration.

Tech companies disclosed their lobbying spending for the fourth quarter of 2020 late Thursday night, revealing big swings in spending from 2019 to 2020. Combined, however, the five biggest companies ([Amazon](#), [Apple](#), [Facebook](#), [Google](#) and [Microsoft](#)) spent less in 2020 than in the year before at \$61.09 million, a 4.8% decrease.

In 2020, all of those companies except Microsoft saw their businesses probed by the House Judiciary subcommittee on antitrust, which [concluded that each held monopoly power](#). [Facebook](#) and [Google](#) both saw new antitrust lawsuits from both state and federal enforcers and Amazon and Apple are both said to be under investigation by federal agencies. Meanwhile, the election and the pandemic brought to the forefront other questions about the tech companies' practices, including how they moderate content, display ads and protect users' privacy.



MARKETS



CNBC TV



WATCHLIST



MENU

BREAKING



WATCH LIVE



For the full year 2020, Facebook spent more than any other Big Tech company at \$19.68 million. It increased its lobbying spending by 17.8% from 2019 in a year when the Federal Trade Commission and 48 attorneys general from states and territories filed antitrust complaints against the business.

In the fourth quarter, Facebook lobbied on issues including copyright reform, election integrity, content policy, immigration and international tax policies.

Amazon spent the second most of its Big Tech peers in 2020 at \$17.86 million, up 10.7% from the year before. In the fourth quarter, Amazon lobbied on issues including broadband, intellectual property, postal reform, health care and the Justice in Policing Act.

[Google](#) notably spent 36.2% less on lobbying in 2020 compared with 2019, totaling \$7.53 million. It had [already reduced its lobbying spending](#) by more than 44% from 2018 to 2019 when it offloaded several external lobbying firms.

In the fourth quarter of 2020, Google engaged Congress on topics including online advertising regulation, student digital privacy, pandemic contact tracing and competition law.

TikTok owner ByteDance, a Chinese company, notably ramped up spending in 2020 as the [Trump administration attempted to bar it from operating the app in the U.S.](#) and get it to sell TikTok to a new owner, pointing to alleged security concerns with the China-based parent company. The status of that effort is still pending court action, but it's possible the Biden administration could take a different approach to the business.

ByteDance, which registered to lobby in 2019 and spent less than \$300,000 that year, spent \$2.58 million in 2020 on its efforts, representing an 855.6% increase. It lobbied on issues including a bill meant to bar TikTok from government-owned devices, content



MARKETS



CNBC TV



WATCHLIST



MENU

**BREAKING**

WATCH LIVE



which would allow them to continue hiring drivers as independent workers rather than employees, spending millions of dollars on that state effort alone. [The measure ultimately passed.](#)

On the federal level, Lyft focused its efforts in the fourth quarter on similar issues, according to its public filing, including “the future of work and portable benefits,” tax filing issues for independent contractors and work classification.

Uber also lobbied on issues including “flexible work,” as well as issues related to the Covid-19 vaccine, according to its public filing for the fourth quarter. But it actually spent slightly less on federal lobbying this year compared with 2019 at \$2.33 million, a 1.3% decrease.

[Subscribe to CNBC on YouTube.](#)

[WATCH: Here's why some experts are calling for a breakup of Big Tech after the House antitrust report](#)

**VIDEO** 02:34

Why some experts are calling for a breakup of Big Tech after the House antitrust report



MARKETS



CNBC TV



WATCHLIST



MENU

# Exhibit 9

**UNITED STATES  
SECURITIES AND EXCHANGE COMMISSION  
Washington, D.C. 20549**

**FORM 10-K**

(Mark One)

**ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**  
For the fiscal year ended December 31, 2020

or

**TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**  
For the transition period from \_\_\_\_\_ to \_\_\_\_\_  
Commission File Number: 001-35551

**Facebook, Inc.**

(Exact name of registrant as specified in its charter)

**Delaware**

(State or other jurisdiction of incorporation or organization)

**20-1665019**

(I.R.S. Employer Identification Number)

**1601 Willow Road, Menlo Park, California 94025**

(Address of principal executive offices and Zip Code)

**(650) 543-4800**

(Registrant's telephone number, including area code)

**Securities registered pursuant to Section 12(b) of the Act**

Title of each class	Trading symbol(s)	Name of each exchange on which registered
Class A Common Stock, \$0.000006 par value	FB	The Nasdaq Stock Market LLC

**Securities registered pursuant to Section 12(g) of the Act: None**

Indicate by check mark if the registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act. Yes  No

Indicate by check mark if the registrant is not required to file reports pursuant to Section 13 or Section 15(d) of the Act. Yes  No

Indicate by check mark whether the registrant (1) has filed all reports required to be filed by Section 13 or 15(d) of the Securities Exchange Act of 1934 (Exchange Act) during the preceding 12 months (or for such shorter period that the registrant was required to file such reports), and (2) has been subject to such filing requirements for the past 90 days. Yes  No

Indicate by check mark whether the registrant has submitted electronically every Interactive Data File required to be submitted pursuant to Rule 405 of Regulation S-T (§ 232.405 of this chapter) during the preceding 12 months (or for such shorter period that the registrant was required to submit such files). Yes  No

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer, a smaller reporting company, or an emerging growth company. See the definitions of "large accelerated filer," "accelerated filer," "smaller reporting company," and "emerging growth company" in Rule 12b-2 of the Exchange Act.

Large accelerated filer	<input checked="" type="checkbox"/>	Accelerated filer	<input type="checkbox"/>
Non-accelerated filer	<input type="checkbox"/>	Smaller reporting company	<input type="checkbox"/>
		Emerging growth company	<input type="checkbox"/>

If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13(a) of the Exchange Act.

Indicate by check mark whether the registrant has filed a report on and attestation to its management's assessment of the effectiveness of its internal control over financial reporting under Section 404(b) of the Sarbanes-Oxley Act (15 U.S.C. 7262(b)) by the registered public accounting firm that prepared or issued its audit report.

Indicate by check mark whether the registrant is a shell company (as defined in Rule 12b-2 of the Exchange Act). Yes  No

The aggregate market value of the voting and non-voting stock held by non-affiliates of the registrant as of June 30, 2020, the last business day of the registrant's most recently completed second fiscal quarter, was \$563 billion based upon the closing price reported for such date on the Nasdaq Global Select Market. On January 22, 2021, the registrant had 2,405,448,410 shares of Class A common stock and 442,221,541 shares of Class B common stock outstanding.

**DOCUMENTS INCORPORATED BY REFERENCE**

Portions of the registrant's Proxy Statement for the 2021 Annual Meeting of Stockholders are incorporated herein by reference in Part III of this Annual Report on Form 10-K to the extent stated herein. Such proxy statement will be filed with the Securities and Exchange Commission within 120 days of the registrant's fiscal year ended December 31, 2020.

**Facebook, Inc.**  
**Form 10-K**

**TABLE OF CONTENTS**

	<u>Page</u>
<a href="#">Note About Forward-Looking Statements</a>	<a href="#">3</a>
<a href="#">Limitations of Key Metrics and Other Data</a>	<a href="#">4</a>
<b><u>PART I</u></b>	
<a href="#">Item 1. Business</a>	<a href="#">7</a>
<a href="#">Item 1A. Risk Factors</a>	<a href="#">12</a>
<a href="#">Item 1B. Unresolved Staff Comments</a>	<a href="#">45</a>
<a href="#">Item 2. Properties</a>	<a href="#">45</a>
<a href="#">Item 3. Legal Proceedings</a>	<a href="#">45</a>
<a href="#">Item 4. Mine Safety Disclosures</a>	<a href="#">47</a>
<b><u>PART II</u></b>	
<a href="#">Item 5. Market for Registrant's Common Equity, Related Stockholder Matters and Issuer Purchases of Equity Securities</a>	<a href="#">48</a>
<a href="#">Item 6. Selected Financial Data</a>	<a href="#">50</a>
<a href="#">Item 7. Management's Discussion and Analysis of Financial Condition and Results of Operations</a>	<a href="#">52</a>
<a href="#">Item 7A. Quantitative and Qualitative Disclosures About Market Risk</a>	<a href="#">76</a>
<a href="#">Item 8. Financial Statements and Supplementary Data</a>	<a href="#">77</a>
<a href="#">Item 9. Changes in and Disagreements with Accountants on Accounting and Financial Disclosure</a>	<a href="#">112</a>
<a href="#">Item 9A. Controls and Procedures</a>	<a href="#">112</a>
<a href="#">Item 9B. Other Information</a>	<a href="#">112</a>
<b><u>PART III</u></b>	
<a href="#">Item 10. Directors, Executive Officers and Corporate Governance</a>	<a href="#">113</a>
<a href="#">Item 11. Executive Compensation</a>	<a href="#">113</a>
<a href="#">Item 12. Security Ownership of Certain Beneficial Owners and Management and Related Stockholder Matters</a>	<a href="#">113</a>
<a href="#">Item 13. Certain Relationships and Related Transactions, and Director Independence</a>	<a href="#">113</a>
<a href="#">Item 14. Principal Accounting Fees and Services</a>	<a href="#">113</a>
<b><u>PART IV</u></b>	
<a href="#">Item 15. Exhibits, Financial Statement Schedules</a>	<a href="#">114</a>
<a href="#">Item 16. Form 10-K Summary</a>	<a href="#">116</a>
<a href="#">Signatures</a>	

## NOTE ABOUT FORWARD-LOOKING STATEMENTS

This Annual Report on Form 10-K contains forward-looking statements. All statements contained in this Annual Report on Form 10-K other than statements of historical fact, including statements regarding our future results of operations and financial position, our business strategy and plans, and our objectives for future operations, are forward-looking statements. The words "believe," "may," "will," "estimate," "continue," "anticipate," "intend," "expect," and similar expressions are intended to identify forward-looking statements. We have based these forward-looking statements largely on our current expectations and projections about future events and trends that we believe may affect our financial condition, results of operations, business strategy, short-term and long-term business operations and objectives, and financial needs. These forward-looking statements are subject to a number of risks, uncertainties and assumptions, including those described in Part I, Item 1A, "Risk Factors" in this Annual Report on Form 10-K. Moreover, we operate in a very competitive and rapidly changing environment. New risks emerge from time to time. It is not possible for our management to predict all risks, nor can we assess the impact of all factors on our business or the extent to which any factor, or combination of factors, may cause actual results to differ materially from those contained in any forward-looking statements we may make. In light of these risks, uncertainties and assumptions, the future events and trends discussed in this Annual Report on Form 10-K may not occur and actual results could differ materially and adversely from those anticipated or implied in the forward-looking statements.

We undertake no obligation to revise or publicly release the results of any revision to these forward-looking statements, except as required by law. Given these risks and uncertainties, readers are cautioned not to place undue reliance on such forward-looking statements.

Unless expressly indicated or the context requires otherwise, the terms "Facebook," "company," "we," "us," and "our" in this document refer to Facebook, Inc., a Delaware corporation, and, where appropriate, its subsidiaries. The term "Facebook" may also refer to our products, regardless of the manner in which they are accessed. The term "Family" refers to our Facebook, Instagram, Messenger, and WhatsApp products. For references to accessing Facebook or our other products on the "web" or via a "website," such terms refer to accessing such products on personal computers. For references to accessing Facebook or our other products on "mobile," such term refers to accessing such products via a mobile application or via a mobile-optimized version of our websites such as m.facebook.com, whether on a mobile phone or tablet.

## LIMITATIONS OF KEY METRICS AND OTHER DATA

The numbers for our key metrics are calculated using internal company data based on the activity of user accounts. We have historically reported the numbers of our daily active users (DAUs), monthly active users (MAUs), and average revenue per user (ARPU) (collectively, our "Facebook metrics") based on user activity only on Facebook and Messenger and not on our other products. Beginning with our Annual Report on Form 10-K for the year ended December 31, 2019, we also report our estimates of the numbers of our daily active people (DAP), monthly active people (MAP), and average revenue per person (ARPP) (collectively, our "Family metrics") based on the activity of users who visited at least one of Facebook, Instagram, Messenger, and WhatsApp (collectively, our "Family" of products) during the applicable period of measurement. We believe our Family metrics better reflect the size of our community and the fact that many people are using more than one of our products. As a result, over time we intend to report our Family metrics as key metrics in place of DAUs, MAUs, and ARPU in our periodic reports filed with the Securities and Exchange Commission.

While these numbers are based on what we believe to be reasonable estimates of our user base for the applicable period of measurement, there are inherent challenges in measuring usage of our products across large online and mobile populations around the world. The methodologies used to measure these metrics require significant judgment and are also susceptible to algorithm or other technical errors. In addition, we are continually seeking to improve our estimates of our user base, and such estimates may change due to improvements or changes in our methodology. We regularly review our processes for calculating these metrics, and from time to time we discover inaccuracies in our metrics or make adjustments to improve their accuracy, which can result in adjustments to our historical metrics. Our ability to recalculate our historical metrics may be impacted by data limitations or other factors that require us to apply different methodologies for such adjustments. We generally do not intend to update previously disclosed Family metrics for any such inaccuracies or adjustments that are within the error margins disclosed below.

In addition, our Facebook metrics and Family metrics estimates will differ from estimates published by third parties due to differences in methodology.

### Facebook Metrics

We regularly evaluate our Facebook metrics to estimate the number of "duplicate" and "false" accounts among our MAUs. A duplicate account is one that a user maintains in addition to his or her principal account. We divide "false" accounts into two categories: (1) user-misclassified accounts, where users have created personal profiles for a business, organization, or non-human entity such as a pet (such entities are permitted on Facebook using a Page rather than a personal profile under our terms of service); and (2) violating accounts, which represent user profiles that we believe are intended to be used for purposes that violate our terms of service, such as bots and spam. The estimates of duplicate and false accounts are based on an internal review of a limited sample of accounts, and we apply significant judgment in making this determination. For example, to identify duplicate accounts we use data signals such as identical IP addresses and similar user names, and to identify false accounts we look for names that appear to be fake or other behavior that appears inauthentic to the reviewers. Any loss of access to data signals we use in this process, whether as a result of our own product decisions, actions by third-party browser or mobile platforms, regulatory or legislative requirements, limitations while our personnel work remotely during the COVID-19 pandemic, or other factors, also may impact the stability or accuracy of our estimates of duplicate and false accounts. Our estimates also may change as our methodologies evolve, including through the application of new data signals or technologies or product changes that may allow us to identify previously undetected duplicate or false accounts and may improve our ability to evaluate a broader population of our users. Duplicate and false accounts are very difficult to measure at our scale, and it is possible that the actual number of duplicate and false accounts may vary significantly from our estimates.

In the fourth quarter of 2020, we estimated that duplicate accounts may have represented approximately 11% of our worldwide MAUs. We believe the percentage of duplicate accounts is meaningfully higher in developing markets such as the Philippines and Vietnam, as compared to more developed markets. In the fourth quarter of 2020, we estimated that false accounts may have represented approximately 5% of our worldwide MAUs. Our estimation of false accounts can vary as a result of episodic spikes in the creation of such accounts, which we have seen originate more frequently in specific countries such as Indonesia and Vietnam. From time to time, we disable certain user accounts, make product changes, or take other actions to reduce the number of duplicate or false accounts among our users, which may also reduce our DAU and MAU estimates in a particular period. We intend to disclose our estimates of the number of duplicate and false accounts among our MAUs on an annual basis.

## [Table of Contents](#)

The numbers of DAUs and MAUs discussed in this Annual Report on Form 10-K, as well as ARPU, do not include users on Instagram, WhatsApp, or our other products, unless they would otherwise qualify as DAUs or MAUs, respectively, based on their other activities on Facebook.

### **Family Metrics**

Many people in our community have user accounts on more than one of our products, and some people have multiple user accounts within an individual product. Accordingly, for our Family metrics, we do not seek to count the total number of user accounts across our products because we believe that would not reflect the actual size of our community. Rather, our Family metrics represent our estimates of the number of unique people using at least one of Facebook, Instagram, Messenger, and WhatsApp. We do not require people to use a common identifier or link their accounts to use multiple products in our Family, and therefore must seek to attribute multiple user accounts within and across products to individual people. To calculate these metrics, we rely upon complex techniques, algorithms and machine learning models that seek to count the individual people behind user accounts, including by matching multiple user accounts within an individual product and across multiple products when we believe they are attributable to a single person, and counting such group of accounts as one person. These techniques and models require significant judgment, are subject to data and other limitations discussed below, and inherently are subject to statistical variances and uncertainties. We estimate the potential error in our Family metrics primarily based on user survey data, which itself is subject to error as well. While we expect the error margin for our Family metrics to vary from period to period, we estimate that such margin generally will be approximately 4% of our worldwide MAP. At our scale, it is very difficult to attribute multiple user accounts within and across products to individual people, and it is possible that the actual numbers of unique people using our products may vary significantly from our estimates, potentially beyond our estimated error margins. As a result, it is also possible that our Family metrics may indicate changes or trends in user numbers that do not match actual changes or trends.

To calculate our estimates of Family DAP and MAP, we currently use a series of machine learning models that are developed based on internal reviews of limited samples of user accounts and calibrated against user survey data. We apply significant judgment in designing these models and calculating these estimates. For example, to match user accounts within individual products and across multiple products, we use data signals such as similar device information, IP addresses, and user names. We also calibrate our models against data from periodic user surveys of varying sizes and frequency across our products, which are inherently subject to error. The timing and results of such user surveys have in the past contributed, and may in the future contribute, to changes in our reported Family metrics from period to period. In addition, our data limitations may affect our understanding of certain details of our business and increase the risk of error for our Family metrics estimates. Our techniques and models rely on a variety of data signals from different products, and we rely on more limited data signals for some products compared to others. For example, as a result of limited visibility into encrypted products, we have fewer data signals from WhatsApp user accounts and primarily rely on phone numbers and device information to match WhatsApp user accounts with accounts on our other products. Similarly, although Messenger Kids users are included in our Family metrics, we do not seek to match their accounts with accounts on our other applications for purposes of calculating DAP and MAP. Any loss of access to data signals we use in our process for calculating Family metrics, whether as a result of our own product decisions, actions by third-party browser or mobile platforms, regulatory or legislative requirements, limitations while our personnel work remotely during the COVID-19 pandemic, or other factors, also may impact the stability or accuracy of our reported Family metrics. Our estimates of Family metrics also may change as our methodologies evolve, including through the application of new data signals or technologies, product changes, or other improvements in our user surveys, algorithms, or machine learning that may improve our ability to match accounts within and across our products or otherwise evaluate the broad population of our users. In addition, such evolution may allow us to identify previously undetected violating accounts (as defined below).

We regularly evaluate our Family metrics to estimate the percentage of our MAP consisting solely of "violating" accounts. We define "violating" accounts as accounts which we believe are intended to be used for purposes that violate our terms of service, including bots and spam. In the fourth quarter of 2020, we estimated that approximately 3% of our worldwide MAP consisted solely of violating accounts. Such estimation is based on an internal review of a limited sample of accounts, and we apply significant judgment in making this determination. For example, we look for account information and behaviors associated with Facebook and Instagram accounts that appear to be inauthentic to the reviewers, but we have limited visibility into WhatsApp user activity due to encryption. In addition, if we believe an individual person has one or more violating accounts, we do not include such person in our violating accounts estimation as long as we believe they have one account that does not constitute a violating account. From time to time, we disable certain user accounts, make product changes, or take other actions to reduce the number of violating accounts among our users, which may also reduce our DAP and MAP estimates in a particular period. We intend to disclose our estimates of the percentage of our MAP consisting solely

[Table of Contents](#)

of violating accounts on an annual basis. Violating accounts are very difficult to measure at our scale, and it is possible that the actual number of violating accounts may vary significantly from our estimates.

The numbers of Family DAP and MAP discussed in this Annual Report on Form 10-K, as well as ARPP, do not include users on our other products, unless they would otherwise qualify as DAP or MAP, respectively, based on their other activities on our Family products.

**User Geography**

Our data regarding the geographic location of our users is estimated based on a number of factors, such as the user's IP address and self-disclosed location. These factors may not always accurately reflect the user's actual location. For example, a user may appear to be accessing Facebook from the location of the proxy server that the user connects to rather than from the user's actual location. The methodologies used to measure our metrics are also susceptible to algorithm or other technical errors, and our estimates for revenue by user location and revenue by user device are also affected by these factors.

## PART I

### Item 1. Business

#### Overview

Our mission is to give people the power to build community and bring the world closer together.

We build useful and engaging products that enable people to connect and share with friends and family through mobile devices, personal computers, virtual reality headsets, and in-home devices. We also help people discover and learn about what is going on in the world around them, enable people to share their opinions, ideas, photos and videos, and other activities with audiences ranging from their closest family members and friends to the public at large, and stay connected everywhere by accessing our products, including:

- **Facebook.** Facebook enables people to connect, share, discover, and communicate with each other on mobile devices and personal computers. There are a number of different ways to engage with people on Facebook and build community, including Facebook News Feed, Stories, Groups, Shops, Marketplace, News, and Watch.
- **Instagram.** Instagram brings people closer to the people and things they love. It is a place where people can express themselves through photos, videos, and private messaging, and connect with and shop from their favorite businesses and creators. They can do this through Instagram Feed, Stories, Reels, IGTV, Live, Shops, and messaging.
- **Messenger.** Messenger is a simple yet powerful messaging application for people to connect with friends, family, groups, and businesses across platforms and devices through chat, video, and Rooms.
- **WhatsApp.** WhatsApp is a simple, reliable, and secure messaging application that is used by people and businesses around the world to communicate and transact in a private way.
- **Facebook Reality Labs.** Facebook Reality Labs' augmented and virtual reality products help people feel connected, anytime, anywhere. Oculus Quest lets people defy distance with cutting-edge virtual reality (VR) hardware, software, and content, while Portal helps friends and families stay connected and share the moments that matter in meaningful ways.

We generate substantially all of our revenue from selling advertising placements to marketers. Our ads enable marketers to reach people based on a variety of factors including age, gender, location, interests, and behaviors. Marketers purchase ads that can appear in multiple places including on Facebook, Instagram, Messenger, and third-party applications and websites.

#### Competition

Our business is characterized by innovation, rapid change, and disruptive technologies. We compete with companies providing connection and communication products and services to users online, as well as companies that sell advertising to businesses looking to reach consumers and/or develop tools and systems for managing and optimizing advertising campaigns. We face significant competition in every aspect of our business, including, but not limited to, companies that facilitate the ability of users to share, communicate, and discover content and information online or enable marketers to reach their existing or prospective audiences, including, for example, Google, Apple, YouTube, Tencent, Snap, Twitter, ByteDance, Microsoft, and Amazon. We compete to attract, engage, and retain people who use our products, to attract and retain businesses who use our free or paid business and advertising services, and to attract and retain developers to build compelling mobile and web applications that integrate with our products. We also compete with companies that develop and deliver consumer hardware and virtual reality products and services. As we introduce or acquire new products, as our existing products evolve, or as other companies introduce new products and services, we may become subject to additional competition.

## **Technology**

Our product development philosophy is centered on continuous innovation in creating and improving products that are social by design, which means that our products are designed to place people and their social interactions at the core of the product experience. As our user base grows, as engagement with products like video and VR increases, and as we deepen our investment in new technologies like artificial intelligence, our computing needs continue to expand. We make significant investments in technology both to improve our existing products and services and to develop new ones, as well as for our marketers and developers. We are also investing in protecting the security, privacy, and integrity of our platform by investing in both people and technology to strengthen our systems against abuse.

## **Sales and Operations**

The majority of our marketers use our self-service ad platform to launch and manage their advertising campaigns. We also have a global sales force that is focused on attracting and retaining advertisers and providing support to them throughout the stages of the marketing cycle from pre-purchase decision-making to real-time optimizations to post-campaign analytics. We work directly with these advertisers, as well as through advertising agencies and resellers. We operate in more than 80 cities around the globe, the majority of which have a sales presence. We also invest in and rely on self-service tools to provide direct customer support to our users and partners.

## **Marketing**

Historically, our communities have generally grown organically with people inviting their friends to connect with them, supported by internal efforts to stimulate awareness and interest. In addition, we have invested and will continue to invest in marketing our products and services to grow our brand and help build community around the world.

## **Intellectual Property**

To establish and protect our proprietary rights, we rely on a combination of patents, trademarks, copyrights, trade secrets, including know-how, license agreements, confidentiality procedures, non-disclosure agreements with third parties, employee disclosure and invention assignment agreements, and other contractual rights. In addition, to further protect our proprietary rights, from time to time we have purchased patents and patent applications from third parties. We do not believe that our proprietary technology is dependent on any single patent or copyright or groups of related patents or copyrights. We believe the duration of our patents is adequate relative to the expected lives of our products.

## **Government Regulation**

We are subject to a variety of laws and regulations in the United States and abroad that involve matters central to our business, many of which are still evolving and being tested in courts, and could be interpreted in ways that could harm our business. These laws and regulations involve matters including privacy, data use, data protection and personal information, rights of publicity, content, intellectual property, advertising, marketing, distribution, data security, data retention and deletion, data localization and storage, data disclosure, artificial intelligence, electronic contracts and other communications, competition, protection of minors, consumer protection, telecommunications, product liability, e-commerce, taxation, economic or other trade prohibitions or sanctions, anti-corruption and political law compliance, securities law compliance, and online payment services. In particular, we are subject to federal, state, and foreign laws regarding privacy and protection of people's data. Foreign data protection, privacy, content, competition, and other laws and regulations can impose different obligations or be more restrictive than those in the United States.

These U.S. federal and state and foreign laws and regulations, which in some cases can be enforced by private parties in addition to government entities, are constantly evolving and can be subject to significant change. As a result, the application, interpretation, and enforcement of these laws and regulations are often uncertain, particularly in the new and rapidly evolving industry in which we operate, and may be interpreted and applied inconsistently from country to country and inconsistently with our current policies and practices. For example, regulatory or legislative actions affecting the manner in which we display content to our users or obtain consent to various practices, or otherwise relating to content that is made available on our products, could adversely affect our financial results. In the United States, there have been, and continue to be, various efforts to remove or restrict the scope of the protections available to online platforms under Section 230 of the Communications Decency Act, and any such changes may increase our costs or require significant changes to our products, business practices, or operations, which could adversely affect our business and financial results.

We are also subject to evolving laws and regulations that dictate whether, how, and under what circumstances we can transfer, process and/or receive certain data that is critical to our operations, including data shared between countries or regions in which we operate and data shared among our products and services. If we are unable to transfer data between and among countries and regions in which we operate, or if we are restricted from sharing data among our products and services, it could affect our ability to provide our services, the manner in which we provide our services or our ability to target ads, which could adversely affect our financial results. For example, the Privacy Shield, a transfer framework we relied upon for data transferred from the European Union to the United States, was invalidated in July 2020 by the Court of Justice of the European Union (CJEU). In addition, the other bases upon which Facebook relies to transfer such data, such as Standard Contractual Clauses (SCCs), have been subjected to regulatory and judicial scrutiny. In August 2020, we received a preliminary draft decision from the Irish Data Protection Commission (IDPC) that preliminarily concluded that Facebook Ireland's reliance on SCCs in respect of European user data does not achieve compliance with the GDPR and preliminarily proposed that such transfers of user data from the European Union to the United States should therefore be suspended. Facebook Ireland challenged procedural aspects of this IDPC inquiry in a judicial review commenced in the Irish High Court in September 2020. While we also rely upon alternative legal bases for data transfers, if a new transatlantic data transfer framework is not adopted and we are unable to continue to rely on SCCs or validly rely upon other alternative means of data transfers from Europe to the United States, we may be unable to operate material portions of our business in Europe as a result of the CJEU's invalidation of the Privacy Shield and any final decision of IDPC, which would materially and adversely affect our business, financial condition, and results of operations.

Proposed or new legislation and regulations could also significantly affect our business. For example, the European General Data Protection Regulation (GDPR) took effect in May 2018 and applies to all of our products and services used by people in Europe. The GDPR includes operational requirements for companies that receive or process personal data of residents of the European Union that are different from those previously in place in the European Union, and includes significant penalties for non-compliance. The Brazilian General Data Protection Law recently took effect and imposes data privacy-related requirements similar to GDPR on products and services offered to users in Brazil. The California Consumer Privacy Act, which took effect in January 2020, also establishes certain transparency rules and creates new data privacy rights for users. In addition, effective December 2020, the European Union's ePrivacy Directive includes additional limitations on the use of data across messaging products and includes significant penalties for non-compliance. Changes to our products or business practices as a result of these developments may adversely affect our advertising business. Similarly, there are a number of legislative proposals in the European Union, the United States, at both the federal and state level, as well as other jurisdictions that could impose new obligations or limitations in areas affecting our business, such as liability for copyright infringement. In addition, some countries are considering or have passed legislation implementing data protection requirements or requiring local storage and processing of data or similar requirements that could increase the cost and complexity of delivering our services.

We are, and expect to continue to be, the subject of investigations, inquiries, data requests, requests for information, actions, and audits by government authorities and regulators in the United States, Europe, and around the world, particularly in the areas of privacy, data protection, law enforcement, consumer protection, and competition, as we continue to grow and expand our operations. We are also currently, and may in the future be, subject to regulatory orders or consent decrees, including the modified consent order we entered into with the U.S. Federal Trade Commission (FTC), which took effect in April 2020 and, among other matters, requires us to implement a comprehensive expansion of our privacy program. Orders issued by, or inquiries or enforcement actions initiated by, government or regulatory authorities could cause us to incur substantial costs, expose us to unanticipated civil and criminal liability or penalties (including substantial monetary remedies), interrupt or require us to change our business practices in a manner materially adverse to our business, result in negative publicity and reputational harm, divert resources and the time and attention of management from our business, or subject us to other structural or behavioral remedies that adversely affect our business.

For additional information about government regulation applicable to our business, see Part I, Item 1A, "Risk Factors" in this Annual Report on Form 10-K.

## **Human Capital**

At Facebook, we design products to bring the world closer together, one connection at a time. As a company, we believe that people are at the heart of every connection we build. We are proud of our unique company culture where ideas, innovation, and impact win, and we work hard to build strong teams across engineering, product design, marketing, and other areas to further our mission.

## [Table of Contents](#)

We had a global workforce of 58,604 employees as of December 31, 2020, which represents a 30% year-over-year increase in employee headcount. We expect headcount growth to continue for the foreseeable future, particularly as we continue to focus on recruiting employees in technical functions. In addition, we plan to continue to hire a number of employees and contractors to continue to bolster various privacy, safety, security, and content review initiatives as well as other functions to support our expected growth.

Our headquarters are located in Menlo Park, California and we have offices in more than 80 cities around the globe. The vast majority of our personnel are currently working remotely as a result of the COVID-19 pandemic, and in the long term, we expect some personnel to transition to working remotely on a regular basis.

### ***Diversity and Inclusion***

Diversity and inclusion are core to our work at Facebook. We seek to build a diverse and inclusive workplace where we can leverage our collective cognitive diversity to build the best products and make the best decisions for the global community we serve. While we have made progress, we still have more work to do.

We publish our global gender diversity and U.S. ethnic diversity workforce data annually. In 2020, we announced that as of June 30, 2020, our global employee base was comprised of 37% females and 63% males, and our U.S. employee base was comprised of the following ethnicities: 44.4% Asian, 41% White, 6.3% Hispanic, 4% two or more ethnicities, 3.9% Black, and 0.4% additional groups (including American Indian or Alaska Native and Native Hawaiian or Other Pacific Islander). We also announced our goals to have 50% of our workforce made up of underrepresented populations by 2024, and to increase the representation of people of color in leadership positions in the United States, including Black leadership, by 30% from 2020 to 2025. We will also continue our ongoing efforts to increase the representation of women in leadership.

We work to support our goals of diversifying our workforce through recruiting, retention, people development, and inclusion. We employ our Diverse Slate Approach in our global recruitment efforts, which ensures that teams and hiring managers have the opportunity to consider qualified people from underrepresented groups for open roles. We have seen steady increases in hiring rates of people from underrepresented groups since we started testing this approach in 2015. We also continue to provide diversity and inclusion training for our recruiting team and develop inclusive internship programs. Facebook University, our training program for college freshmen and sophomores with an interest in Computer Science, also utilizes a proactive and inclusive approach to promote participation by people from underrepresented groups. To help build community among our people and support their professional development, we invest in our internal Facebook Resource Groups and our annual Community events such as Women's Community Summit, Black Community Summit, Latin Community Summit, and Pride Community Summit. We also offer Managing Unconscious Bias, Managing Inclusion, and Be the Ally trainings to promote an inclusive workplace by helping people understand the issues that affect underrepresented communities and how to reduce the effects of bias in the workplace.

### ***Compensation and Benefits***

We offer competitive compensation to attract and retain the best people, and we help care for our people so they can focus on our mission. Our employees' total compensation package includes market-competitive salary, bonuses or sales commissions, and equity. We generally offer full-time employees equity at the time of hire and through annual equity grants because we want them to be owners of the company and committed to our long-term success. We have conducted pay equity analyses for many years, and continue to be committed to pay equity. In 2020, we announced that our analyses indicate that we continue to have pay equity across gender globally and race in the United States for people in similar jobs, accounting for factors such as location, role, and level.

Through Life@ Facebook, our holistic approach to benefits, we provide our employees and their loved ones resources to help them thrive. We offer a wide range of benefits across areas such as health, family, finance, community, and time away, including healthcare and wellness benefits, adoption and surrogacy assistance, family care resources, a 401(k) plan, access to tax and legal services, Facebook Resource Groups to build community at Facebook, family leave, and paid time off.

## **Corporate Information**

We were incorporated in Delaware in July 2004. We completed our initial public offering in May 2012 and our Class A common stock is listed on The Nasdaq Global Select Market under the symbol "FB." Our principal executive offices are located at 1601 Willow Road, Menlo Park, California 94025, and our telephone number is (650) 543-4800.

Facebook, the Facebook logo, FB, the Like button, Instagram, Oculus, WhatsApp, and our other registered or common law trademarks, service marks, or trade names appearing in this Annual Report on Form 10-K are the property of Facebook, Inc. or its affiliates. Other trademarks, service marks, or trade names appearing in this Annual Report on Form 10-K are the property of their respective owners.

## **Available Information**

Our website address is [www.facebook.com](http://www.facebook.com). Our Annual Reports on Form 10-K, Quarterly Reports on Form 10-Q, Current Reports on Form 8-K, and amendments to reports filed pursuant to Sections 13(a) and 15(d) of the Securities Exchange Act of 1934, as amended (Exchange Act), are filed with the U.S. Securities and Exchange Commission (SEC). We are subject to the informational requirements of the Exchange Act and file or furnish reports, proxy statements, and other information with the SEC. Such reports and other information filed by us with the SEC are available free of charge on our website at [investor.fb.com](http://investor.fb.com) when such reports are available on the SEC's website. We use our [investor.fb.com](http://investor.fb.com) and [about.fb.com/news/](http://about.fb.com/news/) websites as well as Mark Zuckerberg's Facebook Page (<https://www.facebook.com/zuck>) as means of disclosing material non-public information and for complying with our disclosure obligations under Regulation FD.

The SEC maintains an Internet site that contains reports, proxy and information statements, and other information regarding issuers that file electronically with the SEC at [www.sec.gov](http://www.sec.gov).

The contents of the websites referred to above are not incorporated into this filing. Further, our references to the URLs for these websites are intended to be inactive textual references only.

## **Item 1A. Risk Factors**

*Certain factors may have a material adverse effect on our business, financial condition, and results of operations. You should consider carefully the risks and uncertainties described below, in addition to other information contained in this Annual Report on Form 10-K, including our consolidated financial statements and related notes. The risks and uncertainties described below are not the only ones we face. Additional risks and uncertainties that we are unaware of, or that we currently believe are not material, may also become important factors that adversely affect our business. If any of the following risks actually occurs, our business, financial condition, results of operations, and future prospects could be materially and adversely affected. In that event, the trading price of our Class A common stock could decline, and you could lose part or all of your investment.*

### **Summary Risk Factors**

Our business is subject to a number of risks, including risks that may prevent us from achieving our business objectives or may adversely affect our business, financial condition, results of operations, cash flows, and prospects. These risks are discussed more fully below and include, but are not limited to, risks related to:

#### ***Risks Related to Our Product Offerings***

- our ability to add and retain users and maintain levels of user engagement with our products;
- the loss of, or reduction in spending by, our marketers;
- reduced availability of data signals used by our ad targeting and measurement tools;
- ineffective operation with mobile operating systems or changes in our relationships with mobile operating system partners;
- failure of our new products, or changes to our existing products, to attract or retain users or generate revenue;

#### ***Risks Related to Our Business Operations and Financial Results***

- the COVID-19 pandemic, including its impact on our advertising business;
- our ability to compete effectively;
- unfavorable media coverage and other risks affecting our ability to maintain and enhance our brands;
- volatile or slower user and revenue growth rates in the future;
- acquisitions and our ability to successfully integrate our acquisitions;
- our ability to build, maintain, and scale our technical infrastructure, and risks associated with disruptions in our service;
- operating our business in multiple countries around the world;
- litigation, including class action lawsuits;

#### ***Risks Related to Government Regulation and Enforcement***

- government restrictions on access to Facebook or our other products, or other actions that impair our ability to sell advertising, in their countries;
- complex and evolving U.S. and foreign privacy, data use and data protection, content, competition, consumer protection, and other laws and regulations;

## [Table of Contents](#)

- the impact of government investigations, enforcement actions, and settlements, including litigation and investigations by privacy and competition authorities;
- our ability to comply with regulatory and legislative privacy requirements, including our consent order with the Federal Trade Commission;

### ***Risks Related to Data, Security, and Intellectual Property***

- the occurrence of security breaches, improper access to or disclosure of our data or user data, and other cyber incidents or undesirable activity on our platform;
- our ability to obtain, maintain, protect, and enforce our intellectual property rights; and

### ***Risks Related to Ownership of Our Class A Common Stock***

- limitations on the ability of holders of our Class A Common Stock to influence corporate matters due to the dual class structure of our common stock and the control of a majority of the voting power of our outstanding capital stock by our founder, Chairman, and CEO.

### **Risks Related to Our Product Offerings**

***If we fail to retain existing users or add new users, or if our users decrease their level of engagement with our products, our revenue, financial results, and business may be significantly harmed.***

The size of our user base and our users' level of engagement are critical to our success. Our financial performance has been and will continue to be significantly determined by our success in adding, retaining, and engaging active users of our products, particularly for Facebook and Instagram. We anticipate that our active user growth rate will generally decline over time as the size of our active user base increases, and we expect that the size of our active user base will fluctuate or decline in one or more markets from time to time, particularly in markets where we have achieved higher penetration rates. For example, beginning in the first quarter of 2020, we experienced significant increases in the size and engagement of our active user base across a number of regions as a result of the COVID-19 pandemic. More recently, we have seen user growth and engagement returning to pre-pandemic trends, and in each of the third and fourth quarters of 2020, we experienced slight declines on a quarter-over-quarter basis in the number of daily active users on Facebook in the United States & Canada region. We are unable to predict the impact of the pandemic on user growth and engagement with any certainty, and we expect these trends to continue to be subject to volatility. If people do not perceive our products to be useful, reliable, and trustworthy, we may not be able to attract or retain users or otherwise maintain or increase the frequency and duration of their engagement. A number of other social networking companies that achieved early popularity have since seen their active user bases or levels of engagement decline, in some cases precipitously. There is no guarantee that we will not experience a similar erosion of our active user base or engagement levels. Our user engagement patterns have changed over time, and user engagement can be difficult to measure, particularly as we introduce new and different products and services. Any number of factors can negatively affect user retention, growth, and engagement, including if:

- users increasingly engage with other competitive products or services;
- we fail to introduce new features, products, or services that users find engaging or if we introduce new products or services, or make changes to existing products and services, that are not favorably received;
- users feel that their experience is diminished as a result of the decisions we make with respect to the frequency, prominence, format, size, and quality of ads that we display;
- users have difficulty installing, updating, or otherwise accessing our products on mobile devices as a result of actions by us or third parties that we rely on to distribute our products and deliver our services;
- user behavior on any of our products changes, including decreases in the quality and frequency of content shared on our products and services;

## [Table of Contents](#)

- we are unable to continue to develop products for mobile devices that users find engaging, that work with a variety of mobile operating systems and networks, and that achieve a high level of market acceptance;
- there are decreases in user sentiment due to questions about the quality or usefulness of our products or our user data practices, concerns about the nature of content made available on our products, or concerns related to privacy, safety, security, well-being, or other factors;
- we are unable to manage and prioritize information to ensure users are presented with content that is appropriate, interesting, useful, and relevant to them;
- we are unable to obtain or attract engaging third-party content;
- we are unable to successfully maintain or grow usage of and engagement with mobile and web applications that integrate with Facebook and our other products;
- users adopt new technologies where our products may be displaced in favor of other products or services, or may not be featured or otherwise available;
- there are changes mandated by legislation, government and regulatory authorities, or litigation that adversely affect our products or users;
- we are unable to operate material portions of our business in Europe, or are otherwise limited in such operations, as a result of European regulators, courts, or legislative bodies determining that our reliance on Standard Contractual Clauses (SCCs) or other legal bases we rely upon to transfer user data from the European Union to the United States is invalid;
- there is decreased engagement with our products, or failure to accept our terms of service, as part of privacy-focused changes that we have implemented or may implement in the future, whether voluntarily, in connection with the General Data Protection Regulation (GDPR), the European Union's ePrivacy Directive, the California Consumer Privacy Act (CCPA), or other laws, regulations, or regulatory actions, or otherwise;
- technical or other problems prevent us from delivering our products in a rapid and reliable manner or otherwise affect the user experience, such as security breaches or failure to prevent or limit spam or similar content;
- we adopt terms, policies, or procedures related to areas such as sharing, content, user data, or advertising, or take actions to enforce our policies, that are perceived negatively by our users or the general public, including as a result of decisions or recommendations from the independent Oversight Board regarding content on our platform;
- we elect to focus our product decisions on longer-term initiatives that do not prioritize near-term user growth and engagement;
- we make changes in how we promote different products and services across our family of products;
- initiatives designed to attract and retain users and engagement are unsuccessful or discontinued, whether as a result of actions by us, third parties, or otherwise;
- third-party initiatives that may enable greater use of our products, including low-cost or discounted data plans, are discontinued;
- there is decreased engagement with our products as a result of taxes imposed on the use of social media or other mobile applications in certain countries, internet shutdowns, or other actions by governments that affect the accessibility of our products in their countries;
- we fail to provide adequate customer service to users, marketers, developers, or other partners;

## [Table of Contents](#)

- we, developers whose products are integrated with our products, or other partners and companies in our industry are the subject of adverse media reports or other negative publicity, including as a result of our or their user data practices; or
- our current or future products, such as our development tools and application programming interfaces that enable developers to build, grow, and monetize mobile and web applications, reduce user activity on our products by making it easier for our users to interact and share on third-party mobile and web applications.

From time to time, certain of these factors have negatively affected user retention, growth, and engagement to varying degrees. If we are unable to maintain or increase our user base and user engagement, particularly for our significant revenue-generating products like Facebook and Instagram, our revenue and financial results may be adversely affected. Any significant decrease in user retention, growth, or engagement could render our products less attractive to users, marketers, and developers, which is likely to have a material and adverse impact on our revenue, business, financial condition, and results of operations. If our active user growth rate continues to slow, we will become increasingly dependent on our ability to maintain or increase levels of user engagement and monetization in order to drive revenue growth.

***We generate substantially all of our revenue from advertising. The loss of marketers, or reduction in spending by marketers, could seriously harm our business.***

Substantially all of our revenue is currently generated from third parties advertising on Facebook and Instagram. As is common in the industry, our marketers do not have long-term advertising commitments with us. Many of our marketers spend only a relatively small portion of their overall advertising budget with us. Marketers will not continue to do business with us, or they will reduce the budgets they are willing to commit to us, if we do not deliver ads in an effective manner, or if they do not believe that their investment in advertising with us will generate a competitive return relative to other alternatives. We have implemented, and we will continue to implement, changes to our user data practices. Some of these changes reduce our ability to effectively target ads, which has to some extent adversely affected, and will continue to adversely affect, our advertising business. If we are unable to provide marketers with a suitable return on investment, the pricing of our ads may not increase, or may decline, in which case our revenue and financial results may be harmed.

Our advertising revenue can also be adversely affected by a number of other factors, including:

- decreases in user engagement, including time spent on our products;
- our inability to continue to increase user access to and engagement with our products;
- product changes or inventory management decisions we may make that change the size, format, frequency, or relative prominence of ads displayed on our products or of other unpaid content shared by marketers on our products;
- our inability to maintain or increase marketer demand, the pricing of our ads, or both;
- our inability to maintain or increase the quantity or quality of ads shown to users;
- changes to third-party policies that limit our ability to deliver, target, or measure the effectiveness of advertising, including changes by mobile operating system and browser providers such as Apple and Google;
- adverse government actions or legislative, regulatory, or other legal developments relating to advertising, including developments that may impact our ability to deliver, target, or measure the effectiveness of advertising;
- user behavior or product changes that may reduce traffic to features or products that we successfully monetize, including as a result of increased usage of the Stories format or our messaging products;
- reductions of advertising by marketers due to our efforts to implement or enforce advertising policies that protect the security and integrity of our platform;

## [Table of Contents](#)

- the availability, accuracy, utility, and security of analytics and measurement solutions offered by us or third parties that demonstrate the value of our ads to marketers, or our ability to further improve such tools;
- loss of advertising market share to our competitors, including if prices to purchase our ads increase or if competitors offer lower priced, more integrated, or otherwise more effective products;
- limitations on our ability to operate material portions of our business in Europe as a result of European regulators, courts, or legislative bodies determining that our reliance on SCCs or other legal bases we rely upon to transfer user data from the European Union to the United States is invalid;
- changes in our marketing and sales or other operations that we are required to or elect to make as a result of risks related to complying with foreign laws or regulatory requirements or other government actions;
- decisions by marketers to reduce their advertising as a result of adverse media reports or other negative publicity involving us, our user data practices, our advertising metrics or tools, content on our products, our efforts to implement or enforce policies relating to content on our products (including as a result of decisions or recommendations from the independent Oversight Board), developers with mobile and web applications that are integrated with our products, or other companies in our industry;
- reductions of advertising by marketers due to objectionable content made available on our products by third parties, questions about our user data practices, concerns about brand safety or potential legal liability, or uncertainty regarding their own legal and compliance obligations (for example, a number of marketers announced that they paused advertising with us in July 2020 due to concerns about content on our products);
- the effectiveness of our ad targeting or degree to which users opt out of the use of data for ads, including as a result of product changes and controls that we have implemented or may implement in the future in connection with the GDPR, ePrivacy Directive, California Consumer Privacy Act (CCPA), other laws, regulations, or regulatory actions, or otherwise, that impact our ability to use data for advertising purposes;
- the degree to which users cease or reduce the number of times they engage with our ads;
- changes in the way advertising on mobile devices or on personal computers is measured or priced;
- the success of technologies designed to block the display of ads or ad measurement tools;
- changes in the composition of our marketer base or our inability to maintain or grow our marketer base; and
- the impact of macroeconomic conditions, whether in the advertising industry in general, or among specific types of marketers or within particular geographies.

From time to time, certain of these factors have adversely affected our advertising revenue to varying degrees. The occurrence of any of these or other factors in the future could result in a reduction in demand for our ads, which may reduce the prices we receive for our ads, or cause marketers to stop advertising with us altogether, either of which would negatively affect our revenue and financial results. For example, macroeconomic conditions have affected, and may in the future affect, marketers' ability or willingness to spend with us, as we have seen with the regional and worldwide economic disruption related to the COVID-19 pandemic and associated declines in advertising activity on our products. The effects of the pandemic previously resulted in reduced demand for our ads, a related decline in pricing of our ads, and additional demands on our technical infrastructure as a result of increased usage of our services, and any similar occurrences in the future may impair our ability to maintain or increase the quantity or quality of ads shown to users and adversely affect our revenue and financial results.

***Our advertising revenue is dependent on targeting and measurement tools that incorporate data signals from user activity on websites and services that we do not control, and changes to the regulatory environment, third-party mobile operating systems and browsers, and our own products have impacted, and we expect will continue to impact, the availability of such signals, which will adversely affect our advertising revenue.***

We rely on data signals from user activity on websites and services that we do not control in order to deliver relevant and effective ads to our users. Our advertising revenue is dependent on targeting and measurement tools that incorporate these signals, and any changes in our ability to use such signals will adversely affect our business. For example, legislative and regulatory developments, such as the GDPR, ePrivacy Directive, and CCPA, have impacted, and we expect will continue to impact, our ability to use such signals in our ad products. In particular, we have seen an increasing number of users opt out of certain types of ad targeting in Europe following adoption of the GDPR, and we have introduced product changes that limit data signal use for certain users in California following adoption of the CCPA. Regulatory guidance or decisions or new legislation may require us to make additional changes to our products in the future that further reduce our ability to use these signals. In addition, mobile operating system and browser providers, such as Apple and Google, have announced product changes as well as future plans to limit the ability of application developers to collect and use these signals to target and measure advertising. For example, in June 2020, Apple announced that it plans to make certain changes to its products and data use policies in connection with the release of its iOS 14 operating system that will reduce our and other iOS developers' ability to target and measure advertising, which we expect will in turn reduce the budgets marketers are willing to commit to us and other advertising platforms. In addition, we have implemented, and may continue to implement, product changes that give users the ability to limit our use of such data signals to improve ads and other experiences on our products and services, including our Off-Facebook Activity tool and our worldwide offering of certain product changes we implemented in connection with the GDPR. These developments have limited our ability to target and measure the effectiveness of ads on our platform, and negatively impacted our advertising revenue, and if we are unable to mitigate these developments as they take further effect in the future, our targeting and measurement capabilities will be materially and adversely affected, which would in turn significantly impact our future advertising revenue growth.

***Our user growth, engagement, and monetization on mobile devices depend upon effective operation with mobile operating systems, networks, technologies, products, and standards that we do not control.***

The substantial majority of our revenue is generated from advertising on mobile devices. There is no guarantee that popular mobile devices will continue to feature Facebook or our other products, or that mobile device users will continue to use our products rather than competing products. We are dependent on the interoperability of Facebook and our other products with popular mobile operating systems, networks, technologies, products, and standards that we do not control, such as the Android and iOS operating systems and mobile browsers. Any changes, bugs, or technical issues in such systems, or changes in our relationships with mobile operating system partners, handset manufacturers, browser developers, or mobile carriers, or in their terms of service or policies that degrade our products' functionality, reduce or eliminate our ability to update or distribute our products, give preferential treatment to competitive products, limit our ability to deliver, target, or measure the effectiveness of ads, or charge fees related to the distribution of our products or our delivery of ads could adversely affect the usage of Facebook or our other products and monetization on mobile devices. For example, Apple previously released an update to its Safari browser that limits the use of third-party cookies, which reduces our ability to provide the most relevant ads to our users and impacts monetization, and more recently announced changes to iOS 14 that will limit our ability to target and measure ads effectively. We expect that any similar changes to its, Google's, or other browser or mobile platforms will further limit our ability to target and measure the effectiveness of ads and impact monetization. Additionally, in order to deliver high quality mobile products, it is important that our products work well with a range of mobile technologies, products, systems, networks, and standards that we do not control, and that we have good relationships with handset manufacturers, mobile carriers, and browser developers. We may not be successful in maintaining or developing relationships with key participants in the mobile ecosystem or in developing products that operate effectively with these technologies, products, systems, networks, or standards. In the event that it is more difficult for our users to access and use Facebook or our other products on their mobile devices, or if our users choose not to access or use Facebook or our other products on their mobile devices or use mobile products that do not offer access to Facebook or our other products, our user growth and user engagement could be harmed. From time to time, we may also take actions regarding the distribution of our products or the operation of our business based on what we believe to be in our long-term best interests. Such actions may adversely affect our users and our relationships with the operators of mobile operating systems, handset manufacturers, mobile carriers, browser developers, other business partners, or advertisers, and there is no assurance that these actions will result in the anticipated long-term benefits. In the event that our users are adversely affected by these actions or if our relationships with such third parties deteriorate, our user growth, engagement, and monetization could be adversely affected.

and our business could be harmed. We have in the past experienced challenges in operating with mobile operating systems, networks, technologies, products, and standards that we do not control, and any such occurrences in the future may negatively impact our user growth, engagement, and monetization on mobile devices, which may in turn materially and adversely affect our business and financial results.

***Our new products and changes to existing products could fail to attract or retain users or generate revenue and profits.***

Our ability to retain, increase, and engage our user base and to increase our revenue depends heavily on our ability to continue to evolve our existing products and to create successful new products, both independently and in conjunction with developers or other third parties. We may introduce significant changes to our existing products or acquire or introduce new and unproven products, including using technologies with which we have little or no prior development or operating experience. For example, we do not have significant experience with consumer hardware products or virtual or augmented reality technology, which may adversely affect our ability to successfully develop and market these products and technologies. We continue to incur substantial costs, and we may not be successful in generating profits, in connection with these efforts. In addition, the introduction of new products, or changes to existing products, may result in new or enhanced governmental or regulatory scrutiny, litigation, or other complications that could adversely affect our business and financial results. We have also invested, and expect to continue to invest, significant resources in growing our WhatsApp and Messenger products to support increasing usage of such products. We have historically monetized messaging in only a limited fashion, and we may not be successful in our efforts to generate meaningful revenue or profits from messaging over the long term. In addition, we are moving forward with plans to implement end-to-end encryption across our messaging services, as well as facilitate cross-app communication between these platforms, which plans have drawn governmental and regulatory scrutiny in multiple jurisdictions. If our new or enhanced products fail to engage users, marketers, or developers, or if our business plans are unsuccessful, we may fail to attract or retain users or to generate sufficient revenue, operating margin, or other value to justify our investments, and our business may be adversely affected.

***We make product and investment decisions that may not prioritize short-term financial results and may not produce the long-term benefits that we expect.***

We frequently make product and investment decisions that may not prioritize short-term financial results if we believe that the decisions are consistent with our mission and benefit the aggregate user experience and will thereby improve our financial performance over the long term. For example, we have implemented, and we will continue to implement, changes to our user data practices. Some of these changes reduce our ability to effectively target ads, which has to some extent adversely affected, and will continue to adversely affect, our advertising business. For example, our Off-Facebook Activity tool enables users to place limits on our storage and use of information about their interactions with advertisers' apps and websites, which reduces our ability to deliver the most relevant and effective ads to our users. Similarly, from time to time we update our News Feed ranking algorithm to optimize the user experience, and these changes have had, and may in the future have, the effect of reducing time spent and some measures of user engagement with Facebook, which could adversely affect our financial results. From time to time, we may also change the size, frequency, or relative prominence of ads in order to improve ad quality and overall user experience. In addition, we have made, and we expect to continue to make, other changes to our products which may adversely affect the distribution of content of publishers, marketers, and developers, and could reduce their incentive to invest in their efforts on Facebook or our other products. We also may introduce new features or other changes to existing products, or introduce new stand-alone products, that attract users away from properties, formats, or use cases where we have more proven means of monetization. For example, we previously introduced the Stories format, which we do not currently monetize at the same rate as News Feed. In addition, as we focus on growing users and engagement across our family of products, from time to time these efforts have reduced, and may in the future reduce, engagement with one or more products and services in favor of other products or services that we monetize less successfully or that are not growing as quickly. These decisions may adversely affect our business and results of operations and may not produce the long-term benefits that we expect.

***If we are not able to maintain and enhance our brands, our ability to expand our base of users, marketers, and developers may be impaired, and our business and financial results may be harmed.***

We believe that our brands have significantly contributed to the success of our business. We also believe that maintaining and enhancing our brands is critical to expanding our base of users, marketers, and developers. Many of our new users are referred by existing users. Maintaining and enhancing our brands will depend largely on our ability to continue to provide useful, reliable, trustworthy, and innovative products, which we may not do successfully. We may introduce new

products or terms of service or policies that users do not like, which may negatively affect our brands. Additionally, the actions of our developers or advertisers may affect our brands if users do not have a positive experience using third-party mobile and web applications integrated with our products or interacting with parties that advertise through our products. We will also continue to experience media, legislative, or regulatory scrutiny of our actions or decisions regarding user privacy, data use, encryption, content, advertising, competition, and other issues, including actions or decisions in connection with elections or the COVID-19 pandemic, which has in the past adversely affected, and may in the future adversely affect, our reputation and brands. For example, in March 2018, we announced developments regarding the misuse of certain data by a developer that shared such data with third parties in violation of our terms and policies. We also may fail to respond expeditiously or appropriately to the sharing of objectionable content on our services or objectionable practices by advertisers or developers, or to otherwise address user concerns, which has occurred in the past and which could erode confidence in our brands. Our brands may also be negatively affected by the actions of users that are deemed to be hostile or inappropriate to other users, by the actions of users acting under false or inauthentic identities, by the use of our products or services to disseminate information that is deemed to be misleading (or intended to manipulate opinions), by perceived or actual efforts by governments to obtain access to user information for security-related purposes or to censor certain content on our platform, by the use of our products or services for illicit or objectionable ends, including, for example, any such actions around the pandemic or elections in the United States and around the world, by decisions or recommendations regarding content on our platform from the independent Oversight Board, or by our decisions to remove content or suspend participation on our platform by persons who violate our community standards or terms of service. Maintaining and enhancing our brands will require us to make substantial investments and these investments may not be successful. Certain of our past actions, such as the foregoing matter regarding developer misuse of data and concerns around our handling of political speech and advertising, hate speech, and other content, have eroded confidence in our brands, and if we fail to successfully promote and maintain our brands or if we incur excessive expenses in this effort, our business and financial results may be adversely affected.

***We may not be able to continue to successfully maintain or grow usage of and engagement with mobile and web applications that integrate with Facebook and our other products.***

We have made and are continuing to make investments to enable developers to build, grow, and monetize mobile and web applications that integrate with Facebook and our other products. Such existing and prospective developers may not be successful in building, growing, or monetizing mobile and/or web applications that create and maintain user engagement. Additionally, developers may choose to build on other platforms, including mobile platforms controlled by third parties, rather than building products that integrate with Facebook and our other products. We are continuously seeking to balance the distribution objectives of our developers with our desire to provide an optimal user experience, and we may not be successful in achieving a balance that continues to attract and retain such developers. For example, from time to time, we have taken actions to reduce the volume of communications from these developers to users on Facebook and our other products with the objective of enhancing the user experience, and such actions have reduced distribution from, user engagement with, and our monetization opportunities from, mobile and web applications integrated with our products. In addition, as part of our efforts related to privacy, safety, and security, we conduct investigations and audits of platform applications from time to time, and we also have announced several product changes that restrict developer access to certain user data. In some instances, these actions, as well as other actions to enforce our policies applicable to developers, have adversely affected, or will adversely affect, our relationships with developers. If we are not successful in our efforts to maintain or grow the number of developers that choose to build products that integrate with Facebook and our other products or if we are unable to continue to build and maintain good relations with such developers, our user growth and user engagement and our financial results may be adversely affected.

#### **Risks Related to Our Business Operations and Financial Results**

***The COVID-19 pandemic has had, and may in the future have, a significant adverse impact on our advertising revenue and also exposes our business to other risks.***

The COVID-19 pandemic has resulted in authorities implementing numerous preventative measures to contain or mitigate the outbreak of the virus, such as travel bans and restrictions, limitations on business activity, quarantines, and shelter-in-place orders. These measures have caused, and are continuing to cause, business slowdowns or shutdowns in affected areas, both regionally and worldwide, which have significantly impacted our business and results of operations. For example, in the second quarter of 2020, our advertising revenue grew 10% year-over-year, which was the slowest growth rate for any fiscal quarter since our initial public offering. While our advertising revenue growth rate improved in subsequent

## [Table of Contents](#)

quarters, there can be no assurance that it will not decrease again as a result of the effects of the pandemic. In addition, we believe that the pandemic has contributed to an acceleration in the shift of commerce from offline to online, as well as increasing consumer demand for purchasing products as opposed to services, which in turn have increased demand for our advertising services; however, it is possible that this increased demand may not continue in future periods and may even recede as the effects of the pandemic subside, which could adversely affect our advertising revenue growth. The demand for and pricing of our advertising services may be materially and adversely impacted by the pandemic for the foreseeable future, and we are unable to predict the duration or degree of such impact with any certainty. In addition to the impact on our advertising business, the pandemic exposes our business, operations, and workforce to a variety of other risks, including:

- volatility in the size of our user base and user engagement, particularly for our messaging products, whether as a result of shelter-in-place measures or other factors;
- decreased user engagement as a result of users' inability to purchase data packs or devices to access our products and services;
- interruptions in the accessibility or performance of our products and services due to capacity constraints from increased usage, or product changes we implement to maintain accessibility of our services, such as reducing the quality of video to reduce bandwidth usage;
- delays in product development or releases, or reductions in manufacturing production and sales of consumer hardware, as a result of inventory shortages, supply chain or labor shortages, or diversion of our efforts and resources to projects related to COVID-19;
- increased misuse of our products and services or user data by third parties, including improper advertising practices or other activity inconsistent with our terms, contracts, or policies, misinformation or other illicit or objectionable material on our platforms, election interference, or other undesirable activity;
- adverse impacts to our efforts to combat misuse of our products and services and user data as a result of limitations on our safety, security, and content review efforts while our workforce is working remotely, such as the necessity to rely more heavily on artificial intelligence to perform tasks that our workforce is unable to perform;
- our inability to recognize revenue, collect payment, or generate future revenue from marketers, including from those that have been or may be forced to close their businesses or are otherwise impacted by the economic downturn;
- increased expenses resulting from our initiatives or donations related to the pandemic;
- significant volatility and disruption of global financial markets, which could cause fluctuations in currency exchange rates or negatively impact our ability to access capital in the future;
- negative impact on our workforce productivity, product development, and research and development due to difficulties resulting from our personnel working remotely;
- illnesses to key employees, or a significant portion of our workforce, which may result in inefficiencies, delays, and disruptions in our business; and
- increased volatility and uncertainty in the financial projections we use as the basis for estimates used in our financial statements.

Any of these developments may adversely affect our business, harm our reputation, or result in legal or regulatory actions against us. The persistence of COVID-19, and the preventative measures implemented to help limit the spread of the illness, have impacted, and will continue to impact, our ability to operate our business and may materially and adversely impact our business, financial condition, and results of operations.

***Our business is highly competitive. Competition presents an ongoing threat to the success of our business.***

We compete with companies providing connection and communication products and services to users online, as well as companies that sell advertising to businesses looking to reach consumers and/or develop tools and systems for managing

## [Table of Contents](#)

and optimizing advertising campaigns. We face significant competition in every aspect of our business, including, but not limited to, companies that facilitate the ability of users to share, communicate, and discover content and information online or enable marketers to reach their existing or prospective audiences, including, for example, Google, Apple, YouTube, Tencent, Snap, Twitter, ByteDance, Microsoft, and Amazon. We compete to attract, engage, and retain people who use our products, to attract and retain businesses that use our free or paid business and advertising services, and to attract and retain developers who build compelling mobile and web applications that integrate with our products. We also compete with companies that develop and deliver consumer hardware and virtual reality products and services. As we introduce or acquire new products, as our existing products evolve, or as other companies introduce new products and services, we may become subject to additional competition.

Some of our current and potential competitors may have greater resources or stronger competitive positions in certain product segments, geographic regions, or user demographics than we do. For example, some of our competitors may be domiciled in different countries and subject to political, legal, and regulatory regimes that enable them to compete more effectively than us. These factors may allow our competitors to respond more effectively than us to new or emerging technologies and changes in market conditions. We believe that some users, particularly younger users, are aware of and actively engaging with other products and services similar to, or as a substitute for, our products and services, and we believe that some users have reduced their use of and engagement with our products and services in favor of these other products and services. In the event that users increasingly engage with other products and services, we may experience a decline in use and engagement in key user demographics or more broadly, in which case our business would likely be harmed.

Our competitors may develop products, features, or services that are similar to ours or that achieve greater acceptance, may undertake more far-reaching and successful product development efforts or marketing campaigns, or may adopt more aggressive pricing policies. Some competitors may gain a competitive advantage against us in areas where we operate, including: by making acquisitions; by limiting our ability to deliver, target, or measure the effectiveness of ads; by imposing fees or other charges related to our delivery of ads; by making access to our products more difficult or impossible; by making it more difficult to communicate with our users; or by integrating competing platforms, applications, or features into products they control such as mobile device operating systems, search engines, browsers, or e-commerce platforms. For example, each of Apple and Google have integrated competitive products with iOS and Android, respectively. In addition, Apple has announced changes to iOS 14 that will limit our ability, and the ability of others in the digital advertising industry, to target and measure ads effectively. As a result, our competitors may, and in some cases will, acquire and engage users or generate advertising or other revenue at the expense of our own efforts, which would negatively affect our business and financial results. In addition, from time to time, we may take actions in response to competitive threats, but we cannot assure you that these actions will be successful or that they will not negatively affect our business and financial results.

We believe that our ability to compete effectively depends upon many factors both within and beyond our control, including:

- the popularity, usefulness, ease of use, performance, and reliability of our products compared to our competitors' products;
- the size and composition of our user base;
- the engagement of users with our products and competing products;
- our ability to attract and retain businesses who use our free or paid business and advertising services;
- the timing and market acceptance of products, including developments and enhancements to our or our competitors' products;
- our safety and security efforts and our ability to protect user data and to provide users with control over their data;
- our ability to distribute our products to new and existing users;
- our ability to monetize our products;

## [Table of Contents](#)

- the frequency, size, format, quality, and relative prominence of the ads displayed by us or our competitors;
- customer service and support efforts;
- marketing and selling efforts, including our ability to measure the effectiveness of our ads and to provide marketers with a compelling return on their investments;
- our ability to establish and maintain developers' interest in building mobile and web applications that integrate with Facebook and our other products;
- our ability to establish and maintain publisher interest in integrating their content with Facebook and our other products;
- changes mandated by legislation, regulatory authorities, or litigation, some of which may have a disproportionate effect on us;
- acquisitions or consolidation within our industry, which may result in more formidable competitors;
- our ability to attract, retain, and motivate talented employees, particularly software engineers, designers, and product managers;
- our ability to cost-effectively manage and grow our operations; and
- our reputation and brand strength relative to those of our competitors.

If we are not able to compete effectively, our user base and level of user engagement may decrease, we may become less attractive to developers and marketers, and our revenue and results of operations may be materially and adversely affected.

### ***Unfavorable media coverage negatively affects our business from time to time.***

We receive a high degree of media coverage around the world. Unfavorable publicity regarding, for example, our privacy practices, terms of service, advertising policies, product changes, product quality, litigation or regulatory activity, government surveillance, the actions of our advertisers, the actions of our developers whose products are integrated with our products, the use of our products or services for illicit or objectionable ends, the substance or enforcement of our community standards, the actions of our users, the quality and integrity of content shared on our platform, or the actions of other companies that provide similar services to ours, has in the past, and could in the future, adversely affect our reputation. For example, we have been the subject of significant media coverage involving concerns around our handling of political speech and advertising, hate speech, and other content, and we continue to receive negative publicity related to these topics. In addition, we have been, and may in the future be, subject to negative publicity in connection with our handling of misinformation and other illicit or objectionable use of our products or services, including in connection with the COVID-19 pandemic and elections in the United States and around the world. Any such negative publicity could have an adverse effect on the size, engagement, and loyalty of our user base and marketer demand for advertising on our products, which could result in decreased revenue and adversely affect our business and financial results, and we have experienced such adverse effects to varying degrees from time to time.

### ***Our financial results will fluctuate from quarter to quarter and are difficult to predict.***

Our quarterly financial results have fluctuated in the past and will fluctuate in the future. Additionally, we have a limited operating history with the current scale of our business, which makes it difficult to forecast our future results. As a result, you should not rely upon our past quarterly financial results as indicators of future performance. You should take into account the risks and uncertainties frequently encountered by companies in rapidly evolving markets. Our financial results in any given quarter can be influenced by numerous factors, many of which we are unable to predict or are outside of our control, including:

- our ability to maintain and grow our user base and user engagement;

## [Table of Contents](#)

- our ability to attract and retain marketers in a particular period;
- our ability to recognize revenue or collect payments from marketers in a particular period, including as a result of the effects of the COVID-19 pandemic;
- fluctuations in spending by our marketers due to seasonality, such as historically strong spending in the fourth quarter of each year, episodic regional or global events, including the COVID-19 pandemic, or other factors;
- the frequency, prominence, size, format, and quality of ads shown to users;
- the success of technologies designed to block the display of ads;
- changes to third-party policies that limit our ability to deliver, target, or measure the effectiveness of advertising, including changes by mobile operating system and browser providers such as Apple and Google;
- the pricing of our ads and other products;
- the diversification and growth of revenue sources beyond advertising on Facebook and Instagram;
- our ability to generate revenue from Payments, or the sale of our consumer hardware products or other products we may introduce in the future;
- changes to existing products or services or the development and introduction of new products or services by us or our competitors;
- user behavior or product changes that may reduce traffic to features or products that we successfully monetize;
- increases in marketing, sales, and other operating expenses that we will incur to grow and expand our operations and to remain competitive, including costs related to our data centers and technical infrastructure;
- costs related to our privacy, safety, security, and content review efforts, including as a result of implementing changes to our practices, whether voluntarily, in connection with laws, regulations, regulatory actions, or decisions or recommendations from the independent Oversight Board, or otherwise;
- costs and expenses related to the development and delivery of our consumer hardware products;
- our ability to maintain gross margins and operating margins;
- costs related to acquisitions, including costs associated with amortization and additional investments to develop the acquired technologies;
- charges associated with impairment of any assets on our balance sheet;
- our ability to obtain equipment, components, and labor for our data centers and other technical infrastructure in a timely and cost-effective manner;
- system failures or outages or government blocking, which could prevent us from serving ads for any period of time;
- breaches of security or privacy, and the costs associated with any such breaches and remediation;
- changes in the manner in which we distribute our products or inaccessibility of our products due to third-party actions;
- fees paid to third parties for content or the distribution of our products;

## [Table of Contents](#)

- refunds or other concessions provided to advertisers;
- share-based compensation expense, including acquisition-related expense;
- adverse litigation judgments, settlements, or other litigation-related costs;
- changes in the legislative or regulatory environment, including with respect to privacy and data protection, or actions by governments or regulators, including fines, orders, or consent decrees;
- the overall tax rate for our business, which is affected by the mix of income we earn in the U.S. and in jurisdictions with different tax rates, the effects of share-based compensation, the effects of integrating intellectual property from acquisitions, the effects of changes in our business or structure, and the effects of discrete items such as legal and tax settlements and tax elections;
- the impact of changes in tax laws or judicial or regulatory interpretations of tax laws, which are recorded in the period such laws are enacted or interpretations are issued, and may significantly affect the effective tax rate of that period;
- tax obligations that may arise from resolutions of tax examinations, including the examination we are currently under by the Internal Revenue Service (IRS), that materially differ from the amounts we have anticipated;
- fluctuations in currency exchange rates and changes in the proportion of our revenue and expenses denominated in foreign currencies;
- trading activity in our share repurchase program;
- fluctuations in the market values of our investments in marketable securities, in the valuation of our equity investments, and in interest rates;
- changes in U.S. generally accepted accounting principles; and
- changes in regional or global business or macroeconomic conditions, including as a result of the COVID-19 pandemic, which may impact the other factors described above.

***We expect our rates of growth to be volatile in the near term as a result of the COVID-19 pandemic and to decline over time in the future.***

We expect our user and revenue growth rates to be volatile in the near term as a result of the COVID-19 pandemic, although we are unable to predict the duration or degree of such volatility with any certainty. In the long term, we expect that our user growth rate will generally decline over time as the size of our active user base increases, and the size of our active user base may fluctuate or decline in one or more markets, particularly as we achieve greater market penetration. We also expect our revenue growth rate will continue to decline over time as our revenue increases to higher levels. As our growth rates experience volatility or decline, investors' perceptions of our business may be adversely affected and the trading price of our Class A common stock could decline.

***Our costs are continuing to grow, and some of our investments, particularly our investments in virtual and augmented reality, have the effect of reducing our operating margin and profitability. If our investments are not successful longer-term, our business and financial performance will be harmed.***

Operating our business is costly, and we expect our expenses to continue to increase in the future as we broaden our user base, as users increase the amount and types of content they consume and the data they share with us, for example with respect to video, as we develop and implement new products, as we market new and existing products and promote our brands, as we continue to expand our technical infrastructure, as we continue to invest in new and unproven technologies, and as we continue to hire additional employees and contractors to support our expanding operations, including our efforts to focus on privacy, safety, security, and content review. In addition, from time to time we are subject to settlements, judgments,

ines, or other monetary penalties in connection with legal and regulatory developments that may be material to our business. We are also continuing to increase our investments in new platforms and technologies. Some of these investments, particularly our significant investments in virtual and augmented reality, have generated only limited revenue and reduced our operating margin and profitability, and we expect the adverse financial impact of such investments to continue for the foreseeable future. If our investments are not successful longer-term, our business and financial performance will be harmed.

***We plan to continue to make acquisitions and pursue other strategic transactions, which could harm our financial condition or results of operations and may adversely affect the price of our common stock.***

As part of our business strategy, we have made and intend to continue to make acquisitions to add specialized employees and complementary companies, products, or technologies, and from time to time may enter into other strategic transactions such as investments and joint ventures. We may not be able to find suitable acquisition candidates, and we may not be able to complete acquisitions or other strategic transactions on favorable terms, if at all, including as a result of regulatory challenges. In some cases, the costs of such acquisitions or other strategic transactions may be substantial, and there is no assurance that we will receive a favorable return on investment for our acquisitions or other strategic transactions.

We may pay substantial amounts of cash or incur debt to pay for acquisitions or other strategic transactions, which has occurred in the past and could adversely affect our liquidity. The incurrence of indebtedness would also result in increased fixed obligations and increased interest expense, and could also include covenants or other restrictions that would impede our ability to manage our operations. We may also issue equity securities to pay for acquisitions and we regularly grant RSUs to retain the employees of acquired companies, which could increase our expenses, adversely affect our financial results, and result in dilution to our stockholders. In addition, any acquisitions or other strategic transactions we announce could be viewed negatively by users, marketers, developers, or investors, which may adversely affect our business or the price of our Class A common stock.

We may also discover liabilities, deficiencies, or other claims associated with the companies or assets we acquire that were not identified in advance, which may result in significant unanticipated costs. The effectiveness of our due diligence review and our ability to evaluate the results of such due diligence are dependent upon the accuracy and completeness of statements and disclosures made or actions taken by the companies we acquire or their representatives, as well as the limited amount of time in which acquisitions are executed. In addition, we may fail to accurately forecast the financial impact of an acquisition or other strategic transaction, including tax and accounting charges. Acquisitions or other strategic transactions may also result in our recording of significant additional expenses to our results of operations and recording of substantial finite-lived intangible assets on our balance sheet upon closing. Any of these factors may adversely affect our financial condition or results of operations.

***We may not be able to successfully integrate our acquisitions, and we incur significant costs to integrate and support the companies we acquire.***

The integration of acquisitions requires significant time and resources, and we may not manage these processes successfully. Our ability to successfully integrate complex acquisitions is unproven, particularly with respect to companies that have significant operations or that develop products where we do not have prior experience. We continue to make substantial investments of resources to support our acquisitions, which will result in significant ongoing operating expenses and may divert resources and management attention from other areas of our business. We cannot assure you that these investments will be successful. If we fail to successfully integrate the companies we acquire, we may not realize the benefits expected from the transaction and our business may be harmed.

***Our business is dependent on our ability to maintain and scale our technical infrastructure, and any significant disruption in our service, including as a result of the COVID-19 pandemic, could damage our reputation, result in a potential loss of users and engagement, and adversely affect our financial results.***

Our reputation and ability to attract, retain, and serve our users is dependent upon the reliable performance of our products and our underlying technical infrastructure. We have in the past experienced, and may in the future experience, interruptions in the availability or performance of our products from time to time. Our systems may not be adequately designed or may not operate with the reliability and redundancy necessary to avoid performance delays or outages that could be harmful to our business. If our products are unavailable when users attempt to access them, or if they do not load as quickly as expected, users may not use our products as often in the future, or at all, and our ability to serve ads may be

disrupted, any of which could adversely affect our business and financial performance. As the amount and types of information shared on Facebook and our other products continue to grow and evolve, as the usage patterns of our global community continue to evolve, and as our internal operational demands continue to grow, we will need an increasing amount of technical infrastructure, including network capacity and computing power, to continue to satisfy our needs. It is possible that we may fail to continue to effectively scale and grow our technical infrastructure to accommodate these increased demands, which may adversely affect our user engagement and advertising revenue growth. In addition, our business may be subject to interruptions, delays, or failures resulting from earthquakes, adverse weather conditions, other natural disasters, power loss, terrorism, geopolitical conflict, other physical security threats, cyber-attacks, or other catastrophic events. If such an event were to occur, users may be subject to service disruptions or outages and we may not be able to recover our technical infrastructure and user data in a timely manner to restart or provide our services, which may adversely affect our financial results.

For example, the increase in the use of our products as a result of the COVID-19 pandemic increased demands on our technical infrastructure. Additional product development efforts during this time have put additional pressure on our technical infrastructure. We may not be able to accommodate these demands, including as a result of our reduced data center operations and personnel working remotely during the pandemic.

A substantial portion of our network infrastructure is provided by third parties. Any disruption or failure in the services we receive from these providers could harm our ability to handle existing or increased traffic and could significantly harm our business. Any financial or other difficulties these providers face may adversely affect our business, and we exercise little control over these providers, which increases our vulnerability to problems with the services they provide. The effects of the COVID-19 pandemic have increased the risk of supply or labor shortages or other disruptions in logistics or the supply chain for our technical infrastructure. As a result, we may not be able to procure sufficient equipment or services from third parties to satisfy our needs, or we may be required to procure such services or equipment on unfavorable terms.

Any of these developments may result in interruptions in the availability or performance of our products, require unfavorable changes to existing products, delay the introduction of future products, or otherwise adversely affect our business and financial results.

***We could experience unforeseen difficulties in building and operating key portions of our technical infrastructure.***

We have designed and built our own data centers and key portions of our technical infrastructure through which we serve our products, and we plan to continue to significantly expand the size of our infrastructure primarily through data centers, subsea and terrestrial fiber optic cable systems, and other projects. The infrastructure expansion we are undertaking is complex and involves projects in multiple locations around the world, including in emerging markets that expose us to increased risks relating to anti-corruption compliance and political challenges, among others. We have in the past suspended, and may in the future suspend, certain of these projects as a result of the COVID-19 pandemic. Additional unanticipated delays or disruptions in the completion of these projects, including due to any shortage of labor necessary in building portions of such projects, or availability of components, challenges in obtaining required government or regulatory approvals, or other geopolitical challenges or actions by governments, whether as a result of the pandemic, trade disputes, or otherwise, may lead to increased project costs, operational inefficiencies, interruptions in the delivery or degradation of the quality or reliability of our products, or impairment of assets on our balance sheet. In addition, there may be issues related to this infrastructure that are not identified during the testing phases of design and implementation, which may only become evident after we have started to fully utilize the underlying equipment, that could further degrade the user experience or increase our costs. Further, much of our technical infrastructure is located outside the United States, and it is possible that action by a foreign government, or our response to such government action, could result in the impairment of a portion of our technical infrastructure, which may interrupt the delivery or degrade the quality or reliability of our products and lead to a negative user experience or increase our costs. Any of these events could adversely affect our business, reputation, or financial results.

***Real or perceived inaccuracies in our community and other metrics may harm our reputation and negatively affect our business.***

The numbers for our key metrics, which include our Facebook metrics (DAUs, MAUs, and average revenue per user (ARPU)) and Family metrics (DAP, MAP, and average revenue per person (ARPP)), are calculated using internal company data based on the activity of user accounts. While these numbers are based on what we believe to be reasonable estimates of our user base for the applicable period of measurement, there are inherent challenges in measuring usage of our products across large online and mobile populations around the world. The methodologies used to measure these metrics require

## [Table of Contents](#)

significant judgment and are also susceptible to algorithm or other technical errors. In addition, we are continually seeking to improve our estimates of our user base, and such estimates may change due to improvements or changes in our methodology. We regularly review our processes for calculating these metrics, and from time to time we discover inaccuracies in our metrics or make adjustments to improve their accuracy, which can result in adjustments to our historical metrics. Our ability to recalculate our historical metrics may be impacted by data limitations or other factors that require us to apply different methodologies for such adjustments. We generally do not intend to update previously disclosed Family metrics for any such inaccuracies or adjustments that are within the error margins disclosed below.

In addition, our Facebook metrics and Family metrics estimates will differ from estimates published by third parties due to differences in methodology.

We regularly evaluate our Facebook metrics to estimate the number of "duplicate" and "false" accounts among our MAUs. A duplicate account is one that a user maintains in addition to his or her principal account. We divide "false" accounts into two categories: (1) user-misclassified accounts, where users have created personal profiles for a business, organization, or non-human entity such as a pet (such entities are permitted on Facebook using a Page rather than a personal profile under our terms of service); and (2) violating accounts, which represent user profiles that we believe are intended to be used for purposes that violate our terms of service, such as bots and spam. The estimates of duplicate and false accounts are based on an internal review of a limited sample of accounts, and we apply significant judgment in making this determination. For example, to identify duplicate accounts we use data signals such as identical IP addresses and similar user names, and to identify false accounts we look for names that appear to be fake or other behavior that appears inauthentic to the reviewers. Any loss of access to data signals we use in this process, whether as a result of our own product decisions, actions by third-party browser or mobile platforms, regulatory or legislative requirements, limitations while our personnel work remotely during the COVID-19 pandemic, or other factors, also may impact the stability or accuracy of our estimates of duplicate and false accounts. Our estimates also may change as our methodologies evolve, including through the application of new data signals or technologies or product changes that may allow us to identify previously undetected duplicate or false accounts and may improve our ability to evaluate a broader population of our users. Duplicate and false accounts are very difficult to measure at our scale, and it is possible that the actual number of duplicate and false accounts may vary significantly from our estimates.

In the fourth quarter of 2020, we estimated that duplicate accounts may have represented approximately 11% of our worldwide MAUs. We believe the percentage of duplicate accounts is meaningfully higher in developing markets such as the Philippines and Vietnam, as compared to more developed markets. In the fourth quarter of 2020, we estimated that false accounts may have represented approximately 5% of our worldwide MAUs. Our estimation of false accounts can vary as a result of episodic spikes in the creation of such accounts, which we have seen originate more frequently in specific countries such as Indonesia and Vietnam. From time to time, we disable certain user accounts, make product changes, or take other actions to reduce the number of duplicate or false accounts among our users, which may also reduce our DAU and MAU estimates in a particular period. We intend to disclose our estimates of the number of duplicate and false accounts among our MAUs on an annual basis.

Many people in our community have user accounts on more than one of our products, and some people have multiple user accounts within an individual product. Accordingly, for our Family metrics, we do not seek to count the total number of user accounts across our products because we believe that would not reflect the actual size of our community. Rather, our Family metrics represent our estimates of the number of unique people using at least one of Facebook, Instagram, Messenger, and WhatsApp. We do not require people to use a common identifier or link their accounts to use multiple products in our Family, and therefore must seek to attribute multiple user accounts within and across products to individual people. To calculate these metrics, we rely upon complex techniques, algorithms and machine learning models that seek to count the individual people behind user accounts, including by matching multiple user accounts within an individual product and across multiple products when we believe they are attributable to a single person, and counting such group of accounts as one person. These techniques and models require significant judgment, are subject to data and other limitations discussed below, and inherently are subject to statistical variances and uncertainties. We estimate the potential error in our Family metrics primarily based on user survey data, which itself is subject to error as well. While we expect the error margin for our Family metrics to vary from period to period, we estimate that such margin generally will be approximately 4% of our worldwide MAP. At our scale, it is very difficult to attribute multiple user accounts within and across products to individual people, and it is possible that the actual numbers of unique people using our products may vary significantly from our estimates, potentially beyond our estimated error margins. As a result, it is also possible that our Family metrics may indicate changes or trends in user numbers that do not match actual changes or trends.

Page Intentionally Left Blank

[Table of Contents](#)

**Item 6. Selected Financial Data**

You should read the following selected consolidated financial data in conjunction with Part II, Item 7, "Management's Discussion and Analysis of Financial Condition and Results of Operations," and our consolidated financial statements and the related notes included in Part II, Item 8, "Financial Statements and Supplementary Data" of this Annual Report on Form 10-K.

The consolidated statements of income data for each of the years ended December 31, 2020, 2019, and 2018 and the consolidated balance sheets data as of December 31, 2020 and 2019 are derived from our audited consolidated financial statements included in Part II, Item 8, "Financial Statements and Supplementary Data" of this Annual Report on Form 10-K. The consolidated statements of income data for the years ended December 31, 2017 and 2016 and the consolidated balance sheets data as of December 31, 2018, 2017, and 2016 are derived from our audited consolidated financial statements, except as otherwise noted, that are not included in this Annual Report on Form 10-K. Our historical results are not necessarily indicative of our results in any future period.

	Year Ended December 31,				
	2020	2019	2018	2017	2016
	(in millions, except per share data)				
<b>Consolidated Statements of Income Data:</b>					
Revenue	\$ 85,965	\$ 70,697	\$ 55,838	\$ 40,653	\$ 27,638
Total costs and expenses <sup>(1)</sup>	\$ 53,294	\$ 46,711	\$ 30,925	\$ 20,450	\$ 15,211
Income from operations	\$ 32,671	\$ 23,986	\$ 24,913	\$ 20,203	\$ 12,427
Income before provision for income taxes	\$ 33,180	\$ 24,812	\$ 25,361	\$ 20,594	\$ 12,518
Net income	\$ 29,146	\$ 18,485	\$ 22,112	\$ 15,934	\$ 10,217
Net income attributable to Class A and Class B common stockholders	\$ 29,146	\$ 18,485	\$ 22,111	\$ 15,920	\$ 10,188
Earnings per share attributable to Class A and Class B common stockholders:					
Basic	\$ 10.22	\$ 6.48	\$ 7.65	\$ 5.49	\$ 3.56
Diluted	\$ 10.09	\$ 6.43	\$ 7.57	\$ 5.39	\$ 3.49

(1) Total costs and expenses include \$6.54 billion, \$4.84 billion, \$4.15 billion, \$3.72 billion, and \$3.22 billion of share-based compensation for the years ended December 31, 2020, 2019, 2018, 2017, and 2016, respectively.

	As of December 31,				
	2020	2019	2018	2017	2016
	(in millions)				
<b>Consolidated Balance Sheets Data:</b>					
Cash, cash equivalents, and marketable securities	\$ 61,954	\$ 54,855	\$ 41,114	\$ 41,711	\$ 29,449
Working capital	\$ 60,689	\$ 51,172	\$ 43,463	\$ 44,803	\$ 31,526
Property and equipment, net	\$ 45,633	\$ 35,323	\$ 24,683	\$ 13,721	\$ 8,591
Total assets	\$ 159,316	\$ 133,376	\$ 97,334	\$ 84,524	\$ 64,961
Operating lease liabilities <sup>(1)</sup>	\$ 10,654	\$ 10,324	\$ —	\$ —	\$ —
Total liabilities	\$ 31,026	\$ 32,322	\$ 13,207	\$ 10,177	\$ 5,767
Additional paid-in capital	\$ 50,018	\$ 45,851	\$ 42,906	\$ 40,584	\$ 38,227
Total stockholders' equity	\$ 128,290	\$ 101,054	\$ 84,127	\$ 74,347	\$ 59,194

(1) On January 1, 2019, we adopted Accounting Standards Update No. 2016-02, Leases (Topic 842). Prior period amounts have not been adjusted under the modified retrospective method.

## Free Cash Flow

In addition to other financial measures presented in accordance with U.S. generally accepted accounting principles (GAAP), we monitor free cash flow (FCF) as a non-GAAP measure to manage our business, make planning decisions, evaluate our performance, and allocate resources. We define FCF as net cash provided by operating activities reduced by net purchases of property and equipment and principal payments on finance leases.

We believe that FCF is one of the key financial indicators of our business performance over the long term and provides useful information regarding how cash provided by operating activities compares to the property and equipment investments required to maintain and grow our business.

We have chosen our definition for FCF because we believe that this methodology can provide useful supplemental information to help investors better understand underlying trends in our business. We use FCF in discussions with our senior management and board of directors.

FCF has limitations as an analytical tool, and you should not consider it in isolation or as a substitute for analysis of other GAAP financial measures, such as net cash provided by operating activities. FCF is not intended to represent our residual cash flow available for discretionary expenses. Some of the limitations of FCF are:

- FCF does not reflect our future contractual commitments; and
- other companies in our industry present similarly titled measures differently than we do, limiting their usefulness as comparative measures.

Management compensates for the inherent limitations associated with using the FCF measure through disclosure of such limitations, presentation of our financial statements in accordance with GAAP, and reconciliation of FCF to the most directly comparable GAAP measure, net cash provided by operating activities, as presented below.

The following is a reconciliation of FCF to the most comparable GAAP measure, net cash provided by operating activities:

	Year Ended December 31,				
	2020	2019	2018	2017	2016
	(in millions)				
Net cash provided by operating activities	\$ 38,747	\$ 36,314	\$ 29,274	\$ 24,216	\$ 16,108
Less: Purchases of property and equipment	(15,115)	(15,102)	(13,915)	(6,733)	(4,491)
Less: Principal payments on finance leases	(604)	(552)	—	—	—
Free cash flow	<u>\$ 23,028</u>	<u>\$ 20,660</u>	<u>\$ 15,359</u>	<u>\$ 17,483</u>	<u>\$ 11,617</u>

## Item 7. Management's Discussion and Analysis of Financial Condition and Results of Operations

*You should read the following discussion of our financial condition and results of operations in conjunction with our consolidated financial statements and the related notes included in Part II, Item 8, "Financial Statements and Supplementary Data" of this Annual Report on Form 10-K. In addition to our historical consolidated financial information, the following discussion contains forward-looking statements that reflect our plans, estimates, and beliefs. Our actual results could differ materially from those discussed in the forward-looking statements. Factors that could cause or contribute to these differences include those discussed below and elsewhere in this Annual Report on Form 10-K, particularly in Part I, Item 1A, "Risk Factors." For a discussion of limitations in the measurement of certain of our community metrics, see the section entitled "Limitations of Key Metrics and Other Data" in this Annual Report on Form 10-K.*

*Certain revenue information in the section entitled "—Revenue—Foreign Exchange Impact on Revenue" is presented on a constant currency basis. This information is a non-GAAP financial measure. To calculate revenue on a constant currency basis, we translated revenue for the full year 2020 using 2019 monthly exchange rates for our settlement or billing currencies other than the U.S. dollar. This non-GAAP financial measure is not intended to be considered in isolation or as a substitute for, or superior to, financial information prepared and presented in accordance with GAAP. This measure may be different from non-GAAP financial measures used by other companies, limiting its usefulness for comparison purposes. Moreover, presentation of revenue on a constant currency basis is provided for year-over-year comparison purposes, and investors should be cautioned that the effect of changing foreign currency exchange rates has an actual effect on our operating results. We believe this non-GAAP financial measure provides investors with useful supplemental information about the financial performance of our business, enables comparison of financial results between periods where certain items may vary independent of business performance, and allows for greater transparency with respect to key metrics used by management in operating our business.*

### Executive Overview of Full Year 2020 Results

Our key community metrics and financial results for 2020 are as follows:

#### **Community growth:**

- Facebook daily active users (DAUs) were 1.84 billion on average for December 2020, an increase of 11% year-over-year.
- Facebook monthly active users (MAUs) were 2.80 billion as of December 31, 2020, an increase of 12% year-over-year.
- Family daily active people (DAP) was 2.60 billion on average for December 2020, an increase of 15% year-over-year.
- Family monthly active people (MAP) was 3.30 billion as of December 31, 2020, an increase of 14% year-over-year.

#### **Financial results:**

- Revenue was \$85.97 billion, up 22% year-over-year, and advertising revenue was \$84.17 billion, up 21% year-over-year.
- Total costs and expenses were \$53.29 billion.
- Income from operations was \$32.67 billion and operating margin was 38%.
- Net income was \$29.15 billion with diluted earnings per share of \$10.09.
- Capital expenditures, including principal payments on finance leases, were \$15.72 billion.
- Effective tax rate was 12.2%.
- Cash and cash equivalents and marketable securities were \$61.95 billion as of December 31, 2020.
- Headcount was 58,604 as of December 31, 2020, an increase of 30% year-over-year.

Our mission is to give people the power to build community and bring the world closer together.

In response to the COVID-19 pandemic, we have focused on helping people stay connected, assisting the public health response, and working on the economic recovery. We have also continued to invest based on the following company priorities: (i) continue making progress on the major social issues facing the internet and our company, including privacy, safety, and security; (ii) build new experiences that meaningfully improve people's lives today and set the stage for even bigger improvements in the future; (iii) keep building our business by supporting the millions of businesses that rely on our

[Table of Contents](#)

services to grow and create jobs; and (iv) communicate more transparently about what we're doing and the role our services play in the world.

In 2020, we also continued to focus on our main revenue growth priorities: (i) helping marketers use our products to connect with consumers where they are and (ii) making our ads more relevant and effective.

Our business has been impacted by the COVID-19 pandemic, which has resulted in authorities implementing numerous preventative measures to contain or mitigate the outbreak of the virus, such as travel bans and restrictions, limitations on business activity, quarantines, and shelter-in-place orders. These measures have caused, and are continuing to cause, business slowdowns or shutdowns in affected areas, both regionally and worldwide, which have significantly impacted our business and results of operations. Beginning in the first quarter of 2020, we experienced significant increases in the size and engagement of our active user base across a number of regions as a result of the COVID-19 pandemic. More recently, we have seen user growth and engagement returning to pre-pandemic trends, particularly in the United States & Canada region. We are unable to predict the impact of the pandemic on user growth and engagement with any certainty, and we expect these trends to continue to be subject to volatility.

The COVID-19 pandemic has also previously caused a reduction in the demand for advertising, as well as a related decline in the pricing of our ads, particularly in the second quarter of 2020. More recently, we believe the pandemic has contributed to an acceleration in the shift of commerce from offline to online, as well as increasing consumer demand for purchasing products as opposed to services, and we experienced increasing demand for advertising as a result of these trends. However, it is possible that this increased demand may not continue in future periods and may even recede as the effects of the pandemic subside, which could adversely affect our advertising revenue growth. The impact of the pandemic on user growth and engagement, the demand for and pricing of our advertising services, as well as on our overall results of operations, remains highly uncertain for the foreseeable future. In addition, we expect that future advertising revenue growth will continue to be adversely affected by limitations on our ad targeting and measurement tools arising from changes to the regulatory environment and third-party mobile operating systems and browsers.

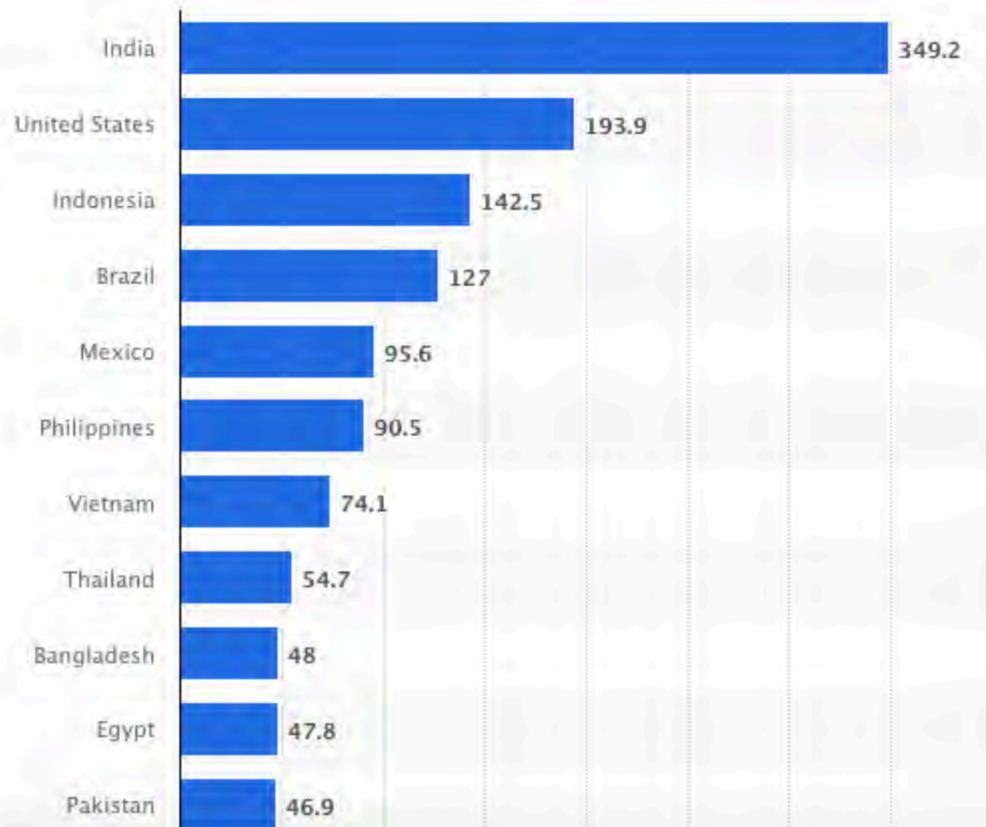
We intend to continue to invest in our business based on our company priorities, and we anticipate that additional investments in our data center capacity, servers, network infrastructure, and office facilities, as well as scaling our headcount to support our growth, will continue to drive expense growth in 2021. We expect 2021 capital expenditures to be in the range of \$21-23 billion and total expenses to be in the range of \$68-73 billion.

# Exhibit 10

Internet > Social Media & User-Generated Content

# Leading countries based on Facebook audience size as of October 2021

(in millions)



## DOWNLOAD



PDF



XLS



PNG



PPT

## Sources

- [Show sources information](#)
- [Show publisher information](#)
- [Use Ask Statista Research Service](#)

## Release date

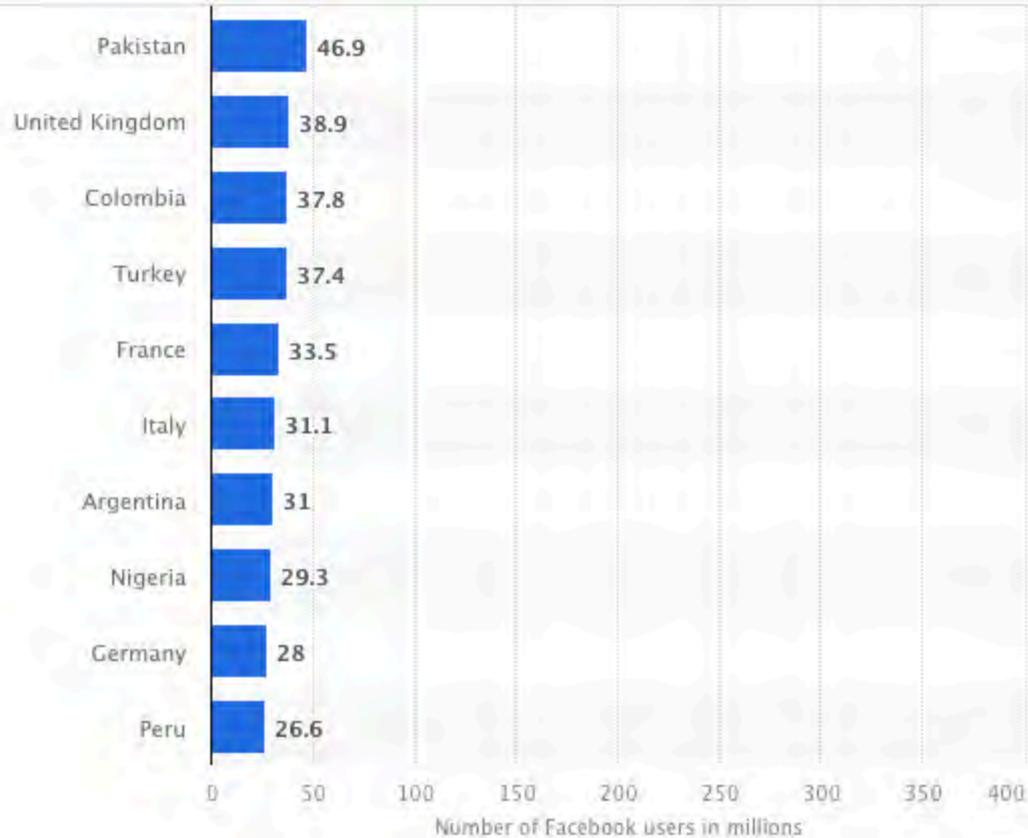
October 2021

## Region

Worldwide

## Survey time period

October 2021



[Collapse statistic](#)

© Statista 2021

[Show source](#)

[Additional Information](#)

### Sources

- [→ Show sources information](#)
- [→ Show publisher information](#)
- [→ Use Ask Statista Research Service](#)

### Release date

October 2021

### Region

Worldwide

### Survey time period

October 2021

### Age group

13 years and older

### Special properties

Based on addressable audience only

### Supplementary notes

Internet users who access their Facebook account via any device at least once per month. All values are estimates. Figures relate to addressable audience only, and may

## Countries with the most Facebook users 2021

Published by [Statista Research Department](#), Nov 16, 2021

[What is the county with the most Facebook users?](#)

## Countries with the most Facebook users 2021

Published by [Statista Research Department](#), Nov 16, 2021

### What is the county with the most Facebook users?

There are nearly 350 million Facebook users in India alone, making it the leading country in terms of Facebook audience size. To put this into context, if India's Facebook audience were a country then it would be ranked third in terms of [largest population worldwide](#). Apart from India, there are several other markets with more than 100 million Facebook users each: The United States, Indonesia, and Brazil with 200 million, 140 million, and 130 million Facebook users respectively.

### Facebook - the most used social media

With more than 2.8 billion monthly active users, [Facebook is the most popular social media worldwide](#). With an audience of this scale, it is no surprise that the vast majority of [Facebook's revenue](#) is generated through advertising.

### Facebook usage by device

As of July 2021, it was found that 98.5 percent of [active users accessed their Facebook account from mobile devices](#). In fact, almost 81.8 percent of Facebook audiences worldwide access the platform only via mobile phone. Facebook is not only available through mobile browser as the company has published several mobile apps for users to access their products and services. Facebook and its core group of products regularly rank among the [most downloaded apps worldwide](#).

Hide

## OTHER STATISTICS ON THE TOPIC

→ [Facebook usage in the United States](#)

## What is the county with the most Facebook users?

There are nearly 350 million Facebook users in India alone, making it the leading country in terms of Facebook audience size. To put this into context, if India's Facebook audience were a country then it would be ranked third in terms of [largest population worldwide](#). Apart from India, there are several other markets with more than 100 million Facebook users each: The United States, Indonesia, and Brazil with 200 million, 140 million, and 130 million Facebook users respectively.

[Read more](#)

### OTHER STATISTICS ON THE TOPIC

→ [Facebook usage in the United States](#)



#### SOCIAL MEDIA & USER-GENERATED CONTENT

Global social networks ranked by number of users 2021



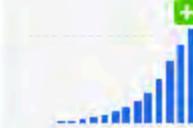
#### SOCIAL MEDIA & USER-GENERATED CONTENT

Facebook: number of monthly active users worldwide 2008-2021



#### SOCIAL MEDIA & USER-GENERATED CONTENT

Facebook: annual revenue and net income 2007-2020



#### SOCIAL MEDIA & USER-GENERATED CONTENT

Number of Facebook employees 2004-2020

# Exhibit 11

1. The services we provide

2. How our services are funded

3. Your commitments to Facebook and our community

4. Additional provisions

5. Other terms and policies that may apply to you

Facebook Ads Controls

Privacy Basics

Cookies Policy

Data Policy

## Terms of Service

Welcome to Facebook!

Facebook builds technologies and services that enable people to connect with each other, build communities, and grow businesses. These Terms govern your use of Facebook, Messenger, and the other products, features, apps, services, technologies, and software we offer (the [Facebook Products](#) or [Products](#)), except where we expressly state that separate terms (and not these) apply. These Products are provided to you by Facebook, Inc.

We don't charge you to use Facebook or the other products and services covered by these Terms. Instead, businesses and organizations pay us to show you ads for their products and services. By using our Products, you agree that we can show you ads that we think will be relevant to you and your interests. We

> [Data Policy](#)

> [More Resources](#)

- [View a printable version of the Terms of Service](#)

services. By using our Products, you agree that we can show you ads that we think will be relevant to you and your interests. We use your personal data to help determine which ads to show you.

We don't sell your personal data to advertisers, and we don't share information that directly identifies you (such as your name, email address or other contact information) with advertisers unless you give us specific permission. Instead, advertisers can tell us things like the kind of audience they want to see their ads, and we show those ads to people who may be interested. We provide advertisers with reports about the performance of their ads that help them understand how people are interacting with their content. See Section 2 below to learn more.

Our [Data Policy](#) explains how we collect and use your personal data to determine some of the ads you see and provide all of the other services described below. You can also go to your [settings](#) at any time to review the privacy choices you have about how we use your data.



[Return to top](#)

## 1. The services we provide

Our mission is to give people the power to build community and bring the world closer together. To help advance this mission, we provide the Products and services described below to you:

### **Provide a personalized experience for you:**

Your experience on Facebook is unlike anyone else's: from the posts, stories, events, ads, and other content you see in News Feed or our video platform to the Pages you follow and other features you might use, such as Trending, Marketplace, and search. We use the data we have - for example, about the connections you make, the choices and settings you select, and what you share and do on and off our Products - to personalize your experience.

### **Connect you with people and organizations you care about:**

We help you find and connect with people, groups, businesses, organizations, and others that matter to you across the Facebook Products you use. We use the data we have to make suggestions for you and others - for example, groups to join, events to attend, Pages to follow or send a message to, shows to watch, and people you may want to become friends with. Stronger ties make for better communities, and we believe our services are most useful when people are connected to people, groups, and organizations they care about.

**Empower you to express yourself and communicate about what matters to you:**

There are many ways to express yourself on Facebook and to communicate with friends, family, and others about what matters to you - for example, sharing status updates, photos, videos, and stories across the Facebook Products you use, sending messages to a friend or several people, creating events or groups, or adding content to your profile. We have also developed, and continue to explore, new ways for people to use technology, such as augmented reality and 360 video to create and share more expressive and engaging content on Facebook.

**Help you discover content, products, and services that may interest you:**

We show you ads, offers, and other sponsored content to help you discover content, products, and services that are offered by the many businesses and organizations that use Facebook and other Facebook Products. Section 2 below explains this in more detail.

**Combat harmful conduct and protect and support our community:**

People will only build community on Facebook if they feel safe. We employ dedicated teams around the world and develop advanced technical systems to detect misuse of our Products, harmful conduct towards others, and situations where we may be able to help support or protect our community. If we learn of content or conduct like this, we will take appropriate action - for example, offering help, removing content, removing or restricting access to certain features, disabling an account, or contacting law enforcement. We share data with other [Facebook Companies](#) when we detect misuse or harmful conduct by

[Facebook Companies](#) when we detect misuse or harmful conduct by someone using one of our Products.

**Use and develop advanced technologies to provide safe and functional services for everyone:**

We use and develop advanced technologies - such as artificial intelligence, machine learning systems, and augmented reality - so that people can use our Products safely regardless of physical ability or geographic location. For example, technology like this helps people who have visual impairments understand what or who is in photos or videos shared on Facebook or Instagram. We also build sophisticated network and communication technology to help more people connect to the internet in areas with limited access. And we develop automated systems to improve our ability to detect and remove abusive and dangerous activity that may harm our community and the integrity of our Products.

**Research ways to make our services better:**

We engage in research to develop, test, and improve our Products. This includes analyzing the data we have about our users and understanding how people use our Products, for example by conducting surveys and testing and troubleshooting new features. Our [Data Policy](#) explains how we use data to support this research for the purposes of developing and improving our services.

**Provide consistent and seamless experiences across the Facebook Company Products:**

Our Products help you find and connect with people, groups, businesses, organizations, and others that are important to you. We design our

organizations, and others that are important to you. We design our systems so that your experience is consistent and seamless across the different [Facebook Company Products](#) that you use. For example, we use data about the people you engage with on Facebook to make it easier for you to connect with them on Instagram or Messenger, and we enable you to communicate with a business you follow on Facebook through Messenger.

**Enable global access to our services:**

To operate our global service, we need to store and distribute content and data in our data centers and systems around the world, including outside your country of residence. This infrastructure may be operated or controlled by Facebook, Inc., Facebook Ireland Limited, or its affiliates.



[Return to Top](#)

## 2. How our services are funded

Instead of paying to use Facebook and the other products and services we offer, by using the Facebook Products covered by these Terms, you agree that we can show you ads that businesses and organizations pay us to promote on and off the [Facebook Company Products](#). We use your personal data, such as information about your activity and interests, to show you ads that are more relevant to you.

about your activity and interests, to show you ads that are more relevant to you.

Protecting people's privacy is central to how we've designed our ad system. This means that we can show you relevant and useful ads without telling advertisers who you are. We don't sell your personal data. We allow advertisers to tell us things like their business goal, and the kind of audience they want to see their ads (for example, people between the age of 18-35 who like cycling). We then show their ad to people who might be interested.

We also provide advertisers with reports about the performance of their ads to help them understand how people are interacting with their content on and off Facebook. For example, we provide general demographic and interest information to advertisers (for example, that an ad was seen by a woman between the ages of 25 and 34 who lives in Madrid and likes software engineering) to help them better understand their audience. We don't share information that directly identifies you (information such as your name or email address that by itself can be used to contact you or identifies who you are) unless you give us specific permission. Learn more about how Facebook ads work [here](#).

We collect and use your personal data in order to provide the services described above to you. You can learn about how we collect and use your data in our [Data Policy](#). You have controls over the types of ads and advertisers you see, and the types of information we use to determine which ads we show you. [Learn more](#).



Return to top

2 Your commitments to Facebook

### 3. Your commitments to Facebook and our community

We provide these services to you and others to help advance our mission. In exchange, we need you to make the following commitments:

#### 1. Who can use Facebook

When people stand behind their opinions and actions, our community is safer and more accountable. For this reason, you must:

- Use the same name that you use in everyday life.
- Provide accurate information about yourself.
- Create only one account (your own) and use your timeline for personal purposes.
- Not share your password, give access to your Facebook account to others, or transfer your account to anyone else (without our permission).

We try to make Facebook broadly available to everyone, but you cannot use Facebook if:

- You are under 13 years old.
- You are a convicted sex offender.
- We've previously disabled your account for violations of our Terms or Policies.
- You are prohibited from receiving our products, services, or

- You are prohibited from receiving our products, services, or software under applicable laws.

## 2. What you can share and do on Facebook

We want people to use Facebook to express themselves and to share content that is important to them, but not at the expense of the safety and well-being of others or the integrity of our community. You therefore agree not to engage in the conduct described below (or to facilitate or support others in doing so):

1. You may not use our Products to do or share anything:
  - That violates these Terms, our [Community Standards](#), and [other terms and policies](#) that apply to your use of Facebook.
  - That is unlawful, misleading, discriminatory or fraudulent.
  - That infringes or violates someone else's rights, including their intellectual property rights.
2. You may not upload viruses or malicious code or do anything that could disable, overburden, or impair the proper working or appearance of our Products.
3. You may not access or collect data from our Products using automated means (without our prior permission) or attempt to access data you do not have permission to access.

We can remove or restrict access to content that is in violation of these provisions.

If we remove content that you have shared in violation of our Community

If we remove content that you have shared in violation of our Community Standards, we'll let you know and explain any options you have to request another review, unless you seriously or repeatedly violate these Terms or if doing so may expose us or others to legal liability; harm our community of users; compromise or interfere with the integrity or operation of any of our services, systems or Products; where we are restricted due to technical limitations; or where we are prohibited from doing so for legal reasons.

To help support our community, we encourage you to [report](#) content or conduct that you believe violates your rights (including [intellectual property rights](#)) or our terms and policies.

We also can remove or restrict access to your content, services or information if we determine that doing so is reasonably necessary to avoid or mitigate adverse legal or regulatory impacts to Facebook.

### **3. The permissions you give us**

We need certain permissions from you to provide our services:

1. [Permission to use content you create and share](#): Some content that you share or upload, such as photos or videos, may be protected by intellectual property laws.

You own the intellectual property rights (things like copyright or trademarks) in any such content that you create and share on Facebook and the other [Facebook Company Products](#) you use. Nothing in these Terms takes away the rights you have to your own content. You are free to share your content with anyone else, wherever you want.

However, to provide our services we need you to give us some legal permissions (known as a "license") to use this content. This is solely for the purposes of providing and improving our Products and services as described in Section 1 above.

Specifically, when you share, post, or upload content that is covered by intellectual property rights on or in connection with our Products, you grant us a non-exclusive, transferable, sub-licensable, royalty-free, and worldwide license to host, use, distribute, modify, run, copy, publicly perform or display, translate, and create derivative works of your content (consistent with your [privacy](#) and [application](#) settings). This means, for example, that if you share a photo on Facebook, you give us permission to store, copy, and share it with others (again, consistent with your settings) such as service providers that support our service or other Facebook Products you use. This license will end when your content is deleted from our systems.

You can delete content individually or all at once by deleting your account. [Learn more](#) about how to delete your account. You can [download a copy](#) of your data at any time before deleting your account.

When you delete content, it's no longer visible to other users; however it may continue to exist elsewhere on our systems where:

- immediate deletion is not possible due to technical limitations (in which case, your content will be deleted within a maximum of 90 days from when you delete it);
- your content has been used by others in accordance with this license and they have not deleted it (in which case this

- your content has been used by others in accordance with this license and they have not deleted it (in which case this license will continue to apply until that content is deleted); or
- where immediate deletion would restrict our ability to:
  - investigate or identify illegal activity or violations of our terms and policies (for example, to identify or investigate misuse of our Products or systems);
  - comply with a legal obligation, such as the preservation of evidence; or
  - comply with a request of a judicial or administrative authority, law enforcement or a government agency;

in which case, the content will be retained for no longer than is necessary for the purposes for which it has been retained (the exact duration will vary on a case-by-case basis).

In each of the above cases, this license will continue until the content has been fully deleted.

2. Permission to use your name, profile picture, and information about your actions with ads and sponsored content: You give us permission to use your name and profile picture and information about actions you have taken on Facebook next to or in connection with ads, offers, and other sponsored content that we display across our Products, without any compensation to you. For example, we may show your friends that you are interested in an advertised event or have liked a Page created by a brand that has paid us to display its ads on Facebook. Ads like this can be seen

paid us to display its ads on Facebook. Ads like this can be seen only by people who have your permission to see the actions you've taken on Facebook. You can [learn more](#) about your ad settings and preferences.

3. **Permission to update software you use or download:** If you download or use our software, you give us permission to download and install updates to the software where available.

#### 4. Limits on using our intellectual property

If you use content covered by intellectual property rights that we have and make available in our Products (for example, images, designs, videos, or sounds we provide that you add to content you create or share on Facebook), we retain all rights to that content (but not yours). You can only use our copyrights or [trademarks \(or any similar marks\)](#) as expressly permitted by our [Brand Usage Guidelines](#) or with our prior written permission. You must obtain our written permission (or permission under an open source license) to modify, create derivative works of, decompile, or otherwise attempt to extract source code from us.



[Return to top](#)

## 4. Additional provisions

## **1. Updating our Terms**

We work constantly to improve our services and develop new features to make our Products better for you and our community. As a result, we may need to update these Terms from time to time to accurately reflect our services and practices. Unless otherwise required by law, we will notify you before we make changes to these Terms and give you an opportunity to review them before they go into effect. Once any updated Terms are in effect, you will be bound by them if you continue to use our Products.

We hope that you will continue using our Products, but if you do not agree to our updated Terms and no longer want to be a part of the Facebook community, you can [delete](#) your account at any time.

## **2. Account suspension or termination**

We want Facebook to be a place where people feel welcome and safe to express themselves and share their thoughts and ideas.

If we determine that you have clearly, seriously or repeatedly breached our Terms or Policies, including in particular our Community Standards, we may suspend or permanently disable access to your account. We may also suspend or disable your account if you repeatedly infringe other people's intellectual property rights or where we are required to do so for legal reasons.

Where we take such action we'll let you know and explain any options you have to request a review, unless doing so may expose us or others to legal liability; harm our community of users; compromise or interfere with the integrity or operation of any of our services, systems or Products; or where we are restricted due to technical limitations, or

Products; or where we are restricted due to technical limitations; or where we are prohibited from doing so for legal reasons.

You can [learn more](#) about what you can do if your account has been disabled and how to contact us if you think we have disabled your account by mistake.

If you delete or we disable your account, these Terms shall terminate as an agreement between you and us, but the following provisions will remain in place: 3, 4.2-4.5.

### **3. Limits on liability**

We work hard to provide the best Products we can and to specify clear guidelines for everyone who uses them. Our Products, however, are provided "as is," and we make no guarantees that they always will be safe, secure, or error-free, or that they will function without disruptions, delays, or imperfections. To the extent permitted by law, we also DISCLAIM ALL WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT. We do not control or direct what people and others do or say, and we are not responsible for their actions or conduct (whether online or offline) or any content they share (including offensive, inappropriate, obscene, unlawful, and other objectionable content).

We cannot predict when issues might arise with our Products.

Accordingly, our liability shall be limited to the fullest extent permitted by applicable law, and under no circumstance will we be liable to you for any lost profits, revenues, information, or data, or consequential, special, indirect, exemplary, punitive, or incidental damages arising out of or

indirect, exemplary, punitive, or incidental damages arising out of or related to these Terms or the Facebook Products, even if we have been advised of the possibility of such damages. Our aggregate liability arising out of or relating to these Terms or the Facebook Products will not exceed the greater of \$100 or the amount you have paid us in the past twelve months.

#### **4. Disputes**

We try to provide clear rules so that we can limit or hopefully avoid disputes between you and us. If a dispute does arise, however, it's useful to know up front where it can be resolved and what laws will apply.

For any claim, cause of action, or dispute you have against us that arises out of or relates to these Terms or the Facebook Products ("claim"), you agree that it will be resolved exclusively in the U.S. District Court for the Northern District of California or a state court located in San Mateo County. You also agree to submit to the personal jurisdiction of either of these courts for the purpose of litigating any such claim, and that the laws of the State of California will govern these Terms and any claim, without regard to conflict of law provisions.

#### **5. Other**

1. These Terms (formerly known as the Statement of Rights and Responsibilities) make up the entire agreement between you and Facebook, Inc. regarding your use of our Products. They supersede any prior agreements.
2. Some of the Products we offer are also governed by supplemental terms. If you use any of those Products, supplemental terms will be

terms. If you use any of those Products, supplemental terms will be made available and will become part of our agreement with you. For instance, if you access or use our Products for commercial or business purposes, such as buying ads, selling products, developing apps, managing a group or Page for your business, or using our measurement services, you must agree to our [Commercial Terms](#). If you post or share content containing music, you must comply with our [Music Guidelines](#). To the extent any supplemental terms conflict with these Terms, the supplemental terms shall govern to the extent of the conflict.

3. If any portion of these Terms is found to be unenforceable, the remaining portion will remain in full force and effect. If we fail to enforce any of these Terms, it will not be considered a waiver. Any amendment to or waiver of these Terms must be made in writing and signed by us.
4. You will not transfer any of your rights or obligations under these Terms to anyone else without our consent.
5. You may designate a person (called a legacy contact) to manage your account if it is memorialized. Only your legacy contact or a person who you have identified in a valid will or similar document expressing clear consent to disclose your content upon death or incapacity will be able to seek [disclosure](#) from your account after it is memorialized.
6. These Terms do not confer any third-party beneficiary rights. All of our rights and obligations under these Terms are freely assignable by us in connection with a merger, acquisition, or sale of assets, or by operation of law or otherwise.

7. You should know that we may need to change the username for your account in certain circumstances (for example, if someone else claims the username and it appears unrelated to the name you use in everyday life).
8. We always appreciate your feedback and other suggestions about our products and services. But you should know that we may use them without any restriction or obligation to compensate you, and we are under no obligation to keep them confidential.
9. We reserve all rights not expressly granted to you.



## 5. Other terms and policies that may apply to you

- Community Standards: These guidelines outline our standards regarding the content you post to Facebook and your activity on Facebook and other Facebook Products.
- Commercial Terms: These terms apply if you also access or use our Products for any commercial or business purpose, including advertising, operating an app on

- Commercial Terms: These terms apply if you also access or use our Products for any commercial or business purpose, including advertising, operating an app on our Platform, using our measurement services, managing a group or a Page for a business, or selling goods or services.
- Advertising Policies: These policies specify what types of ad content are allowed by partners who advertise across the Facebook Products.
- Self-Serve Ad Terms: These terms apply when you use self-serve advertising interfaces to create, submit, or deliver advertising or other commercial or sponsored activity or content.
- Pages, Groups and Events Policy: These guidelines apply if you create or administer a Facebook Page, group, or event, or if you use Facebook to communicate or administer a promotion.
- Facebook Platform Policy: These guidelines outline the policies that apply to your use of our Platform (for example, for developers or operators of a Platform application or website or if you use social plugins).
- Developer Payment Terms: These terms apply to developers of applications that use Facebook Payments.
- Community Payment Terms: These terms apply to payments made on or through Facebook.
- Commerce Policies: These guidelines outline the policies that apply when you offer products and services for sale on Facebook.
- Facebook Brand Resources: These guidelines outline the policies that apply to use of Facebook trademarks, logos, and screenshots.
- Music Guidelines: These guidelines outline the policies that apply if you post or share content containing music on Facebook.

- [Facebook Platform Policy](#): These guidelines outline the policies that apply to your use of our Platform (for example, for developers or operators of a Platform application or website or if you use social plugins).
- [Developer Payment Terms](#): These terms apply to developers of applications that use Facebook Payments.
- [Community Payment Terms](#): These terms apply to payments made on or through Facebook.
- [Commerce Policies](#): These guidelines outline the policies that apply when you offer products and services for sale on Facebook.
- [Facebook Brand Resources](#): These guidelines outline the policies that apply to use of Facebook trademarks, logos, and screenshots.
- [Music Guidelines](#): These guidelines outline the policies that apply if you post or share content containing music on Facebook.
- [Live Policies](#): These policies apply to all content broadcast to Facebook Live.

Date of Last Revision: October 22, 2020

[English \(US\)](#) [Español](#) [Français \(France\)](#) [中文\(简体\)](#) [العربية](#) [Português \(Brasil\)](#) [Italiano](#) [Deutsch](#) [日本語](#) [+](#)

[Sign Up](#) [Log In](#) [Messenger](#) [Facebook Lite](#) [Watch](#) [Places](#) [Games](#) [Marketplace](#) [Facebook Pay](#) [Jobs](#) [Oculus](#) [Portal](#) [Instagram](#) [Local](#) [Fundraisers](#)  
[Services](#) [Voting Information Center](#) [About](#) [Create Ad](#) [Create Page](#) [Developers](#) [Careers](#) [Privacy](#) [Cookies](#) [Ad Choices](#) [Terms](#) [Help](#)

# Exhibit 12

DAVID NIELD SECURITY 01.12.2020 07:00 AM

# All the Ways Facebook Tracks You—and How to Limit It

If you have a Facebook account—and even if you don't—the company is going to collect data about you. But you can at least control how it gets used.



ILLUSTRATION: ELENA LACEY; GETTY IMAGES

**IT WON'T COME** as much of a surprise that Facebook tracks you on its platform—that's why it can resurface your birthday photos from five years ago—but you might not yet realize the scope and the depth of its tracking all across the internet. Facebook's tentacles stretch out

across other websites and services, into the various apps you're using on your phone, and to the places you physically visit in the real world—especially if you decide to check in on Facebook while you're there.

Some of this comes with the territory of using Facebook: If you want to take advantage of its features, then you have to give up a certain amount of information about yourself. But Facebook has ways of keeping tabs on people who aren't even signed up for the service. Fortunately, there are numerous ways to limit the volume of data that it logs.

How hard you want to pull back depends to a certain extent on how much you trust Facebook. The social network behemoth says it uses your data to show relevant ads and keep you safe; if someone signs into your account from a country you're not usually in, for instance, Facebook can flag the activity as suspicious.

However, this is not a company with a good track record when it comes to looking after your data. Irrespective of how Facebook itself has used your information, it's certainly been careless in the ways that information has been shared with third parties.

To make matters more complicated, Facebook owns WhatsApp and Instagram too, and can pool some of the information it gathers in those apps as well. The best way to limit Facebook's tracking is to quit all three apps for good. If that's too extreme for you, we've got some more suggestions.

For reference, the Facebook data policy is here, and you can read a more user-friendly explainer on how your data is handled here.

## On the Web

COURTESY OF FACEBOOK

If you want to use Facebook, you give it permission to log your activity on the site: where you check into, the groups you join, who you interact with. This data is primarily used to serve up advertising that's more relevant to you, which in turn makes more money for Facebook.

You can't really stop Facebook from collecting this information—it's the deal you make when you sign up—but you can limit how it affects the advertising you see by visiting the [ad preferences page](#) in your account on the web. Open up **Your interests** to get a quick glance at what Facebook thinks you're into. It might have made some assumptions that are well wide of the mark.

Under the **Your information** tab, you can see some of the ways Facebook is targeting advertising at you: your relationship status, your job title, where you went to college, and more. If you don't want some or all of these pieces of information to be used by advertisers, hit the relevant toggle switch.

Open up **Ad settings** to make even more changes. Here you can control whether Facebook can use data from its marketing partners—and there are an awful lot of them—to put more relevant advertising in front of you. If you don't want this to happen, switch the setting from **Allowed** to **Not allowed**.

Bear in mind that these settings don't reduce the number of advertisements you see on Facebook, nor do they delete the data that Facebook has amassed on you. They just stop advertisers from specifically targeting you using that data. If you're happily married, you might suddenly start seeing ads for dating sites, but Facebook itself will still know your relationship status.

---

### See What's Next in Tech With the Fast Forward Newsletter

From artificial intelligence and self-driving cars to transformed cities and new startups, sign up for the latest news.

Your email \_\_\_\_\_

Enter your email

## SUBMIT

By signing up you agree to our [User Agreement](#) and [Privacy Policy & Cookie Statement](#)

Facebook's reach also goes way beyond Facebook itself. It has partnerships with a whole host of marketing firms and ad networks so that activities on other sites—including but not limited to logging into a third-party service with your Facebook account—can be combined with your Facebook profile.

This activity has attracted enough bad press that Facebook [announced a tool in August called "Off-Facebook Activity"](#) that will disconnect this data from what you actually do on Facebook. It's a more comprehensive solution, but still not widely available. It also still doesn't affect how much data Facebook actually *collects*, it just breaks the association between what you do on Facebook and off it. If you're shopping for shoes on a third-party retail site, you won't suddenly see ads for them all over your News Feed.

COURTESY OF FACEBOOK

This off-Facebook activity is also monitored whether or not you have a Facebook account. Tracking tools like the Facebook Pixel enable websites and online retailers to get information about their visitors, including whether they come back. A vast number of third parties are using Facebook's advertising and tracking technologies, which means it isn't just Facebook you need to worry about.

Site owners are able to build up a profile of who is visiting their pages, and Facebook collects even more data about what people are shopping for and looking at on the web. If that data can be added to a Facebook profile so much the better for Facebook, but the social network can still use in general terms to analyze aggregated user behavior.

More broadly, you can stop some of the web activity being used to target you with ads by visiting the [YourAdChoices site](#) run by the Digital Advertising Alliance. You'll notice Facebook advertising targeting is on the list of entries—tick the **Opt Out** box to do just that. Note that you'll need to do this separately for each browser you use; for the biggest impact, you should opt out of all the other platforms as well.

Locking down tracking in your browser is also recommended: Look out for the option to block third-party cookies in your browser settings (the sort that can track activity across multiple sites), and consider using well-respected tracker blocking browser extensions such as [Ghostery](#) or [Privacy Badger](#).

## On Mobile Devices

COURTESY OF FACEBOOK

Much of what we've already said applies to Facebook's mobile apps as well. If you want to limit what Facebook knows about you, you're best off not installing the mobile apps at all. Doing so gives Facebook [permission](#) to log the Wi-Fi networks you connect to, the type of phone you have, the other apps you have installed, and more besides, as well as everything you do on Facebook itself

you do on Facebook itself.

You can't stop all of this data collection, but you can curb it. Head to the Facebook permissions page—under **Apps and notifications** and **Facebook** in Android settings and under **Facebook** in iOS settings—to block Facebook's access to your phone's location, your contacts, your phone's microphone and camera, and more.

The bad news? Even with location tracking turned off, Facebook still makes note of the approximate location that you access the web from via your IP address. It's only a rough guide—and Facebook says it's necessary to keep accounts secure and users verified—but you can't stop this from happening if you use Facebook.

More bad news: Other apps send data to Facebook as well, often automatically. Almost everyone has a Facebook account, and third-party apps want to make use of that data, whether it's to target users with advertising or to simplify the login process and get more user data as a result. Facebook isn't working in isolation here, and has many profitable partnerships with other apps and data brokers.

It's worth emphasizing that Facebook, like Google, promises to use this treasure trove of data to improve its services and make life safer and more convenient for its users, as well as generating more profitable ads across its network. You are, after all, using everything Facebook offers for free. If you don't trust Facebook's intentions—which is by now understandable—then you really need to quit using it altogether.

If you're going to stay with it, limit your activity and become a social media lurker. Don't check into locations, don't tag photos, and don't fill out quizzes that tell you which Disney character you are. Keep your profile information down to a minimum, and think twice about sharing anything at all. On the phone, consider using Facebook on the mobile web instead of in the app.

COURTESY OF FACEBOOK

Keep the apps you've connected to Facebook down to a minimum as well; you can find a list on the web [here](#). Not only does this restrict the third parties who have access to your data, it's also a good idea from a security point of view, limiting the number of ways hackers could potentially get at your data.

Facebook knows full well that users are uneasy about its data collection policies, and is trying to [push out tools](#) that ostensibly offer more control. In reality, these don't do much in regards to data collection, and are more about how that data is used to personalize ads. At this stage, if you don't want Facebook to know a lot about you, you really need to close down your Facebook, Instagram, and WhatsApp accounts and not look back.

More general privacy tips can slow down Facebook, too: [Use a VPN](#) to disguise your location, [lock down your browser's privacy settings](#) so you're not tracked so extensively by marketers, and make liberal use of your browser's incognito mode wherever you can. Ultimately though, using Facebook comes with a cost, even if it's not paid up front in dollars and cents.

## More Great WIRED Stories

- Here's what directing a [Star Wars movie is really like](#)
- Bored with Sunday service? [Maybe nudist church is your thing](#)
- The mad scientist who wrote the book [on how to hunt hackers](#)
- How the US prepares its embassies [for potential attacks](#)
- When the transportation revolution [hit the real world](#)
- 🕸 Will AI as a field ["hit the wall" soon?](#) Plus, the [latest news on artificial intelligence](#)
- ✨ Optimize your home life with our Gear team's best picks, from [robot vacuums](#) to [affordable mattresses](#) to [smart speakers](#)

---

[TOPICS](#) [FACEBOOK](#) [PRIVACY](#)

---

# Exhibit 13

Report ad



April 19, 2021 1:31 PM EDT Last Updated 7 months ago

**Technology**

# Facebook takes on Clubhouse, unveils upcoming audio products

By Elizabeth Culliford and Munsif Vengattil, Sheila Dang

3 minute read



April 19 (Reuters) - Facebook Inc. (**FB.O**) CEO Mark Zuckerberg said on Monday the company planned to launch several audio products, including Clubhouse-style live audio rooms and a way for users to find and play podcasts.

Facebook's incursion into the audio market comes as the sudden explosion of interest in Clubhouse, an audio app where billionaires and celebrities including Tesla CEO Elon Musk have popped in to chat, could be waning. Downloads of the Clubhouse app, which is only available on Apple's iOS devices, suffered an estimated 70% decline in downloads in March from February when it hit a high.



**Sponsored by SAP**

**Manage spend to drive business**

Manage spending for better, faster decisions with Intelligent Spend Management from SAP.

[See more](#)

Report ad

Zuckerberg said the world's largest social media network planned in the coming months to launch features including short-form audio clips called "Soundbites" and ways to create sound effects or improve audio quality. Facebook said in a [blog post](#) it would begin to test live audio rooms, which would launch by the summer.

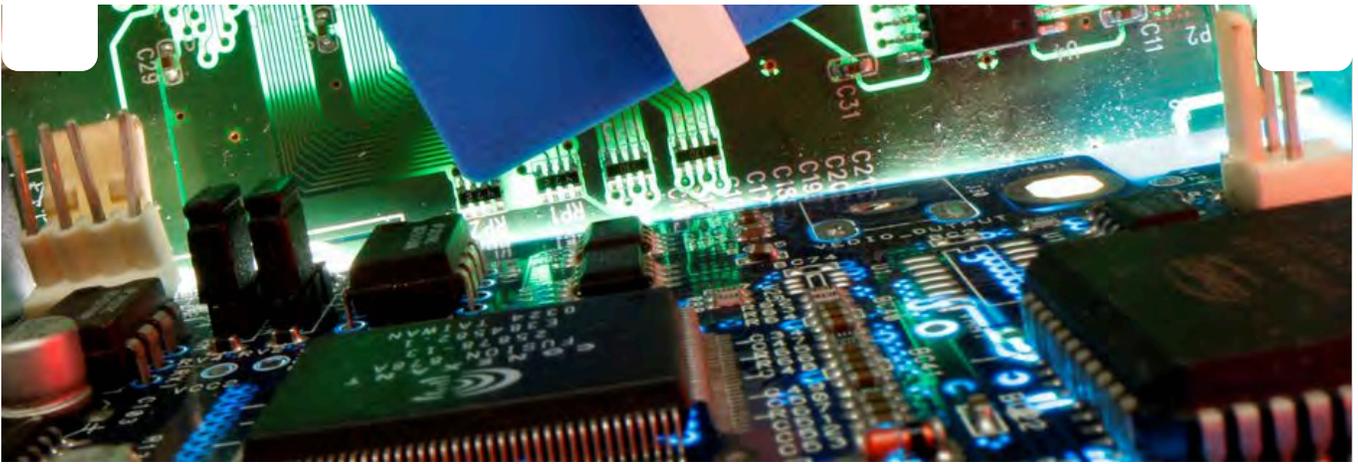
Zuckerberg said Facebook was looking to "treat audio as a first-class medium in the way that we would photos or video" in an interview on Discord with Casey Newton, editor of newsletter Platformer.

The rapid growth of the year-old app Clubhouse has demonstrated the potential of audio chat services.

What is not clear is if Clubhouse, which just closed a new round of Series C funding in which a source said it was valued at \$4 billion, will have staying power as installs decline.

The app, which is not yet available on Android, faces competition from multiple companies working on Clubhouse clones. Twitter Inc ([TWTR.N](#)) is testing its [live audio feature Spaces](#), along with new features from Discord, Microsoft-owned ([MSFT.O](#)) LinkedIn, Slack and Spotify Technology ([SPOT.N](#)).





1/2

Facebook symbol is seen on a motherboard in this picture illustration taken April 24, 2020. REUTERS/Dado Ruvic /Illustration

Reddit also unveiled a preview of its "Reddit Talks" product to moderators on Monday.

Analytics firm Sensor Tower estimated Clubhouse had a 72% decline in growth from about 9.6 million February installs to about 2.4 million in March.

Facebook, which has long been criticized for its handling of problematic content across its products, will face the challenges of moderating live and recorded audio content.

Facebook said its live audio rooms would be available on its Messenger product and in its main app. It said it would test the rooms with public figures as well as in Groups - a product the company has vigorously promoted as providing places for people with common interests but which have also been used to spread misinformation and organize extremist activity.

As part of the announcements, Zuckerberg also said Facebook is working with Spotify on "Project Boombox" to share and listen to music on its platform.

Facebook said users would be able to send donations, or tips, to creators in live audio rooms through "Stars". After launch, it will offer other types of monetization like single-

purchase access or subscription for rooms. It also announced an audio creator fund for Soundbites.

The company is working to attract more creators who are accustomed to receiving tips and other direct payments from fans.

Reporting by Munsif Vengattil in Bengaluru and Elizabeth Culliford in New York; Editing by Arun Koyyur

Our Standards: [The Thomson Reuters Trust Principles.](#)

## More from Reuters



AD

Musk sells \$5bln in Tesla shares after Twitter poll

Twitter users tell Musk to sell Tesla shares

Incoming NYC mayor vows to take initial pay in bitcoin

Skepticism, surprise as

## Read Next

United Kingdom

6:02 PM EST

**Amazon may drop Visa as partner on U.S. credit card**

# Exhibit 14

INC. 5000 CONFERENCE

## Facebook's Sheryl Sandberg Breaks Silence About Business Practices, Outage

Sandberg, the COO of Facebook, discussed the news about the company's decisions on content and algorithms while speaking to small-business owners at the Inc. 5000 Vision Conference. [🔗](#)

BY CHRISTINE LAGORIO-CHAFKIN, SENIOR WRITER, INC. @LAGORIO

---

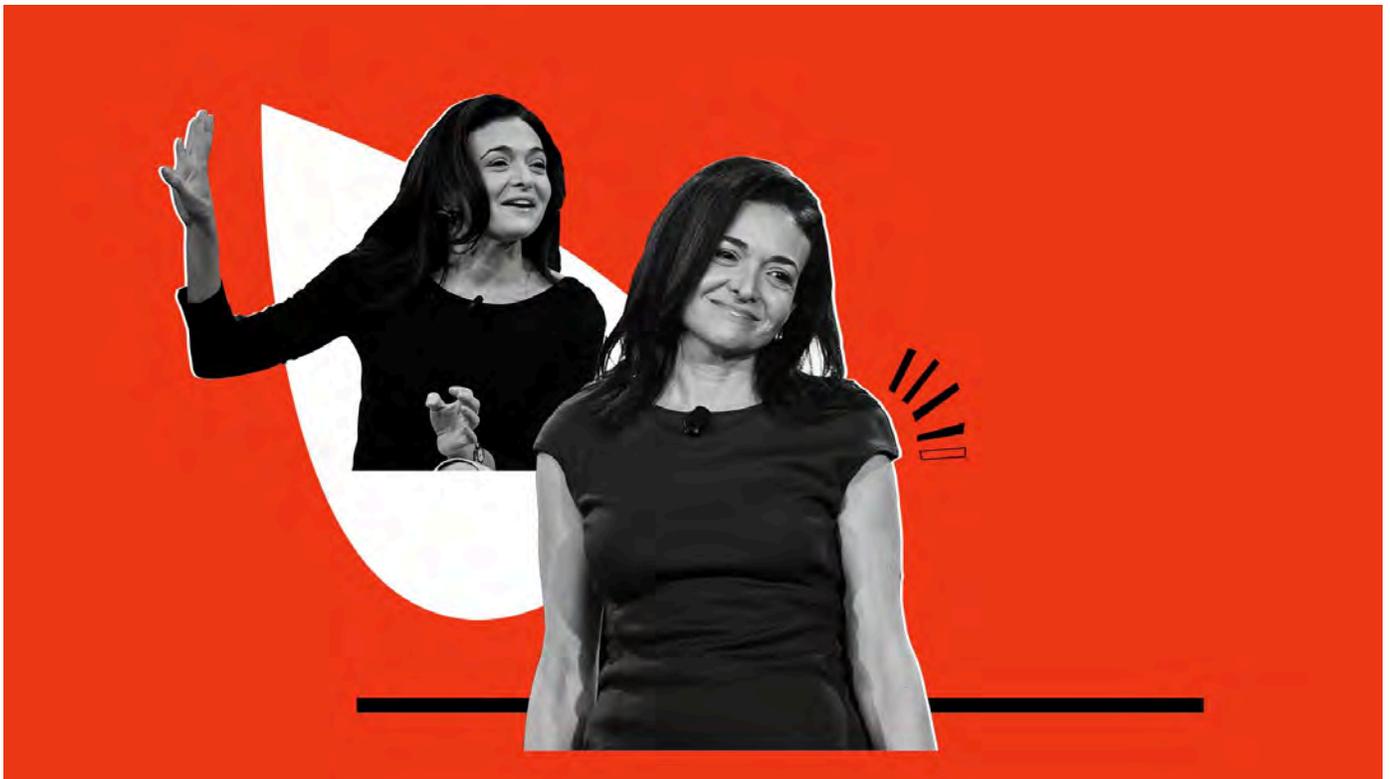


Photo: Getty Images. Illustration: Reagan Allen.

---

In her first time speaking publicly since Facebook's safety systems controversy, Sheryl Sandberg contested recent complaints that the social network cares more about profits than people.

"We know that with a platform like ours, with billions of people on it, we're gonna see all the bad of humanity and all the good and our job is very simple. It is to minimize that bad with every, every bit of strength we have, and give the opportunity for that good to flourish," the social network's COO said at the Inc. 5000 Vision Conference. "And that's what we work on every single day."

The scrutiny of the company follows news reports of the observations and documents from Frances Haugen, a former Facebook product manager, which led to a series of articles in the Wall Street Journal, a 60 Minutes episode, and congressional testimony stating that the social network is misleading the public on its actions to quell hate speech, misinformation, and other harmful content. Since then, Sandberg and Facebook founder and CEO Mark Zuckerberg have been largely silent.

Zuckerberg did post on Facebook last Tuesday, writing that Facebook's internal research was not used in the fashion he intended.

*Article continues after sponsored content*

**YOUR NEXT MOVE SPONSORED CONTENT**

How This VC Is Helping Female Founders Raise Millions

---

"It's disheartening to see that work taken out of context and used to construct a false narrative that we don't care," Zuckerberg wrote. He added that he's particularly focused on how Facebook products affect minors, and that it's important to him that "everything we build is safe and good for kids."

Haugen shared with a *Wall Street Journal* reporter an internal study that found that 13.5 percent of teenage girls in the U.K. said their suicidal thoughts became more frequent after joining Instagram.

Sandberg addressed some of the research by saying, "We have a deep commitment to putting out products that keep everyone safe, that minimize harm, that maximize good. We care tremendously about the well-being of everyone, but especially young people. And that's why we do research. We do research to understand how our products are being used, the impact they have, and so that we continually evolve them."

Sandberg also addressed the outage on October 4. "People were worried that this was a hack. It wasn't," she said. "It was an outage caused by routine maintenance."

For that, she echoed what Zuckerberg had previously said: "We're sorry for the inconvenience."

Sandberg's full interview with Inc. editor-in-chief Scott Omelianuk took place as part of the [Inc. 5000 Vision Conference](#), which begins on October 19 and concludes on October 21.

**Inc. helps entrepreneurs change the world. Get the advice you need to start, grow, and lead your business today. [Subscribe here](#) for unlimited access.**

OCT 19, 2021

# Exhibit 15

EDITORS' PICK | Sep 28, 2020, 01:07pm EDT | 2,150 views

# Sheryl Sandberg On Facebook's Role In Small Business Support And Voter Registration During The Pandemic



**Abigail Freeman** Forbes Staff

[Business](#)

*I'm an assistant editor at Forbes covering media and entertainment.*

Listen to article 4 minutes



Sheryl Sandberg, COO of Facebook spoke at Forbes' first-ever Small Business Summit on Friday.

(Photo ... [+] GETTY IMAGES FOR VANITY FAIR

With more than 180 million businesses relying on its social media platforms every month, Facebook FB -0.6% has a crucial role in helping small businesses change course and stay connected with customers during the pandemic.

At *Forbes'* first-ever Small Business Summit held virtually on Friday, COO Sheryl Sandberg discussed how Facebook has “doubled down” on product launches for small businesses and how Congress can do more to help them survive coronavirus.

Digital migration is “definitely an accelerating trend and it's here to stay,” Sandberg said. “Businesses were already moving online, but what we found during this period is businesses are migrating much more quickly.”

To bolster that shift over the last few months, Facebook has launched Facebook Shops, an app where businesses can create online stores to sell directly to consumers, and Facebook Business Suite, a “one-stop shop where you can manage all your pages, your profiles and your messages across Facebook and Instagram and Messenger.”

Sandberg also said fundraisers — typically used on the social media app for nonprofits in honor of users' birthdays — are available for small businesses now.

“I never thought we would do fundraisers for small businesses,” she said. “But people said to us they know small businesses are so important to their community, and they want to fundraise.”

---

MORE FOR YOU

**Why Liverpool's Scientists Will Decide The Premier League Title**

**Ron Paul 'Doing Fine' In Hospital After Appearing To Suffer Medical Episode On Camera**

**Pulitzer Prizes 2020: The Full List Of Winners**

---

The social media giant committed \$200 million of its own cash for two grant programs dedicated to small and Black-owned businesses.

“We're working on getting the money out the door as soon as we can, because there is no time to waste in a crisis like this,” Sandberg said.

Aside from determining what Facebook can do to help, [Sandberg](#), along with former Starbucks [SBUX +0.3%](#) head Howard Schultz and Microsoft [MSFT +0.1%](#) CEO Satya Nadella, called on Congress last month to offer additional long-term financial support for small businesses. She said a major issue that needs to be debunked is the notion that big data only helps big corporations.

**F**

**Former WNBA Star Renee Montgomery  
Has A New Position, Venture Capitalist**

---





---

“A lot of people are calling for no use of data in targeting, [saying] don't let big companies use data. They're not understanding that the people who are benefiting from that are not just the big companies, but are small businesses that rely on that targeting to grow and stay in business,” Sandberg said. “I think that's something we need to do a much better job explaining so that we have small business growth.”

While holding the government accountable to do more for small businesses, Facebook's part in the upcoming presidential election is not lost on Sandberg. She admitted to Facebook's failure to catch Russian interference in 2016. “We missed it, and that's on us,” she said. “The FBI missed it. We had never seen anything like this. We weren't prepared for state attacks.”

Since then, Facebook has shut down more than 50 networks spreading misinformation, and launched, what Sandberg believes, is the largest voter registration effort ever, with a goal of 4 million people registered to vote through the Facebook and Instagram apps.

“This is a critical election. We want to make sure everyone votes and everyone gets accurate information on how to vote.”

The main takeaway from Sandberg's keynote discussion: Everyone should contribute to democracy and small businesses' survival.

“It's all of us stepping up. Government doing its part, big business like us doing our part, and communities doing our part to keep small businesses growing. We need that.”

## **Full coverage and live updates on the Coronavirus**

*Follow me on [Twitter](#). Send me a secure [tip](#).*



**Abigail Freeman**

I'm an assistant editor at Forbes covering media and entertainment with a focus on...

**Read More**

Reprints & Permissions

ADVERTISEMENT

---

# Exhibit 16

## **Excerpts of Facebook's Community Standards on 04/08/2021**

### **Hate Speech**

[W]e don't allow hate speech on Facebook. It creates an environment of intimidation and exclusion, and in some cases may promote offline violence. We define hate speech as a direct attack against people on the basis of what we call protected characteristics: race, ethnicity, national origin, disability, religious affiliation, caste, sexual orientation, sex, gender identity and serious disease. We define attacks as violent or dehumanizing speech, harmful stereotypes, statements of inferiority, expressions of contempt, disgust or dismissal, cursing, and calls for exclusion or segregation. . . .

Do not post:

Content targeting a person or group of people (including all subsets except those described as having carried out violent crimes or sexual offenses) on the basis of their aforementioned protected characteristic(s) or immigration status with:

- Violent speech or support in written or visual form
- Dehumanizing speech or imagery in the form of comparisons, generalizations, or unqualified behavioral statements (in written or visual form) to or about:
  - Insects
  - Animals that are culturally perceived as intellectually or physically inferior
  - Filth, bacteria, disease and feces
  - Sexual predator
  - Subhumanity
  - Violent and sexual criminals
  - Other criminals (including but not limited to “thieves,” “bank robbers,” or saying “All [protected characteristic or quasi-protected characteristic] are ‘criminals’”)
  - Statements denying existence
- Mocking the concept, events or victims of hate crimes even if no real person is depicted in an image
- Designated dehumanizing comparisons, generalizations, or behavioral statements (in written or visual form)- that include:
  - Black people and apes or ape-like creatures
  - Black people and farm equipment
  - Caricatures of Black people in the form of blackface
  - Jewish people and rats
  - Jewish people running the world or controlling major institutions such as media networks, the economy or the government
  - Denying or distorting information about the Holocaust
  - Muslim people and pigs
  - Muslim person and sexual relations with goats or pigs
  - Mexican people and worm like creatures

- Women as household objects or referring to women as property or “objects”
- Transgender or non-binary people referred to as “it”
- Dalits, scheduled caste or ‘lower caste’ people as menial laborers

## **Violent and Graphic Content**

We remove content that glorifies violence or celebrates the suffering or humiliation of others because it may create an environment that discourages participation.

## **Violence and Incitement**

We aim to prevent potential offline harm that may be related to content on Facebook. While we understand that people commonly express disdain or disagreement by threatening or calling for violence in non-serious ways, we remove language that incites or facilitates serious violence. We remove content, disable accounts, and work with law enforcement when we believe there is a genuine risk of physical harm or direct threats to public safety. We also try to consider the language and context in order to distinguish casual statements from content that constitutes a credible threat to public or personal safety. In determining whether a threat is credible, we may also consider additional information like a person's public visibility and the risks to their physical safety.

## **Dangerous Individuals and Organizations**

In an effort to prevent and disrupt real-world harm, we do not allow any organizations or individuals that proclaim a violent mission or are engaged in violence to have a presence on Facebook. This includes organizations or individuals involved in the following:

- Terrorist activity
- Organized hate
- Mass murder (including attempts) or multiple murder
- Human trafficking
- Organized violence or criminal activity

We also remove content that expresses support or praise for groups, leaders, or individuals involved in these activities.

## **Coordinating Harm and Publicizing Crime**

In an effort to prevent and disrupt offline harm and copycat behavior, we prohibit people from facilitating, organizing, promoting, or admitting to certain criminal or harmful activities targeted at people, businesses, property or animals.

## **Bullying and Harassment**

Bullying and harassment happen in many places and come in many different forms, from making threats to releasing personally identifiable information, to sending threatening messages, and making unwanted malicious contact. We do not tolerate this kind of behavior because it prevents people from feeling safe and respected on Facebook.

We distinguish between public figures and private individuals because we want to allow discussion, which often includes critical commentary of people who are featured in the news or who have a large public audience. For public figures, we remove attacks that are severe as well as certain attacks where the public figure is directly tagged in the post or comment. For private individuals, our protection goes further: we remove content that's meant to degrade or shame, including, for example, claims about someone's sexual activity. We recognize that bullying and harassment can have more of an emotional impact on minors, which is why our policies provide heightened protection for users between the ages of 13 and 18.

## **Cruel and Insensitive**

We believe that people share and connect more freely when they do not feel targeted based on their vulnerabilities. As such, we have higher expectations for content that we call cruel and insensitive, which we define as content that targets victims of serious physical or emotional harm. We remove explicit attempts to mock victims[.]

# Exhibit 17

— ANONYMOUS WHISTLEBLOWER DISCLOSURE —

[REDACTED]

SEC Office of the Whistleblower  
Via Online Portal & Fax

Re: Supplemental Disclosure of Securities Law Violations by Facebook, Inc. (NASDAQ: FB), SEC TCR # [REDACTED]

**Facebook misled investors and the public about the negative consequences of its algorithms, which claim to prioritize “meaningful social interactions” or “MSI” (e.g., reshares of friends’ posts) but which actually promote virality of polarizing misinformation and hate speech.**

To the SEC Office of the Whistleblower:

1. The instant letter is one of multiple disclosures related to the above-captioned matter. Our anonymous client is disclosing original evidence showing that **Facebook, Inc. (NASDAQ: FB)** has, for years past and ongoing, violated U.S. securities laws by making **material misrepresentations and omissions in statements to investors and prospective investors**, including, *inter alia*, through filings with the SEC, testimony to Congress, online statements and media stories.
2. **Summary.** Since 2018, Facebook (and in particular Mark Zuckerberg) has prioritized “meaningful social interactions” or “MSI,” which means that its algorithms are more likely to show content that is predicted to get reactions or “content” (e.g., comments, reshares, or “likes”) from friends or family. However, although Facebook promotes “MSI” as being beneficial for relationships and wellbeing, the algorithm increases divisive, hateful content.

---

Whistleblower Aid is a U.S. tax-exempt, 501(c)(3) organization, EIN 26-4716045.

<https://WhistleblowerAid.org> — Anonymously via **Tor Browser**:

<http://p6ufg73qskew53cglxt6hktyt35rbl46yultzyuytq3tvicywa3pclid.onion>

Contact via **SecureDrop** over Tor: <http://whistlebloweraid.securedrop.tor.onion> — via **Signal App**: +1 201-773-1371

---

## **BACKGROUND AND MATERIAL MISSTATEMENTS AND OMISSIONS**

3. As background, **“meaningful social interactions” or “MSI” is defined as:**

*“[A]ll **interactions between two users** where the initiator is not the same as receiver (e.g. a like on a friend reshare, or a comment reply to a user’s comment on a public post).”<sup>1</sup>*

4. Facebook’s public priority shifted to “MSI” because it was a way to increase “content” on the platform (e.g., a reshare of a friend’s post is considered “content”) when content was otherwise in decline in 2018.
5. “Downstream MSI” is the process by which:

*A user posts content, then it gets shown to a viewer using an algorithm (d\_share\_msi\_score), who then reshares the content, which then creates “downstream MSI” through likes/reactions, comments, comment likes/reactions, and comment replies to and from the viewer’s friends, who then continue to reshare the content and so on.<sup>2</sup>*

6. **In 2018, Mark Zuckerberg announced a shift from prioritizing “time spent” on Facebook to focusing on “meaningful social interactions,” emphasizing a focus on showing friend/family content in news feeds:**

*“[T]he time we all spend on Facebook is time well spent . . . we’ve always put friends and family at the core of the experience. Research shows that strengthening our relationships improves our well-being and happiness . . . Since there’s more public content than posts from your friends and family, the balance of what’s in News Feed has shifted away from the most important thing Facebook can do -- help us connect with each other. . .*

*The research shows that when we use social media to connect with people we care about, it can be good for our well-being. We can feel more connected and less lonely, and that correlates with long term measures of happiness and health. . . I’m changing the goal I give our product teams from **focusing on helping you find relevant content to helping you have more meaningful social interactions.** . . . The first changes you’ll see will be in News Feed, where you can expect to see more from your friends, family and groups. . . . you’ll see less public content like posts from businesses, brands, and media. . . . the time you do spend on Facebook will be more valuable. And if we do the right thing, I believe that will be good for our community and*

---

<sup>1</sup> [REDACTED] *Deriving MSI Weight*, p. 5. Emphasis is added throughout this disclosure in bold/underlined text.

<sup>2</sup> [REDACTED] *Replacing Downstream MSI for Civic and Health*, p. 7.

---

*our business over the long term too. . . By focusing on bringing people closer together . . . Facebook is time well spent.”<sup>3</sup>*

7. **Facebook, and in particular Mark Zuckerberg, have continued to make these types of statements through the present time.** For example, in the March 2021 hearing “*Disinformation Nation: Social Media’s Role in Promoting Extremism and Misinformation*,”<sup>4</sup> Congressman Kinzinger asked:

*“So Mr. Zuckerberg, let me ask you: According to Hany Farid at Berkeley, numerous external studies and some of your own internal studies have revealed that **your algorithms are actively promoting divisive, hateful, and conspiratorial content because it engages users to spend more time. Do you think those studies are wrong?** And if not, what are you guys doing to reverse course on that?”*

8. Mark Zuckerberg responded:

*“For the rest of the content in News Feed and on Instagram, the main thing that I would say is I do think that there is quite a bit of misperception about how our algorithms work and what we optimize for. I have heard a lot of people say that we are optimizing for keeping people on the service. The way that we view this is that **we are trying to help people have meaningful social interactions.** People come to social networks to be able to connect with people. If we deliver that value, then it will be natural that people use our services more. But that is very different from setting up algorithms in order to just kind of try to tweak and optimize and get people to spend every last minute on our service, which is not how we designed the company or the services.”*

9. In Facebook’s Q4 2020 results conference call, Mark Zuckerberg stated:

*“So now that we’ve **helped billions of people stay connected** with friends and family, helping everyone find and **participate in communities that are meaningful to them has been our next goal.** We even updated our mission a few years ago to reflect this, making it: ‘give people the power to build community and bring the world closer together.’”<sup>5</sup>*

---

<sup>3</sup><https://about.fb.com/news/2018/01/news-feed-fyi-bringing-people-closer-together/>.

<sup>4</sup><https://docs.house.gov/meetings/IF/IF16/20210325/111407/HHRG-117-IF16-Transcript-20210325.pdf>.

<sup>5</sup>[https://s21.q4cdn.com/399680738/files/doc\\_financials/2020/q4/FB-Q4-2020-Conference-Call-Transcript.pdf](https://s21.q4cdn.com/399680738/files/doc_financials/2020/q4/FB-Q4-2020-Conference-Call-Transcript.pdf).

10. In addition, in its Notice of Annual Meeting and Proxy Statement in 2021, shareholders made a proposal to address widespread platform misuse. In opposing this proposal, Facebook represented:

*“[W]e have taken a number of steps to help prioritize News Feed content that is **more focused on meaningful interactions for our users**. In 2018, we made a fundamental change to the way content is surfaced in people’s News Feed to prioritize posts from friends and family . . . to try and **minimize the amount of divisive content that people see**. We have **reduced clickbait headlines**, reduced links to misleading and spam posts, and improved how comments are ranked to show people those that are more relevant and of **higher quality**. . . . We also regularly partner with external researchers in efforts to better understand the impact of platforms like ours on social issues . . . . Given our **efforts and transparency around our actions to counter platform misuse**. . . [we are] against this proposal.”<sup>6</sup>*

11. Similarly, Facebook has made misstatements in its public pages. For example, in its public page on “Bringing People Closer Together,” Facebook outlines:

*“Today we use signals like how many people react to, comment on or share posts to determine how high they appear in News Feed.*

*With this update, we will also prioritize posts that spark conversations and meaningful interactions between people. To do this, we will predict which posts you might want to interact with your friends about, and show these posts higher in feed. These are posts that inspire back-and-forth discussion in the comments and posts that you might want to share and react to—whether that’s a post from a friend seeking advice, a friend asking for recommendations for a trip, or a news article or video prompting lots of discussion . . .*

***Using ‘engagement-bait’ to goad people into commenting on posts is not a meaningful interaction, and we will continue to demote these posts in News Feed.**”<sup>7</sup>*

### **SUMMARY OF ORIGINAL EVIDENCE**

12. Facebook’s records confirm that Facebook’s statements were false.
13. Internal documents highlight how prioritizing “MSI” such as “reshares” actually furthers misinformation and other divisive, low-quality content:

<sup>6</sup><https://www.sec.gov/Archives/edgar/data/1326801/000132680121000022/facebook2021definitiveprox.htm>.

<sup>7</sup><https://www.facebook.com/business/news/news-feed-fyi-bringing-people-closer-together>.

“Our ranking systems have specific separate predictions for not just what you would engage with, but what we think you may pass along so that others may engage with. Unfortunately, **research has shown how outrage and misinformation are more likely to be viral**, and recent experiments that deprecate these models indicate that **removing these models does positively impact metrics for misinformation and hate**.”<sup>8</sup>

“Feedback and UX research with news publishers and political actors also suggests that share downstream **MSI is leading them to post more divisive and sensationalist content in order to gain distribution**.”<sup>9</sup>

“The result was a bit concerning: net sentiment was inversely correlated with FB-generated traffic (outbound clicks). In other words: **the more negative comments a piece of content instigates, the higher likelihood for the link to get more traffic** . . . might reach the conclusion that darker, more divisive content is better for business.”<sup>10</sup>

“Taking all US outbound clicks and comment sentiment scores on posts linking to \*the same\* popular domain in the US (3wk dataset), I find the following:

There’s a (visible) general correlation between negative correlation between negative comment sentiment and number of outbound clicks (imperfect proxy for VPVs). From a publisher’s point of view, this data would seem to encourage posting more content that leads to negatively charged comment threads.

Chart: To each url, assign a net sentiment score = 95th percentile pos\_hi sentiment - 95th percentile neg\_hi sentiment. Binning by net\_sentiment\_score, plot the average number of clicks (blue) as well the 95th percentile num\_clicks (orange).”<sup>11</sup>

“Political parties . . . claim that Facebook’s algorithm change in 2018 (MSI) has **changed the nature of politics. For the worse**. They argue that the **emphasis on ‘reshareability’ systematically rewards provocative, low-quality content**.”<sup>12</sup>

<sup>8</sup> [REDACTED] We are Responsible for Viral Content, p. 5.

<sup>9</sup> [REDACTED] Replacing Downstream MSI for Civic and Health, p. 3.

<sup>10</sup> [REDACTED] Does Facebook Reward Outrage? Posts that generate negative reactions get more clicks, p. 2.

<sup>11</sup> [REDACTED] “Case Study: (Controlling for Publisher) Posts with Negatively Charged Comment Threads Fare Better in Feed”

<sup>12</sup> [REDACTED] Political Party response to the ‘18 Algorithm change, p. 1.

*“The problem is that we do not and possibly never will have a model that captures even a majority of integrity harms, particularly in sensitive areas . . . Hate Speech<sup>13</sup> is one of the ‘big three’ community integrity problems on Facebook (along with Nudity & Pornography and Graphic Violence). The hate speech team has a classifier for both predicted violating and also borderline hate speech . . . Misinformation is another core integrity problem . . . Even in the best of circumstances (e.g., in the US), the fact checkers have fairly slow response time and don’t check that many pieces of content. That means that content is often not caught until after it has gotten a lot of distribution, and many things are never caught. In most other countries, we do not have any fact-checking partners at all . . . we know that divisive content (particularly divisive political content) is one of the biggest problems facing the platform. . . So far, the existing technology does not appear to meet the bar for monitoring, not to mention demotion”<sup>14</sup>*

**“Reshares also seem to be associated with integrity problems disproportionately.”<sup>15</sup>**

14. Specifically, evidence outlines how harmful content is more viral (e.g., content eliciting anger produces more “reshares” and other indicators of “MSI”):

*“Our aim to foster more meaningful interactions (MSI) with close friends is deeply laudable. But **our approach has had unhealthy side effects on important slices of public content, such as politics and news.** As we will see, there is strong evidence that this is attributable to our downstream models.”*

*“comment thread **negativity correlates well with** expected value for **number of outbound clicks.**”<sup>16</sup>*

15. This has resulted in a notable increase in “negative” political posts:

*“Research conducted in the EU reveals that **political parties ‘feel strongly that the change to the algorithm has forced them to skew negative in their communications on Facebook, with the downstream effect of leading them into more extreme policy positions.’** For example, in Poland, ‘one party’s social media management team estimate that they have shifted*

<sup>13</sup> See also disclosure re. Hate Speech.

<sup>14</sup> [REDACTED] *Demoting on Integrity Signals is Not Enough*, p. 1-3.

<sup>15</sup> *Docs MSI Metric FAST Review 2019-11-14*, p. 19, 21, 26.

<sup>16</sup> [REDACTED] *Does Facebook Reward Outrage? Posts that generate negative reactions get more clicks*, p. 3.

*the proportion of their posts **from 50/50 positive/negative to 80% negative and 20% positive, explicitly as a function of the change to the algorithm** . . . Many parties, including those that have shifted strongly to the negative, **worry about the long-term effects** on democracy.’ We have heard similar feedback from parties in India and Taiwan. News publishers, too, are **concerned about the incentives MSI created.**”<sup>17</sup>*

*“Political parties across Europe claim that **Facebook’s algorithm change in 2018 (MSI) has changed the nature of politics. For the worse** . . . they feel that they have been forced to adapt to the change by producing far more negative content than before. . . Many parties. . . worry about the long-term effects on democracy. . . **they are trapped in an inescapable cycle of negative campaigning by the incentive structures of the platform** . . . evidence around how **anger reactions, overall, is weaponized** by political figures and creating negative incentives on the platform.”<sup>18</sup>*

16. In particular, “downstream MSI” prioritizes “interactions” over quality:

*“**The principal way MSI works** on such public content, however, **is via downstream models**, particularly `d_share_msi_score`. **Because MSI is designed to boost friend interactions, it doesn’t value whether you’ll like a piece of content posted by the New York Times, Donald Trump, the Wall Street Journal, etc.** Instead, the way such content creators can **contribute to MSI is by posting content that you might reshare** for your friends to engage on or reshare themselves. This is precisely what we predict and uprank via `d_share_msi_score`.”<sup>19</sup>*

17. Facebook knows that “downstream MSI” or “deep reshared” content that is reshared multiple times is more likely to contain harmful content:

*“Our observational results confirm that for Groups posts deeper reshares are associated with higher prevalence of FUSS Red or Yellow content to about depth 10 [define] . . . Overall Red and Yellow content can be quite high--it can add up to about 20% of total VPVs [“View Port Views”, the company term of art for viewer impressions] . . . **The multi group picker looks great for increasing engagement--MSI, sharing, and many other metrics are up. Unfortunately post repetitiveness goes up also and that may be the biggest issue** . . . the problematic content is indeed associated with higher*

<sup>17</sup> [REDACTED] Replacing Downstream MSI for Civic and Health, p. 8.

<sup>18</sup> [REDACTED] Political Party response to the '18 Algorithm change, p. 4, 24, 26.

<sup>19</sup> [REDACTED] Replacing Downstream MSI for Civic and Health, p. 9.

reshare depths up to depth 10.”<sup>20</sup>

“**[R]eshare depth** [the number of shares in the chain from a given piece of shared content] **is correlated with misinformation** . . . other integrity harms also correlate with reshare depth.”<sup>21</sup>

18. Further, internal teams have identified these issues with MSI and proposed recommendations to address the harms (without losing other value):

**“We propose to re-weight the existing predictive models that comprise the scoring function for Civic posts in feed to better optimize for both integrity outcomes and individual civic value . . . Currently, Newsfeed ranks all posts by primarily optimizing for Sessions and MSI. For Civic posts in particular, however, we believe Newsfeed should rank for different objectives.”**<sup>22</sup>

“Why do we think we need to change the ranking objective for Civic posts? 1. We have evidence that people think that political content on Facebook is low quality, untrustworthy, and divisive. So our current ranking objectives are not creating a wholly valuable civic experience for users . . . 2. User’s perceptions of valuable civic content does not always line up with civic content that scores highest for them. 3. **Our current ranking objectives do not optimize for integrity outcomes, which can have dangerous consequences. For example, the downstream MSI model, while designed to increase overall MSI, was contributing hugely to Civic misinfo. Its removal for Civic posts is going to result in a 30 - 50% decrease in Civic misinformation.**”<sup>23</sup>

“These experiments strongly suggested that **we could reduce distribution of link misinfo by 40-50% and photo misinfo by 20-30% in these topics,** compared to a 10-15% reduction in civic distribution and a 15-20% reduction in health distribution overall.”<sup>24</sup>

**“A ranking change which reduces ranking based on max reshare depth produces significant wins on a variety of integrity measures . . .**

Observed reductions in integrity harms including misinformation, N&P [nudity

<sup>20</sup> [REDACTED] Groups Reshare Depth, p. 2, 17.

<sup>21</sup> [REDACTED] Max Reshare Depth experiment, p. 2-3.

<sup>22</sup> [REDACTED] Product brief – ranking for civic health, p. 1.

<sup>23</sup> [REDACTED] Product brief – ranking for civic health, p. 2.

<sup>24</sup> [REDACTED] Replacing Downstream MSI for Civic and Health, p. 11.

and pornography], violence, disturbing, and bullying varied from 2-15% with no impact to DAP, time spent, or sessions. **However, achieving such a win in practice might require a change in the way we formulate and goal on MSI,** as the current formulation of MSI is explicitly reduced by a reduction in sharing behaviors despite other core engagement measures being unmoved.”

25

An experiment **setting a maximum reshare depth found “Reshares were reduced significantly** . . . greatly reducing MSI. Users instead redirected their attention to other sources . . . This suggests that the specific shares reduced may not have been as important to users’ experiences as MSI would indicate. If so, it would further suggest **MSI is not capturing user value precisely** . . . opening the door for further optimizations which could have net increases to both user value and integrity concerns . . . This sort of ranking change may be a net win in terms of moving the integrity-engagement frontier outward. However, achieving such a win in practice might require a change in the way we formulate and goal on MSI.”<sup>26</sup>

**“An effective, content-agnostic approach to mitigate the harms posed by high-harm misinfo** (e.g. civic or health) would be to dampen virality within these topics **by hard demoting all deep reshares** where the viewer is not a friend or follower of the original poster . . . it is easily scalable and could catch loads of misinfo that might never be caught by classifiers or human reviewers . . . there’s minimal risk of unfairness . . . In the US [ ] This could **reduce civic link misinfo VPVs [n.b. viewer impressions] by 25% and civic photo misinfo VPVs by 50%.**”<sup>27</sup>

“[W]e . . . realized **MSI currently has lacked an important dimension around social context and content quality** . . . we ran a big interaction-level meaningfulness survey to understand better how meaningful people feel interactions are that tend to be associated with lower quality and some integrity problems (eg some types of reactions, reshares).”<sup>28</sup>

“There’s a growing set of research showing that some viral channels are used for bad . . . we’ve also identified **opportunities where reducing virality may**

25 [REDACTED] Max Reshare Depth experiment, p. 1.

26 [REDACTED] Max Reshare Depth experiment, p. 4-5.

27 [REDACTED] Fighting high harm misinfo with deep reshare damping.

28 [REDACTED] MSI Metric Changes for 2020H1, p. 1.

**significantly reduce prevalence of Integrity problems (10% in some cases)**, across the Family of Apps . . .”<sup>29</sup>

“We have further [MSI] rules under consideration (these could be added to the metrics”: “Engagement bait comments,” “Bullying comments,” “Other integrity rules,” and “Various user-level capping schemes.”<sup>30</sup>

19. For instance, integrity and other teams developed tracking metrics for these types of issues (related to prioritizing “MSI”):

“spam comments, single character comments, deleted comments, engagement bait comments, and bullying comments . . . Engagement bait [encompasses] Comments that goad users into interacting with likes, shares, comments, and other actions . . . to take advantage of our News Feed algorithm by boosting engagement in order to get greater reach.”<sup>31</sup>

20. In fact, in India, Facebook adopted a “hybrid-MSI” approach to address the above-referenced issues (but did not use similar measures elsewhere):

“[W]e found that **an MSI heavy optimization strategy was hurting Android DAP in India and we could recover the DAP losses by reducing the emphasis on MSI** and increasing emphasis on video in the form of In Feed Recommendations (IFR) . . . we had identified 11 countries where we were following a more balanced strategy of MSI mixed with appropriate amounts of video [i.e., non-MSI public content] . . . **So it is right to think of the ranking strategy . . . as a hybrid MSI optimization approach subject to constraints and guardrails.**”<sup>32</sup>

21. For example, in a proposal to cap the number of comments for each user (to address issues with high-volume commenters and fake engagement):

“Approximately 3M users per day would hit the proposed cap of 100 comments per day . . . Over the course of one week 10.5M commenters would hit the cap at least once . . . over the course of one month 28M commenters would hit the cap at least once.”<sup>33</sup>

22. Teams also proposed:

<sup>29</sup> [REDACTED] Virality Reduction as Integrity Strategy.pdf, p. 1

<sup>30</sup> [REDACTED] Metric Changes in the next couple of weeks to make MSI capture more useful social interactions, p. 2.

<sup>31</sup> [REDACTED] Comment Quality: Integrity Deltoid Metrics, p. 1, 7.

<sup>32</sup> [REDACTED] MSI Revisited Part 4, p. 3-4.

<sup>33</sup> [REDACTED] Commentor Capping (I), p. 3.

*"If the same author, on same post created 10 short (< = 5 characters) comments or more, filter them all out from the metric . . ." Examples include short repeated comments such as: "the ones who shouldn't die died because of you." "Fucking garbage!!" "fuck your mother! Why don't you just die" "Monkey" "Die loyal fans" "Crazy woman" "Thief" etc.<sup>34</sup>*

23. Likewise, while tests to give "anger" reactions lower weight finally occurred in late 2020 (a year after knowing that would decrease violating, low quality content), these measures were only temporary in scope (despite being effective):

*[2019] "**We find that angrys, hahas, wows seem more frequent on civic low quality news, civic misinfo, civic toxicity, health misinfo, and health antivax content** . . . while loves, sorrys and likes are typically less frequent on these integrity harms". . . **Comments with good motifs [e.g., "love" icon] are 15x less likely to be violating** . . . 1.5x less likely to be hateful . . . 18% more likely to be high quality."<sup>35</sup>*

*"[W]e find that civic content classified as toxic has 2X more hahas and 33% more angers than it has heart reactions . . . In particular, we consistently find that shares, angrys, and hahas are much more frequent on civic low quality news, civic misinfo, civic toxicity, health misinfo, and health antivax content . . . Comments are often . . . also more frequent on these Integrity harms."<sup>36</sup>*

*"[W]e want to see if we should change the MSI weight for different reaction types . . . [for example] we see that the anger and haha reactions are highly prevalent on misinfo and toxicity. They are also connected to subjective bad experiences (Haha is an especially high predictor of civic content viewers rate to be not important, trustworthy, or good for their communities [After further review of integrity evidence below, we decided the evidence for Anger is stronger than for Haha])."<sup>37</sup>*

*[2020] "**MSI weights for each reaction type have been re-evaluated. . . Anger reactions have been set to a weight of 0 . . . Content dominated by anger reactions is significantly more likely to go against community standards** while also showing mixed results in MSI surveys. Note that **this launch is temporary** until core models get updated to exclude anger. At that time, in a few weeks from now, this launch will be reversed."<sup>38</sup>*

<sup>34</sup> [REDACTED] Filtering out low value interactions from MSI, p. 7, 47.

<sup>35</sup> [REDACTED] FAST Review 2019-11-14, p. 19, 21, 26.

<sup>36</sup> [REDACTED] A Quick Look at MSI Components and Integrity, p. 2-5.

<sup>37</sup> [REDACTED] Reaction weight Revisions 2020H2, p. 1, 3.

<sup>38</sup> [REDACTED] Using p(anger) to reduce the impact angry reactions have on ranking levers, p. 1.

24. **However, Mark Zuckerberg refused to adopt recommendations to combat harmful content** (even hate speech and content invoking violence off of the platform) if it impacted his “metric” of “meaningful social interactions” or “MSI”. For example, after specialists met in April 2020 to discuss suggestions for “soft actions” to reduce the prevalence of bad content in “News Feed,” it was summarized:

*“Downstream model depreciation: **Mark doesn’t think we could go broad . . . We wouldn’t launch if there was a material tradeoff with MSI impact.**”<sup>39</sup>*

25. Furthermore, as outlined by former employees and other internal records:

*“(1) I think FB is probably having a net negative influence on politics in Western countries; (2) **I don’t think that leadership is involved in a good-faith effort to fix this** . . . Facebook could substantially decrease the amount of harmful political content by being more opinionated on quality. **I have seen a dozen proposals to measure the objective quality of content on News Feed diluted or killed** because either (1) they have a disproportionate impact across the US political spectrum, typically harming conservative content more; or (2) they cannot be framed in terms of subjective quality (“what the users want”) . . . Facebook’s content policy decisions are routinely influenced by political considerations.”<sup>40</sup>*

*“time and again **I’ve seen promising interventions from integrity product teams, with strong research and data support, be prematurely stifled or severely constrained by key decision makers**--often based on fears of public and policy stakeholder responses . . . Out of fears over potential public and policy stakeholder responses, **we are knowingly exposing users to risks of integrity harms.** [ ] For example, we’ve known for over a year now that our recommendation systems can very quickly lead users down the path to conspiracy theories and groups . . . . The end result is . . . . falling victim to integrity harms that are facilitated or amplified by unforeseen interactions between features and surfaces . . . **To discourage harmful content distribution** . . . **we should** . . . Identify ways to remove or reduce engagement boosts for high confidence predicted low-integrity content . . . e.g., **continue to explore solutions like removing downstream MSI boosts for sensitive content** . . .”<sup>41</sup>*

<sup>39</sup> [REDACTED] Mark Feedback on Soft Action Proposal + Deck presented to Mark, p. 1-2.

<sup>40</sup> [REDACTED] Last Day at Facebook - Badge Post, p. 1-2.

<sup>41</sup> [REDACTED] Badge Post - DS Misinfo, p. 2-4, 16.

**“Facebook’s decision-making on content policy is routinely influenced by political considerations.** . . . Communications and Public Policy teams . . . often block changes when they see that they could harm powerful political actors . . . We can and should set up a firewall between content-policy and other parts of the company.”<sup>42</sup>

### **MATERIALITY AND CONCLUSION**

**26. This is a material issue.** For example, Facebook conceded in its 10-K:<sup>43</sup>

*“[F]rom time to time we update our News Feed ranking algorithm to optimize the user experience, and these changes have had, and may in the future have, the effect of reducing time spent and some measures of user engagement with Facebook, which could adversely affect our financial results.”*

*“In addition, we have been, and may in the future be, subject to negative publicity in connection with our handling of misinformation and other illicit or objectionable use of our products or services, including in connection with the COVID-19 pandemic and elections in the United States and around the world. Any such negative publicity could have an adverse effect on the size, engagement, and loyalty of our user base and marketer demand for advertising on our products, which could result in decreased revenue and adversely affect our business and financial results, and we have experienced such adverse effects to varying degrees from time to time.”*

**27. Role for the SEC.** The SEC is charged with enforcing the laws that protect investors in public companies like Facebook. Facebook’s investors care about misrepresentations and omissions by Mark Zuckerberg and other Facebook executives on the topic of how its algorithms and business priorities impact harmful content, such as hate speech and misinformation for two reasons. First, to the extent that users become aware of the dangers and limitations that Facebook platforms present, they are likely to use the platforms less, leading to lower advertising revenue and lower profits. Second, some investors simply will not want to invest in a company that prioritizes a metric (“MSI”) over quality content and user experience and then engages in misstatements and omissions on the topic.

---

<sup>42</sup> [REDACTED] *Political Influence Content Policy*, p. 2, 6, 12, 23.

<sup>43</sup> <https://sec.report/Document/0001326801-21-000014/>.

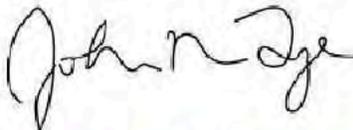
28. Whistleblower Aid is a non-profit legal organization that helps workers report their concerns about violations of the law safely, lawfully, and responsibly. We respectfully request the SEC's assistance ensuring that our client never faces retaliation.

29. On information and belief, none of the documents enclosed here constitute attorney-client communications, were obtained during a meeting with an attorney, or otherwise indicate that they are in any way privileged.

30. We plan to continue supplementing this disclosure with additional information and evidence. Our client would be happy to meet with investigators at your convenience. Please feel free to contact us using the information below.

31. We are representing an anonymous whistleblower who is making the above disclosures solely for reporting the suspected violation of laws as outlined.

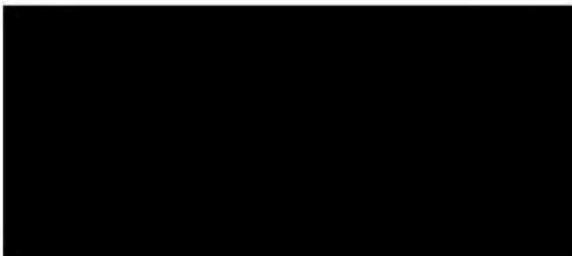
Sincerely,

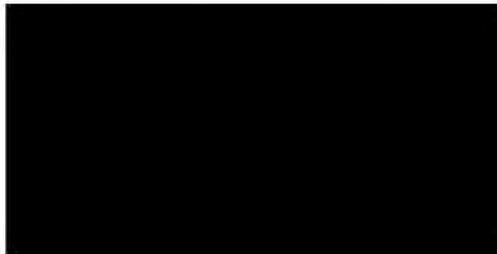


John N. Tye, Attorney at Law  
Chief Disclosure Officer



Andrew Bakaj, Attorney at Law  
Of Counsel





Enclosures: Internal Facebook documents including —

- Deriving MSI Weight
- Replacing Downstream MSI for Civic and Health Mark Feedback on Soft Action Proposal + Deck presented to Mark
- Political Party response to the '18 Algorithm change
- Product brief – ranking for civic health
- Demoting on Integrity Signals is Not Enough
- Groups Reshare Depth
- A drill-down Analysis of MSI/VPV and Distribution of Expert Posts
- Max Reshare Depth experiment
- Fighting high harm misinfo with deep reshare damping
- MSI Revisited Part 4
- Last Day at Facebook - Badge Post
- Badge Post - DS Misinfo
- Political Influence Content Policy
- Using p(anger) to reduce the impact angry reactions have on ranking levers
- We are Responsible for Viral Content
- Metric Changes for 2020H1
- FAST Review 2019-11-14
- Metric Changes in the next couple of weeks to make MSI capture more useful social interactions
- Commentor Capping (I)
- A Quick Look at MSI Componenteets [sic] and Integrity
- Comment Quality: Integrity Deltoid Metrics
- Filtering out low value interactions from MSI
- Reaction weight Revisions 2020H2
- Does Facebook Reward Outrage?

# Exhibit 18

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit <https://www.djreprints.com>.

<https://www.wsj.com/articles/facebook-ai-enforce-rules-engineers-doubtful-artificial-intelligence-11634338184>

# Facebook Says AI Will Clean Up the Platform. Its Own Engineers Have Doubts.

AI has only minimal success in removing hate speech, violent images and other problem content, according to internal company reports

By [Deepa Seetharaman](#), [Jeff Horwitz](#) and [Justin Scheck](#)

Oct. 17, 2021 9:17 am ET

**F**acebook Inc. executives have long said that artificial intelligence would address the company's chronic problems keeping what it deems hate speech and excessive violence as well as underage users off its platforms.

That future is farther away than those executives suggest, according to internal documents reviewed by The Wall Street Journal. Facebook's AI can't consistently identify first-person shooting videos, racist rants and even, in one notable episode that puzzled internal researchers for weeks, the difference between cockfighting and car crashes.

On hate speech, the documents show, Facebook employees have estimated the company removes only a sliver of the posts that violate its rules—a low-single-digit percent, they say. When Facebook's algorithms aren't certain enough that content violates the rules to delete it, the platform shows that material to users less often—but the accounts that posted the material go unpunished.

The employees were analyzing Facebook's success at enforcing its own rules on content that it spells out in detail internally and in public documents like its community standards.



— Facebook senior engineer and research scientist

The documents reviewed by the Journal also show that Facebook two years ago cut the time human reviewers focused on hate-speech complaints from users and made other tweaks that reduced the overall number of complaints. That made the company more dependent on AI enforcement of its rules and inflated the apparent success of the technology in its public statistics.

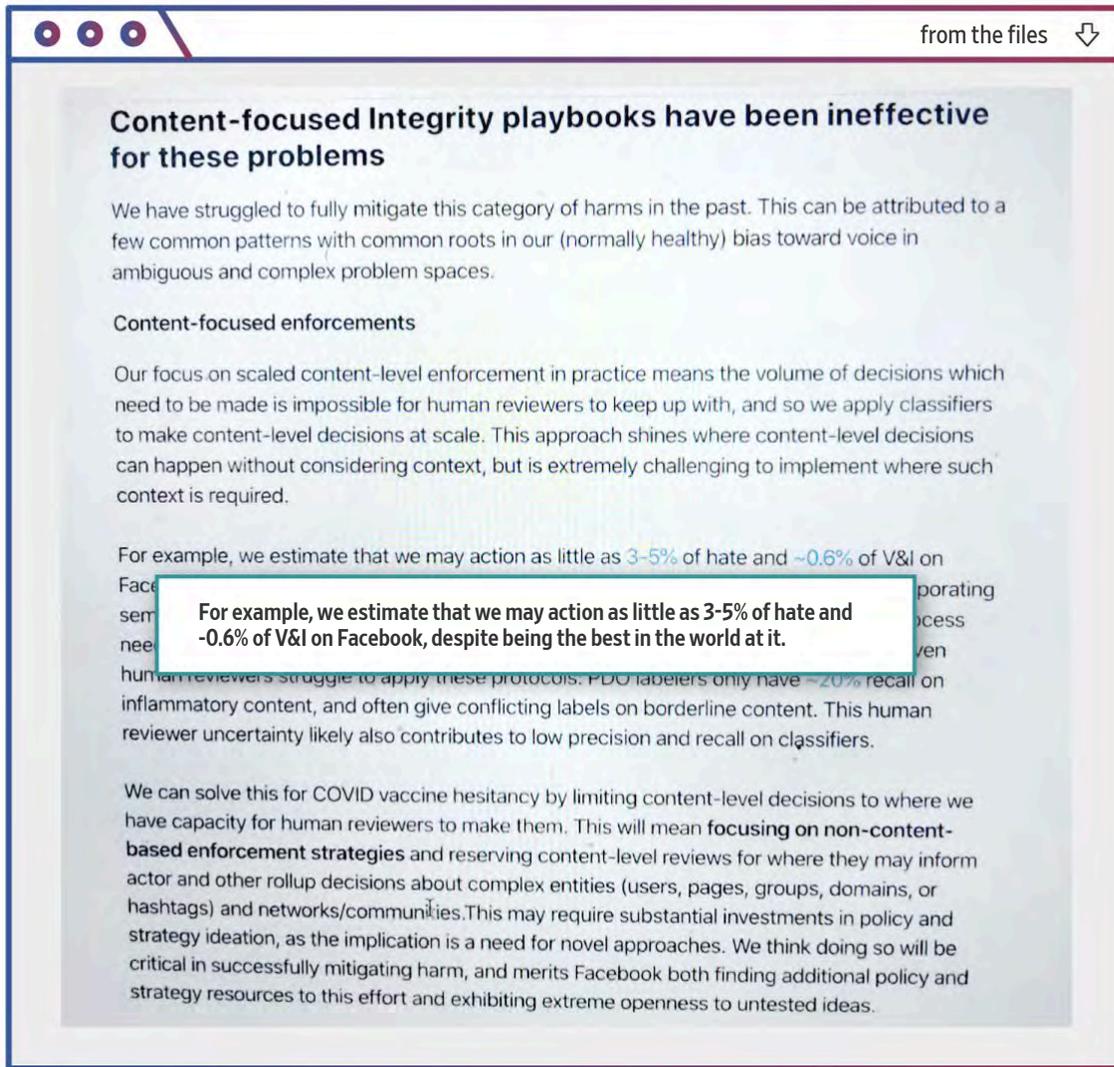
According to the documents, those responsible for keeping the platform free from content Facebook deems offensive or dangerous acknowledge that the company is nowhere close to being able to reliably screen it.

“The problem is that we do not and possibly never will have a model that captures even a majority of integrity harms, particularly in sensitive areas,” wrote a senior engineer and research scientist in a mid-2019 note.

He estimated the company’s automated systems removed posts that generated just 2% of the views of hate speech on the platform that violated its rules. “Recent estimates suggest that unless there is a major change in strategy, it will be very difficult to improve this beyond 10-20% in the short-medium term,” he wrote.

This March, another team of Facebook employees drew a similar conclusion, estimating that those systems were removing posts that generated 3% to 5% of the views of hate speech on the platform, and 0.6% of all content that violated Facebook’s policies against violence and incitement.





Source: Internal report titled, "Harmful Non-Violating Narratives" is a Problem Archetype in Need of Novel Solutions'

Facebook spokesman Andy Stone said that these percentages referred to posts that were removed using AI, and didn't include other actions the company takes to reduce how many people view hate speech, including ranking posts lower in news feeds. Facebook says by that measure, the prevalence of content that violates its policies has been shrinking, and that is what the company considers its most important enforcement metric.

The statistics contrast starkly with the confidence in AI presented by Facebook's top executives, including CEO Mark Zuckerberg, who previously said he expected Facebook would use AI to detect "the vast majority of problematic content" by the end of 2019.

The company often says that nearly all of the hate speech it takes down was discovered by AI before it was reported by users. It calls this figure its proactive detection rate, and it had reached nearly 98% as of earlier this year.



Civil rights groups and academics have long been skeptical that the AI detection rate shows meaningful progress, saying it doesn't seem to match user experiences or their own studies. "They won't ever show their work," said Rashad Robinson, president of the civil rights group Color of Change, which helped organize an advertiser boycott of Facebook last year due to what it called the company's failure to control hate speech.

"We ask, what's the numerator? What's the denominator? How did you get that number?" he said. "And then it's like crickets."

---

## [THE FACEBOOK FILES »](#)

---

[Facebook Files](#)

[Sign up here](#)

---

In an interview, Facebook's head of integrity, Guy Rosen, said it was more important to look at other data points that show the amount of hate speech shrinking as a percentage of what people see on the platform overall. Facebook says five out of every 10,000 content views contained hate speech, an improvement from roughly 10 of every 10,000 views in mid-2020, according to its latest public report on how it enforces its policies, for the second quarter of this year.

"Prevalence is the most important metric, and it represents not what we caught, but what we missed, and what people saw, and it's the primary metric we hold ourselves accountable to," Mr. Rosen said. "We've been successful in moving it down, and it's the one that we really focus on."

Mr. Stone, the spokesman, said Facebook executives have increasingly emphasized this measurement in their public comments. He said much of the improvement has come because AI ranks suspected content lower to give it less visibility.

Mr. Rosen also said the documents reviewed by the Journal were outdated, but that they had informed Facebook's broader thinking about AI-driven content moderation.

Last month, the company said its AI systems were getting better at "proactively removing content that violates our standards on hate speech" and said it was removing 15 times more of this content than in 2017.

systems at the heart of its business success.

The Journal's series, based on the documents and interviews with current and former employees, describes how the company's rules favor elites; how its algorithms foster discord; that it has long known drug cartels and human traffickers use its services openly; and how Facebook is used by antivaccine activists, among other issues. An article about Instagram's effects on teenage girls' mental health spurred a Senate hearing in late September.

Examples of content that Facebook's AI should have detected but missed include close-up videos of a person shooting someone, and videos of car crashes with "dismemberment and visible innards," according to the documents. Other violations of Facebook's policies that slipped through AI were violent threats directed at transgender children.

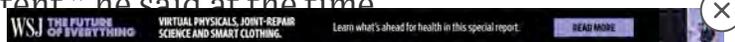


A memorial site for the shooting victims in Christchurch, New Zealand, in 2019. The attack was live streamed on Facebook.

PHOTO: VINCENT THIAN/ASSOCIATED PRESS

Facebook says it has spent about \$13 billion on "safety and security" since 2016, or nearly 4% of its revenue in that time. Mr. Rosen said that in 2016, Facebook's content-moderation system relied largely on user complaints and that the company has since built AI tools to find the objectionable content.

In 2018, Mr. Zuckerberg told a Senate committee that he was optimistic that within five to 10 years, Facebook would have the AI tools to proactively detect most hate speech. "Over the long term, building AI tools is going to be the scalable way to identify and root out most of this harmful content," he said at the time.



In July 2020, he told Congress: “In terms of fighting hate, we’ve built really sophisticated systems.”

A Facebook executive testified at the late-September Senate hearing that the company is using AI to keep kids under 13 off Instagram.

Facebook’s artificial-intelligence systems comb through billions of posts looking for items that might match the company’s definitions of content that violates its rules. The screening algorithms, called classifiers, are the bedrock of the company’s content-moderation system.

Building these classifiers is labor intensive and complex, requiring an army of humans to mark a vast number of posts based on a set of rules. Engineers then take these examples and train their systems to determine the probability that other posts violate the rules.

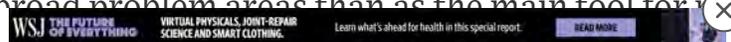
Facebook’s algorithms can automatically remove hate speech when they reach a certain level of confidence that the post violates policies, or they can push lower on feeds more questionable posts to limit their spread.

In some areas, such as with spam, Facebook’s classifiers work relatively well. But they often fall short in sensitive and controversial areas, especially when Facebook’s rules are complex and cultural context matters, according to the documents and people familiar with the matter.

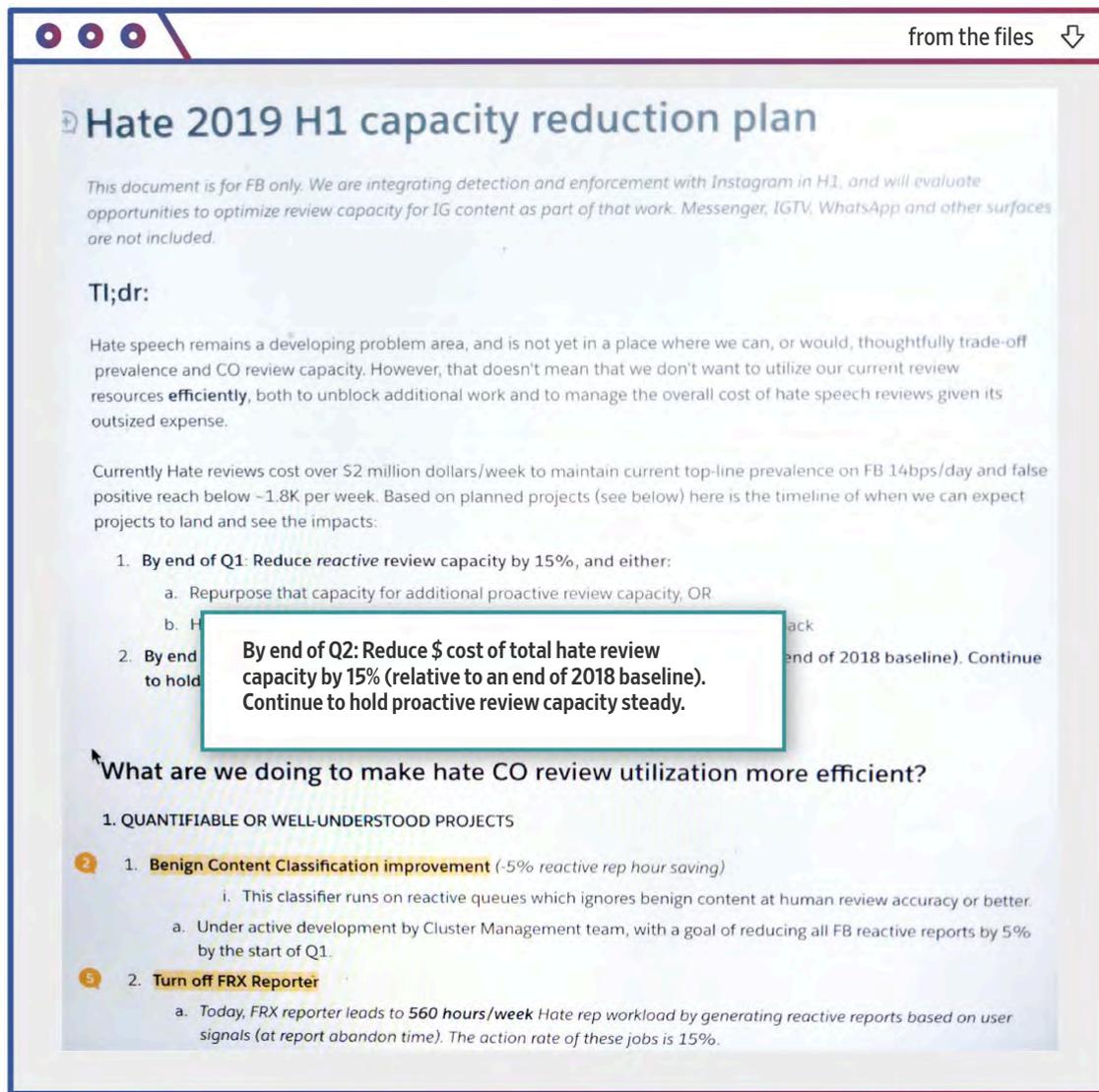
“The classifiers are like elementary school students and they need teachers (human reviewers) to grow into PhDs,” one Facebook engineer wrote in a discussion about hate-speech costs on Facebook’s internal employee platform in August 2019. Based on one measure of success, the engineer wrote, “our classifiers are still pretty naive.”

In one example, AI labeled a video of a carwash as a first-person shooter video, according to the documents. In another, it mistook a video of a shooting for a car crash.

Some employees say Facebook is misusing the classifiers, which they say are more effective as tools to flag broad problem areas than as the main tool for removing specific



In 2019, documents reviewed by the Journal show, Facebook introduced “hate speech cost controls” to save money on its human content review operations. Review of hate speech by human staff was costing \$2 million a week, or \$104 million a year, according to an internal document covering planning for the first half of that year.



Source: 2019 document titled 'Hate 2019 H1 capacity reduction plan'

“Within our total budget, hate speech is clearly the most expensive problem,” a manager wrote of the effort in a separate document, declaring that the cost of policing slurs and the denigration of minority groups, which Facebook rules bar, “adds up to real money.”

Mr. Stone, the spokesman, said the funds were shifted to hire more people to train Facebook’s algorithms and that the overall budget stayed steady.

Roughly 75% of the costs came from employing people to review user complaints, the vast

In 2019, beyond simply cutting the number of contractor hours dedicated to reviewing hate speech, the company began employing an algorithm that led them to ignore a larger percentage of user reports that the system deemed unlikely to be violations.

It also introduced “friction” to the content reporting process, adding hoops for aggrieved users to jump through that sharply reduced how many complaints about content were made, according to the documents.

“We may have moved the needle too far,” the author of one of the documents acknowledged of the company’s efforts to make it less likely that users would complete their reports on hate speech to the company.

The moves helped boost the company’s proactive detection rate, meaning, a greater proportion of the content that was removed was flagged by AI—the figure that is now nearly 98%. In December 2017, 24% of removed hate speech was detected by AI, and the rest from user reports, according to Facebook’s quarterly public report on how it enforces its policies.

Mr. Stone said the moves to ignore user reports deemed unlikely to be violations and the addition of friction weren’t intended to change the proactive detection rate but instead were intended to make the system more efficient. He added that some of that additional friction has since been rolled back.

The performance of Facebook’s automated systems illustrates how difficult it is for Facebook and other tech companies to build systems that reliably and comprehensively detect content that breaks their rules.

“This is one of the hardest problems in machine learning,” said J. Nathan Matias, an assistant professor at Cornell University. “It’s also an area that so many companies and policy makers have just decided was going to be the solution—without understanding the problem.”

The discrepancy between Facebook’s public claims about the effectiveness of its AI and



In 2016, pop star Selena Gomez flew to Facebook's Menlo Park headquarters to pose for pictures with Mr. Zuckerberg and Facebook's Chief Operating Officer Sheryl Sandberg to celebrate her status as the most-followed account on Instagram. Not long after, she was startled to read a user comment on one of her Instagram posts: "Go kill yourself," according to the star's spokesman.

She grew increasingly concerned about the spread of hate speech on these platforms, and in September 2020 she sent an Instagram message that she later posted on her account to Mr. Zuckerberg and Ms. Sandberg, saying the company had a "serious problem" with hate, misinformation, racism and bigotry.





selenagomez  
273M followers

[View profile](#)



[View more on Instagram](#)

2,914,635 likes  
selenagomez

When you meet the boss and talk tech in a very unusual office @zuck  
[view all 16,759 comments](#)

WSJ THE FUTURE OF EVERYTHING VIRTUAL PHYSICALS, JOINT-REPAIR SCIENCE AND SMART CLOTHING. Learn what's ahead for health in this special report. [READ MORE](#)

Ms. Gomez then followed up by email to ask why Facebook allowed hate groups to thrive on the site, according to emails reviewed by the Journal and previously reported by the Associated Press. Ms. Sandberg responded that Facebook's AI had detected 91% of the 1.5 million posts it removed for violating its rules against using symbols or phrases from hate groups.

Ms. Gomez wrote back that Ms. Sandberg hadn't addressed her broader questions, sending screenshots of Facebook groups that promoted violent ideologies.

"You refuse to even mention, let alone address, the problem Facebook has with white supremacists and bigots," Ms. Gomez wrote in an Oct. 10, 2020, email to Ms. Sandberg and other executives, adding that there were plenty of Facebook groups "full of hate and lies that might lead to people being hurt or, even worse, killed."

Ms. Gomez declined requests for further comment.

Mr. Stone said Ms. Sandberg has publicly highlighted Facebook's hate-speech prevalence figures this year.

Fadi Quran, a researcher at the human-rights group Avaaz, which advocates for citizen action in areas such as climate change and poverty, said he has repeatedly asked Facebook employees if they understood how much hate speech was on their platform and how much they acted on. "They said verbatim that that was almost impossible, and they can only report with certainty on what they detect," he said.

"By hiding the problem and giving the opposite impression—that the issue is under control—they're actually complicit in allowing those community violations to go forward with minimal accountability," he said.

Mr. Stone said Facebook provided Mr. Quran with public prevalence figures and other metrics.

In its quarterly public reports on how it enforces its policies, Facebook measures the prevalence of certain types of content, like hate speech, by the number of views that content attracts. The company says this is a more accurate way of measuring the true impact of a piece of content that violates its policies. In other words, hate speech viewed a million times is more of a problem than hate speech viewed just once.

The company doesn't publicly report what percentage of hate-speech views it removes. Internally, the company calculates this figure by applying their hate-speech classifiers to a sample of posts and then having humans review the same posts to see how much the classifiers missed, according to a person with direct knowledge of the estimates. The number is then used as an estimate for the amount of hate-speech views removed across the whole platform.



Guy Rosen, Facebook's head of integrity, during a 2018 interview on Frontline.

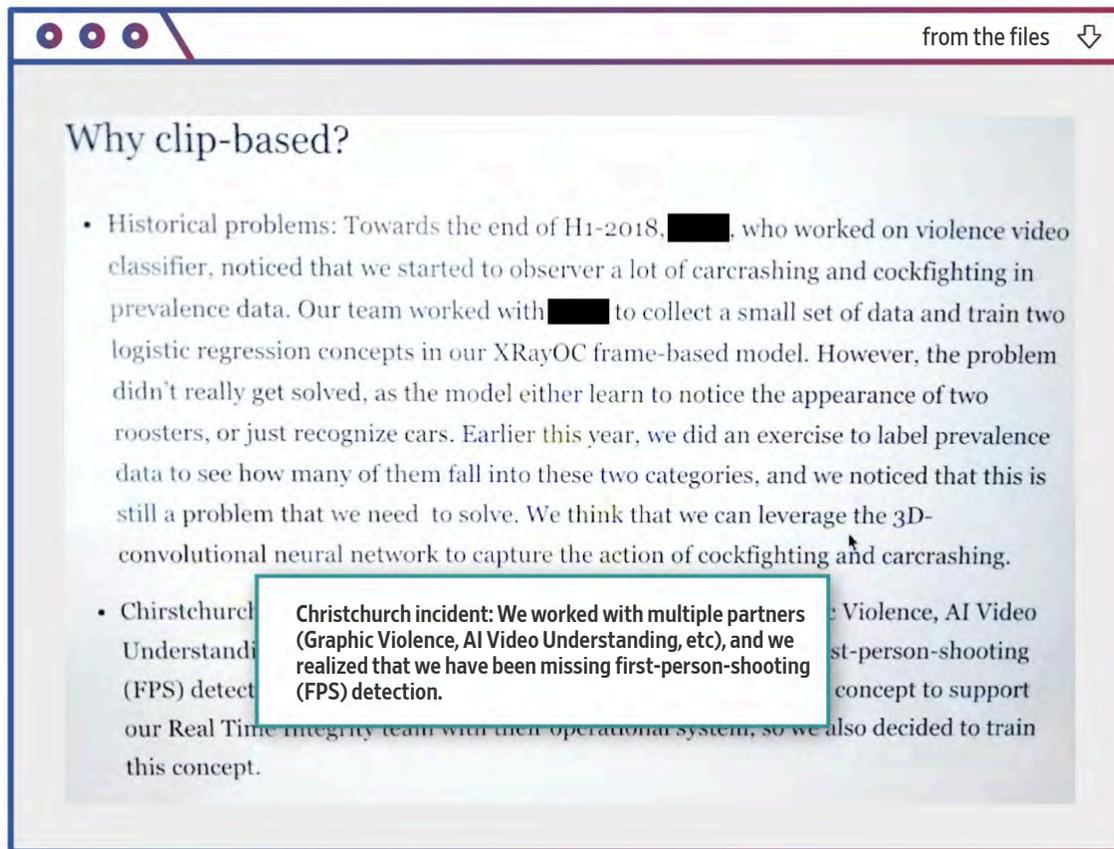
PHOTO: PHOTO COURTESY OF FRONTLINE

Mr. Rosen, the integrity chief, said in the interview that the company's quarterly public reports are evidence it is taking these problems seriously.

In mid-2018, an engineer noticed a troubling trend: "a lot of car crashing and cockfighting in prevalence data," he wrote in a 2019 internal report. Facebook users were finding in their feeds videos of crashing cars and fighting roosters, which would normally violate Facebook's rules. Data scientists weren't sure why.

The engineer and a team of colleagues trained an artificial intelligence system to recognize videos of cockfights and car crashes and weed them out. "However," the engineers wrote in a memo, "the problem didn't really get solved."





Note: A name has been redacted on this document.

Source: June 2019 internal note titled 'XRayOC 2019a clip-based model'

The same team hit obstacles around shootings recorded by the perpetrator, known as “first-person shooter” videos, the internal memo says. Three months before the memo was written, a man in Christchurch, New Zealand, used Facebook to live stream his fatal shooting of 51 people in two mosques.

In some cases, the AI didn't recognize shootings. In others, it mislabeled innocuous videos, such as paintball games, or the carwash, the researchers wrote.

The AI must also be trained in foreign languages.

According to a December 2020 memo, Facebook employees debated creating a hate-speech classifier for various Arabic dialects. But the lack of training data—such as samples of the various dialects—was a problem, especially since they were having trouble



Indian students and doctors protest in Assam state, India. A Facebook employee warned that hate speech related to ethnic violence in Assam was a major risk on the platform.

PHOTO: DAVID TALUKDAR/AGENCE FRANCE-PRESSE/GETTY IMAGES

WSJ THE FUTURE OF EVERYTHING VIRTUAL PHYSICALS, JOINT-REPAIR SCIENCE AND SMART CLOTHING. Learn what's ahead for health in this special report. READ MORE

— Facebook data scientist

which was previously reported by BuzzFeed.

The outgoing data scientist noted that despite intense investment by Facebook, the company's success rate at removing banned content remained dismal. "Each half [year] we make incremental progress on the amount of content we're able to proactively detect," he wrote. "But an incremental increase on a very small number is still a very small number."

"We might just be the very best in the world at it," he wrote, "but the best in the world isn't good enough to find a fraction of it."



*A Wall Street Journal investigation*

A series offering an unparalleled look inside the social-media giant's failings—and its unwillingness or inability to address them.

[VIEW THE FULL SERIES →](#)

Deepa.Seetharaman@wsj.com, Jeff Horwitz at  
Jeff.Horwitz@wsj.com and Justin Scheck at justin.scheck@wsj.com



# Exhibit 19

[Skip to main content](#)

Thank you for visiting nature.com. You are using a browser version with limited support for CSS. To obtain the best experience, we recommend you use a more up to date browser (or turn off compatibility mode in Internet Explorer). In the meantime, to ensure continued support, we are displaying the site without styles and JavaScript.

## Advertisement

Humanities & Social Sciences  
Communications

- [View all journals](#)
- [Search](#) 
- [Login](#) 
  
- [Explore content](#) 
- [About the journal](#) 
- [Publish with us](#) 
  
- [Sign up for alerts](#) 
- [RSS feed](#)

[nature](#) >

[humanities and social sciences communications](#) >

[articles](#) >

article

Angry by design: toxic communication and technical architectures

[Download PDF](#) 

- Article
- Open Access
- [Published: 30 July 2020](#)

# Angry by design: toxic communication and technical architectures

- [Luke Munn](#)✉ [ORCID: orcid.org/0000-0002-1018-7433](https://orcid.org/0000-0002-1018-7433)<sup>1</sup>

*Humanities and Social Sciences Communications* **volume 7**, Article number: 53 (2020)

- 8478 Accesses
- 4 Citations
- 194 Altmetric
- [Metrics details](#)

## Abstract

---

Hate speech and toxic communication online is on the rise. Responses to this issue tend to offer technical (automated) or non-technical (human content moderation) solutions, or see hate speech as a natural product of hateful people. In contrast, this article begins by recognizing platforms as designed environments that support particular practices while discouraging others. In what ways might these design architectures be contributing to polarizing, impulsive, or antagonistic behaviors? Two platforms are examined: Facebook and YouTube. Based on engagement, Facebook's Feed drives views but also privileges incendiary content, setting up a stimulus–response loop that promotes outrage expression. YouTube's recommendation system is a key interface for content consumption, yet this same design has been criticized for leading users towards more extreme content. Across both platforms, design is central and influential, proving to be a productive lens for understanding toxic communication.

[Download PDF](#) ↓

## Introduction

Hate speech online is on the rise (Oboler, 2016; Perrigo, 2019; Pachego and Melhuish, 2020)<sup>Footnote 1</sup>. The response to this rise has broadly taken two approaches to harm reduction on platforms. The first approach is technical, attempting to develop software models to detect and remove problematic content. Indeed over the last few years in particular, significant attention has been directed at abusive speech online, with huge amounts of work poured into constructing and improving automated systems (Pavlopoulos et al., 2017; Fortuna and Nunes, 2018). Articles in computer science and software engineering in particular often claim to have studied the failings of previous techniques and discovered a new method that finally solves the issue (Delort et al., 2011; Mulla and Palave, 2016; Tulkens et al., 2016). And yet the inventiveness of users and the ambiguity of language mean that toxic communication remains complex and difficult to address. Technical understanding of this content will inevitably be limited, explains researcher Robyn Caplan (quoted in Vincent, 2019), because automated systems are being asked to understand human culture—racial histories, gender relations, power dynamics and so on—“a phenomenon too fluid and subtle to be described in simple, machine-readable rules”.

The second approach is non-technical, stressing that hate speech online is a problem that only humans can address. This framing, not incorrectly, points out that automated interventions will always be inherently limited, unable to account for the nuances of particular contexts and the complexities of language. The response is to dramatically expand content moderation teams. In May 2018, for example, Facebook announced that it would be hiring 10,000 new workers into its trust and safety team (Freeman, 2018). However, the toll for those carrying out this kind of work, where hate speech, graphic images, and racist epithets must be carefully reviewed, is incredibly high, leading to depression and other mental health issues. In being forced to parse this material, workers “do not escape unscathed” (Madrigal, 2017). As well as the hazards of the content itself, employees are often under intense pressure to meet performance targets, an anxiety that only adds to the inherent psychological toll (Newton, 2019).

In addition to these two approaches, there also seems to be a popular assumption, evidenced in online comments and in more mainstream literature, that hate speech is the natural product of hateful people. One user stated that the toxic comments she encountered online were simply produced by rude and frustrated people, perhaps with a difficult background or early life, who have not been taught general

manners. Another blog post blames toxic communication on an inherently toxic individual, someone with a predilection for hating or bullying, racism or sexism (Jennings-Edquist, 2014). In this understanding, hate speech results from people translating their fundamental nastiness in the offline world into the online environment.

In contrast to the approaches and assumptions discussed above, this study adopts a design-centric approach. It seeks to understand how hate might be facilitated in particular ways by hate-inducing architectures. Just as the design of urban space influences the practices within it (Jacobs, 1992; Birenboim, 2018), the design of platforms, apps and technical environments shapes our behavior in digital space. This design is not a neutral environment that simply appears, but is instead planned, prototyped, and developed with particular intentions in mind. Indeed, a platform can be conceived as a set of “core design problems” (Tura et al., 2018, Table 1).

This method thus examines a platform’s interfaces, architectures, and functionality, focusing on the types of communicative practices and social interactions they afford (Bucher and Helmond, 2017). As Gillespie (2017, n.p.) argues, these structures:

are designed to invite and shape participation toward particular ends. This includes what kind of participation they invite and encourage; what gets displayed first or most prominently; how the platforms design navigation from content to user to exchange... and how they organize information through algorithmic sorting, privileging some content over others in opaque ways. And it includes what is not permitted, and how and why they police objectionable content and behavior.

A platform’s design is the result of certain decisions, and these decisions have influence. Acknowledging this influence allows us to draw “connections between the design (technical, economic, and political) of platforms and the contours of the public discourse they host” (Gillespie, 2015, p. 2). How might the design of technical environments be promoting toxic communication?

This project examined two notable platforms: Facebook and YouTube. Both platforms have millions or even billions of monthly active users. Both platforms have a global reach, with access available in hundreds of countries worldwide. And both have been linked to hate speech, online harassment, and more overt acts of physical violence in the “real world”. Both platforms are thus highly influential,

shaping the beliefs and ideologies of individuals, their media production and consumption, and their relations to others on an everyday basis.

Following the method sketched above, this analysis meant identifying key elements of the platform's design—the news feed or a recommendation engine, for instance. The analysis then honed in on these architectures and affordances, asking how this design operates, what is its logic, and what type of speech and behavior does it encourage. While using these platforms provided insight, these questions frequently also meant drawing on secondary literature from designers, platform users, and software engineers. This core design analysis was supplemented by two unstructured interviews. The first was with a young social media user. The second was with a former online community manager, whose previous role ranged from guiding forum discussions to offering user assistance and moderating content. Both of these inputs are drawn on at several points to offer a “vernacular” perspective on design (McVeigh-Schultz and Baym, 2015)—foregrounding how it is perceived and dealt with on a practical everyday level.

While this method is novel in some ways, the attention to the design of platforms and their potential to shape behavior is not unprecedented. Over the last few years, we have witnessed a confessional moment from the designers of platforms.<sup>Footnote 2</sup> Designers have admitted that their systems are addictive and exploit negative “triggers” (Lewis, 2017). They have explained that Facebook's design privileges base impulses rather than considered reflection (Bosker, 2016). Others have spoken about their tools “ripping apart the social fabric of how society works” (Vincent, 2017). And these confessions have been echoed with criticism and studies from others. Social media enables negative messages to be distributed farther and faster (Vosoughi et al., 2018) and its affordances enable anger to spread contagiously (Fan et al., 2016). The “incentive structures and social cues of algorithm-driven social media sites” amplify the anger of users over time until they “arrive at hate speech” (Fisher and Taub, 2018). In warning others of these negative social effects, designers have described themselves as canaries in the coal mine (Mac, 2019).

Indeed, we have already begun witnessing the fallout of platform-amplified hate. Shootings in El Paso, Pittsburgh, and Christchurch have been linked to users on Gab and 8chan (Mezzofiore and O'Sullivan, 2019; Silverstein, 2018). Ethnic violence against Rohingya has been connected to material circulating

on Facebook (Stevenson, 2018). And anti-Muslim Tweets have been correlated with anti-Muslim hate crime (Williams et al., 2020). These overt acts of hate in the “real world” materialize this issue and highlight its significant stakes. Toxic communication is not just a nuisance or a nasty byproduct of online environments, but has more fundamental implications for human rights. “Online hate is no less harmful because it is online”, stressed a recent U.N. report (Kaye, 2019): “To the contrary, online hate, with the speed and reach of its dissemination, can incite grave offline harm and nearly always aims to silence others”. Hate forms a broad spectrum with extremist ideologies at one end. Online environments allow users to migrate smoothly along this spectrum, forming a kind of pipeline for radicalization (O’Callaghan et al., 2015; Munn, 2019). In this respect, the hate-based violence of the last few years is not random or anomalous, but a logical result of individuals who have spent years inhabiting hate-filled spaces where racist, sexist, and anti-Semitic views were normalized.

Very recently, then, a new wave of designers and technologists have begun thinking about how to redesign platforms to foster calmer behavior and more civil discourse. How might design create ethical platforms that enhance users wellbeing (Han, 2019)? Could technology be designed in a more humane way (Harris, 2019)? And what would be the core principles and processes of such designs (Yablonski, 2019)? Identifying a set of hate-promoting architectures would allow designers and developers to construct future platforms that mitigate communication used to harass or harm, and instead construct more inclusive and affirmative environments.

This article picks up on this nascent work, tracing the relationship between technical architectures and toxic communication. It examines two highly influential global platforms, Facebook and YouTube, unpacking the design of several key features, identifying how they are problematic, and suggesting some possible alternatives.

## Platform analysis: Facebook

---

Facebook is the giant of social media. With 2.41 billion active users worldwide (Noyes, 2019), it is the largest platform, and arguably one of the most significant. On average, users spend 58 min every day on the platform (Molla and Wagner, 2018). While some signs indicate that the platform is plateauing

in terms of use, these statistics remain compelling and mean that it cannot be overlooked. From the perspective of this project, Facebook is a technically mediated environment where vast numbers of people spend significant amounts of time. Yet if the platform is influential, it is also increasingly recognized as detrimental. “As Facebook grew, so did the hate speech, bullying and other toxic content on the platform”, one investigation found (Frenkel et al., 2018), “when researchers and activists in Myanmar, India, Germany and elsewhere warned that Facebook had become an instrument of government propaganda and ethnic cleansing, the company largely ignored them”. What kinds of experiences are all of these users having, and how does the design of this environment contribute to this? Rather than calm and civil, this analysis will show how the platform’s affordances can induce experiences that are stressful and impulsive, establishing some of the key conditions necessary for angry communication.

A design approach to Facebook stresses that it was designed—a result of particular decisions made over time. For users, Facebook appears as a highly mature and highly refined environment. Every area has undergone meticulous scrutiny and crafting by teams of developers and designers. This provides the environment with a degree of stability and authority, even inevitability. In this sense, giants like Facebook claim a kind of de-facto standard: this is the way our communication media operates. Yet Facebook has evolved significantly since its inception. Launching in 2004, the site was billed as an “online directory”; in these early days, the site emulated the approach of MySpace, where each user had a profile, populated with fields for status, education, hobbies, relationships, and so on; in 2007, Facebook added a Mini-Feed feature that listed recent changes to friends profiles, and in 2011 Facebook released the Timeline that “told the story of your life” as a move away from the directory or database structures of the past (Albenesius, 2014). Rather than inevitable, then, the design evolution of Facebook reminds us that it has evolved through conscious decisions in response to a particular set of priorities (Fig. 1).

**Fig. 1: Early Facebook Screenshot.**

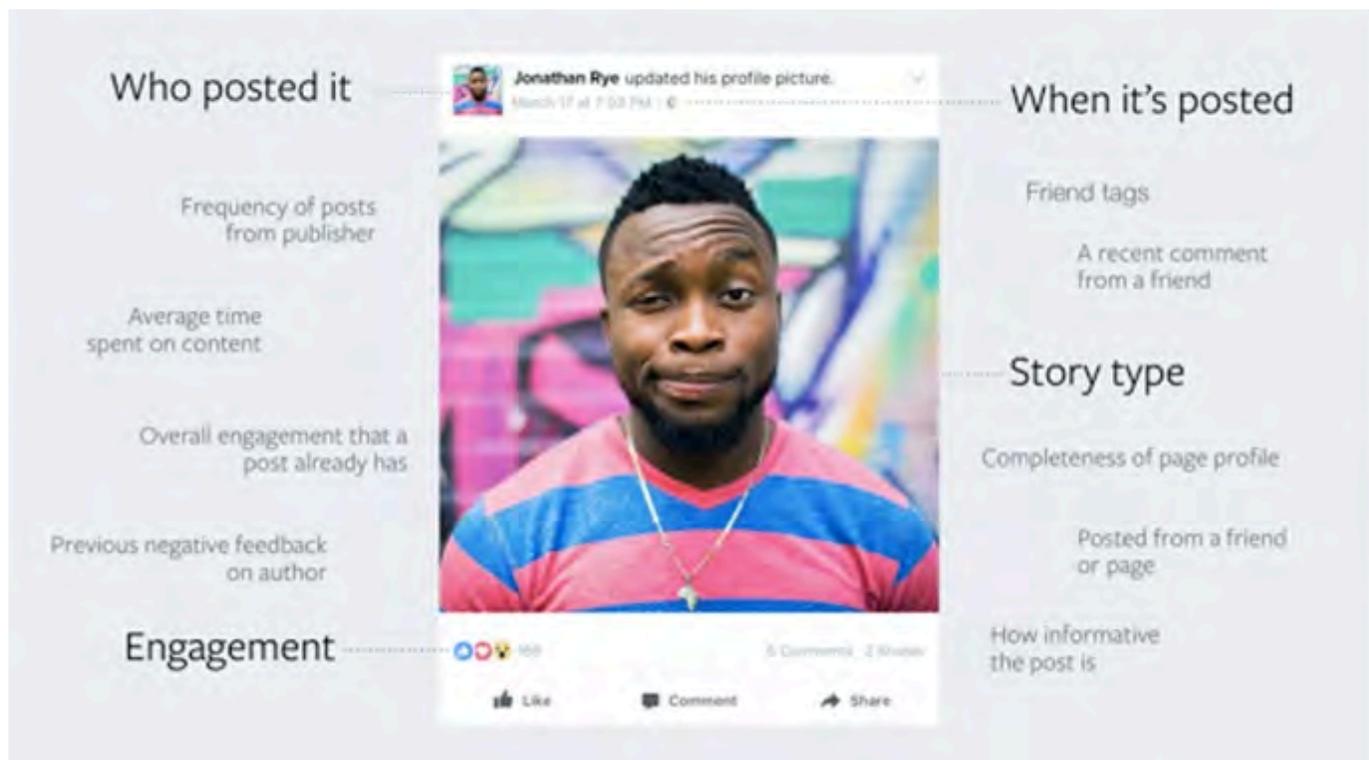


Early screenshot from “The Facebook” indicating its significant design progression over time.

Design wise, the Feed remains one of the key pieces of functionality within Facebook. The Feed, or the News Feed as it is officially known, is described by the company as a “personalized, ever-changing collection of photos, videos, links, and updates from the friends, family, businesses, and news sources you’ve connected to on Facebook” (Facebook, 2019). It is the first thing that users see when bringing up the app or entering the site. It is the center of the Facebook experience, the core space where content is presented to users. What’s more, because user actions are primed by this content and linked to it—whether commenting on a post, sharing an event, or liking a status update—the Feed acts as the gateway for most user activity, structuring the actions they will perform during that particular session. Indeed, for many users, Facebook is the Feed and the Feed is Facebook (Manjoo, 2017).

Key to the Feed is the idea of automatic curation. Before the Feed, users would have to manually visit each one of their friend's profile pages in order to discover what had changed in his or her life. Once introduced, the Feed now carries out this onerous task for each user. "It hunts through the network, collecting every post from every connection—information that, for most Facebook users, would be too overwhelming to process themselves" (Manjoo, 2017). In this sense, the Feed provides both personalization and convenience, assembling a list of updates and bringing them together into a single location. Yet from a critical design perspective (Dunne and Raby, 2001; Dunne, 2006; Bardzell and Bardzell, 2013), this begs some fundamental questions about values, ideologies, and norms. What is prioritized in this Feed, bubbling to the top of view and clamoring for a user's attention? What is deemphasized, only appearing after a long scroll to the bottom? And what are the factors that influence this invisible curation work? In short: what is shown, what is hidden, and how is this decided (see Fig. 2)?

**Fig. 2: News Criteria.**



Screenshot of Facebook page listing some of the criteria used by its News Feed.

The Feed is designed according to a particular logic. Since 2009, stories are not sorted chronologically, where updates from friends would simply be listed in reverse order, with the most recent appearing first (Wallaroo Media, 2019). While this change induced a degree of backlash from users, the chronology itself proved to be overwhelming, especially with the hundreds of friends that each user has. “If you have 1500 or 3000 items a day, then the chronological feed is actually just the items you can be bothered to scroll through before giving up”, explains analyst Benedict Evans (2018), “which can only be 10% or 20% of what’s actually there”. Instead, the Feed is driven by Engagement. In this design, Facebook weighs dozens of factors, from who posted the content to their frequency of posts and the average time spent on this piece of content. Posts with higher engagement scores are included and prioritized; posts with lower scores are buried or excluded altogether (see Fig. 3).

**Fig. 3: Content Prioritization.**

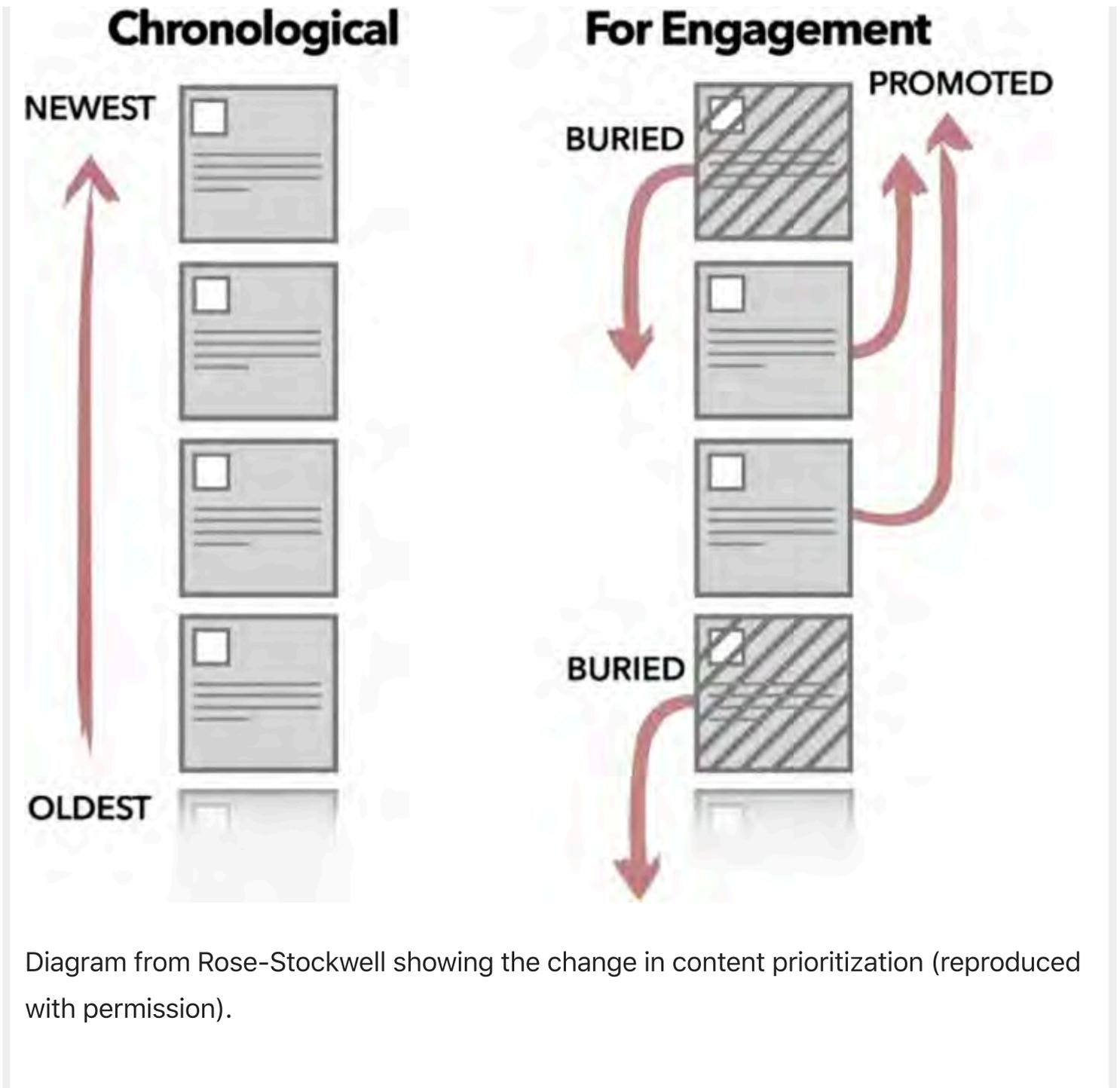


Diagram from Rose-Stockwell showing the change in content prioritization (reproduced with permission).

The problem with such sorting, of course, is that incendiary, polarizing posts consistently achieve high engagement (Levy, 2020, p. 627). This content is meant to draw engagement, to provoke a reaction. Indeed, in 2018 an internal research team at Facebook reported precisely this finding: by design it was feeding people “more and more divisive content in an effort to gain user attention and increase time on the platform” (Horwitz and Seetharaman, 2020). However, Facebook management ignored these findings and shelved the research.

This divisive material often has a strong moral charge. It takes a controversial topic and establishes two sharply opposed camps, championing one group while condemning the other. These are the headlines and imagery that leap out at a user as they scroll past, forcing them to come to a halt. This offensive material hits a nerve, inducing a feeling of disgust or outrage. “Emotional reactions like outrage are strong indicators of engagement”, observes designer and technologist Tobias Rose-Stockwell (2018), “this kind of divisive content will be shown first, because it captures more attention than other types of content”. While speculative, perhaps sharing this content is a way to offload these feelings, to remove their burden on us individually by spreading them across our social network and gaining some sympathy or solidarity.

The design of Facebook means that this forwarding and redistribution is only a few clicks away. As the user I interviewed stated: “it is so easy to share stuff”. Moreover, the networked nature of social media amplifies this single response, distributing it to hundreds of friends and acquaintances. They too receive this incendiary content and they too share, inducing what Rose-Stockwell (2018) calls “outrage cascades—viral explosions of moral judgment and disgust”. Outrage does not just remain constrained to a single user, but proliferates, spilling out to provoke other users and appear in other online environments.

At its worst, then, Facebook’s Feed stimulates the user with outrage-inducing content while also enabling its seamless sharing, allowing such content to rapidly proliferate across the network. In increasing the prevalence of such content and making it easier to share, it becomes normalized. Outrage retains its ability to provoke engagement, but in many ways becomes an established aspect of the environment. For neuroscientist Molly Crockett, this is one of the keys to understanding the rise of hate speech online. Crockett (2017, p. 770) stresses that “when outrage expression moves online it becomes more readily available, requires less effort, and is reinforced on a schedule that maximizes the likelihood of future outrage expression in ways that might divorce the feeling of outrage from its behavioral expression”. Design, in this sense, works to reduce the barrier to outrage expression. Sharing a divisive post to an audience of hundreds or thousands is just a click away.

How might the Feed be redesigned? Essentially there are two separate design problems here. Firstly, there is the stimulus aspect—the content included in the Feed. While the Feed’s filtering operations

undoubtedly remain highly technical, its logics can be understood through a design decision to elevate and amplify “engaging” content. Facebook has admitted that hate speech is a problem and has redesigned the Feed dozens of times since its debut in an effort to curtail this problem and the broader kind of misinformation that often stirs it up (Wallaroo Media, 2019). But the core logic of engagement remains baked into the design of the Feed at a deep level. Design, then, might start by experimenting quite concretely with different kinds of values. If the hyperlocal was privileged, for example, then posts from friends or community members in a 5 km radius might only be shown. This would be more mundane in many ways—everyday updates from those in our immediate vicinity rather than vicious attacks from anyone in a friend network. Or following the success of more targeted messaging apps like Messenger and WhatsApp, the Feed might emphasize close familial or friend connections above all. This pivot to a more intimate relational sphere would certainly be quieter and less “engaging” but ultimately more meaningful and civil.

Secondly, there is the response aspect—the platform affordances that make outrage expression online more effortless. Such expression is often impulsive, done in the moment, and so one possible design focus would be time itself. Temporality is a key part of community, stated the community manager I interviewed. “Legacy environments” such as traditional forums simply moved slower, she recalled, and in general there was “just more oxygen between things happening”. This time gap between reading and posting provided both a kind of deceleration and de-escalation, a chance to pause and reconsider. Rather than an instant reaction, would a built-in delay add a kind of emotional weight to such an action? An interval of a few seconds, even if nominal, might introduce a micro-reflection and suggest an alternative response. As a means of combating the effortless and abstract nature of outrage expression, Rose-Stockwell (2018) suggests a number of humanizing prompts that might be designed into platforms: an “empathetic prompt” that asks whether a user really wants to post hurtful content; an “ideological prompt” that stresses how this post will never be seen by those with opposing viewpoints; and a “public/private prompt” that would allow disagreements to take place between individuals rather than in the pressurized public arena. Such design interventions, while clearly not silver bullet solutions, might contribute in their own small way towards a more civil and less reactive online environment.

# Exhibit 20

S&P 500  
4,710.65  
+27.85 (+0.59%)



Dow 30  
36,245.89  
+158.44 (+0.44%)



Nasdaq  
15,978.88  
+125.04 (+0.79%)



U.S. markets close in 1 hour 31 minutes

thinkorswim trading Access thinkorswim web Open an account. E\*TRADE

yahoo!finance Register now

WEBINAR: Yahoo Finance Plus presents 'Energy: A Return to Fossil Fuels' Is the fossil fuel recovery real, or a stepping stone to a fossil-free future? Register now for our 11/17 webinar at 2PM...



Quote Lookup

yahoo!finance

# Exclusive: Facebook's Zuckerberg and Sandberg are this involved with the company's content issues

Andy Serwer with Max Zahn

September 9, 2019

In this article:

### Related Quotes

Symbol	Last Price	Change	% Change
<b>FB</b> Meta Platforms, Inc.	344.43	-3.13	-0.90%
<b>FB.BA</b> Meta Platforms, Inc.	9,080.00	-46.50	-0.51%
<b>FBOK34.SA</b> Meta Platforms, Inc.	67.70	+1.32	+1.99%

### TRENDING

1. UPDATE 1-U.S. intends to move forward on F-35 sale to UAE, U.S. official says
2. Citadel's Pablo Salame to Become Co-CIO as Yeh Departs
3. Large retailers 'have levers to manage inflation': Analyst
4. Activision Plummets on Report CEO Knew of Misconduct
5. S&P 500 Set for All-Time High on Economic Optimism: Markets Wrap

Just how hands-on are Mark Zuckerberg and Sheryl Sandberg when it comes to sensitive content issues at Facebook (FB)? According to top executives at the social media giant, they are “incredibly involved.”

That’s important because with Facebook under fire from regulators over questions on several fronts including possible antitrust violations, freedom of speech, data security, and national security, the focus of the company’s two top executives reflects the social media giant’s priorities and how it responds to myriad criticisms and challenges.

In an exclusive interview at Facebook’s Menlo Park headquarters with the three executives who oversee content at Facebook — Monika Bickert, Head of Global Policy Management; John DeVine, VP of Global Operations; and Guy Rosen, VP of Integrity — all three executives spoke at length about the efforts the company was making to moderate content and mitigate and adjudicate hot-button issues like hate speech, misinformation, and hacking. With 2.4 billion monthly users spread globally across the company’s four primary platforms — Facebook, Instagram, WhatsApp, and Messenger — it’s no small task.



How involved is Zuckerberg and Sandberg in Faceb...  
In an exclusive interview with Yahoo Finance Editor-in-Chief ...

### ‘The involvement is very deep’

The three executives who spoke to Yahoo Finance describe the process of navigating sensitive content issues as “nuanced” where intelligent and good-intentioned participants often disagree. And they,

**Stay ahead of the market**Get expert research, investment ideas and more. [Start your free trial today!](#)

“Any time that we're dealing with something that is close to the line or it's something where it's not really clear how the policies apply or it's something that's particularly important, we will, at the very least, send an email up to Mark and Sheryl so that they know what's going on,” Bickert told me. “Very often, we will end up having a back-and-forth with them about why we're making the decision we're making, and make sure they're OK with it.”



Facebook Head of Policy Management Monika Bickert participates in a discussion and question-and-answer session about 'Internet Security and Privacy in the Age of Islamic State' at the Washington Institute for Near [More](#)

I asked Bickert if this would include for instance the [doctored video of Nancy Pelosi](#) posted on Facebook that appeared to show her slurring her words or drunk. “With anything that is very big that a lot of people are talking about, we will absolutely loop them in,” said Bickert, who has testified before Congress twice on behalf of the company and who previously worked for 10 years as an Assistant U.S. Attorney for the Department of Justice.

Facebook decided to leave the Pelosi video up. But it directed anyone seeing the post to fact-checking sites that described how the footage was manipulated. [Bickert also told Anderson Cooper](#)

Facebook, though Facebook says it hasn't been removed. The video appeared on other sites, as well. Twitter kept the video up, while YouTube [reportedly took it down](#), stating that it violated its policies against deceptive practices.



Facebook was widely criticized — including by Pelosi herself — for keeping the video up, though again, it appears to be unfindable on Facebook at this point. It's just one example of what the company has to address, as well as the different responses by its social media competitors. It's also worth noting that there are all sorts of distorted images of President Donald Trump on social media, including Facebook.

With the president, as well as high-level Democrats, highly tuned to the vagaries of social media, it's understandable that Zuckerberg and Sandberg would want to be kept in the loop when these issues crop up. It might also make it difficult, however, for them later to suggest they were out of the loop when it comes to a content issue at the company.

"The leadership is very involved," says John DeVine, who's in charge of the global operations of content management, which includes overseeing the now 15,000 full-time, part-time employees, and contractors who monitor content. "At a minimum, on a weekly basis, we're all sitting down, the three of us, as well as a group of other people and Sheryl and Mark and going over some of our most important topics that week, to check to see, are we getting it right."

"Mark [is] incredibly involved in...the deepest, hardest, especially product issues, that we're looking

will likely continue for the foreseeable future.

*This is the first in a series of articles Yahoo Finance will be publishing from this interview.*



Reserve your ticket to AMS!

-

*Andy Serwer is editor-in-chief of Yahoo Finance. Follow him on Twitter: @serwer.*

#### Read more:

- [The most crucial distinction between generations right now](#)
- [Why Big Tech is the new Wall Street, Washington's whipping boy](#)
- [Jamie Dimon: Donald Trump should 'walk away' if he can't get a good deal with China](#)
- [Jamie Dimon: Donald Trump deserves 'some' credit for the strong economy](#)
- [Charlie Munger: Trump is not primarily responsible for US economic success](#)

*Follow Yahoo Finance on [Twitter](#), [Facebook](#), [Instagram](#), [Flipboard](#), [SmartNews](#), [LinkedIn](#), [YouTube](#), and [reddit](#).*

# Exhibit 21

# BuzzFeed News

REPORTING TO YOU

[SIGN IN](#)

[ABOUT US](#)

[GOT A TIP?](#)

[SUPPORT US](#)

[BUZZFEED.COM](#)

[SECTIONS](#) ▼

TRENDING

[Astroworld Tragedy](#)

[#FreedBritney](#)

[Kyle Rittenhouse Trial](#)

[“Unite The Right” Rally](#)

[Yassify Meme](#)

*BuzzFeed News; Getty Images*





TECH

# "Mark Changed The Rules": How Facebook Went Easy On Alex Jones And Other Right-Wing Figures

Facebook's rules to combat misinformation and hate speech are subject to the whims and political considerations of its CEO and his policy team leader.



**Ryan Mac**  
BuzzFeed News Reporter



**Craig Silverman**  
BuzzFeed Staff

Last updated on February 22, 2021, at 1:14 p.m. ET

Posted on February 21, 2021, at 9:59 a.m. ET

In April 2019, Facebook was preparing to ban one of the internet's most notorious spreaders of misinformation and hate, Infowars founder Alex Jones. Then CEO Mark Zuckerberg personally intervened.

Jones had gained infamy for claiming that the 2012 Sandy Hook elementary school massacre was a "giant hoax," and that the teenage survivors of the 2018 Parkland shooting were "crisis actors." But Facebook had found that he was also relentlessly spreading hate against various groups, including Muslims and trans people. That behavior qualified him for expulsion from the social network under the company's policies for "dangerous individuals and organizations," which required Facebook to also remove any content that expressed "praise or support" for them.

But Zuckerberg didn't consider the Infowars founder to be a hate figure, according to a person familiar with the decision, so he overruled his own internal experts and opened a gaping loophole: Facebook would permanently ban Jones and his company — but would not touch posts of praise and support for them from other Facebook users. This meant that Jones' legions of followers could continue to share his lies across the world's largest social network.

"Mark personally didn't like the punishment, so he changed the rules," a former policy employee told BuzzFeed News, noting that the original rule had already been in use and represented the product of untold hours of work between multiple teams and experts.

**"Mark personally didn't like the punishment, so he changed the rules."**

"That was the first time I experienced having to create a new category of policy to fit what Zuckerberg wanted. It's somewhat demoralizing when we have established a policy and it's gone through rigorous cycles.

Like, what the fuck is that for?" said a second former policy employee who, like the first, asked not to be named so they could speak about internal matters.

"Mark called for a more nuanced policy and enforcement strategy," Facebook spokesperson Andy Stone said of the Alex Jones decision, which also affected the bans of other extremist figures.

Zuckerberg's "more nuanced policy" set off a cascading effect, the two former employees said, which delayed the company's efforts to remove right-wing militant organizations such as the Oath Keepers, which were involved the Jan. 6 insurrection at the US Capitol. It is also a case study in Facebook's willingness to change its rules to placate America's right wing and avoid political backlash.

Internal documents obtained by BuzzFeed News and interviews with 14 current

Internal documents obtained by BuzzFeed News and interviews with 14 current and former employees show how the company's policy team — guided by Joel Kaplan, the vice president of global public policy, and Zuckerberg's whims — has exerted outsized influence while obstructing content moderation decisions, stymieing product rollouts, and intervening on behalf of popular conservative figures who have violated Facebook's rules.

In December, a former core data scientist wrote a memo titled, "Political Influences on Content Policy." Seen by BuzzFeed News, the memo stated that Kaplan's policy team "regularly protects powerful constituencies" and listed several examples, including: removing penalties for misinformation from right-wing pages, blunting attempts to improve content quality in News Feed, and briefly blocking a proposal to stop recommending political groups ahead of the US election.

Since the November vote, at least six Facebook employees have resigned with farewell posts that have called out leadership's failures to heed its own experts on misinformation and hate speech. Four departing employees explicitly cited the policy organization as an impediment to their work and called for a reorganization so that the public policy team, which oversees lobbying and government relations, and the content policy team, which sets and enforces the platform's rules, would not both report to Kaplan.

Facebook declined to make Kaplan or other executives available for an

Facebook declined to make Kaplan or other executives available for an interview. Stone, the company spokesperson, dismissed concerns about the vice president's influence.

"Recycling the same warmed over conspiracy theories about the influence of one person at Facebook doesn't make them true," he said. "The reality is big decisions at Facebook are made with input from people across different teams who have different perspectives and expertise in different areas. To suggest otherwise is absurd."

An integrity researcher who worked on Facebook's efforts to protect the democratic process and rein in radicalization said the company caused direct harm to users by rejecting product changes due to concerns of political backlash.

**"At some point Zuckerberg has to be held responsible for his role in allowing his platform to be weaponized."**

"Out of fears over *potential* public and policy stakeholder responses, we are *knowingly* exposing users to risks of integrity," they wrote in an internal note seen by BuzzFeed News. They quit in August.

Those most affected by Jones' rhetoric have taken notice, too. Lenny Pozner, whose 6-year-

old son Noah was the youngest victim of the Sandy Hook shooting, called the

**"At some point Zuckerberg has to be held responsible for his role in allowing his platform to be weaponized."**

"Out of fears over *potential* public and policy stakeholder responses, we are *knowingly* exposing users to risks of integrity," they wrote in an internal note seen by BuzzFeed News. They quit in August.

Those most affected by Jones' rhetoric have taken notice, too. Lenny Pozner, whose 6-year-old son Noah was the youngest victim of the Sandy Hook shooting, called the revelation that Zuckerberg weakened penalties facing the Infowars founder "disheartening, but not surprising." He said the company had made a promise to do better in dealing with hate and hoaxes following a 2018 letter from HONR Network, his organization for survivors of mass casualty events. Yet Facebook continues to fail to remove harmful content.

"At some point," Pozner told BuzzFeed News, "Zuckerberg has to be held responsible for his role in allowing his platform to be weaponized and for ensuring that the ludicrous and the dangerous are given equal importance as the factual."

# Exhibit 22

**UNITED STATES  
SECURITIES AND EXCHANGE COMMISSION  
Washington, D.C. 20549**

**FORM 10-K**

(Mark One)

- ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**  
For the fiscal year ended December 31, 2018
- or
- TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**  
For the transition period from \_\_\_\_\_ to \_\_\_\_\_  
Commission File Number: 001-35551

**FACEBOOK, INC.**

(Exact name of registrant as specified in its charter)

**Delaware** **20-1665019**  
(State or other jurisdiction of incorporation or organization) (I.R.S. Employer Identification Number)  
**1601 Willow Road, Menlo Park, California 94025**  
(Address of principal executive offices and Zip Code)  
**(650) 543-4800**  
(Registrant's telephone number, including area code)

**Securities registered pursuant to Section 12(b) of the Act:**

<b>Class A Common Stock, \$0.000006 par value</b>	<b>The Nasdaq Stock Market LLC</b>
(Title of each class)	(Name of each exchange on which registered)

**Securities registered pursuant to Section 12(g) of the Act:**

**None**  
(Title of class)

Indicate by check mark if the registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act. Yes  No

Indicate by check mark if the registrant is not required to file reports pursuant to Section 13 or Section 15(d) of the Act. Yes  No

Indicate by check mark whether the registrant (1) has filed all reports required to be filed by Section 13 or 15(d) of the Securities Exchange Act of 1934 (Exchange Act) during the preceding 12 months (or for such shorter period that the registrant was required to file such reports), and (2) has been subject to such filing requirements for the past 90 days. Yes  No

Indicate by check mark whether the registrant has submitted electronically every Interactive Data File required to be submitted pursuant to Rule 405 of Regulation S-T (§ 232.405 of this chapter) during the preceding 12 months (or for such shorter period that the registrant was required to submit such files). Yes  No

Indicate by check mark if disclosure of delinquent filers pursuant to Item 405 of Regulation S-K (§ 229.405 of this chapter) is not contained herein, and will not be contained, to the best of registrant's knowledge, in definitive proxy or information statements incorporated by reference in Part III of this Form 10-K or any amendment to this Form 10-K.

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer, a smaller reporting company, or an emerging growth company. See definition of "large accelerated filer," "accelerated filer," "smaller reporting company," and "emerging growth company" in Rule 12b-2 of the Exchange Act.

Large accelerated filer	<input checked="" type="checkbox"/>	Accelerated filer	<input type="checkbox"/>
Non-accelerated filer	<input type="checkbox"/>	Smaller reporting company	<input type="checkbox"/>
		Emerging growth company	<input type="checkbox"/>

If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13(a) of the Exchange Act.

Indicate by check mark whether the registrant is a shell company (as defined in Rule 12b-2 of the Exchange Act). Yes  No

The aggregate market value of the voting and non-voting stock held by non-affiliates of the registrant as of June 29, 2018, the last business day of the registrant's most recently completed second fiscal quarter, was \$486 billion based upon the closing price reported for such date on the Nasdaq Global Select Market.

On January 28, 2019, the registrant had 2,385,533,940 shares of Class A common stock and 468,455,860 shares of Class B common stock outstanding.

**DOCUMENTS INCORPORATED BY REFERENCE**

Portions of the registrant's Proxy Statement for the 2019 Annual Meeting of Stockholders are incorporated herein by reference in Part III of this Annual Report on Form 10-K to the extent stated herein. Such proxy statement will be filed with the Securities and Exchange Commission within 120 days of the registrant's fiscal year ended December 31, 2018.

---

---

**FACEBOOK, INC.**  
**FORM 10-K**  
**TABLE OF CONTENTS**

<a href="#"><u>Note About Forward-Looking Statements</u></a>	<a href="#"><u>3</u></a>
<a href="#"><u>Limitations of Key Metrics and Other Data</u></a>	<a href="#"><u>4</u></a>
<b><u>PART I</u></b>	
<a href="#"><u>Item 1. Business</u></a>	<a href="#"><u>5</u></a>
<a href="#"><u>Item 1A. Risk Factors</u></a>	<a href="#"><u>8</u></a>
<a href="#"><u>Item 1B. Unresolved Staff Comments</u></a>	<a href="#"><u>30</u></a>
<a href="#"><u>Item 2. Properties</u></a>	<a href="#"><u>30</u></a>
<a href="#"><u>Item 3. Legal Proceedings</u></a>	<a href="#"><u>30</u></a>
<a href="#"><u>Item 4. Mine Safety Disclosures</u></a>	<a href="#"><u>30</u></a>
<b><u>PART II</u></b>	
<a href="#"><u>Item 5. Market for Registrant's Common Equity, Related Stockholder Matters and Issuer Purchases of Equity Securities</u></a>	<a href="#"><u>31</u></a>
<a href="#"><u>Item 6. Selected Financial Data</u></a>	<a href="#"><u>33</u></a>
<a href="#"><u>Item 7. Management's Discussion and Analysis of Financial Condition and Results of Operations</u></a>	<a href="#"><u>35</u></a>
<a href="#"><u>Item 7A. Quantitative and Qualitative Disclosures About Market Risk</u></a>	<a href="#"><u>54</u></a>
<a href="#"><u>Item 8. Financial Statements and Supplementary Data</u></a>	<a href="#"><u>55</u></a>
<a href="#"><u>Item 9. Changes in and Disagreements with Accountants on Accounting and Financial Disclosure</u></a>	<a href="#"><u>84</u></a>
<a href="#"><u>Item 9A. Controls and Procedures</u></a>	<a href="#"><u>84</u></a>
<a href="#"><u>Item 9B. Other Information</u></a>	<a href="#"><u>84</u></a>
<b><u>PART III</u></b>	
<a href="#"><u>Item 10. Directors, Executive Officers and Corporate Governance</u></a>	<a href="#"><u>85</u></a>
<a href="#"><u>Item 11. Executive Compensation</u></a>	<a href="#"><u>85</u></a>
<a href="#"><u>Item 12. Security Ownership of Certain Beneficial Owners and Management and Related Stockholder Matters</u></a>	<a href="#"><u>85</u></a>
<a href="#"><u>Item 13. Certain Relationships and Related Transactions, and Director Independence</u></a>	<a href="#"><u>85</u></a>
<a href="#"><u>Item 14. Principal Accounting Fees and Services</u></a>	<a href="#"><u>85</u></a>
<b><u>PART IV</u></b>	
<a href="#"><u>Item 15. Exhibits, Financial Statement Schedules</u></a>	<a href="#"><u>86</u></a>
<a href="#"><u>Signatures</u></a>	



## NOTE ABOUT FORWARD-LOOKING STATEMENTS

This Annual Report on Form 10-K contains forward-looking statements within the meaning of the Private Securities Litigation Reform Act of 1995. All statements contained in this Annual Report on Form 10-K other than statements of historical fact, including statements regarding our future results of operations and financial position, our business strategy and plans, and our objectives for future operations, are forward-looking statements. The words "believe," "may," "will," "estimate," "continue," "anticipate," "intend," "expect," and similar expressions are intended to identify forward-looking statements. We have based these forward-looking statements largely on our current expectations and projections about future events and trends that we believe may affect our financial condition, results of operations, business strategy, short-term and long-term business operations and objectives, and financial needs. These forward-looking statements are subject to a number of risks, uncertainties and assumptions, including those described in Part I, Item 1A, "Risk Factors" in this Annual Report on Form 10-K. Moreover, we operate in a very competitive and rapidly changing environment. New risks emerge from time to time. It is not possible for our management to predict all risks, nor can we assess the impact of all factors on our business or the extent to which any factor, or combination of factors, may cause actual results to differ materially from those contained in any forward-looking statements we may make. In light of these risks, uncertainties and assumptions, the future events and trends discussed in this Annual Report on Form 10-K may not occur and actual results could differ materially and adversely from those anticipated or implied in the forward-looking statements.

We undertake no obligation to revise or publicly release the results of any revision to these forward-looking statements, except as required by law. Given these risks and uncertainties, readers are cautioned not to place undue reliance on such forward-looking statements.

Unless expressly indicated or the context requires otherwise, the terms "Facebook," "company," "we," "us," and "our" in this document refer to Facebook, Inc., a Delaware corporation, and, where appropriate, its wholly owned subsidiaries. The term "Facebook" may also refer to our products, regardless of the manner in which they are accessed. For references to accessing Facebook on the "web" or via a "website," such terms refer to accessing Facebook on personal computers. For references to accessing Facebook on "mobile," such term refers to accessing Facebook via a mobile application or via a mobile-optimized version of our website such as m.facebook.com, whether on a mobile phone or tablet.

## LIMITATIONS OF KEY METRICS AND OTHER DATA

The numbers for our key metrics, which include our daily active users (DAUs), monthly active users (MAUs), and average revenue per user (ARPU), are calculated using internal company data based on the activity of user accounts. While these numbers are based on what we believe to be reasonable estimates of our user base for the applicable period of measurement, there are inherent challenges in measuring usage of our products across large online and mobile populations around the world. In addition, we are continually seeking to improve our estimates of our user base, and such estimates may change due to improvements or changes in our methodology.

We regularly evaluate these metrics to estimate the number of "duplicate" and "false" accounts among our MAUs. A duplicate account is one that a user maintains in addition to his or her principal account. We divide "false" accounts into two categories: (1) user-misclassified accounts, where users have created personal profiles for a business, organization, or non-human entity such as a pet (such entities are permitted on Facebook using a Page rather than a personal profile under our terms of service); and (2) undesirable accounts, which represent user profiles that we determine are intended to be used for purposes that violate our terms of service, such as spamming. The estimates of duplicate and false accounts are based on an internal review of a limited sample of accounts, and we apply significant judgment in making this determination. For example, to identify duplicate accounts we use data signals such as similar IP addresses or user names, and to identify false accounts we look for names that appear to be fake or other behavior that appears inauthentic to the reviewers. Our estimates may change as our methodologies evolve, including through the application of new data signals or technologies, which may allow us to identify previously undetected duplicate or false accounts and may improve our ability to evaluate a broader population of our users. Duplicate and false accounts are very difficult to measure at our scale, and it is possible that the actual number of duplicate and false accounts may vary significantly from our estimates.

In the fourth quarter of 2018, we estimate that duplicate accounts may have represented approximately 11% of our worldwide MAUs. We believe the percentage of duplicate accounts is meaningfully higher in developing markets such as the Philippines and Vietnam, as compared to more developed markets. In the fourth quarter of 2018, we estimate that false accounts may have represented approximately 5% of our worldwide MAUs. Our estimation of false accounts can vary as a result of episodic spikes in the creation of such accounts, which we have seen originate more frequently in specific countries such as Indonesia and Vietnam. From time to time, we may make product changes or take other actions to reduce the number of duplicate or false accounts among our users, which may also reduce our DAU and MAU estimates in a particular period.

Our data limitations may affect our understanding of certain details of our business. For example, while user-provided data indicates a decline in usage among younger users, this age data is unreliable because a disproportionate number of our younger users register with an inaccurate age. Accordingly, our understanding of usage by age group may not be complete.

In addition, our data regarding the geographic location of our users is estimated based on a number of factors, such as the user's IP address and self-disclosed location. These factors may not always accurately reflect the user's actual location. For example, a user may appear to be accessing Facebook from the location of the proxy server that the user connects to rather than from the user's actual location. The methodologies used to measure user metrics may also be susceptible to algorithm or other technical errors. Our estimates for revenue by user location and revenue by user device are also affected by these factors.

We regularly review our processes for calculating these metrics, and from time to time we may discover inaccuracies in our metrics or make adjustments to improve their accuracy, including adjustments that may result in the recalculation of our historical metrics. We believe that any such inaccuracies or adjustments are immaterial unless otherwise stated. We intend to disclose our estimates of the number of duplicate and false accounts among our MAUs on an annual basis. In addition, our DAU and MAU estimates will differ from estimates published by third parties due to differences in methodology.

The numbers of DAUs and MAUs discussed in this Annual Report on Form 10-K, as well as ARPU, do not include Instagram, WhatsApp, or Oculus users unless they would otherwise qualify as such users, respectively, based on their other activities on Facebook.

In addition, other user engagement metrics included herein do not include Instagram, WhatsApp, or Oculus unless otherwise specifically stated.

## PART I

### Item 1. Business

#### Overview

Our mission is to give people the power to build community and bring the world closer together.

Our top priority is to build useful and engaging products that enable people to connect and share with friends and family through mobile devices, personal computers, and other surfaces. We also help people discover and learn about what is going on in the world around them, enable people to share their opinions, ideas, photos and videos, and other activities with audiences ranging from their closest friends to the public at large, and stay connected everywhere by accessing our products, including:

- **Facebook.** Facebook enables people to connect, share, discover, and communicate with each other on mobile devices and personal computers. There are a number of different ways to engage with people on Facebook, including News Feed which displays an algorithmically-ranked series of stories and advertisements individualized for each person.
- **Instagram.** Instagram brings people closer to the people and things they love. It is a community for sharing photos, videos, and messages, and enables people to discover interests that they care about.
- **Messenger.** Messenger is a simple yet powerful messaging application for people to connect with friends, family, groups and businesses across platforms and devices.
- **WhatsApp.** WhatsApp is a simple, reliable and secure messaging application that is used by people and businesses around the world to communicate in a private way.
- **Oculus.** Our hardware, software, and developer ecosystem allows people around the world to come together and connect with each other through our Oculus virtual reality (VR) products.

We generate substantially all of our revenue from selling advertising placements to marketers. Our ads enable marketers to reach people based on a variety of factors including age, gender, location, interests, and behaviors. Marketers purchase ads that can appear in multiple places including on Facebook, Instagram, Messenger, and third-party applications and websites.

We are also investing in other consumer hardware products and a number of longer-term initiatives, such as connectivity efforts, artificial intelligence (AI), and augmented reality, to develop technologies that we believe will help us better serve our mission to give people the power to build community and bring the world closer together.

#### Competition

Our business is characterized by innovation, rapid change, and disruptive technologies. We compete with companies that sell advertising, as well as with companies that provide social, media, and communication products and services that are designed to engage users on the web, mobile devices and online generally. We face significant competition in every aspect of our business, including from companies that facilitate communication and the sharing of content and information, companies that enable marketers to display advertising, companies that distribute video and other forms of media content, and companies that provide development platforms for applications developers. We compete to attract, engage, and retain people who use our products, to attract and retain marketers, and to attract and retain developers to build compelling mobile and web applications that integrate with our products.

We also compete with the following:

- Companies that offer products across broad platforms that replicate capabilities we provide. For example, among other areas, we compete with Apple in messaging, Google and YouTube in advertising and video, Tencent in messaging and social media, and Amazon in advertising.
- Companies that provide regional social networks, many of which have strong positions in particular countries.
- Traditional, online, and mobile businesses that provide media for marketers to reach their audiences and/or develop tools and systems for managing and optimizing advertising campaigns.
- Companies that develop and deliver consumer hardware and virtual reality products and services.

As we introduce or acquire new products, as our existing products evolve, or as other companies introduce new products and services, we may become subject to additional competition.



## **Technology**

Our product development philosophy is centered on continuous innovation in creating and improving products that are social by design, which means that our products are designed to place people and their social interactions at the core of the product experience. As our user base grows, as engagement with products like video increases, and as we deepen our investment in new technologies like AI, our computing needs continue to expand. We make significant investments in technology both to improve our existing products and services and to develop new ones, as well as for our marketers and developers. We are also investing in protecting the security and integrity of our platform by investing in both people and technology to strengthen our systems against abuse.

## **Sales and Operations**

The majority of our marketers use our self-service ad platform to launch and manage their advertising campaigns. We also have a global sales force that is focused on attracting and retaining advertisers and providing support to them throughout the stages of the marketing cycle from pre-purchase decision-making to real-time optimizations to post-campaign analytics. We work directly with these advertisers, as well as through advertising agencies and resellers. We operate more than 60 offices around the globe, the majority of which have a sales presence. We also invest in and rely on self-service tools to provide direct customer support to our users and partners.

## **Marketing**

To date, our communities have grown organically with people inviting their friends to connect with them, supported by internal efforts to stimulate awareness and interest. In addition, we have invested and will continue to invest in marketing our products and services to grow our brand and help build community around the world.

## **Intellectual Property**

To establish and protect our proprietary rights, we rely on a combination of patents, trademarks, copyrights, trade secrets, including know-how, license agreements, confidentiality procedures, non-disclosure agreements with third parties, employee disclosure and invention assignment agreements, and other contractual rights. In addition, to further protect our proprietary rights, from time to time we have purchased patents and patent applications from third parties. We do not believe that our proprietary technology is dependent on any single patent or copyright or groups of related patents or copyrights. We believe the duration of our patents is adequate relative to the expected lives of our products.

## **Government Regulation**

We are subject to a variety of laws and regulations in the United States and abroad that involve matters central to our business. Many of these laws and regulations are still evolving and being tested in courts, and could be interpreted in ways that could harm our business. These may involve privacy, data protection and personal information, rights of publicity, content, intellectual property, advertising, marketing, distribution, data security, data retention and deletion, electronic contracts and other communications, competition, protection of minors, consumer protection, telecommunications, product liability, taxation, economic or other trade prohibitions or sanctions, securities law compliance, and online payment services. In particular, we are subject to federal, state, and foreign laws regarding privacy and protection of people's data. Foreign data protection, privacy, content, competition, and other laws and regulations can impose different obligations or be more restrictive than those in the United States. U.S. federal and state and foreign laws and regulations, which in some cases can be enforced by private parties in addition to government entities, are constantly evolving and can be subject to significant change. As a result, the application, interpretation, and enforcement of these laws and regulations are often uncertain, particularly in the new and rapidly evolving industry in which we operate, and may be interpreted and applied inconsistently from country to country and inconsistently with our current policies and practices.

Proposed or new legislation and regulations could also significantly affect our business. For example, the European General Data Protection Regulation (GDPR) took effect in May 2018 and applies to all of our products and services used by people in Europe. The GDPR includes operational requirements for companies that receive or process personal data of residents of the European Union that are different from those previously in place in the European Union, and includes significant penalties for non-compliance. Similarly, there are a number of legislative proposals in the European Union, the United States, at both the federal and state level, as well as other jurisdictions that could impose new obligations in areas affecting our business, such as liability for copyright infringement. In addition, some countries are considering or have passed legislation implementing data protection requirements or requiring local storage and processing of data or similar requirements that could increase the cost and complexity of delivering our services.

We are and expect to continue to be the subject of investigations, inquiries, data requests, actions, and audits by government authorities and regulators in the United States, Europe, and around the world, particularly in the areas of privacy, data protection, law enforcement, consumer protection, and competition, as we continue to grow and expand our operations. We are currently, and may in the future be, subject to regulatory orders or consent decrees. Orders issued by, or inquiries or enforcement actions initiated by,



government or regulatory authorities could cause us to incur substantial costs, expose us to unanticipated civil and criminal liability or penalties (including substantial monetary fines), or require us to change our business practices in a manner materially adverse to our business.

## **Employees**

As of December 31, 2018, we had 35,587 employees.

## **Corporate Information**

We were incorporated in Delaware in July 2004. We completed our initial public offering in May 2012 and our Class A common stock is listed on The Nasdaq Global Select Market under the symbol "FB." Our principal executive offices are located at 1601 Willow Road, Menlo Park, California 94025, and our telephone number is (650) 543-4800.

Facebook, the Facebook logo, FB, the Like button, Instagram, Oculus, WhatsApp, and our other registered or common law trademarks, service marks, or trade names appearing in this Annual Report on Form 10-K are the property of Facebook, Inc. or its affiliates. Other trademarks, service marks, or trade names appearing in this Annual Report on Form 10-K are the property of their respective owners.

## **Available Information**

Our website address is [www.facebook.com](http://www.facebook.com). Our Annual Report on Form 10-K, Quarterly Reports on Form 10-Q, Current Reports on Form 8-K, and amendments to reports filed pursuant to Sections 13(a) and 15(d) of the Securities Exchange Act of 1934, as amended (Exchange Act), are filed with the U.S. Securities and Exchange Commission (SEC). We are subject to the informational requirements of the Exchange Act and file or furnish reports, proxy statements, and other information with the SEC. Such reports and other information filed by us with the SEC are available free of charge on our website at [investor.fb.com](http://investor.fb.com) when such reports are available on the SEC's website. We use our [investor.fb.com](http://investor.fb.com) and [newsroom.fb.com](http://newsroom.fb.com) websites as well as Mark Zuckerberg's Facebook Page (<https://www.facebook.com/zuck>) as means of disclosing material non-public information and for complying with our disclosure obligations under Regulation FD.

The SEC maintains an Internet site that contains reports, proxy and information statements, and other information regarding issuers that file electronically with the SEC at [www.sec.gov](http://www.sec.gov).

The contents of the websites referred to above are not incorporated into this filing. Further, our references to the URLs for these websites are intended to be inactive textual references only.

## Item 1A. Risk Factors

*Certain factors may have a material adverse effect on our business, financial condition, and results of operations. You should consider carefully the risks and uncertainties described below, in addition to other information contained in this Annual Report on Form 10-K, including our consolidated financial statements and related notes. The risks and uncertainties described below are not the only ones we face. Additional risks and uncertainties that we are unaware of, or that we currently believe are not material, may also become important factors that adversely affect our business. If any of the following risks actually occurs, our business, financial condition, results of operations, and future prospects could be materially and adversely affected. In that event, the trading price of our Class A common stock could decline, and you could lose part or all of your investment.*

### Risks Related to Our Business and Industry

***If we fail to retain existing users or add new users, or if our users decrease their level of engagement with our products, our revenue, financial results, and business may be significantly harmed.***

The size of our user base and our users' level of engagement are critical to our success. Our financial performance has been and will continue to be significantly determined by our success in adding, retaining, and engaging active users of our products, particularly for Facebook and Instagram. We anticipate that our active user growth rate will generally decline over time as the size of our active user base increases, and it is possible that the size of our active user base may fluctuate or decline in one or more markets, particularly in markets where we have achieved higher penetration rates. For example, in the fourth quarter of 2017, we experienced a slight decline on a quarter-over-quarter basis in the number of daily active users on Facebook in the United States & Canada region. If people do not perceive our products to be useful, reliable, and trustworthy, we may not be able to attract or retain users or otherwise maintain or increase the frequency and duration of their engagement. A number of other social networking companies that achieved early popularity have since seen their active user bases or levels of engagement decline, in some cases precipitously. There is no guarantee that we will not experience a similar erosion of our active user base or engagement levels. Our user engagement patterns have changed over time, and user engagement can be difficult to measure, particularly as we introduce new and different products and services. Any number of factors could potentially negatively affect user retention, growth, and engagement, including if:

- users increasingly engage with other competitive products or services;
- we fail to introduce new features, products or services that users find engaging or if we introduce new products or services, or make changes to existing products and services, that are not favorably received;
- users feel that their experience is diminished as a result of the decisions we make with respect to the frequency, prominence, format, size, and quality of ads that we display;
- users have difficulty installing, updating, or otherwise accessing our products on mobile devices as a result of actions by us or third parties that we rely on to distribute our products and deliver our services;
- user behavior on any of our products changes, including decreases in the quality and frequency of content shared on our products and services;
- we are unable to continue to develop products for mobile devices that users find engaging, that work with a variety of mobile operating systems and networks, and that achieve a high level of market acceptance;
- there are decreases in user sentiment due to questions about the quality or usefulness of our products or our user data practices, or concerns related to privacy and sharing, safety, security, well-being, or other factors;
- we are unable to manage and prioritize information to ensure users are presented with content that is appropriate, interesting, useful, and relevant to them;
- we are unable to obtain or attract engaging third-party content;
- we are unable to successfully maintain or grow usage of and engagement with mobile and web applications that integrate with Facebook and our other products;
- users adopt new technologies where our products may be displaced in favor of other products or services, or may not be featured or otherwise available;
- there are changes mandated by legislation, regulatory authorities, or litigation that adversely affect our products or users;
- there is decreased engagement with our products, or failure to accept our terms of service, as part of changes that we implemented in connection with the General Data Protection Regulation (GDPR) in Europe, other similar changes that



we implemented in the United States and around the world, or other changes we may implement in the future in connection with other regulations, regulatory actions or otherwise;

- technical or other problems prevent us from delivering our products in a rapid and reliable manner or otherwise affect the user experience, such as security breaches or failure to prevent or limit spam or similar content;
- we adopt terms, policies, or procedures related to areas such as sharing, content, user data, or advertising that are perceived negatively by our users or the general public;
- we elect to focus our product decisions on longer-term initiatives that do not prioritize near-term user growth and engagement;
- we make changes in how we promote different products and services across our family of apps;
- initiatives designed to attract and retain users and engagement are unsuccessful or discontinued, whether as a result of actions by us, third parties, or otherwise;
- third-party initiatives that may enable greater use of our products, including low-cost or discounted data plans, are discontinued;
- there is decreased engagement with our products as a result of taxes imposed on the use of social media or other mobile applications in certain countries, or other actions by governments that may affect the accessibility of our products in their countries;
- we fail to provide adequate customer service to users, marketers, developers, or other partners;
- we, developers whose products are integrated with our products, or other partners and companies in our industry are the subject of adverse media reports or other negative publicity, including as a result of our or their user data practices; or
- our current or future products, such as our development tools and application programming interfaces that enable developers to build, grow, and monetize mobile and web applications, reduce user activity on our products by making it easier for our users to interact and share on third-party mobile and web applications.

If we are unable to maintain or increase our user base and user engagement, our revenue and financial results may be adversely affected. Any decrease in user retention, growth, or engagement could render our products less attractive to users, marketers, and developers, which is likely to have a material and adverse impact on our revenue, business, financial condition, and results of operations. If our active user growth rate continues to slow, we will become increasingly dependent on our ability to maintain or increase levels of user engagement and monetization in order to drive revenue growth.

***We generate substantially all of our revenue from advertising. The loss of marketers, or reduction in spending by marketers, could seriously harm our business.***

Substantially all of our revenue is currently generated from third parties advertising on Facebook and Instagram. As is common in the industry, our marketers do not have long-term advertising commitments with us. Many of our marketers spend only a relatively small portion of their overall advertising budget with us. Marketers will not continue to do business with us, or they will reduce the budgets they are willing to commit to us, if we do not deliver ads in an effective manner, or if they do not believe that their investment in advertising with us will generate a competitive return relative to other alternatives. We have recently implemented, and we may continue to implement, changes to our user data practices. Some of these changes will reduce marketers' ability to effectively target their ads, which has to some extent adversely affected, and will continue to adversely affect, our advertising business. If we are unable to provide marketers with a suitable return on investment, the pricing of our ads may not increase, or may decline, in which case our revenue and financial results may be harmed.

Our advertising revenue could also be adversely affected by a number of other factors, including:

- decreases in user engagement, including time spent on our products;
- our inability to continue to increase user access to and engagement with our products;
- product changes or inventory management decisions we may make that change the size, format, frequency, or relative prominence of ads displayed on our products or of other unpaid content shared by marketers on our products;
- our inability to maintain or increase marketer demand, the pricing of our ads, or both;





***Our user growth, engagement, and monetization on mobile devices depend upon effective operation with mobile operating systems, networks, technologies, products, and standards that we do not control.***

The substantial majority of our revenue is generated from advertising on mobile devices. There is no guarantee that popular mobile devices will continue to feature Facebook or our other products, or that mobile device users will continue to use our products rather than competing products. We are dependent on the interoperability of Facebook and our other products with popular mobile operating systems, networks, technologies, products, and standards that we do not control, such as the Android and iOS operating systems and mobile browsers. Any changes, bugs, or technical issues in such systems, or changes in our relationships with mobile operating system partners, handset manufacturers, browser developers, or mobile carriers, or in their terms of service or policies that degrade our products' functionality, reduce or eliminate our ability to distribute our products, give preferential treatment to competitive products, limit our ability to deliver, target, or measure the effectiveness of ads, or charge fees related to the distribution of our products or our delivery of ads could adversely affect the usage of Facebook or our other products and monetization on mobile devices. For example, Apple recently released an update to its Safari browser that limits the use of third-party cookies, which reduces our ability to provide the most relevant ads to our users and impacts monetization. Additionally, in order to deliver high quality mobile products, it is important that our products work well with a range of mobile technologies, products, systems, networks, and standards that we do not control, and that we have good relationships with handset manufacturers, mobile carriers and browser developers. We may not be successful in maintaining or developing relationships with key participants in the mobile ecosystem or in developing products that operate effectively with these technologies, products, systems, networks, or standards. In the event that it is more difficult for our users to access and use Facebook or our other products on their mobile devices, or if our users choose not to access or use Facebook or our other products on their mobile devices or use mobile products that do not offer access to Facebook or our other products, our user growth and user engagement could be harmed. From time to time, we may also take actions regarding the distribution of our products or the operation of our business based on what we believe to be in our long-term best interests. Such actions may adversely affect our users and our relationships with the operators of mobile operating systems, handset manufacturers, mobile carriers, browser developers, or other business partners, and there is no assurance that these actions will result in the anticipated long-term benefits. In the event that our users are adversely affected by these actions or if our relationships with such third parties deteriorate, our user growth, engagement, and monetization could be adversely affected and our business could be harmed.

***Our business is highly competitive. Competition presents an ongoing threat to the success of our business.***

We compete with companies that sell advertising, as well as with companies that provide social, media, and communication products and services that are designed to engage users on the web, mobile devices and online generally. We face significant competition in every aspect of our business, including from companies that facilitate communication and the sharing of content and information, companies that enable marketers to display advertising, companies that distribute video and other forms of media content, and companies that provide development platforms for applications developers. We compete with companies that offer products across broad platforms that replicate capabilities we provide. For example, among other areas, we compete with Apple in messaging, Google and YouTube in advertising and video, Tencent in messaging and social media, and Amazon in advertising. We also compete with companies that provide regional social networks, many of which have strong positions in particular countries. Some of our competitors may be domiciled in different countries and subject to political, legal, and regulatory regimes that enable them to compete more effectively than us. In addition, we face competition from traditional, online, and mobile businesses that provide media for marketers to reach their audiences and/or develop tools and systems for managing and optimizing advertising campaigns. We also compete with companies that develop and deliver consumer hardware and virtual reality products and services.

Some of our current and potential competitors may have greater resources or stronger competitive positions in certain product segments, geographic regions, or user demographics than we do. These factors may allow our competitors to respond more effectively than us to new or emerging technologies and changes in market conditions. We believe that some users, particularly younger users, are aware of and actively engaging with other products and services similar to, or as a substitute for, Facebook products and services, and we believe that some users have reduced their use of and engagement with our products and services in favor of these other products and services. In the event that users increasingly engage with other products and services, we may experience a decline in use and engagement in key user demographics or more broadly, in which case our business would likely be harmed.

Our competitors may develop products, features, or services that are similar to ours or that achieve greater acceptance, may undertake more far-reaching and successful product development efforts or marketing campaigns, or may adopt more aggressive pricing policies. In addition, developers whose mobile and web applications are integrated with Facebook or our other products may use information shared by our users through our products in order to develop products or features that compete with us. Some competitors may gain a competitive advantage against us in areas where we operate, including: by making acquisitions; by limiting our ability to deliver, target, or measure the effectiveness of ads; by imposing fees or other charges related to our delivery of ads; by making access to our products more difficult or impossible; by making it more difficult to communicate with our users; or by integrating competing platforms, applications, or features into products they control such as mobile device operating systems, search engines,

browsers, or e-commerce platforms. For example, each of Apple and Google have integrated competitive products with iOS and Android, respectively. As a result, our competitors may acquire and engage users or generate advertising or other revenue at the

expense of our own efforts, which may negatively affect our business and financial results. In addition, from time to time, we may take actions in response to competitive threats, but we cannot assure you that these actions will be successful or that they will not negatively affect our business and financial results.

We believe that our ability to compete effectively depends upon many factors both within and beyond our control, including:

- the popularity, usefulness, ease of use, performance, and reliability of our products compared to our competitors' products;
- the size and composition of our user base;
- the engagement of users with our products and competing products;
- the timing and market acceptance of products, including developments and enhancements to our or our competitors' products;
- our safety and security efforts and our ability to protect user data and to provide users with control over their data;
- our ability to distribute our products to new and existing users;
- our ability to monetize our products;
- the frequency, size, format, quality, and relative prominence of the ads displayed by us or our competitors;
- customer service and support efforts;
- marketing and selling efforts, including our ability to measure the effectiveness of our ads and to provide marketers with a compelling return on their investments;
- our ability to establish and maintain developers' interest in building mobile and web applications that integrate with Facebook and our other products;
- our ability to establish and maintain publisher interest in integrating their content with Facebook and our other products;
- changes mandated by legislation, regulatory authorities, or litigation, some of which may have a disproportionate effect on us;
- acquisitions or consolidation within our industry, which may result in more formidable competitors;
- our ability to attract, retain, and motivate talented employees, particularly software engineers, designers, and product managers;
- our ability to cost-effectively manage and grow our operations; and
- our reputation and brand strength relative to those of our competitors.

If we are not able to compete effectively, our user base and level of user engagement may decrease, we may become less attractive to developers and marketers, and our revenue and results of operations may be materially and adversely affected.

***Actions by governments that restrict access to Facebook or our other products in their countries, or that otherwise impair our ability to sell advertising in their countries, could substantially harm our business and financial results.***

Governments of one or more countries in which we operate from time to time seek to censor content available on Facebook or our other products in their country, restrict access to our products from their country entirely, or impose other restrictions that may affect the accessibility of our products in their country for an extended period of time or indefinitely. For example, user access to Facebook and certain of our other products has been or is currently restricted in whole or in part in China, Iran, and North Korea. In addition, government authorities in other countries may seek to restrict user access to our products if they consider us to be in violation of their laws or a threat to public safety or for other reasons, and certain of our products have been restricted by governments in other countries from time to time. It is possible that government authorities could take action that impairs our ability to sell advertising, including in countries where access to our consumer-facing products may be blocked or restricted. For example, we generate meaningful revenue from a limited number of resellers representing advertisers based in China. In the event that content shown on Facebook or our other products is subject to censorship, access to our products is restricted, in whole or in part, in one or more countries, or other restrictions are imposed on our products, or our competitors are able to successfully penetrate new geographic markets or capture a greater share of existing geographic markets that we cannot access or where we face other restrictions, our ability to retain or increase our user base, user engagement, or the level of advertising by marketers may be adversely affected, we may not be able to maintain or grow our revenue as anticipated, and our financial results could be adversely affected.

***Our new products and changes to existing products could fail to attract or retain users or generate revenue and profits.***

Our ability to retain, increase, and engage our user base and to increase our revenue depends heavily on our ability to continue to evolve our existing products and to create successful new products, both independently and in conjunction with developers or other third parties. We may introduce significant changes to our existing products or acquire or introduce new and unproven products, including using technologies with which we have little or no prior development or operating experience. For example, we do not have significant experience with consumer hardware products or virtual or augmented reality technology, which may adversely affect our ability to successfully develop and market these products and technologies, and we will incur increased costs in connection with the development and marketing of such products and technologies. In addition, the introduction of new products, or changes to existing products, may result in new or enhanced governmental or regulatory scrutiny or other complications that could adversely affect our business and financial results. We have also invested, and expect to continue to invest, significant resources in growing our WhatsApp and Messenger products. We have historically monetized messaging in only a very limited fashion, and we may not be successful in our efforts to generate meaningful revenue from messaging over the long term. If these or other new or enhanced products fail to engage users, marketers, or developers, or if our business plans are unsuccessful, we may fail to attract or retain users or to generate sufficient revenue, operating margin, or other value to justify our investments, and our business may be adversely affected.

***We make product and investment decisions that may not prioritize short-term financial results and may not produce the long-term benefits that we expect.***

We frequently make product and investment decisions that may not prioritize short-term financial results if we believe that the decisions are consistent with our mission and benefit the aggregate user experience and will thereby improve our financial performance over the long term. For example, we have recently implemented, and we may continue to implement, changes to our user data practices. Some of these changes will reduce marketers' ability to effectively target their ads, which has to some extent adversely affected, and will continue to adversely affect, our advertising business. Similarly, we previously announced changes to our News Feed ranking algorithm to help our users have more meaningful interactions, and these changes have had, and we expect will continue to have, the effect of reducing time spent and some measures of user engagement with Facebook, which could adversely affect our financial results. From time to time, we may also change the size, frequency, or relative prominence of ads in order to improve ad quality and overall user experience. In addition, we have made, and we expect to continue to make, other changes to our products which may adversely affect the distribution of content of publishers, marketers, and developers, and could reduce their incentive to invest in their efforts on Facebook. We also may introduce new features or other changes to existing products, or introduce new stand-alone products, that attract users away from properties, formats, or use cases where we have more proven means of monetization. For example, we plan to continue to promote the Stories format, which is becoming increasingly popular for sharing content across our products, but our advertising efforts with this format are still under development and we do not currently monetize Stories at the same rate as News Feed. In addition, as we focus on growing users and engagement across our family of apps, it is possible that these efforts may from time to time reduce engagement with one or more products and services in favor of other products or services that we monetize less successfully or that are not growing as quickly. These decisions may adversely affect our business and results of operations and may not produce the long-term benefits that we expect.

***If we are not able to maintain and enhance our brands, our ability to expand our base of users, marketers, and developers may be impaired, and our business and financial results may be harmed.***

We believe that our brands have significantly contributed to the success of our business. We also believe that maintaining and enhancing our brands is critical to expanding our base of users, marketers, and developers. Many of our new users are referred by existing users. Maintaining and enhancing our brands will depend largely on our ability to continue to provide useful, reliable, trustworthy, and innovative products, which we may not do successfully. We may introduce new products or terms of service or policies that users do not like, which may negatively affect our brands. Additionally, the actions of our developers or advertisers may affect our brands if users do not have a positive experience using third-party mobile and web applications integrated with our products or interacting with parties that advertise through our products. We will also continue to experience media, legislative, or regulatory scrutiny of our actions or decisions regarding user privacy, content, advertising, and other issues, including actions or decisions in connection with elections, which may adversely affect our reputation and brands. For example, we previously announced our discovery of certain ads and other content previously displayed on our products that may be relevant to government investigations relating to Russian interference in the 2016 U.S. presidential election. In addition, in March 2018, we announced developments regarding the misuse of certain data by a developer that shared such data with third parties in violation of our terms and policies. We also may fail to respond expeditiously or appropriately to the sharing of objectionable content on our services or objectionable practices by advertisers or developers, or to otherwise address user concerns, which could erode confidence in our brands. Our brands may also be negatively affected by the actions of users that are deemed to be hostile or inappropriate to other users, by the actions of users acting under false or inauthentic identities, by the use of our products or services to disseminate information that is deemed to be misleading (or intended to manipulate opinions), by perceived or actual efforts by governments to obtain access to user information for security-related purposes or to censor certain content on our platform, or by the use of our products or services for illicit, objectionable, or illegal ends. Maintaining and enhancing our brands may require us to make substantial investments and these investments may not be successful. Certain of our past actions, such as the foregoing matter regarding developer misuse of data, have eroded confidence in our brands, and if we fail to successfully promote and maintain our brands or if we incur excessive expenses in this effort, our business and financial results may be adversely affected.

***Security breaches and improper access to or disclosure of our data or user data, or other hacking and phishing attacks on our systems, could harm our reputation and adversely affect our business.***

Our industry is prone to cyber-attacks by third parties seeking unauthorized access to our data or users' data or to disrupt our ability to provide service. Any failure to prevent or mitigate security breaches and improper access to or disclosure of our data or user data, including personal information, content, or payment information from users, or information from marketers, could result in the loss or misuse of such data, which could harm our business and reputation and diminish our competitive position. In addition, computer malware, viruses, social engineering (predominantly spear phishing attacks), and general hacking have become more prevalent in our industry, have occurred on our systems in the past, and will occur on our systems in the future. We also regularly encounter attempts to create false or undesirable user accounts, purchase ads, or take other actions on our platform for purposes such as spamming, spreading misinformation, or other objectionable ends. As a result of our prominence, the size of our user base, and the types and volume of personal data on our systems, we believe that we are a particularly attractive target for such breaches and attacks. Our efforts to address undesirable activity on our platform may also increase the risk of retaliatory attacks. Such attacks may cause interruptions to the services we provide, degrade the user experience, cause users or marketers to lose confidence and trust in our products, impair our internal systems, or result in financial harm to us. Our efforts to protect our company data or the information we receive may also be unsuccessful due to software bugs or other technical malfunctions; employee, contractor, or vendor error or malfeasance; government surveillance; or other threats that evolve. In addition, third parties may attempt to fraudulently induce employees or users to disclose information in order to gain access to our data or our users' data. Cyber-attacks continue to evolve in sophistication and volume, and inherently may be difficult to detect for long periods of time. Although we have developed systems and processes that are designed to protect our data and user data, to prevent data loss, to disable undesirable accounts and activities on our platform, and to prevent or detect security breaches, we cannot assure you that such measures will provide absolute security, and we may incur significant costs in protecting against or remediating cyber-attacks.

In addition, some of our developers or other partners, such as those that help us measure the effectiveness of ads, may receive or store information provided by us or by our users through mobile or web applications integrated with Facebook. We provide limited information to such third parties based on the scope of services provided to us. However, if these third parties or developers fail to adopt or adhere to adequate data security practices, or in the event of a breach of their networks, our data or our users' data may be improperly accessed, used, or disclosed.

Affected users or government authorities could initiate legal or regulatory actions against us in connection with any actual or perceived security breaches or improper disclosure of data, which could cause us to incur significant expense and liability or result in orders or consent decrees forcing us to modify our business practices. Such incidents or our efforts to remediate such incidents may

also result in a decline in our active user base or engagement levels. Any of these events could have a material and adverse effect on our business, reputation, or financial results.

For example, in September 2018, we announced our discovery of a third-party cyber-attack that exploited a vulnerability in Facebook's code to steal user access tokens, which were then used to access certain profile information from approximately 29 million user accounts on Facebook. While we took steps to remediate the attack, including fixing the vulnerability, resetting user access tokens and notifying affected users, we may discover and announce additional developments, which could further erode confidence in our brand. In addition, the events surrounding this cyber-attack became the subject of Irish Data Protection Commission, U.S. Federal Trade Commission and other government inquiries in the United States, Europe, and other jurisdictions. Any such inquiries could subject us to substantial fines and costs, require us to change our business practices, divert resources and the attention of management from our business, or adversely affect our business.

***We anticipate that our ongoing investments in safety, security, and content review will identify additional instances of misuse of user data or other undesirable activity by third parties on our platform.***

In addition to our efforts to mitigate cybersecurity risks, we are making significant investments in safety, security, and content review efforts to combat misuse of our services and user data by third parties, including investigations and audits of platform applications that previously accessed information of a large number of users of our services. As a result of these efforts we have discovered and announced, and anticipate that we will continue to discover and announce, additional incidents of misuse of user data or other undesirable activity by third parties. We may not discover all such incidents or activity, including as a result of our data limitations or the scale of activity on our platform, and we may be notified of such incidents or activity via the media or other third parties. Such incidents and activities may include the use of user data in a manner inconsistent with our terms, contracts or policies, the existence of false or undesirable user accounts, election interference, improper ad purchases, activities that threaten people's safety on- or offline, or instances of spamming, scraping, or spreading misinformation. The discovery of the foregoing may negatively affect user trust and engagement, harm our reputation and brands, require us to change our business practices in a manner adverse to our business, and adversely affect our business and financial results. Any such discoveries may also subject us to additional litigation and regulatory inquiries, which could subject us to monetary penalties and damages, divert management's time and attention, and lead to enhanced regulatory oversight.

***Unfavorable media coverage could negatively affect our business.***

We receive a high degree of media coverage around the world. Unfavorable publicity regarding, for example, our privacy practices, terms of service, product changes, product quality, litigation or regulatory activity, government surveillance, the actions of our advertisers, the actions of our developers whose products are integrated with our products, the use of our products or services for illicit, objectionable, or illegal ends, the substance or enforcement of our community standards, the actions of our users, the quality and integrity of content shared on our platform, or the actions of other companies that provide similar services to ours, has in the past, and could in the future, adversely affect our reputation. For example, beginning in March 2018, we were the subject of intense media coverage involving the misuse of certain data by a developer that shared such data with third parties in violation of our terms and policies, and we have continued to receive negative publicity. Such negative publicity could have an adverse effect on the size, engagement, and loyalty of our user base and result in decreased revenue, which could adversely affect our business and financial results.

***Our financial results will fluctuate from quarter to quarter and are difficult to predict.***

Our quarterly financial results have fluctuated in the past and will fluctuate in the future. Additionally, we have a limited operating history with the current scale of our business, which makes it difficult to forecast our future results. As a result, you should not rely upon our past quarterly financial results as indicators of future performance. You should take into account the risks and uncertainties frequently encountered by companies in rapidly evolving markets. Our financial results in any given quarter can be influenced by numerous factors, many of which we are unable to predict or are outside of our control, including:

- our ability to maintain and grow our user base and user engagement;
- our ability to attract and retain marketers in a particular period;
- fluctuations in spending by our marketers due to seasonality, such as historically strong spending in the fourth quarter of each year, episodic regional or global events, or other factors;
- the frequency, prominence, size, format, and quality of ads shown to users;
- the success of technologies designed to block the display of ads;
- the pricing of our ads and other products;
- the diversification and growth of revenue sources beyond advertising on Facebook and Instagram;



- our ability to generate revenue from Payments, or the sale of our consumer hardware products or other products we may introduce in the future;
- changes to existing products or services or the development and introduction of new products or services by us or our competitors;
- user behavior or product changes that may reduce traffic to features or products that we successfully monetize;
- increases in marketing, sales, and other operating expenses that we will incur to grow and expand our operations and to remain competitive, including costs related to our data centers and technical infrastructure;
- costs related to our safety, security, and content review efforts;
- costs and expenses related to the development and delivery of our consumer hardware products;
- our ability to maintain gross margins and operating margins;
- costs related to acquisitions, including costs associated with amortization and additional investments to develop the acquired technologies;
- charges associated with impairment of any assets on our balance sheet;
- our ability to obtain equipment, components, and labor for our data centers and other technical infrastructure in a timely and cost-effective manner;
- system failures or outages or government blocking, which could prevent us from serving ads for any period of time;
- breaches of security or privacy, and the costs associated with any such breaches and remediation;
- changes in the manner in which we distribute our products or inaccessibility of our products due to third-party actions;
- fees paid to third parties for content or the distribution of our products;
- share-based compensation expense, including acquisition-related expense;
- adverse litigation judgments, settlements, or other litigation-related costs;
- changes in the legislative or regulatory environment, including with respect to privacy and data protection, or actions by governments or regulators, including fines, orders, or consent decrees;
- the overall tax rate for our business, which may be affected by the mix of income we earn in the U.S. and in jurisdictions with comparatively lower tax rates, the effects of share-based compensation, the effects of integrating intellectual property from acquisitions, and the effects of changes in our business;
- the impact of changes in tax laws or judicial or regulatory interpretations of tax laws, which are recorded in the period such laws are enacted or interpretations are issued, and may significantly affect the effective tax rate of that period;
- tax obligations that may arise from resolutions of tax examinations, including the examination we are currently under by the Internal Revenue Service (IRS), that materially differ from the amounts we have anticipated;
- fluctuations in currency exchange rates and changes in the proportion of our revenue and expenses denominated in foreign currencies;
- fluctuations in the market values of our portfolio investments and in interest rates;
- changes in U.S. generally accepted accounting principles; and
- changes in global business or macroeconomic conditions.

***We expect our rates of growth to decline in the future.***

We expect that our user growth rate will generally decline over time as the size of our active user base increases, and it is possible that the size of our active user base may fluctuate or decline in one or more markets, particularly as we achieve greater market penetration. We expect our revenue growth rate will continue to decline over time as our revenue increases to higher levels. As our growth rates decline, investors' perceptions of our business may be adversely affected and the trading price of our Class A common stock could decline.

***Our costs are continuing to grow, which could reduce our operating margin and profitability. If our investments are not successful, our business and financial performance could be harmed.***

Operating our business is costly, and we expect our expenses to continue to increase in the future as we broaden our user base, as users increase the amount and types of content they consume and the data they share with us, for example with respect to video, as we develop and implement new products, as we market new and existing products and promote our brands, as we continue to expand our technical infrastructure, as we continue to invest in new and unproven technologies, and as we continue to hire additional employees and contractors to support our expanding operations, including our efforts to focus on safety, security, and content review. We will continue to invest in our messaging, video content, and global connectivity efforts, as well as other initiatives that may not have clear paths to monetization. In addition, we will incur increased costs in connection with the development and marketing of our consumer hardware and virtual and augmented reality products and technologies. Any such investments may not be successful, and any such increases in our costs may reduce our operating margin and profitability. In addition, if our investments are not successful, our ability to grow revenue will be harmed, which could adversely affect our business and financial performance.

***Given our levels of share-based compensation, our tax rate may vary significantly depending on our stock price.***

The tax effects of the accounting for share-based compensation may significantly impact our effective tax rate from period to period. In periods in which our stock price is higher than the grant price of the share-based compensation vesting in that period, we will recognize excess tax benefits that will decrease our effective tax rate. For example, in 2018, excess tax benefits recognized from share-based compensation decreased our provision for income taxes by \$717 million and our effective tax rate by approximately three percentage points as compared to the tax rate without such benefits. In future periods in which our stock price is lower than the grant price of the share-based compensation vesting in that period, our effective tax rate may increase. The amount and value of share-based compensation issued relative to our earnings in a particular period will also affect the magnitude of the impact of share-based compensation on our effective tax rate. These tax effects are dependent on our stock price, which we do not control, and a decline in our stock price could significantly increase our effective tax rate and adversely affect our financial results.

***Our business is subject to complex and evolving U.S. and foreign laws and regulations regarding privacy, data protection, content, competition, consumer protection, and other matters. Many of these laws and regulations are subject to change and uncertain interpretation, and could result in claims, changes to our business practices, monetary penalties, increased cost of operations, or declines in user growth or engagement, or otherwise harm our business.***

We are subject to a variety of laws and regulations in the United States and abroad that involve matters central to our business, including privacy, data protection and personal information, rights of publicity, content, intellectual property, advertising, marketing, distribution, data security, data retention and deletion, electronic contracts and other communications, competition, protection of minors, consumer protection, telecommunications, product liability, taxation, economic or other trade prohibitions or sanctions, securities law compliance, and online payment services. The introduction of new products, expansion of our activities in certain jurisdictions, or other actions that we may take may subject us to additional laws, regulations, or other government scrutiny. In addition, foreign data protection, privacy, content, competition, and other laws and regulations can impose different obligations or be more restrictive than those in the United States.

These U.S. federal and state and foreign laws and regulations, which in some cases can be enforced by private parties in addition to government entities, are constantly evolving and can be subject to significant change. As a result, the application, interpretation, and enforcement of these laws and regulations are often uncertain, particularly in the new and rapidly evolving industry in which we operate, and may be interpreted and applied inconsistently from country to country and inconsistently with our current policies and practices. For example, regulatory or legislative actions affecting the manner in which we display content to our users or obtain consent to various practices could adversely affect user growth and engagement. Such actions could affect the manner in which we provide our services or adversely affect our financial results.

We are also subject to laws and regulations that dictate whether, how, and under what circumstances we can transfer, process and/or receive certain data that is critical to our operations, including data shared between countries or regions in which we operate and data shared among our products and services. For example, in 2016, the European Union and United States agreed to an alternative transfer framework for data transferred from the European Union to the United States, called the Privacy Shield, but this new framework is subject to an annual review that could result in changes to our obligations and also is subject to challenge by regulators and private parties. In addition, the other bases upon which Facebook relies to legitimize the transfer of such data, such as Standard Contractual Clauses (SCCs), have been subjected to regulatory and judicial scrutiny. For example, the Irish Data Protection Commissioner has challenged the legal grounds for transfers of user data to Facebook, Inc., and the Irish High Court has referred this challenge to the Court of Justice of the European Union for decision. We have also been managing investigations and lawsuits in Europe, India, and other jurisdictions regarding the August 2016 update to WhatsApp's terms of service and privacy policy and its sharing of certain data with other Facebook products and services, including a lawsuit currently pending before the Supreme Court of India. If one or more of the legal bases for transferring data from Europe to the United States is invalidated, if we are unable to transfer data between and among countries and regions in which we operate, or if we are restricted from sharing data among our products and services, it could affect the manner in which we provide our services or our ability to target ads, which could adversely affect our financial results.

Proposed or new legislation and regulations could also significantly affect our business. For example, the European General Data Protection Regulation (GDPR) took effect in May 2018 and applies to all of our products and services used by people in Europe. The GDPR includes operational requirements for companies that receive or process personal data of residents of the European Union that are different from those previously in place in the European Union. As a result, we implemented measures to change our service for minors under the age of 16 for certain countries in Europe that maintain the minimum age of 16 under the GDPR. We also obtain consent and/or offer new controls to existing and new users in Europe before processing data for certain aspects of our service. In addition, the GDPR requires submission of breach notifications to our designated European privacy regulator, the Irish Data Protection Commissioner, and includes significant penalties for non-compliance with the notification obligation as well as other requirements of the regulation. The California Consumer Privacy Act, or AB 375, was also recently passed and creates new data privacy rights for users, effective in 2020. Similarly, there are a number of legislative proposals in the European Union, the United States, at both the federal and state level, as well as other jurisdictions that could impose new obligations in areas affecting our business. In addition, some countries are considering or have passed legislation implementing data protection requirements or requiring local storage and processing of data or similar requirements that could increase the cost and complexity of delivering our services.

These laws and regulations, as well as any associated inquiries or investigations or any other government actions, may be costly to comply with and may delay or impede the development of new products, result in negative publicity, increase our operating costs, require significant management time and attention, and subject us to remedies that may harm our business, including fines or demands or orders that we modify or cease existing business practices.

***We have been subject to regulatory and other government investigations, enforcement actions, and settlements, and we expect to continue to be subject to such proceedings and other inquiries in the future, which could cause us to incur substantial costs or require us to change our business practices in a manner materially adverse to our business.***

From time to time, we receive formal and informal inquiries from government authorities and regulators regarding our compliance with laws and regulations, many of which are evolving and subject to interpretation. We are and expect to continue to be the subject of investigations, inquiries, data requests, actions, and audits in the United States, Europe, and around the world, particularly in the areas of privacy, data protection, law enforcement, consumer protection, and competition, as we continue to grow and expand our operations. In addition, we are currently, and may in the future be, subject to regulatory orders or consent decrees. For example, data protection and consumer protection authorities in the European Union have initiated actions, investigations, or administrative orders seeking to restrict the ways in which we collect and use information, or impose sanctions, and other authorities may do the same. In addition, beginning in March 2018, we became subject to U.S. Federal Trade Commission, Securities and Exchange Commission, state attorneys general, and other government inquiries in the United States, Europe, and other jurisdictions in connection with our platform and user data practices as well as the misuse of certain data by a developer that shared such data with third parties in violation of our terms and policies. Beginning in September 2018, we also became subject to Irish Data Protection Commission, U.S. Federal Trade Commission and other government inquiries in the United States, Europe, and other jurisdictions in connection with a third-party cyber-attack that exploited a vulnerability in Facebook's code to steal user access tokens and access certain profile information from user accounts on Facebook. Orders issued by, or inquiries or enforcement actions initiated by, government or regulatory authorities could cause us to incur substantial costs, expose us to unanticipated civil and criminal liability or penalties (including substantial monetary fines), or require us to change our business practices in a manner materially adverse to our business.

# Exhibit 23

**UNITED STATES  
SECURITIES AND EXCHANGE COMMISSION  
Washington, D.C. 20549**

**FORM 10-K**

(Mark One)

**ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**  
For the fiscal year ended December 31, 2019

or

**TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**  
For the transition period from \_\_\_\_\_ to \_\_\_\_\_  
Commission File Number: 001-35551

**Facebook, Inc.**

(Exact name of registrant as specified in its charter)

**Delaware**

(State or other jurisdiction of incorporation or organization)

**20-1665019**

(I.R.S. Employer Identification Number)

**1601 Willow Road, Menlo Park, California 94025**

(Address of principal executive offices and Zip Code)

**(650) 543-4800**

(Registrant's telephone number, including area code)

**Securities registered pursuant to Section 12(b) of the Act**

Title of each class	Trading symbol(s)	Name of each exchange on which registered
Class A Common Stock, \$0.000006 par value	FB	The Nasdaq Stock Market LLC

**Securities registered pursuant to Section 12(g) of the Act: None**

Indicate by check mark if the registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act. Yes  No

Indicate by check mark if the registrant is not required to file reports pursuant to Section 13 or Section 15(d) of the Act. Yes  No

Indicate by check mark whether the registrant (1) has filed all reports required to be filed by Section 13 or 15(d) of the Securities Exchange Act of 1934 (Exchange Act) during the preceding 12 months (or for such shorter period that the registrant was required to file such reports), and (2) has been subject to such filing requirements for the past 90 days. Yes  No

Indicate by check mark whether the registrant has submitted electronically every Interactive Data File required to be submitted pursuant to Rule 405 of Regulation S-T (§ 232.405 of this chapter) during the preceding 12 months (or for such shorter period that the registrant was required to submit such files). Yes  No

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer, a smaller reporting company, or an emerging growth company. See the definitions of "large accelerated filer," "accelerated filer," "smaller reporting company," and "emerging growth company" in Rule 12b-2 of the Exchange Act.

Large accelerated filer	<input checked="" type="checkbox"/>	Accelerated filer	<input type="checkbox"/>
Non-accelerated filer	<input type="checkbox"/>	Smaller reporting company	<input type="checkbox"/>
		Emerging growth company	<input type="checkbox"/>

If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13(a) of the Exchange Act.

Indicate by check mark whether the registrant is a shell company (as defined in Rule 12b-2 of the Exchange Act). Yes  No

The aggregate market value of the voting and non-voting stock held by non-affiliates of the registrant as of June 28, 2019, the last business day of the registrant's most recently completed second fiscal quarter, was \$478 billion based upon the closing price reported for such date on the Nasdaq Global Select Market. On January 23, 2020, the registrant had 2,405,745,740 shares of Class A common stock and 444,704,919 shares of Class B common stock outstanding.

**DOCUMENTS INCORPORATED BY REFERENCE**

Portions of the registrant's Proxy Statement for the 2020 Annual Meeting of Stockholders are incorporated herein by reference in Part III of this Annual Report on Form 10-K to the extent stated herein. Such proxy statement will be filed with the Securities and Exchange Commission within 120 days of the registrant's fiscal year ended December 31, 2019.

---

---

---

**Facebook, Inc.**  
**Form 10-K**

**TABLE OF CONTENTS**

	<u>Page</u>
<a href="#"><u>Note About Forward-Looking Statements</u></a>	<a href="#"><u>3</u></a>
<a href="#"><u>Limitations of Key Metrics and Other Data</u></a>	<a href="#"><u>4</u></a>
<b><u>PART I</u></b>	
<a href="#"><u>Item 1. Business</u></a>	<a href="#"><u>7</u></a>
<a href="#"><u>Item 1A. Risk Factors</u></a>	<a href="#"><u>10</u></a>
<a href="#"><u>Item 1B. Unresolved Staff Comments</u></a>	<a href="#"><u>38</u></a>
<a href="#"><u>Item 2. Properties</u></a>	<a href="#"><u>38</u></a>
<a href="#"><u>Item 3. Legal Proceedings</u></a>	<a href="#"><u>38</u></a>
<a href="#"><u>Item 4. Mine Safety Disclosures</u></a>	<a href="#"><u>39</u></a>
<b><u>PART II</u></b>	
<a href="#"><u>Item 5. Market for Registrant's Common Equity, Related Stockholder Matters and Issuer Purchases of Equity Securities</u></a>	<a href="#"><u>40</u></a>
<a href="#"><u>Item 6. Selected Financial Data</u></a>	<a href="#"><u>42</u></a>
<a href="#"><u>Item 7. Management's Discussion and Analysis of Financial Condition and Results of Operations</u></a>	<a href="#"><u>44</u></a>
<a href="#"><u>Item 7A. Quantitative and Qualitative Disclosures About Market Risk</u></a>	<a href="#"><u>67</u></a>
<a href="#"><u>Item 8. Financial Statements and Supplementary Data</u></a>	<a href="#"><u>68</u></a>
<a href="#"><u>Item 9. Changes in and Disagreements with Accountants on Accounting and Financial Disclosure</u></a>	<a href="#"><u>103</u></a>
<a href="#"><u>Item 9A. Controls and Procedures</u></a>	<a href="#"><u>103</u></a>
<a href="#"><u>Item 9B. Other Information</u></a>	<a href="#"><u>103</u></a>
<b><u>PART III</u></b>	
<a href="#"><u>Item 10. Directors, Executive Officers and Corporate Governance</u></a>	<a href="#"><u>104</u></a>
<a href="#"><u>Item 11. Executive Compensation</u></a>	<a href="#"><u>104</u></a>
<a href="#"><u>Item 12. Security Ownership of Certain Beneficial Owners and Management and Related Stockholder Matters</u></a>	<a href="#"><u>104</u></a>
<a href="#"><u>Item 13. Certain Relationships and Related Transactions, and Director Independence</u></a>	<a href="#"><u>104</u></a>
<a href="#"><u>Item 14. Principal Accounting Fees and Services</u></a>	<a href="#"><u>104</u></a>

**PART IV**

<u>Item 15.</u>	<u>Exhibits, Financial Statement Schedules</u>	<u>105</u>
<u>Item 16.</u>	<u>Form 10-K Summary</u>	<u>107</u>
<u>Signatures</u>		

## NOTE ABOUT FORWARD-LOOKING STATEMENTS

This Annual Report on Form 10-K contains forward-looking statements. All statements contained in this Annual Report on Form 10-K other than statements of historical fact, including statements regarding our future results of operations and financial position, our business strategy and plans, and our objectives for future operations, are forward-looking statements. The words "believe," "may," "will," "estimate," "continue," "anticipate," "intend," "expect," and similar expressions are intended to identify forward-looking statements. We have based these forward-looking statements largely on our current expectations and projections about future events and trends that we believe may affect our financial condition, results of operations, business strategy, short-term and long-term business operations and objectives, and financial needs. These forward-looking statements are subject to a number of risks, uncertainties and assumptions, including those described in Part I, Item 1A, "Risk Factors" in this Annual Report on Form 10-K. Moreover, we operate in a very competitive and rapidly changing environment. New risks emerge from time to time. It is not possible for our management to predict all risks, nor can we assess the impact of all factors on our business or the extent to which any factor, or combination of factors, may cause actual results to differ materially from those contained in any forward-looking statements we may make. In light of these risks, uncertainties and assumptions, the future events and trends discussed in this Annual Report on Form 10-K may not occur and actual results could differ materially and adversely from those anticipated or implied in the forward-looking statements.

We undertake no obligation to revise or publicly release the results of any revision to these forward-looking statements, except as required by law. Given these risks and uncertainties, readers are cautioned not to place undue reliance on such forward-looking statements.

Unless expressly indicated or the context requires otherwise, the terms "Facebook," "company," "we," "us," and "our" in this document refer to Facebook, Inc., a Delaware corporation, and, where appropriate, its wholly owned subsidiaries. The term "Facebook" may also refer to our products, regardless of the manner in which they are accessed. The term "Family" refers to our Facebook, Instagram, Messenger, and WhatsApp products. For references to accessing Facebook or our other products on the "web" or via a "website," such terms refer to accessing such products on personal computers. For references to accessing Facebook or our other products on "mobile," such term refers to accessing such products via a mobile application or via a mobile-optimized version of our websites such as m.facebook.com, whether on a mobile phone or tablet.

## LIMITATIONS OF KEY METRICS AND OTHER DATA

The numbers for our key metrics are calculated using internal company data based on the activity of user accounts. We have historically reported the numbers of our daily active users (DAUs), monthly active users (MAUs), and average revenue per user (ARPU) (collectively, our "Facebook metrics") based on user activity only on Facebook and Messenger and not on our other products. Beginning with this Annual Report on Form 10-K, we also are reporting our estimates of the numbers of our daily active people (DAP), monthly active people (MAP), and average revenue per person (ARPP) (collectively, our "Family metrics") based on the activity of users who visited at least one of Facebook, Instagram, Messenger, and WhatsApp (collectively, our "Family" of products) during the applicable period of measurement. We believe our Family metrics better reflect the size of our community and the fact that many people are using more than one of our products. As a result, over time we intend to report our Family metrics as our key metrics in place of DAUs, MAUs, and ARPU in our periodic reports filed with the Securities and Exchange Commission.

While these numbers are based on what we believe to be reasonable estimates of our user base for the applicable period of measurement, there are inherent challenges in measuring usage of our products across large online and mobile populations around the world. The methodologies used to measure these metrics require significant judgment and are also susceptible to algorithm or other technical errors. In addition, we are continually seeking to improve our estimates of our user base, and such estimates may change due to improvements or changes in our methodology. We regularly review our processes for calculating these metrics, and from time to time we discover inaccuracies in our metrics or make adjustments to improve their accuracy, which can result in adjustments to our historical metrics. Our ability to recalculate our historical metrics may be impacted by data limitations or other factors that require us to apply different methodologies for such adjustments. We generally do not intend to update previously disclosed Family metrics for any such inaccuracies or adjustments that are within the error margins disclosed below.

In addition, our Facebook metrics and Family metrics estimates will differ from estimates published by third parties due to differences in methodology.

### Facebook Metrics

We regularly evaluate our Facebook metrics to estimate the number of "duplicate" and "false" accounts among our MAUs. A duplicate account is one that a user maintains in addition to his or her principal account. We divide "false" accounts into two categories: (1) user-misclassified accounts, where users have created personal profiles for a business, organization, or non-human entity such as a pet (such entities are permitted on Facebook using a Page rather than a personal profile under our terms of service); and (2) violating accounts, which represent user profiles that we believe are intended to be used for purposes that violate our terms of service, such as bots and spam. The estimates of duplicate and false accounts are based on an internal review of a limited sample of accounts, and we apply significant judgment in making this determination. For example, to identify duplicate accounts we use data signals such as identical IP addresses and similar user names, and to identify false accounts we look for names that appear to be fake or other behavior that appears inauthentic to the reviewers. Any loss of access to data signals we use in this process, whether as a result of our own product decisions, actions by third-party browser or mobile platforms, regulatory or legislative requirements, or other factors, also may impact the stability or accuracy of our estimates of duplicate and false accounts. Our estimates also may change as our methodologies evolve, including through the application of new data signals or technologies or product changes that may allow us to identify previously undetected duplicate or false accounts and may improve our ability to evaluate a broader population of our users. Duplicate and false accounts are very difficult to measure at our scale, and it is possible that the actual number of duplicate and false accounts may vary significantly from our estimates.

In the fourth quarter of 2019, we estimated that duplicate accounts may have represented approximately 11% of our worldwide MAUs. We believe the percentage of duplicate accounts is meaningfully higher in developing markets such as the Philippines and Vietnam, as compared to more developed markets. In the fourth quarter of 2019, we estimated that false accounts may have represented approximately 5% of our worldwide MAUs. Our estimation of false accounts can vary as a result of episodic spikes in the creation of such accounts, which we have seen originate more frequently in specific countries such as Indonesia and Vietnam. From time to time, we disable certain user accounts, make product changes, or take other actions to reduce the number of duplicate or false accounts among our users, which may also reduce our DAU and MAU estimates in a particular period. We intend to disclose our estimates of the number of duplicate and false accounts among our MAUs on an annual basis.

## [Table of Contents](#)

The numbers of DAUs and MAUs discussed in this Annual Report on Form 10-K, as well as ARPU, do not include users on Instagram, WhatsApp, or our other products, unless they would otherwise qualify as DAUs or MAUs, respectively, based on their other activities on Facebook.

### **Family Metrics**

Many people in our community have user accounts on more than one of our products, and some people have multiple user accounts within an individual product. Accordingly, for our Family metrics, we do not seek to count the total number of user accounts across our products because we believe that would not reflect the actual size of our community. Rather, our Family metrics represent our estimates of the number of unique people using at least one of Facebook, Instagram, Messenger, and WhatsApp. We do not require people to use a common identifier or link their accounts to use multiple products in our Family, and therefore must seek to attribute multiple user accounts within and across products to individual people. To calculate these metrics, we rely upon complex techniques, algorithms and machine learning models that seek to count the individual people behind user accounts, including by matching multiple user accounts within an individual product and across multiple products when we believe they are attributable to a single person, and counting such group of accounts as one person. These techniques and models require significant judgment, are subject to data and other limitations discussed below, and inherently are subject to statistical variances and uncertainties. We estimate the potential error in our Family metrics primarily based on user survey data, which itself is subject to error as well. While we expect the error margin for our Family metrics to vary from period to period, we estimate that such margin generally will be approximately 3% of our worldwide MAP. At our scale, it is very difficult to attribute multiple user accounts within and across products to individual people, and it is possible that the actual numbers of unique people using our products may vary significantly from our estimates, potentially beyond our estimated error margins. As a result, it is also possible that our Family metrics may indicate changes or trends in user numbers that do not match actual changes or trends.

To calculate our estimates of Family DAP and MAP, we currently use a series of machine learning models that are developed based on internal reviews of limited samples of user accounts and calibrated against user survey data. We apply significant judgment in designing these models and calculating these estimates. For example, to match user accounts within individual products and across multiple products, we use data signals such as similar device information, IP addresses, and user names. We also calibrate our models against data from periodic user surveys of varying sizes and frequency across our products, which are inherently subject to error. In addition, our data limitations may affect our understanding of certain details of our business and increase the risk of error for our Family metrics estimates. Our techniques and models rely on a variety of data signals from different products, and we rely on more limited data signals for some products compared to others. For example, as a result of limited visibility into encrypted products, we have fewer data signals from WhatsApp user accounts and primarily rely on phone numbers and device information to match WhatsApp user accounts with accounts on our other products. Similarly, although Messenger Kids users are included in our Family metrics, we do not seek to match their accounts with accounts on our other applications for purposes of calculating DAP and MAP. Any loss of access to data signals we use in our process for calculating Family metrics, whether as a result of our own product decisions, actions by third-party browser or mobile platforms, regulatory or legislative requirements, or other factors, also may impact the stability or accuracy of our reported Family metrics. Our estimates of Family metrics also may change as our methodologies evolve, including through the application of new data signals or technologies, product changes, or other improvements in our user surveys, algorithms, or machine learning that may improve our ability to match accounts within and across our products or otherwise evaluate the broad population of our users. In addition, such evolution may allow us to identify previously undetected violating accounts (as defined below).

We regularly evaluate our Family metrics to estimate the percentage of our MAP consisting solely of "violating" accounts. We define "violating" accounts as accounts which we believe are intended to be used for purposes that violate our terms of service, including bots and spam. In the fourth quarter of 2019, we estimated that approximately 3% of our worldwide MAP consisted solely of violating accounts. Such estimation is based on an internal review of a limited sample of accounts, and we apply significant judgment in making this determination. For example, we look for account information and behaviors associated with Facebook and Instagram accounts that appear to be inauthentic to the reviewers, but we have limited visibility into WhatsApp user activity due to encryption. In addition, if we believe an individual person has one or more violating accounts, we do not include such person in our violating accounts estimation as long as we believe they have one account that does not constitute a violating account. From time to time, we disable certain user accounts, make product changes, or take other actions to reduce the number of violating accounts among our users, which may also reduce our DAP and MAP estimates in a particular period. We intend to disclose our estimates of the percentage of our MAP consisting solely of violating accounts on an annual basis. Violating accounts are very difficult to measure at our scale, and it is possible that the actual number of violating accounts may vary significantly from our estimates.



[Table of Contents](#)

The numbers of Family DAP and MAP discussed in this Annual Report on Form 10-K, as well as ARPP, do not include users on our other products, unless they would otherwise qualify as DAP or MAP, respectively, based on their other activities on our Family products.

**User Geography**

Our data regarding the geographic location of our users is estimated based on a number of factors, such as the user's IP address and self-disclosed location. These factors may not always accurately reflect the user's actual location. For example, a user may appear to be accessing Facebook from the location of the proxy server that the user connects to rather than from the user's actual location. The methodologies used to measure our metrics are also susceptible to algorithm or other technical errors, and our estimates for revenue by user location and revenue by user device are also affected by these factors.

Page Intentionally Left Blank

	<b>Year Ended December 31,</b>					
	<b>2019</b>	<b>2018</b>	<b>2017</b>	<b>2016</b>	<b>2015</b>	
	<b>(in millions)</b>					
Net cash provided by operating activities	\$ 36,314	\$ 29,274	\$ 24,216	\$ 16,108	\$ 10,320	
Less: Purchases of property and equipment, net	(15,102)	(13,915)	(6,733)	(4,491)	(2,523)	
Less: Principal payments on finance leases	(552)	—	—	—	—	
Free cash flow	\$ 20,660	\$ 15,359	\$ 17,483	\$ 11,617	\$ 7,797	











# Exhibit 24

04/10/2018 – Zuck and Kaplan behind him the entire day

<https://www.youtube.com/watch?v=BylLTX05jSY>



04/11/2018 – Zuck and Kaplan behind him the entire day

<https://www.youtube.com/watch?v=h3vkyVC7Qj8>



2019 – House Financial Services – Zuck and Kevin Martin behind him entire time

<https://www.youtube.com/watch?v=B1a5h5KncNM>



# Exhibit 25

FACEBOOK, SOCIAL MEDIA PRIVACY,  
AND THE USE AND ABUSE OF DATA

=====

JOINT HEARING

BEFORE THE

COMMITTEE ON COMMERCE,  
SCIENCE, AND TRANSPORTATION  
UNITED STATES SENATE

AND THE

COMMITTEE ON THE JUDICIARY  
UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

APRIL 10, 2018

Serial No. J-115-40

Printed for the use of the Committee on Commerce, Science, and  
Transportation

[GRAPHIC NOT AVAILABLE IN TIFF FORMAT]

Available online: <http://www.govinfo.gov>

U.S. GOVERNMENT PUBLISHING OFFICE

37-801 PDF

WASHINGTON : 2019

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

JOHN THUNE, South Dakota, Chairman

ROGER WICKER, Mississippi

ROY BLUNT, Missouri

TED CRUZ, Texas

DEB FISCHER, Nebraska

JERRY MORAN, Kansas

BILL NELSON, Florida, Ranking

MARIA CANTWELL, Washington

AMY KLOBUCHAR, Minnesota

RICHARD BLUMENTHAL, Connecticut

BRIAN SCHATZ, Hawaii

DAN SULLIVAN, Alaska	EDWARD MARKEY, Massachusetts
DEAN HELLER, Nevada	TOM UDALL, New Mexico
JAMES INHOFE, Oklahoma	GARY PETERS, Michigan
MIKE LEE, Utah	TAMMY BALDWIN, Wisconsin
RON JOHNSON, Wisconsin	TAMMY DUCKWORTH, Illinois
SHELLEY MOORE CAPITO, West Virginia	MAGGIE HASSAN, New Hampshire
CORY GARDNER, Colorado	CATHERINE CORTEZ MASTO, Nevada
TODD YOUNG, Indiana	JON TESTER, Montana

Nick Rossi, Staff Director  
 Adrian Arnakis, Deputy Staff Director  
 Jason Van Beek, General Counsel  
 Kim Lipsky, Democratic Staff Director  
 Chris Day, Democratic Deputy Staff Director  
 Renae Black, Senior Counsel

-----

SENATE COMMITTEE ON THE JUDICIARY

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

	CHUCK GRASSLEY, Iowa, Chairman
ORRIN HATCH, Utah	DIANNE FEINSTEIN, California,
LINDSEY GRAHAM, South Carolina	Ranking
JOHN CORNYN, Texas	PATRICK LEAHY, Vermont
MIKE LEE, Utah	RICHARD DURBIN, Illinois
TED CRUZ, Texas	SHELDON WHITEHOUSE, Rhode Island
BEN SASSE, Nebraska	AMY KLOBUCHAR, Minnesota
JEFF FLAKE, Arizona	CHRISTOPHER COONS, Delaware
MIKE CRAPO, Idaho	RICHARD BLUMENTHAL, Connecticut
THOM TILLIS, North Carolina	MAZIE HIRONO, Hawaii
JOHN KENNEDY, Louisiana	CORY BOOKER, New Jersey
	KAMALA HARRIS, California

C O N T E N T S

-----

	Page
Hearing held on April 10, 2018.....	1
Statement of Senator Grassley.....	1
Prepared statement.....	5
Statement of Senator Thune.....	2
Statement of Senator Feinstein.....	3
Letter dated April 9, 2018 from Faiz Shakir, National Political Director and Neema Singh Guliani, Legislative Counsel, American Civil Liberties Union.....	51
Letter dated April 9, 2018 to Senator Chuck Grassley, Senator Dianne Feinstein, Senator John Thune, and Senator Bill Nelson from Marc Rotenberg, President; Sunny Kang, International Consumer Counsel; Caitriona Fitzgerald, Policy Director; Sam Lester, Consumer Privacy Counsel; and Enid Zhou, Open Government Fellow, Electronic Privacy Information Center.....	54
Letter dated April 9, 2018 to Hon. John Thune, Hon. Charles Grassley, Hon. Bill Nelson and Hon. Dianne Feinstein from Stuart Shapiro, Chair, Association for Computing Machinery.	81
Comments dated April 9, 2018 from Carl Szabo, Vice President and General Counsel, NetChoice.....	84
Letter dated April 10, 2018 to Hon. Chuck Grassley, Hon. Dianne Feinstein, Hon. John Thune and Hon. Bill Nelson from Allison S. Bohm, Policy Counsel, Public Knowledge.....	88
Letter dated April 10, 2018 to Chairmen Grassley and Thune, and Ranking Members Feinstein and Nelson from Charles H.	

Rivkin, Chairman and CEO, Motion Picture Association of America.....	147
Statement of Senator Nelson.....	6
Prepared statement.....	7
Statement of Senator Hatch.....	21
Statement of Senator Cantwell.....	22
Statement of Senator Wicker.....	24
Statement of Senator Leahy.....	27
Statement of Senator Graham.....	29
Statement of Senator Klobuchar.....	32
Statement of Senator Blunt.....	34
Statement of Senator Durbin.....	38
Statement of Senator Cornyn.....	41
Statement of Senator Blumenthal.....	43
Statement of Senator Cruz.....	48
Statement of Senator Whitehouse.....	91
Statement of Senator Lee.....	93
Statement of Senator Schatz.....	95
Statement of Senator Fischer.....	97
Statement of Senator Coons.....	99
Statement of Senator Sasse.....	102
Statement of Senator Markey.....	103
Statement of Senator Flake.....	106
Statement of Senator Hirono.....	107
Statement of Senator Sullivan.....	109
Statement of Senator Udall.....	111
Statement of Senator Moran.....	114
Statement of Senator Booker.....	116
Statement of Senator Heller.....	118
Statement of Senator Peters.....	120
Statement of Senator Tillis.....	123
Statement of Senator Harris.....	125
Statement of Senator Kennedy.....	126
Statement of Senator Baldwin.....	128
Statement of Senator Johnson.....	131
Statement of Senator Hassan.....	133
Statement of Senator Capito.....	135
Statement of Senator Cortez Masto.....	138
Statement of Senator Gardner.....	139
Statement of Senator Tester.....	142
Statement of Senator Young.....	144

Witnesses

Mark Zuckerberg, Chairman and Chief Executive Officer, Facebook..	8
Prepared statement.....	9

Appendix

Letter dated April 10, 2018 to Hon. Chuck Grassley and Hon. Dianne Feinstein from Curt Levey, President, The Committee for Justice; and Ashley Baker, Director of Public Policy, The Committee for Justice.....	151
Statement dated April 10, 2018 from Daniel Castro, Vice President of Information Technology & Innovation Foundation (ITIF).....	154
Letter dated April 16, 2018 to Chairmen Grassley and Thune, and Ranking Members Feinstein and Nelson from Russell Hollander, National Executive Director, Directors Guild of America; David P. White, National Executive Director, SAG-AFTRA; and Matthew D. Loeb, International President, International Alliance of Theatrical Stage Employees.....	155
Letter dated April 19, 2018 to Hon. Chuck Grassley, Hon. Dianne Feinstein, Hon. John Thune and Hon. Bill Nelson from the American Federation of Musicians; Content Creators Coalition; CreativeFuture; and Independent Film & Television Alliance.....	156

Committee on Commerce, Science, and Transportation

Response to written questions submitted to Mark Zuckerberg by:

Hon. John Thune.....	159
Hon. Roger Wicker.....	164
Hon. Roy Blunt.....	168
Hon. Ted Cruz.....	171
Hon. Deb Fischer.....	215
Hon. Jerry Moran.....	217
Hon. Dan Sullivan.....	220
Hon. Bill Nelson.....	223
Hon. Maria Cantwell.....	226
Hon. Amy Klobuchar.....	229
Hon. Richard Blumenthal.....	229
Hon. Brian Schatz.....	243
Hon. Edward Markey.....	248
Hon. Tom Udall.....	249
Hon. Gary Peters.....	257
Hon. Tammy Baldwin.....	261
Hon. Tammy Duckworth.....	262
Hon. Maggie Hassan.....	265
Hon. Catherine Cortez Masto.....	273

Committee on the Judiciary

Response to written questions submitted to Mark Zuckerberg by:

Hon. Chuck Grassley.....	295
Hon. Orrin Hatch.....	307
Hon. Dianne Feinstein.....	309
Hon. Patrick Leahy.....	317
Hon. Richard Durbin.....	323
Hon. Sheldon Whitehouse.....	334
Hon. Amy Klobuchar.....	339
Hon. Christopher Coons.....	342
Hon. Mazie Hirono.....	353
Hon. Cory Booker.....	361
Hon. Kamala Harris.....	363

FACEBOOK, SOCIAL MEDIA PRIVACY,  
AND THE USE AND ABUSE OF DATA

-----

TUESDAY, APRIL 10, 2018

U.S. Senate,  
Committee on Commerce, Science, and Transportation, AND  
Committee on the Judiciary,  
Washington, DC.

The Committees met, pursuant to notice, at 2:30 p.m., in room 216, Hart Senate Office Building, Hon. Chuck Grassley, Chairman of the Committee on the Judiciary, presiding.

Present from the Committee on Commerce, Science, and Transportation: Senators Thune, Wicker, Blunt, Cruz, Fischer, Moran, Sullivan, Heller, Inhofe, Johnson, Capito, Gardner, Young, Nelson, Cantwell, Klobuchar, Blumenthal, Schatz, Markey, Udall, Peters, Baldwin, Hassan, Cortez Masto, and Tester.

Present from the Committee on the Judiciary: Senators Grassley [presiding], Hatch, Graham, Cornyn, Cruz, Lee, Sasse, Flake, Crapo, Tillis, Kennedy, Feinstein, Leahy, Durbin,

Whitehouse, Klobuchar, Coons, Blumenthal, Hirono, Booker, and Harris.

OPENING STATEMENT OF HON. CHUCK GRASSLEY,  
U.S. SENATOR FROM IOWA

Chairman Grassley. The committees on the Judiciary and Commerce, Science, and Transportation will come to order.

We welcome everyone to today's hearing on ``Facebook, Social Media Privacy, and the Use and Abuse of Data.'' Although not unprecedented, this is a unique hearing. The issues we will consider range from data privacy and security to consumer protection and the Federal Trade Commission enforcement, touching on jurisdictions of these two committees.

We have 44 members between our two committees. That may not seem like a large group by Facebook standards, but it is significant here for a hearing in the United States Senate. We will do our best to keep things moving efficiently, given our circumstances.

We will begin with opening statements from the chairmen and ranking members of each committee, starting with Chairman Thune, and then proceed with Mr. Zuckerberg's opening statement. We will then move on to questioning. Each member will have 5 minutes to question witnesses.

I would like to remind the members of both committees that time limits will be and must be strictly enforced given the numbers that we have here today. If you are over your time, Chairman Thune and I will make sure to let you know. There will not be a second round as well. Of course, there will be the usual follow-up written questions through the record. Questioning will alternate between majority and minority and between committees. We will proceed in order based on respective committee seniority.

We will anticipate a couple short breaks later in the afternoon, and so it is my pleasure to recognize the Chairman of the Commerce Committee, Chairman Thune, for his opening statement.

STATEMENT OF HON. JOHN THUNE,  
U.S. SENATOR FROM SOUTH DAKOTA

Chairman Thune. Thank you, Chairman Grassley.

Today's hearing is extraordinary. It is extraordinary to hold a joint committee hearing. It is even more extraordinary to have a single CEO testify before nearly half of the U.S. Senate. But then Facebook is pretty extraordinary. More than 2 billion people use Facebook every month. One point four billion people use it every day, more than the population of any country on Earth except China and more than four times the population of the United States. It is also more than 1,500 times the population of my home state of South Dakota. Plus, roughly 45 percent of American adults report getting at least some of their news from Facebook.

In many respects, Facebook's incredible reach is why we are here today. We are here because of what you, Mr. Zuckerberg, have described as a breach of trust. A quiz app used by approximately 300,000 people led to information about 87 million Facebook users being obtained by the company Cambridge Analytica. There are plenty of questions about the behavior of Cambridge Analytica, and we expect to hold a future hearing on Cambridge and similar firms.

But as you have said, this is not likely to be an isolated incident, a fact demonstrated by Facebook's suspension of another firm just this past weekend. You have promised that when Facebook discovers other apps that access to large amounts

of user data, you will ban them and tell those affected. And that is appropriate. But it is unlikely to be enough for the 2 billion Facebook users.

One reason that so many people are worried about this incident is what it says about how Facebook works. The idea that for every person who decided to try an app, information about nearly 300 other people was scraped from your services, to put it mildly, disturbing. And the fact that those 87 million people may have technically consented to making their data available does not make most people feel any better.

The recent revelation that malicious actors were able to utilize Facebook's default privacy settings to match e-mail addresses and phone numbers found on the so-called dark web to public Facebook profiles, potentially affecting all Facebook users, only adds fuel to the fire.

What binds these two incidents is that they do not appear to be caused by the kind of negligence that allows typical data breaches to happen. Instead, they both appear to be the result of people exploiting the very tools that you have created to manipulate users' information.

I know Facebook has taken several steps and intends to take more to address these issues. Nevertheless, some have warned that the actions Facebook is taking to ensure that third parties do not obtain data from unsuspecting users, while necessary, will actually serve to enhance Facebook's own ability to market such data exclusively.

Most of us understand that, whether you are using Facebook or Google or some other online services, we are trading certain information about ourselves for free or low-cost services. But for this model to persist, both sides of the bargain need to know the stakes that are involved. Right now, I am not convinced that Facebook users have the information that they need to make meaningful choices.

In the past, many of my colleagues on both sides of the aisle have been willing to defer to tech companies' efforts to regulate themselves, but this may be changing. Just last month, in overwhelming bipartisan fashion, Congress voted to make it easier for prosecutors and victims to go after websites that knowingly facilitate sex trafficking. This should be a wake-up call for the tech community. We want to hear more without delay about what Facebook and other companies plan to do to take greater responsibility for what happens on their platforms. How will you protect users' data? How will you inform users about the changes that you are making? And how do you intend to proactively stop harmful conduct instead of being forced to respond to it months or years later?

Mr. Zuckerberg, in many ways, you and the company that you have created, the story that you have created represent the American dream. Many are incredibly inspired by what you have done. At the same time, you have an obligation and it is up to you to ensure that that dream does not become a privacy nightmare for the scores of people who use Facebook.

This hearing is an opportunity to speak to those who believe in Facebook and to those who are deeply skeptical about it. We are listening, America is listening, and quite possibly, the world is listening, too.

Chairman Grassley. Thank you. And now, Ranking Member Feinstein.

STATEMENT OF HON. DIANNE FEINSTEIN,  
U.S. SENATOR FROM CALIFORNIA

Senator Feinstein. Thank you very much, Mr. Chairman. Chairman Grassley, Chairman Thune, thank you both for holding this hearing.

Mr. Zuckerberg, thank you for being here. You have a real opportunity this afternoon to lead the industry and demonstrate a meaningful commitment to protecting individual privacy.

We have learned over the past few months, and we have learned a great deal that is alarming. We have seen how foreign actors are abusing social media platforms like Facebook to interfere in elections and take millions of Americans' personal information without their knowledge in order to manipulate public opinion and target individual voters.

Specifically, on February 16, Special Counsel Mueller issued an indictment against the Russia-based Internet Research Agency and 13 of its employees for interfering with operations targeting the United States. Through this 37-page indictment, we learned that the IRA ran a coordinated campaign through 470 Facebook accounts and pages. The campaign included ads and false information to create discord and harm Secretary Clinton's campaign. And the content was seen by an estimated 157 million Americans.

A month later, on March 17, news broke that Cambridge Analytica exploited the personal information of approximately 50 million Facebook users without their knowledge or permission. And last week, we learned that number was even higher, 87 million Facebook users who had their private information taken without their consent. Specifically, using a personality quiz he created, Professor Kogan collected the personal information of 300,000 Facebook users and then collected data on millions of their friends. It appears the information collected included everything these individuals had on their Facebook pages and, according to some reports, even included private direct messages between users.

Professor Kogan is said to have taken data from over 70 million Americans. It has also been reported that he sold this data to Cambridge Analytica for \$800,000. Cambridge Analytica then took this data and created a psychological welfare tool to influence United States elections. In fact, the CEO Alexander Nix declared that Cambridge Analytica ran all the digital campaign, the television campaign, and its data informed all the strategy for the Trump campaign. The reporting has also speculated that Cambridge Analytica worked with the Internet Research Agency to help Russia identify which American voters to target with its propaganda.

I am concerned that press reports indicate Facebook learned about this breach in 2015 but appears not to have taken significant steps to address it until this year.

So this hearing is important, and I appreciate the conversation we had yesterday. And I believe that Facebook, through your presence here today and the words you are about to tell us, will indicate how strongly your industry will regulate and/or reform the platforms that they control. I believe this is extraordinarily important. You lead a big company with 27,000 employees, and we very much look forward to your comments.

Thank you, Mr. Chairman.

Chairman Grassley. Thank you, Senator Feinstein.

The history and growth of Facebook mirrors that of many of our technological giants. Founded by Mr. Zuckerberg in 2004, Facebook has exploded over the past 14 years. Facebook currently has over 2.13 billion monthly active users across the world, over than 25,000 employees, and offices in 13 U.S. cities and various other countries.

Like their expanding user base, the data collected on Facebook users has also skyrocketed. They have moved on from schools, likes, and relationship statuses. Today, Facebook has access to dozens of data points, ranging from ads that you have clicked on, events you have attended, and your location based

upon your mobile device.

It is no secret that Facebook makes money off this data through advertising revenue, although many seem confused by, or altogether unaware, of this fact. Facebook generated \$40 billion in revenue in 2017, with about 98 percent coming from advertising across Facebook and Instagram.

Significant data collection is also occurring at Google, Twitter, Apple, and Amazon. An ever-expanding portfolio of products and services offered by these companies grant endless opportunities to collect increasing amounts of information on their customers. As we get more free or extremely low-cost services, the tradeoff for the American consumer is to provide more personal data. The potential for further growth and innovation based on collection of data is limitless. However, the potential for abuse is also significant.

While the contours of the Cambridge Analytica situation are still coming to light, there was clearly a breach of consumer trust and a likely improper transfer of data. The Judiciary Committee will hold a separate hearing exploring Cambridge and other data privacy issues. More importantly though, these events have ignited a larger discussion on consumers' expectations and the future of data privacy in our society. It has exposed that consumers may not fully understand or appreciate the extent to which their data is collected, protected, transferred, used, and misused.

Data has been used in advertising and political campaigns for decades. The amount and type of data obtained, however, has seen a very dramatic change. Campaigns, including Presidents Bush, Obama, and Trump, all used these increasing amounts of data to focus on micro-targeting and personalization over numerous social media platforms, and especially Facebook.

In fact, President Obama's campaign developed an app utilizing the same Facebook feature as Cambridge Analytica to capture the information of not just the apps users, but millions of their friends. The digital director for that campaign for 2012 described the data-scraping app as something that would, ``wind up being the most groundbreaking piece of technology developed for this campaign.''

So the effectiveness of these social media tactics can be debated, but their use over the past years across the political spectrum and their increased significance cannot be ignored. Our policy toward data privacy and security must keep pace with these changes. Data privacy should be tethered to consumer needs and expectations.

Now, at a minimum, consumers must have the transparency necessary to make an informed decision about whether to share their data and how it can be used. Consumers ought to have clear information, not opaque policies and complex click-through consent pages. The tech industry has an obligation to respond to widespread and growing concerns over data privacy and security and to restore the public's trust. The status quo no longer works.

Moreover, Congress must determine if and how we need to strengthen privacy standards to ensure transparency and understanding for the billions of consumers who utilize these products.

[The prepared statement of Chairman Grassley follows:]

Prepared Statement of Hon. Chuck Grassley, U.S. Senator from Iowa

The history and growth of Facebook mirrors that of many of our technology giants. Founded by Mr. Zuckerberg in 2004, Facebook has exploded over the last 14 years. Facebook currently has 2.13 billion monthly active users across the world, more than 25,000 employees, and offices in 13 U.S. cities and various other countries.

Like their expanding user base, the data collected on Facebook

users has also skyrocketed. They have moved on from schools, likes, and relationship status. Today, Facebook has access to dozens of data points, ranging from ads you've clicked on, events you've attended, and your location based on your mobile device.

It is no secret that Facebook makes money off this data through advertising revenue, although many seem confused by, or altogether unaware, of this fact. Facebook generated \$40 billion in revenue in 2017, with about 98 percent coming from advertising across Facebook and Instagram.

Significant data collection is also occurring at Google, Twitter, Apple, and Amazon. An ever-expanding portfolio of products and services offered by these companies grant endless opportunities to collect increasing amounts of information on their customers. As we get more free, or extremely low-cost, services, the tradeoff for the American consumer is to provide more personal data.

The potential for further growth and innovation based on the collection of data is limitless. However, the potential for abuse is significant.

While the contours of the Cambridge Analytica situation are still coming to light, there was clearly a breach of consumer trust and a likely improper transfer of data. The Judiciary Committee will hold a separate hearing exploring Cambridge and other data privacy issues.

More importantly though, these events have ignited a larger discussion on consumers' expectations and the future of data privacy in our society.

It has exposed that consumers may not fully understand or appreciate the extent to which their data is collected, protected, transferred, used and misused.

Data has been used in advertising and political campaigns for decades. The amount and types of data obtained, however, has seen a dramatic change. Campaigns, including President Bush, Obama, and Trump, all used these increasing amounts of data to focus on micro-targeting and personalization over numerous social media platforms, especially Facebook.

In fact, President Obama's campaign developed an app utilizing the same Facebook feature as Cambridge Analytica to capture the information of not just the apps users, but millions of their friends. The digital director for Obama for America 2012 described the data-scraping app as something that would ``wind up being the most groundbreaking piece of technology developed for this campaign''.

The effectiveness of these social media tactics can be debated, but their use over the past years across the political spectrum and their increased significance cannot.

Our policy towards data privacy and security must keep pace with these changes. Data privacy should be tethered to consumer needs and expectations.

At a minimum, consumers must have the transparency necessary to make informed decisions about whether to share their data and how it can be used. Consumers ought to have clear information, not opaque policies and complex click-through consent pages.

The tech industry has an obligation to respond to widespread and growing concerns over data privacy and security and to restore the public trust. The status quo no longer works.

Moreover, Congress must determine if and how we need to strengthen privacy standards to ensure transparency and understanding for the billions of consumers who utilize these products.

Chairman Grassley. Senator Nelson.

STATEMENT OF HON. BILL NELSON,  
U.S. SENATOR FROM FLORIDA

Senator Nelson. Thank you, Mr. Chairman.

Mr. Zuckerberg, good afternoon.

Let me just cut to the chase. If you and other social media

companies do not get your act in order, none of us are going to have any privacy anymore. That is what we are facing. We are talking about personally identifiable information that, if not kept by the social media companies from theft, we will not have our personal privacy anymore, a value that we have in America.

It is the advent of technology, and of course all of us are part of it. From the moment that we wake up in the morning until we go to bed, we are on those handheld tablets, and online companies like Facebook are tracking our activities and collecting information. Facebook has a responsibility to protect this personal information.

We had a good discussion yesterday. We went over all of this. You told me that the company had failed to protect privacy. It is not the first time that Facebook has mishandled its users' information. The FTC found that Facebook's privacy policies had deceived users in the past. And in the present case, we recognize that Cambridge Analytica and an app developer lied to consumers and lied to you, lied to Facebook, but did Facebook watch over the operations? We want to know that. And why did Facebook not notify 87 million users that their personally identifiable information had been taken? And why were they not informed that it was also being used for unauthorized political purposes?

So only now--and I appreciate our conversation. Only now, Facebook has pledged to inform those consumers whose accounts were compromised. I think you are genuine. I got that sense in conversing with you. You want to do the right thing. You want to enact reforms. We want to know if it is going to be enough. And I hope that will be in the answers today.

Now, since we still do not know what Cambridge Analytica has done with this data, you heard Chairman Thune say, as we have discussed, we want to haul Cambridge Analytica in to answer these questions at a separate hearing.

I want to thank Chairman Thune for working with all of us on scheduling a hearing. There is obviously a great deal of interest in this subject. I hope we can get to the bottom of this. And if Facebook and other online companies will not or cannot fix the privacy invasions, then we are going to have to, we, the Congress. How can American consumers trust folks like your company to be caretakers of their most personal and identifiable information? And that is the question. Thank you.

[The prepared statement of Senator Nelson follows:]

Prepared Statement of Hon. Bill Nelson, U.S. Senator from Florida

Let me get to the point, one that I made to Mr. Zuckerberg yesterday during our lengthy conversation in my office. If Facebook and other social media and online companies don't do a better job as stewards of our personal information, American consumers are no longer going to have any privacy to protect.

From the minute consumers wake up to the minute they put down their smartphone at the end of the day, online companies like Facebook are tracking their activities and collecting information. Facebook has a responsibility to protect this personal information.

Unfortunately, I believe that the company failed to do so. This is not the first time that Facebook has mishandled its users' information. The Federal Trade Commission found that Facebook's privacy policies had deceived users in the past.

In the present case, I recognize that Cambridge Analytica and an app developer lied to consumers and lied to Facebook. But did Facebook watch over their operations? And why didn't Facebook notify eighty-seven million users when it discovered that Cambridge Analytica had inappropriately gotten hold of their sensitive information and was using it for unauthorized political purposes?

Only now has Facebook pledged to inform those consumers whose accounts were compromised. I know Mr. Zuckerberg wants to do the right

thing and enact reforms, but will it be enough? I hope to get some answers today.

Lastly, we still don't know exactly what Cambridge Analytica has done with this data. That's why I have asked Chairman Thune to haul Cambridge Analytica in to answer these questions at a separate hearing. I want to thank the chairman for working with me on scheduling a hearing in the near future.

There is obviously a great deal of interest in this subject, and I hope that we can get to the bottom line. That is, if Facebook and other online companies will not or cannot fix these privacy invasions, then we will. How can American consumers trust them to be caretakers of their most personal and identifiable information?

Chairman Grassley. Thank you, my colleagues, and Senator Nelson.

Our witness today is Mark Zuckerberg, Founder, Chairman, Chief Executive Officer of Facebook. Mr. Zuckerberg launched Facebook February 4, 2004, at the age of 19. And at that time he was a student at Harvard University. As I mentioned previously, his company now has over \$40 billion of annual revenue and over 2 billion monthly active users. Mr. Zuckerberg, along with his wife, also established the Chan Zuckerberg Initiative to further philanthropic causes.

I now turn to you. Welcome to the Committee. And whatever your statement is orally, if you have a longer one, it will be included in the record. So, proceed, sir.

STATEMENT OF MARK ZUCKERBERG, CHAIRMAN  
AND CHIEF EXECUTIVE OFFICER, FACEBOOK

Mr. Zuckerberg. Chairman Grassley, Chairman Thune, Ranking Member Feinstein, and Ranking Member Nelson and members of the Committee, we face a number of important issues around privacy, safety, and democracy, and you will rightfully have some hard questions for me to answer. Before I talk about the steps we are taking to address them, I want to talk about how we got here.

Facebook is an idealistic and optimistic company. For most of our existence, we focused on all of the good that connecting people can do. And as Facebook has grown, people everywhere have gotten a powerful new tool for staying connected to the people they love, for making their voices heard, and for building communities and businesses. Just recently, we have seen the #metoo movement and the March for Our Lives organized, at least in part, on Facebook. After Hurricane Harvey, people came together to raise more than \$20 million for relief. And more than 70 million small businesses use Facebook to create jobs and grow.

But it is clear now that we did not do enough to prevent these tools for being used for harm as well, and that goes for fake news, for foreign interference in elections, and hate speech, as well as developers and data privacy. We did not take a broad enough view of our responsibility, and that was a big mistake. And it was my mistake, and I am sorry. I started Facebook, I run it, and I am responsible for what happens here.

So now, we have to go through all of our relationship with people and make sure that we are taking a broad enough view of our responsibility. It is not enough to just connect people; we have to make sure that those connections are positive. It is not enough to just give people a voice; we need to make sure that people are not using it to harm other people or to spread misinformation. And it is not enough to just give people control over their information; we need to make sure that the developers they share it with protect their information, too. Across the board, we have a responsibility to not just build

tools but to make sure that they are used for good.

It will take some time to work through all the changes we need to make across the company, but I am committed to getting this right. This includes the basic responsibility of protecting people's information, which we failed to do with Cambridge Analytica. So here are a few things that we are doing to address this and to prevent it from happening again.

First, we are getting to the bottom of exactly what Cambridge Analytica did and telling everyone affected. What we know now is that Cambridge Analytica improperly accessed some information about millions of Facebook members by buying it from an app developer. This was information that people generally shared publicly on their Facebook pages like names and their profile picture and the pages they follow.

When we first contacted Cambridge Analytica, they told us that they had deleted the data. About a month ago, we heard new reports that suggested that was not true. And now, we are working with governments in the U.S., the U.K., and around the world to do a full audit of what they have done and to make sure that they get rid of any data they may still have.

Second, to make sure no other app developers out there are misusing data, we are now investigating every single app that had access to a large amount of information in the past. And if we find that someone improperly used data, we are going to ban them from Facebook and tell everyone affected.

Third, to prevent this from ever happening again going forward, we are making sure that developers cannot access as much information now. The good news here is that we already made big changes to our platform in 2014 that would have prevented this specific situation with Cambridge Analytica from occurring again today. But there is more to do, and you can find more details on the steps we are taking in my written statement.

My top priority has always been our social mission of connecting people, building community, and bringing the world closer together. Advertisers and developers will never take priority over that as long as I am running Facebook.

I started Facebook when I was in college. We have come a long way since then. We now serve more than 2 billion people around the world, and every day, people use our services to stay connected with the people that matter to them most. I believe deeply in what we are doing, and I know that when we address these challenges, we will look back and view helping people connect and giving more people a voice is a positive force in the world.

I realize the issues we are talking about today are not just issues for Facebook and our community; they are issues and

























# Exhibit 26

# FACEBOOK: TRANSPARENCY AND USE OF CONSUMER DATA

---

---

## HEARING BEFORE THE COMMITTEE ON ENERGY AND COMMERCE HOUSE OF REPRESENTATIVES ONE HUNDRED FIFTEENTH CONGRESS SECOND SESSION

APRIL 11, 2018

**Serial No. 115-114**



Printed for the use of the Committee on Energy and Commerce  
*energycommerce.house.gov*

U.S. GOVERNMENT PUBLISHING OFFICE

30-956 PDF

WASHINGTON : 2018

COMMITTEE ON ENERGY AND COMMERCE

GREG WALDEN, Oregon

*Chairman*

JOE BARTON, Texas

*Vice Chairman*

FRED UPTON, Michigan

JOHN SHIMKUS, Illinois

MICHAEL C. BURGESS, Texas

MARSHA BLACKBURN, Tennessee

STEVE SCALISE, Louisiana

ROBERT E. LATTA, Ohio

CATHY McMORRIS RODGERS, Washington

GREGG HARPER, Mississippi

LEONARD LANCE, New Jersey

BRETT GUTHRIE, Kentucky

PETE OLSON, Texas

DAVID B. MCKINLEY, West Virginia

ADAM KINZINGER, Illinois

H. MORGAN GRIFFITH, Virginia

GUS M. BILIRAKIS, Florida

BILL JOHNSON, Ohio

BILLY LONG, Missouri

LARRY BUCSHON, Indiana

BILL FLORES, Texas

SUSAN W. BROOKS, Indiana

MARKWAYNE MULLIN, Oklahoma

RICHARD HUDSON, North Carolina

CHRIS COLLINS, New York

KEVIN CRAMER, North Dakota

TIM WALBERG, Michigan

MIMI WALTERS, California

RYAN A. COSTELLO, Pennsylvania

EARL L. "BUDDY" CARTER, Georgia

JEFF DUNCAN, South Carolina

FRANK PALLONE, JR., New Jersey

*Ranking Member*

BOBBY L. RUSH, Illinois

ANNA G. ESHOO, California

ELIOT L. ENGEL, New York

GENE GREEN, Texas

DIANA DeGETTE, Colorado

MICHAEL F. DOYLE, Pennsylvania

JANICE D. SCHAKOWSKY, Illinois

G.K. BUTTERFIELD, North Carolina

DORIS O. MATSUI, California

KATHY CASTOR, Florida

JOHN P. SARBANES, Maryland

JERRY McNERNEY, California

PETER WELCH, Vermont

BEN RAY LUJAN, New Mexico

PAUL TONKO, New York

YVETTE D. CLARKE, New York

DAVID LOEBSACK, Iowa

KURT SCHRADER, Oregon

JOSEPH P. KENNEDY, III, Massachusetts

TONY CARDENAS, California

RAUL RUIZ, California

SCOTT H. PETERS, California

DEBBIE DINGELL, Michigan

# C O N T E N T S

---

	Page
Hon. Greg Walden, a Representative in Congress from the State of Oregon, opening statement .....	2
Prepared statement .....	4
Hon. Frank Pallone, Jr., a Representative in Congress from the State of New Jersey, opening statement .....	5
Prepared statement .....	6

## WITNESS

Mark Zuckerberg, Cofounder, Chairman, and Chief Executive Officer, Facebook, Inc. ....	8
Prepared statement .....	10
Answers to submitted questions <sup>1</sup> .....	212

## SUBMITTED MATERIAL

Subcommittee memorandum .....	106
Article of November 20, 2012, “Friended: How the Obama Campaign Con- nected with Young Voters,” by Michael Scherer, Time, submitted by Mr. Burgess .....	112
Article of April 9, 2018, “We Already Know How to Protect Ourselves From Facebook,” by Zeynep Tufekci, New York Times, submitted by Mr. Burgess .	114
Article of March 21, 2018, “It’s Time to Break Up Facebook,” by Eric Wilson, Politico, submitted by Mr. Burgess .....	118
Letter of April 9, 2018, from Faiz Shakir, National Political Director, and Neema Singh Guliani, Legislative Counsel, American Civil Liberties Union, to Representatives in Congress, submitted by Mr. Walden .....	120
Statement of NetChoice by Carl Szabo, Vice President and General Counsel, April 9, 2018, submitted by Mr. Walden .....	125
Letter of April 5, 2018, from John Rowan, National President and Chief Executive Officer, Vietnam Veterans of America, to Mr. Walden and Mr. Pallone, submitted by Mr. Walden .....	131
Letter of April 11, 2018, from Allison S. Bohm, Policy Counsel, Public Knowl- edge, to Mr. Walden and Mr. Pallone, submitted by Mr. Walden .....	142
Letter of April 10, 2018, from Marc Rotenberg, President, Electronic Privacy Information Center, et al., to House Energy and Commerce Committee members, submitted by Mr. Walden .....	147
Federal Trade Commission Complaint of December 17, 2009, by Marc Rotenberg, President, Electronic Privacy Information Center, et al., sub- mitted by Mr. Walden .....	163
Letter of April 10, 2018, from Charles H. Rivkin, Chairman and Chief Execu- tive Officer, Motion Picture Association of America, to Mr. Walden and Mr. Pallone, submitted by Mr. Walden .....	192
Letter of April 10, 2018, from Morgan Reed, President, ACT, the App Associa- tion, to Mr. Walden and Mr. Pallone, submitted by Mr. Walden .....	193
Letter of April 10, 2018, from Curt Levey, President, and Ashley Baker, Director of Public Policy, the Committee for Justice, to Mr. Walden and Mr. Pallone, submitted by Mr. Walden .....	201

<sup>1</sup> Questions for the record and responses from Facebook, Inc., have been retained in committee files and also are available at <https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=108090>.

IV

	Page
Letter of April 9, 2018, from Jeffrey Chester, U.S. Co-Chair, and Finn Lützow-Holm Myrstad, EU Co-Chair, Digital Policy Committee, Trans Atlantic Consumer Dialogue, to Mark Zuckerberg, Chief Executive Officer, Facebook, submitted by Mr. Walden .....	205
Letter of October 30, 2017, from Arab American Institute, et al., to Mark Zuckerberg, Chief Executive Officer, and Sheryl Sandberg, Chief Operating Officer, Facebook, submitted by Mr. Walden .....	206
Statement of National Council of Negro Women by Janice L. Mathis, Executive Director, April 10, 2018, submitted by Mr. Walden .....	211

## **FACEBOOK: TRANSPARENCY AND USE OF CONSUMER DATA**

**WEDNESDAY, APRIL 11, 2018**

HOUSE OF REPRESENTATIVES,  
COMMITTEE ON ENERGY AND COMMERCE,  
WASHINGTON, DC.

The committee met, pursuant to call, at 9:59 a.m., in room 2123, Rayburn House Office Building, Hon. Greg Walden (chairman of the committee) presiding.

Members present: Representatives Walden, Barton, Upton, Shimkus, Burgess, Blackburn, Scalise, Latta, McMorris Rodgers, Harper, Lance, Guthrie, Olson, McKinley, Kinzinger, Griffith, Bilirakis, Johnson, Long, Bucshon, Flores, Brooks, Mullin, Hudson, Collins, Cramer, Walberg, Walters, Costello, Carter, Duncan, Pallone, Rush, Eshoo, Engel, Green, DeGette, Doyle, Schakowsky, Butterfield, Matsui, Castor, Sarbanes, McNerney, Welch, Luján, Tonko, Clarke, Loeb sack, Schrader, Kennedy, Cárdenas, Ruiz, Peters, and Dingell.

Staff present: Jon Adame, Policy Coordinator, Communications and Technology; Mike Bloomquist, Staff Director; Daniel Butler, Staff Assistant; Karen Christian, General Counsel; Kelly Collins, Legislative Clerk, Energy/Environment; Zack Dareshori, Legislative Clerk, Health; Jordan Davis, Director of Policy and External Affairs; Melissa Froelich, Chief Counsel, Digital Commerce and Consumer Protection; Adam Fromm, Director of Outreach and Coalitions; Ali Fulling, Legislative Clerk, Oversight and Investigations, Digital Commerce and Consumer Protection; Theresa Gambo, Human Resources and Office Administrator; Brighton Haslett, Counsel, Oversight and Investigations; Elena Hernandez, Press Secretary; Zach Hunter, Communications Director; Paul Jackson, Professional Staff Member, Digital Commerce and Consumer Protection; Peter Kiely, Deputy General Counsel; Bijan Koohmaraie, Counsel, Digital Commerce and Consumer Protection; Ryan Long, Deputy Staff Director; Milly Lothian, Press Assistant and Digital Coordinator; Mark Ratner, Policy Coordinator; Austin Stonebraker, Press Assistant; Evan Viau, Legislative Clerk, Communications and Technology; Hamlin Wade, Special Advisor for External Affairs; Everett Winnick, Director of Information Technology; Greg Zerzan, Counsel, Digital Commerce and Consumer Protection; Michelle Ash, Minority Chief Counsel, Digital Commerce and Consumer Protection; Julie Babayan, Minority Counsel; Jeff Carroll, Minority Staff Director; Jennifer Epperson, Minority FCC Detailee; David Goldman, Minority Chief Counsel, Communications and Technology; Lisa Goldman, Minority Counsel; Tiffany Guarascio,

Minority Deputy Staff Director and Chief Health Advisor; Zach Kahan, Minority Outreach and Member Services Coordinator; Jerry Leverich III, Minority Counsel; Dan Miller, Minority Policy Analyst; Caroline Paris-Behr, Minority Policy Analyst; Kaitlyn Peel, Minority Digital Director; Tim Robinson, Minority Chief Counsel; Michelle Rusk, Minority FTC Detailee; Andrew Souvall, Minority Director of Communications; and C.J. Young, Minority Press Secretary.

Mr. WALDEN. The Committee on Energy and Commerce will now come to order.

Before my opening statement, just as a reminder to our committee members on both sides, it is another busy day at Energy and Commerce. In addition, as you will recall, to this morning's Facebook hearing, later today our Health Subcommittee will hold its third in the series of legislative hearings on solutions to combat the opioid crisis. And remember, our Oversight and Investigations Subcommittee will hold a hearing where we will get an update on the restoration of Puerto Rico's electric infrastructure following last year's hurricane season.

So, just a reminder, when this hearing concludes, I think we have votes on the House floor. Our intent is to get through every Member before that point to be able to ask questions, but then after the votes, we will come back into our subcommittees to do that work. As Ray Baum used to say, the fun never stops.

The Chair now recognizes himself for 5 minutes for purposes of an opening statement.

**OPENING STATEMENT OF HON. GREG WALDEN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OREGON**

Good morning. Welcome, Mr. Zuckerberg, to the Energy and Commerce Committee in the House. We have called you here today for two reasons: One is to examine the alarming reports regarding breaches of trust between your company, one of the biggest and most powerful in the world, and its users; and the second reason is to widen our lens to larger questions about the fundamental relationship tech companies have with their users.

The incident involving Cambridge Analytica and the compromised personal information of approximately 87 million American users—or mostly American users—is deeply disturbing to this committee.

The American people are concerned about how Facebook protects and profits from its users' data. In short, does Facebook keep its end of the agreement with its users? How should we as policymakers evaluate and respond to these events?

Does Congress need to clarify whether or not consumers own or have any real power over their online data? Have edge providers grown to the point that they need Federal supervision?

You and your cofounders started a company in your dorm room that has grown to be one of the biggest and most successful businesses in the entire world. Through innovation and quintessentially American entrepreneurial spirit, Facebook and the tech companies that have flourished in Silicon Valley join the legacy of great American companies who build our Nation, drove our economy forward, and created jobs and opportunity. And you did it

Page Intentionally Left Blank

The second thing that we do is we provide an ad network that third-party websites and apps can run in order to help them make money. And those ads, similar to what Google does and what the rest of the industry does, it is not limited to people who are just on Facebook. So, for the purposes of that, we may also collect information to make it so that those ads are more relevant and work better on those websites.

There is a control that for that second class of information or an ad targeting anyone can turn off, has complete control over it. For obvious reasons, we do not allow people to turn off the measurement that we do around security.

Mr. WALDEN. The gentleman's time has expired.

We now turn to the gentleman from New York, Mr. Engel, for 4 minutes.

Mr. ENGEL. Thank you, Mr. Chairman.

Mr. Zuckerberg, you have roots in my district, the 16th Congressional District of New York. I know that you attended Ardsley High School and grew up in Westchester County. As you know, Westchester has a lot to offer, and I hope that you might commit to returning to Westchester County perhaps to do a forum on this and some other things. I hope you would consider that. We will be in touch with you. But I know that Ardsley High School is very proud of you.

You mentioned yesterday that Facebook was deceived by Aleksandr Kogan when he sold the user information to Cambridge Analytica. Does Facebook therefore plan to sue Aleksandr Kogan, Cambridge University, or Cambridge Analytica perhaps for unauthorized access to computer networks, exceeding access to computer networks, or breach of contract, and why or why not?

Mr. ZUCKERBERG. Congressman, it is something that we are looking into. We already took action by banning him from the platform, and we are going to be doing a full audit to make sure that he gets rid of all the data that he has as well.

To your point about Cambridge University, what we found now is that there was a whole program associated with Cambridge University where a number of researchers, not just Aleksandr Kogan—although to our current knowledge, he is the only one who sold the data to Cambridge Analytica.

There were a number of other researchers who were building similar apps. So we do need to understand whether there is something bad going on at Cambridge University overall that will require a stronger action from us.

Mr. ENGEL. You mentioned before in your remarks hate speech. We have seen the scale and reach of extremism balloon in the last decade, partially because of the expansion of social platforms, whether it is a white supremacist rally in Charlottesville that turned violent or to ethnic cleansing in Burma that resulted in the second largest refugee crisis in the world.

Are you aware of any foreign or domestic terrorist organizations, hate groups, criminal networks, or other extremist networks that have scraped Facebook user data? And if they have and if they do it in the future, how would you go about getting it back or deleting it?

Mr. ZUCKERBERG. Congressman, we are not aware of any specific groups like that that have engaged in this. We are, as I have said, conducting a full investigation of any apps that had access to a large amount of data, and if we find anything suspicious, we will tell everyone affected.

We do not allow hate groups on Facebook overall. So, if there is a group that their primary purpose or a large part of what they do is spreading hate, we will ban them from the platform overall.

Mr. ENGEL. So do you adjust your algorithms to prevent individuals interested in violence or nefarious activities from being connected with other like-minded individuals?

Mr. ZUCKERBERG. Sorry. Could you repeat that?

Mr. ENGEL. Do you adjust your algorithms to prevent individuals interested in violence or bad activities from being connected with other like-minded individuals?

Mr. ZUCKERBERG. Congressman, yes. That is certainly an important thing that we need to do.

Mr. ENGEL. OK. And, finally, let me say this: Many of us are very angry about Russian influence in the 2016 Presidential elections and Russian influence over our Presidential elections.

Does Facebook have the ability to detect when a foreign entity is attempting to buy a political ad, and is that process automated? Do you have procedures in place to inform key Government players when a foreign entity is attempting to buy a political ad or when it might be taking other steps to interfere in an election?

Mr. ZUCKERBERG. Congressman, yes. This is an extremely important area. After we were slow to identify the Russian information operations in 2016, this has become a top priority for our company to prevent that from ever happening again, especially this year in 2018, which is such an important election year with the U.S. midterms, but also major elections in India, Brazil, Mexico, Hungary, Pakistan, a number of other places.

So we are doing a number of things that I am happy to talk about or follow up with afterwards around deploying new AI tools that can proactively catch fake accounts that Russia or others might create to spread misinformation.

And one thing that I will end on here, just because I know we are running low on time, is, since the 2016 election, there have been a number of significant elections, including the French Presidential election, the German election, and last year the U.S. Senate Alabama special election.

And the AI tools that we deployed in those elections were able to proactively take down tens of thousands of fake accounts that may have been trying to do the activity that you are talking about. So our tools are getting better.

For as long as Russia has people who are employed who are trying to perpetrate this kind of interference, it will be hard for us to guarantee that we are going to fully stop everything. But it is an arms race, and I think that we are making ground and are doing better and better and are confident about how we are going to be able to do that.

Mr. WALDEN. The gentleman's time has expired.

Mr. ENGEL. Thank you.

Mr. WALDEN. The Chair recognizes the chairman of the Health Subcommittee, Dr. Burgess of Texas, for 4 minutes.

Mr. BURGESS. Thank you, Mr. Chairman.

And thanks to our witness for being here today.

Mr. Chairman, I have a number of articles that I am going to ask unanimous consent to insert into the record. I know I won't have time to get to all of my questions.

Mr. WALDEN. Without objection.

[The information appears at the conclusion of the hearing.]

Mr. WALDEN. And we put the slide up that you requested.

Mr. BURGESS. And so I am going to be submitting some questions for the record that are referencing these articles: One is, "Friended: How the Obama Campaign Connected With Young Voters," by Michael Scherer; "We Already Know How to Protect Ourselves from Facebook"—and I hope I get this name right—Zeynep Tufekci; and "It's Time to Break Up Facebook" by Eric Wilson, who, in the interest of full disclosure, is a former staffer.

Mr. WALDEN. Without objection.

Mr. BURGESS. And I will be referencing those articles in some written questions.

I consulted my technology guru, Scott Adams, in the form of Dilbert. Going back 21 years ago, when you took the shrink wrap off of a piece of software that you bought, you were automatically agreeing to be bound by the terms and conditions. So we have gone a long way from taking the shrink wrap off of an app.

But I don't know that things have changed all that much. I guess, does Facebook have a position that you recommend for elements of a company's terms and conditions that you encourage consumers to look at before they click on the acceptance?

Mr. ZUCKERBERG. Congressman, yes. I think that it is really important for this service that people understand what they are doing and signing up for and how this service works. We have laid out all of what we do in the terms of service because that is what is legally required of us. But—

Mr. BURGESS. Let me just ask you, because we are going to run short on time, have you laid out for people what it would be indicative of a good actor versus a less-than-good actor in someone who has developed one of these applications?

Mr. ZUCKERBERG. Congressman, yes. We have a developer terms of service, which is separate from the normal terms of service for individuals using the service.

Mr. BURGESS. Is the average consumer able to determine what elements would indicate poor or weak consumer protections just by their evaluation of the terms and conditions? Do you think that is possible?

Mr. ZUCKERBERG. Congressman, I am not sure what you mean by that.

Mr. BURGESS. Well, can the average person, the average layperson look at the terms and conditions and make the evaluation, is this a strong enough protection for me to enter into this arrangement?

Look, I am as bad as anyone else. I see an app. I want it. I download it. I breeze through the stuff. Just take me to the good

Page Intentionally Left Blank

information age. Data breaches and privacy hacks are not a question of if; they are a question of when.

The case with Facebook is slightly different. The 87 million accounts extracted by Cambridge Analytica are just the beginning, with likely dozens of other third parties that have accessed this information. As far as we know, the dam is still broken.

As you have noted, Mr. Zuckerberg, Facebook's business model is based on capitalizing on the private personal information of your users. Data security should be a central pillar of this model.

And with your latest vast breach of privacy and the widespread political manipulation that followed it, the question this committee must ask itself is what role the Federal Government should play in protecting the American people and the democratic institutions that your platform and others like it have put at risk.

In this case, you gave permission to mine the data of some 87 million users based on the deceptive consent of just a fraction of that number. When they found out I was going to be speaking with you today, my constituents asked me to share some of their concerns in person.

How can they protect themselves on your platform? Why should they trust you again with their likes, their loves, their lives? Users trusted Facebook to prioritize user privacy and data security, and that trust has been shattered. I am encouraged that Facebook is committed to making changes, but I am indeed wary that you are only acting now out of concern for your brand and only making changes that should have been made a long time ago.

You have described this as an arms race, but every time we saw what precautions you have or, in most cases, have not taken your company is caught unprepared and ready to issue another apology. I am left wondering again why Congress should trust you again. We will be watching you closely to ensure that Facebook follows through on these commitments.

Many of my constituents have asked about your business model where users are the product. Mary of Halfmoon, in my district, called it infuriating. Andy of Schenectady, New York, asked, why doesn't Facebook pay its users for their incredibly valuable data. Facebook claims that users rightly own and control their data, yet their data keeps being exposed on your platform, and these breaches cause more and more harm each time.

You have said that Facebook was built to empower its users; instead, users are having their information abused with absolutely no recourse. In light of this harm, what liability should Facebook have? When users' data is mishandled, who is responsible, and what recourse do users have? Do you bear that liability?

Mr. ZUCKERBERG. Congressman, I think we are responsible for protecting people's information for sure. But one thing that you said that I want to provide some clarity on—

Mr. TONKO. Do you bear the liability?

Mr. ZUCKERBERG. Well, you said earlier, you referenced that you thought that we were only taking action after this came to light. Actually, we made significant changes to the platform in 2014 that would have made this incident with Cambridge Analytica impossible to happen again today.

I wish we had made those changes a couple of years earlier because this poll app got people to use it back in 2013 and 2014, and if we had made the changes a couple of years earlier, then we would have——

Mr. WALDEN. The gentleman's time has expired.

The Chair recognizes——

Mr. TONKO. Mr. Chairman, if I might ask that other questions that my constituents have be entered by unanimous consent.

Mr. WALDEN. Sure. Without objection, of course.

[The information appears at the conclusion of the hearing.]

Mr. WALDEN. That goes for all Members.

The Chair recognizes the gentleman from Florida, Mr. Bilirakis, for 4 minutes.

Mr. BILIRAKIS. Thank you. Thank you, Mr. Chairman. I appreciate it.

And thanks for your testimony, Mr. Zuckerberg.

Well, first of all, I wanted to follow up with Mr. McKinley's testimony. This is bad stuff, Mr. Zuckerberg, with regard to the illegal online pharmacies. When are those ads—I mean, when are you going to take those off? I think we need an answer to that. I think we need to get these off as soon as possible.

Can you give us an answer, a clear answer as to when these pharmacies—we have an epidemic here with regard to the opioids. I think we are owed a clear answer, a definitive answer as to when these ads will be offline.

Mr. ZUCKERBERG. Congressman, if people flag those ads for us, we will take them down now.

Mr. BILIRAKIS. Now?

Mr. ZUCKERBERG. Yes.

Mr. BILIRAKIS. By the end of the day?

Mr. ZUCKERBERG. If people flag them for us, we will look at them as quickly as we can.

Mr. BILIRAKIS. Well, you have knowledge now, obviously.

Mr. ZUCKERBERG. Sorry?

Mr. BILIRAKIS. You have knowledge of those ads. Will you begin to take them down today?

Mr. ZUCKERBERG. The ads that are flagged for us we will review and take down if they violate our policies, which I believe the ones that you are talking about——

Mr. BILIRAKIS. They clearly do. If they are illegal, they clearly violate your policy.

Mr. ZUCKERBERG. Which they do. But what I think really needs to happen here is not just us reviewing content that gets flagged for us. We need to be able to build tools that can proactively go out and identify what might be these ads for opioids before people even have to flag them for us to review.

Mr. BILIRAKIS. I agree.

Mr. ZUCKERBERG. And that is going to be a longer-term thing in order to build that solution. So but, today, if someone flags the ads for us, we will take them down.

Mr. BILIRAKIS. Work on those tools as soon as possible, please.

OK. Next question. A constituent of mine in District 12 of Florida, Tampa Bay area, came to me recently with what was a clear violation of your privacy policy. In this case, a third-party organiza-

tion publicly posted personal information about my constituent on his Facebook page.

This included his home address, voting record, degrading photos, and other information. In my opinion, this is cyberbullying. For weeks, my constituent tried reaching out to Facebook on multiple occasions through its report feature, but the offending content remained. It was only when my office got involved that the posts were removed almost immediately for violating Facebook policy.

How does Facebook's self-reporting policy work to prevent misuse, and why did it take an act of Congress, a Member of Congress, to get, again, a clear privacy violation removed from Facebook? If you can answer that question, I would appreciate it, please.

Mr. ZUCKERBERG. Congressman, that clearly sounds like a big issue and something that would violate our policies. I don't know have specific knowledge of that case, but what I imagine happened, given what you just said, is they reported it to us and one of the people who reviews content probably made an enforcement error. And then when you reached out, we probably looked at it again and realized that it violated the policies and took it down.

We have a number of steps that we need to take to improve the accuracy of our enforcement.

Mr. BILIRAKIS. Absolutely.

Mr. ZUCKERBERG. That is a big issue, and we need to get to content faster, and we need to be able to do better at this. I think the same solution to the opioid question that you raised earlier of doing more with automated tools will lead to both faster response times and more accurate enforcement of the policies.

Mr. BILIRAKIS. Can you give us a timeline, as to when will this be done? I mean, this is very critical for—I mean, listen, my family uses Facebook, my friends, my constituents. We all use Facebook. I use Facebook. It is wonderful for our seniors to connect with their relatives.

Mr. WALDEN. The gentleman's time has expired.

Mr. BILIRAKIS. Yes. I am sorry. Can I submit for the record my additional questions?

Mr. WALDEN. Yes, sir.

Mr. BILIRAKIS. Thank you. Thank you so much.

Mr. WALDEN. The Chair recognizes the gentlelady from New York, Ms. Clarke, for 4 minutes.

Ms. CLARKE. I thank you, Mr. Chairman.

And thank you for coming before us, Mr. Zuckerberg, today.

I want to take the opportunity to represent the concerns of the newly formed Tech Accountability Caucus, in which I serve as a co-chair with my colleagues, Representative Robin Kelly, Congressman Emanuel Cleaver, and Congresswoman Bonnie Watson Coleman, but, most importantly, people in our country and around the globe or in vulnerable populations, including those who look just like me.

My first question to you is, as you may be aware, there have been numerous media reports about how more than 3,000 Russian ads were bought on Facebook to incite racial and religious division and chaos in the U.S. during the 2016 election.

Those ads specifically characterized and weaponized African American groups like Black Lives Matter, in which ads suggested

# Exhibit 27

June 8, 2018

Chairman Chuck Grassley  
Ranking Member Dianne Feinstein  
U.S. Senate Committee on the Judiciary  
224 Dirksen Senate Office Building  
Washington, D.C. 20510-6050

Dear Chairman Grassley, Ranking Member Feinstein, and Members of the Committee:

Thank you for your questions for the record from the April 10, 2018 Hearing titled Facebook, Social Media Privacy, and the Use and Abuse of Data. Per your request, attached are the answers for the record for your questions.

Please note that we received over 2,000 questions from the Senate and House Committees before which we testified on April 10 and 11, 2018. We appreciate the extra time you gave us to respond to these questions. We did our best to review and answer them in the available timeframe. We respectfully request an opportunity to supplement or amend our responses if needed.

Sincerely,

Facebook, Inc.

## Questions from Senator Booker

1. **In 2016, ProPublica revealed that advertisers could use “ethnic affinity” marketing categories to potentially discriminate against Facebook users in the areas of housing, employment, and credit, in violation of federal law. While you committed in November 2016 to “build tools to detect and automatically disable the use of ethnic-affinity marketing for certain types of ads,” a year later ProPublica found that the system you built was still letting housing ads through without applying the new restrictions. It was chalked up to a “technical failure.” You then opted for system where advertisers self-certify that they are complying with federal law and Facebook’s antidiscrimination policy, but in fact just last month, several fair housing organizations filed a lawsuit against Facebook in the S.D.N.Y. alleging discrimination in housing advertising based not just on race, but also on disability, gender, and familial status. According to the lawsuit, the most recent ad buys were still occurring just weeks ago in late February 2018.**

- a. **Is a self-certification model the strongest way to safeguard against discrimination?**

Our Terms and Advertising Policies have long emphasized our prohibition on the use of Facebook’s platform to engage in wrongful discrimination. Starting in late 2016, we began implementing additional protections for the people who use Facebook. Specifically, we set out to help better educate advertisers about our policies against discrimination and relevant federal and state laws, and to help prevent the abuse of our tools. First, we updated our Advertising Policies applicable to all advertisers and advertisements to strengthen our prohibition against discrimination, and we added a section to provide advertisers with antidiscrimination educational resources from government agencies and civil rights groups. Second, we implemented technical measures aimed at better protecting users from wrongful discrimination by advertisers that offer housing, employment and credit opportunities. Specifically, when we identify one of these types of ads, we require the advertiser to certify that it is complying with our anti-discrimination policy and with applicable law. We reject thousands of ads a day where the advertiser fails to certify.

- b. **Would it be better to not serve ads in certain categories (housing/credit/employment) at all?**

We have heard concerns about third party advertisers misusing these tools to engage in wrongful discrimination with respect to ads for housing, credit, and employment by targeting people based on the protected characteristics outlined in your questions. Based on feedback we have received from our community, and from policymakers, regulators, civil rights experts, and consumer advocates, we have limited the targeting options we offer for such advertisements that relate to protected classes as follows:

- We do not offer targeting based on race, religion, disability, sexual orientation, or gender identity.

- We do not offer targeting based on national origin, but we do have segments composed of “ex-pats”—people who used to live in particular countries (and may or may not be from these countries originally).
- We do permit some targeting based on family status (e.g., people who are parents), but we generally do not permit advertisers to exclude people from their audiences based on family status. Please note, however, that in limited cases and for the purpose of running ads that are not related to housing, employment or credit, we are re-enabling the ability of advertisers to exclude people from their audiences based on family status but are reviewing this as a targeting option.
- Like other major ad platforms, we enable targeting based on age and gender.
- We offer targeting options—called “interests” and “behaviors”—that are based on people’s activities on Facebook, and when, where and how they connect to the Internet (such as the kind of device they use and their mobile carrier). These options do not reflect people’s personal characteristics, but we still take precautions to limit the potential for advertisers to misuse them. For example, we do not create interest or behavior segments that suggest the people in the segment are members of sensitive groups such as particular races, ethnicities, or religions. We therefore would not create an interest segment called “Muslims,” because it could be misunderstood to enable an advertiser to reach people based on their religious beliefs.
- We also offer what we call the multicultural affinity segments, which are groups of people whose activities on Facebook suggest they may be interested in content related to the African American, Asian American, or Hispanic American communities. (For example, if a person “likes” Facebook Pages with the words “African American” in them or likes Pages for Historically Black Colleges and Universities, that person may be included in the African American multicultural segment.) As we explain to advertisers in our tools, these segments are based on people’s activities on Facebook, not on race or ethnicity (which categories Facebook does not enable people to even include on their profiles).
- We have gone even further when it comes to using the “exclude” feature in our ads tools. This feature is designed to help advertisers refine their audiences by, for example, excluding people who are already interested in their products. But we recognize that permitting exclusions could, in some circumstances, raise the risk that an advertiser would engage in wrongful discrimination. For that reason, many of the targeting audiences that advertisers can choose to include in the group eligible to see their ad are not available for exclusion. For example, while we believe it is important that organizations be able to affirmatively reach people in the multicultural affinity segments, advertisers are not able to exclude people from their audiences based on the multicultural affinity segments.
- We also recently added a notice below the “exclude” field that reminds advertisers of their obligations under our non-discrimination policy as well as under relevant

applicable law in a persistent manner when they create their advertisements and define their audiences.

- In early 2017, we launched machine learning tools (called “classifiers”) that were intended to automatically identify, once an ad was entered into our systems, employment, credit, and housing ads. We built these classifiers so that when one of these kinds of ads was identified, we could take two actions that would make it harder for advertisers to misuse our tools.
- c. Given your inability to fix something as straightforward as discriminatory housing ads, why should Congress trust Facebook’s ability to target and reduce suspicious election activity?**

These industry-wide problems are not easy to solve, but we are committed to doing better by implementing the steps outlined throughout this document.

- d. How does Facebook prevent advertisers from using their own data to segment users by race or other protected categories using Facebook’s Custom Audiences feature?**

See Response to Question 1, part c.

- 2. In responding to a November 2016 class action lawsuit against Facebook for discrimination in housing, employment, and credit, Facebook moved to dismiss the complaint on the basis that the plaintiffs were not injured.**
- a. Do you believe that people of color who are not recruited for various economic opportunities are harmed by not hearing about those opportunities?**

We have Community Standards that prohibit hate speech, bullying, intimidation, and other kinds of harmful behavior. We hold advertisers to even stricter advertising policies to protect users from things like discriminatory ads. We don’t want advertising to be used for hate or discrimination, and our policies reflect that. For example, we make it clear that advertisers may not discriminate against people based on personal attributes such as race, ethnicity, color, national origin, religion, age, sex, sexual orientation, gender identity, family status, disability, and medical or genetic condition. We educate advertisers on our anti-discrimination policy, and in some cases—including when we detect that an advertiser is running a housing ad—we require advertisers to certify compliance with our anti-discrimination policy and anti-discrimination laws.

- 3. A 2016 investigation by the ACLU of California revealed that another app developer, Geofeedia, was using data from Facebook and other platforms to help law enforcement monitor the activities of peacefully protesting civilians of color. In response, Facebook changed its policy to prohibit any developers from facilitating the surveillance of Facebook users.**

- a. You have endorsed Black Lives Matter and expressed sympathy after Philando Castile’s killing, which was broadcast on Facebook Live. Despite this, why should communities of color trust Facebook has sufficiently addressed this surveillance issue?**
- b. Is simply changing the language of your terms of service enough? Have you taken any other steps to prevent another Geofeedia from attempting something similar?**

In March 2017, we added language to our Facebook and Instagram platform policies to more clearly explain that developers cannot use data obtained from us to provide tools that are used for surveillance. Our previous policy limited developers’ use of data but did not explicitly mention surveillance. We found out that some developers created and marketed tools meant for surveillance, took action, and we clarified our policy.

Page Intentionally Left Blank

about Facebook as a service rather than as an entity, please answer the question as applied to both Facebook as a service as well as all of Facebook’s affiliated entities or platforms.

## II. Questions

- 1) **Please attach a copy of each and every formal or informal policy, whether presently written or otherwise, regarding the moderation, promotion, evaluation, or alteration of users or content on Facebook. These include, for example, Facebook’s Terms of Service, its Community Guidelines, and similar policies.**

Facebook’s Terms and Policies are available here: <https://www.facebook.com/policies>.  
Facebook’s Community Standards are available at <https://www.facebook.com/communitystandards/>.

- 2) **Yes or no: Are Facebook’s decisions to permit users access to its services or to permit content to remain displayed on its services, or the prominence or accessibility of that content, including its order, visibility, duration visible, inclusion in searches or order within search results, inclusion within “Trending” lists or analogous suggestions of content to users, determined in whole or part by Facebook’s corporate values, beliefs, priorities, or opinions?**
  - a) **Yes or no: Does Facebook promote, demote, or block users or content based on its assessment of the social value or social desirability of that content?**
  - b) **Yes or no: Does Facebook promote, demote, or block users or content based on its assessment of that content’s truth or falsity?**
  - c) **Yes or no: Does Facebook promote, demote, or block users or content based on its assessment of the content’s agreement or disagreement with Facebook’s corporate values, beliefs, priorities, or opinions?**

The conversations that happen on Facebook reflect the diversity and free expression of a community of more than two billion people communicating across countries and cultures and in dozens of languages, posting everything from text to photos and videos.

With regard the order and visibility of content, a user’s News Feed is made up of stories from their friends, Pages they’ve chosen to follow and groups they’ve joined. *Ranking* is the process we use to organize all of those stories so that users can see the most relevant content at the top, every time they open Facebook. Ranking has four elements: the available *inventory* of stories; the *signals*, or data points that can inform ranking decisions; the *predictions* we make, including how likely we think they are to comment on a story, share with a friend, etc.; and a *relevancy score* for each story.

Misleading or harmful content on Facebook comes in many different forms, from annoyances like clickbait to hate speech and violent content. When we detect this kind of content in News Feed, there are three types of actions we take: remove it, reduce its spread, or inform people with additional context.

Our Community Standards and Ads Policies outline the content that is not allowed on the platform, such as hate speech, fake accounts, and praise, support, or representation of terrorism/terrorists. When we find things that violate these standards, we remove them. There are other types of problematic content that, although they don't violate our policies, are still misleading or harmful and that our community has told us they don't want to see on Facebook—things like clickbait or sensationalism. When we find examples of this kind of content, we reduce its spread in News Feed using ranking and, increasingly, we inform users with additional context so they can decide whether to read, trust, or share it.

The goal of our Community Standards is to encourage expression and create a safe environment. We base our policies on input from our community and from experts in fields such as technology and public safety. Our policies are also rooted in the following principles:

- (1) Safety: People need to feel safe in order to build community. We are committed to removing content that encourages real-world harm, including (but not limited to) physical, financial, and emotional injury.
- (2) Voice: Our mission is all about embracing diverse views. We err on the side of allowing content, even when some find it objectionable, unless removing that content can prevent a specific harm. Moreover, at times we will allow content that might otherwise violate our standards if we feel that it is newsworthy, significant, or important to the public interest. We do this only after weighing the public interest value of the content against the risk of real-world harm; and
- (3) Equity: Our community is global and diverse. Our policies may seem broad, but that is because we apply them consistently and fairly to a community that transcends regions, cultures, and languages. As a result, our Community Standards can sometimes appear less nuanced than we would like, leading to an outcome that is at odds with their underlying purpose. For that reason, in some cases, and when we are provided with additional context, we make a decision based on the spirit, rather than the letter, of the policy.

**3) Yes or no: Have Facebook's decisions to permit users access to its services or to permit content to remain displayed on its services, or the prominence or accessibility of that content, including its order, visibility, duration visible, inclusion in searches or order within search results, inclusion within "Trending" lists or analogous suggestions of content to users, ever been determined in whole or part by Facebook's corporate values, beliefs, priorities, or opinions?**

See Response to Question 2.

- a) **Yes or no: Has Facebook ever promoted, demoted, or blocked users or content based on its assessment of the social value or social desirability of that content?**

See Response to Question 2.

**b) Yes or no: Has Facebook ever promoted, demoted, or blocked users or content based on its assessment of that content’s truth or falsity?**

See Response to Question 2.

**c) Yes or no: Has Facebook ever promoted, demoted, or blocked users or content based on its assessment of the content’s agreement or disagreement with Facebook’s corporate values, beliefs, priorities, or opinions?**

See Response to Question 2.

**4) Yes or no: Does Facebook employ its corporate values, beliefs, priorities, or opinions when deciding what content Facebook removes, republishes, moderates, promotes, or otherwise increases or decreases access to content?**

The conversations that happen on Facebook reflect the diversity of a community of more than two billion people communicating across countries and cultures and in dozens of languages, posting everything from text to photos and videos.

We recognize how important it is for Facebook to be a place where people feel empowered to communicate, and we take our role in keeping abuse off our service seriously. That’s why we have developed a set of Community Standards that outline what is and is not allowed on Facebook. Our Standards apply around the world to all types of content. They’re designed to be comprehensive—for example, content that might not be considered hate speech may still be removed for violating our bullying policies.

The goal of our Community Standards is to encourage expression and create a safe environment. We base our policies on input from our community and from experts in fields such as technology and public safety. Our policies are also rooted in the following principles:

- (1) **Safety:** People need to feel safe in order to build community. We are committed to removing content that encourages real-world harm, including (but not limited to) physical, financial, and emotional injury.
- (2) **Voice:** Our mission is all about embracing diverse views. We err on the side of allowing content, even when some find it objectionable, unless removing that content can prevent a specific harm. Moreover, at times we will allow content that might otherwise violate our standards if we feel that it is newsworthy, significant, or important to the public interest. We do this only after weighing the public interest value of the content against the risk of real-world harm; and
- (3) **Equity:** Our community is global and diverse. Our policies may seem broad, but that is because we apply them consistently and fairly to a community that transcends regions, cultures, and languages. As a result, our Community Standards can sometimes appear less nuanced than we would like, leading to an outcome that is at odds with their underlying purpose. For that reason, in some cases, and when we are provided with additional context, we make a decision based on the spirit, rather than the letter, of the policy.

Page Intentionally Left Blank

**marriage? If so, please include the removed post identifying information indicating its author.**

- j) Under what circumstances does Facebook remove, downgrade, conceal, or otherwise censor content that, though not threatening physical harm, promoting imminent physical self-harm, or advocating for terrorism, opposes same-sex marriage?**
- k) Under what circumstances does Facebook remove, downgrade, conceal, or otherwise censor content that, though not threatening physical harm, promoting imminent physical self-harm, or advocating for terrorism, supports same-sex marriage?**

In July 2012, our automated systems incorrectly removed an event page entitled “Chick-fil-A Appreciation Day.” The page was restored within hours of coming to our attention. When we make mistakes on these important content decisions, we make every attempt to make it right as quickly as we can.

Our goal is to allow people to have as much expression as possible, including on the issue of same-sex marriage. We err on the side of allowing content, even when some find it objectionable, unless removing that content prevents a specific harm.

See also Response to Question 27.

**36) As described in the Washington Post, in October 2012, Facebook removed a post by a group called “Special Operations Speaks.” The post said: “Obama called the SEALs and THEY got bin Laden. When the SEALs called Obama, they got denied,” a reference to the failure of the Executive Branch to provide military support to Americans under assault, and later killed, in Benghazi. Facebook first warned the group that the post violated its rules and then subsequently removed the post as a violation of “Facebook’s Statements of Rights and Responsibilities.” Facebook further suspended Special Operations Speaks for 24 hours following the removal. Facebook later admitted error and permitted the content to remain on its platform.**

- a) Why was Special Operations Speaks’ post removed?**
- b) What term of Facebook’s then-extant 2012 Statement of Rights and Responsibilities was Special Operations Speaks’ post thought to have violated before Facebook reversed its decision?**
- c) Yes or no: Did any member of the Obama Administration, including any administrative agency then-directed by an executive official appointed by the Obama administration, contact Facebook to request that the post be removed?**
  - i) If so, whom?**
  - ii) What was Facebook’s response?**

- d) **Yes or no: Did Facebook assure any government official or employee that this post would be removed? If so, whom?**
- e) **Did Special Operations Speaks' post violate Facebook's prohibition on "hate speech," either in 2012 or now?**
- f) **As of October 2012, had Facebook removed, downgraded, concealed, or otherwise censored any other content created by a political action committee on the basis of that content's disapproval of how the Obama administration handled the attack on U.S. diplomats and servicemen in Benghazi? If so, please include the removed content including identifying information about its author.**
- g) **As of October 2012, had Facebook removed, downgraded, concealed, or otherwise censored any content created by a political action committee on the basis of that content's approval of how the Obama administration handled the attack on U.S. diplomats and servicemen in Benghazi? If so, please include the removed content including identifying information about its author.**
- h) **Has, since October 2012, Facebook removed, downgraded, concealed, or otherwise censored any posts by a political action committee on the basis of that content's disapproval of how the Obama administration handled the attack on U.S. diplomats and servicemen in Benghazi? If so, please include the removed content including identifying information about its author.**
- i) **Has, since October 2012, Facebook removed, downgraded, concealed, or otherwise censored any posts by a political action committee on the basis of that content's disapproval of how the Obama administration handled the attack on**  
**U.S. diplomats and servicemen in Benghazi? If so, please include the removed content including identifying information about its author.**
- j) **Under what circumstances does Facebook remove, downgrade, conceal, or otherwise censor content that, though not threatening physical harm, promoting imminent physical self-harm, or advocating for terrorism, opposes the Obama Administration's handling of the attacks on U.S. diplomats and servicemen in Benghazi?**
- k) **Under what circumstances does Facebook remove, downgrade, conceal, or otherwise censor content that, though not threatening physical harm, promoting imminent physical self-harm, supports the Obama Administration's handling of the attacks on U.S. diplomats and servicemen in Benghazi?**

In this particular case, we removed the content as a violation of our standards. The content was deleted for 29 hours. However, we realized that we made a mistake, and we restored the content and apologized for the error.

We define hate speech as a direct attack on people based on what we call protected characteristics—race, ethnicity, national origin, religious affiliation, sexual orientation, sex, gender, gender identity, and serious disability or disease. We also provide some protections for immigration status. We define attack as violent or dehumanizing speech, statements of inferiority, and calls for exclusion or segregation. Our detailed hate speech policies are available at [https://www.facebook.com/communitystandards/objectionable\\_content/hate\\_speech](https://www.facebook.com/communitystandards/objectionable_content/hate_speech).

Our Community Standards prohibit hate speech and celebrating graphic violence and allow people to use Facebook to raise awareness of and condemn violence. Drawing that line requires complex and nuanced judgments, and we carefully review reports that we receive from the public, media, civil society, and governments. We remove content that violates our policies, regardless of who posted the content.

**37) In September 2017, Facebook deemed the videos of two African American Trump supporters, known as Diamond and Silk, as “dangerous.” In a company email, Facebook stated that the decision was final and “not appealable in any way.” Facebook then retracted this statement, explaining that the determination was inaccurate.**

- a) What about Diamond and Silk did Facebook initially determine to be “dangerous?”**
- b) What is Facebook’s criteria for determining whether content that neither depicts nor advocates for violence as “dangerous?”**
- c) Aside from the illustration of or advocacy for violence, under what conditions is the discussion of non-classified speech “dangerous?”**
- d) Has Facebook implemented an appeals system by which users can challenge a determination of dangerousness?**
- e) How often does Facebook retract these determinations?**
- f) What is the internal review process for these types of determinations?**

We mishandled communication with Diamond and Silk for months. Their frustration was understandable, and we apologized to them. The message they received on April 5, 2018 that characterized their Page as “dangerous” was incorrect and not reflective of the way we seek to communicate with our community and the people who run Pages on our platform.

As part of our commitment to continually improve our products and to minimize risks where human judgment is involved, we are making a number of changes:

- We have engaged an outside advisor, former Senator Jon Kyl, to advise the company on potential bias against conservative voices. We believe this external feedback will help us improve over time and ensure we can most effectively serve our diverse community.
- We continue to expand our list of outside organizations from across the political spectrum to provide feedback on potential changes to our content standards.
- We have made our detailed reviewer guidelines public to help people understand how and why we make decisions about the content that is and is not allowed on Facebook.
- We have launched an appeals process to enable people to contest content decisions with which they disagree. We recognize that we make enforcement errors on both sides of the equation—what to allow, and what to remove—and that our mistakes cause a great deal of concern for people, which is why we need to allow the option to request review of the decision and provide additional context that will help our team see the fuller picture as they review the post again. This type of feedback will allow us to continue improving our systems and processes so we can prevent similar mistakes in the future.

See also Response to Question 27.

**38) In October 2017, the social-media company Twitter refused to permit Representative Marsha Blackburn to pay to promote a campaign advertisement because Rep. Blackburn stated that she fought to stop the sale of children’s body parts. Twitter’s explanation was that Blackburn’s critique of “the sale of baby body parts” was an “inflammatory statement” that Twitter refused to advertise.**

- a) Does Representative Blackburn’s campaign advertisement (available readily on the internet) violate Facebook’s policies regarding acceptable advertisements?**
- b) Does Representative Blackburn’s campaign advertisement violate Facebook’s policies against “hate speech?”**
- c) Would the statement, standing alone, that Planned Parenthood sells baby body parts qualify as “hate speech?”**
- d) Would Facebook censor or otherwise downgrade or make unavailable the statement that Planned Parenthood sells baby body parts for any other reason?**

As Facebook indicated publicly in October 2017, Representative Blackburn’s campaign advertisement, in which she mentioned “the sale of baby body parts” does not violate our Advertising Policies or our Community Standards.

We work to strike the right balance between enabling free expression around the globe and ensuring that our platform is safe. We currently define hate speech as anything that directly

attacks people based on protected characteristics—race, ethnicity, national origin, religious affiliation, sexual orientation, sex, gender, gender identity, or serious disability or disease. We remove content that violates our policies, regardless of who posted the content, including the government.

Our policies allow content that may be controversial and at times even distasteful, but which does not cross the line into hate speech. This may include criticism of public figures, religions, professions, and political ideologies.

**39) Louis Farrakhan presently employs Facebook to reach numerous individuals. At present, he has over a million followers.**

**a) On his Facebook page, Farrakhan links to an open letter of his which states: “We can now present to our people and the world a *true*, undeniable record of the relationship between Blacks and Jews from their own mouths and pens. These scholars, Rabbis and historians have given to us an undeniable record of Jewish anti-Black behavior, starting with the horror of the trans-Atlantic slave trade, plantation slavery, Jim Crow, sharecropping, the labor movement of the North and South, the unions and the misuse of our people that continues to this very moment.”**

**i) Does this statement violate Facebook’s policies against “hate speech?”**

**ii) If so, why has this post been permitted to remain?**

**iii) If not, why not?**

**b) On his Facebook page, Farrakhan links to a sermon in which he describes the “Synagogue of Satan” and its attempts to harm him.**

**i) Is the term “Synagogue of Satan” a violation of Facebook’s policies against “hate speech?”**

**ii) If so, why has this post been permitted to remain?**

**iii) If not, why not?**

We are committed to designing our products to give all people a voice and foster the free flow of ideas and culture. That said, when something crosses the line into hate speech, it has no place on Facebook, and we are committed to removing it from our platform any time we become aware of it.

We define hate speech as a direct attack on people based on what we call protected characteristics—race, ethnicity, national origin, religious affiliation, sexual orientation, sex, gender, gender identity, and serious disability or disease. We also provide some protections for immigration status. We define attack as violent or dehumanizing speech, statements of inferiority, and calls for exclusion or segregation. The detailed guidelines our reviewers use to

assess whether content violates our hate speech policies are available at [https://www.facebook.com/communitystandards/objectionable\\_content/hate\\_speech](https://www.facebook.com/communitystandards/objectionable_content/hate_speech).

**40) In June 2013, Facebook blocked the following post written by Fox News Radio’s Todd Starnes for violating Facebook’s community standards, “I’m about as politically incorrect as you can get. I’m wearing an NRA ball cap, eating a Chick-fil-A sandwich, reading a Paula Deen cookbook and sipping a 20-ounce sweet tea while sitting in my Cracker Barrel rocking chair with the Gather Vocal Band singing ‘Jesus Saves’ on the stereo and a Gideon’s Bible in my pocket. Yes sir, I’m politically incorrect and happy as a June bug.” Although Facebook ultimately reversed its decision, for several hours, Todd Starnes could not access either his fan or person page.**

- a) Why was Todd Starnes’ post removed?**
- b) What Facebook rule was Todd Starnes’ post thought to have violated before it was reinstated?**
- c) Was any part of Starnes’ statement “hate speech?”**
- d) Was any part of Starnes’ statement considered harassment?**
- e) Yes or no: must posted content be “politically correct” to remain in accordance with Facebook’s community standards?**
- f) Is a statement that something is not “politically correct” a violation of Facebook’s standards?**

The page where Todd Starnes posted the content was not unpublished. He was the administrator that made the post, and the action was taken on his profile. He posted the content at around 2 am on June 29, 2013, and it was restored shortly before 10 am the same day. During that time, he did not lose his ability to access either his profile or his page, just the post itself. When we reinstated the post, we sent him an apology the same day.

Our policies apply equally to individuals and entities across the political spectrum. We are committed to designing our products to give all people a voice and foster the free flow of ideas and culture. That said, when something crosses the line into hate speech, it has no place on Facebook, and we are committed to removing it from our platform any time we become aware of it.

We recognize that our policies are only as good as the strength and accuracy of our enforcement—and our enforcement is not perfect. We make mistakes because our processes involve people, and people are not infallible. We are always working to improve.

When we’re made aware of incorrect content removals, we review them with team members so as to prevent similar mistakes in the future. We also audit the accuracy of reviewer decisions on an ongoing basis to coach them and follow up on improving, where errors are being made.

# Exhibit 28

OPEN HEARING ON FOREIGN INFLUENCE  
OPERATIONS' USE OF SOCIAL MEDIA PLATFORMS  
(COMPANY WITNESSES)

=====

HEARING  
BEFORE THE  
SELECT COMMITTEE ON INTELLIGENCE  
OF THE  
UNITED STATES SENATE  
ONE HUNDRED FIFTEENTH CONGRESS  
SECOND SESSION

\_\_\_\_\_  
WEDNESDAY, SEPTEMBER 5, 2018  
\_\_\_\_\_

Printed for the use of the Select Committee on Intelligence

[GRAPHIC NOT AVAILABLE IN TIFF FORMAT]

Available via the World Wide Web: <http://www.govinfo.gov>

\_\_\_\_\_  
U.S. GOVERNMENT PUBLISHING OFFICE  
31-350 PDF WASHINGTON : 2019

-----  
For sale by the Superintendent of Documents, U.S. Government Publishing Office,  
<http://bookstore.gpo.gov>. For more information, contact the GPO Customer Contact Center,  
U.S. Government Publishing Office. Phone 202-512-1800, or 866-512-1800 (toll-free).  
E-mail, [gpo@custhelp.com](mailto:gpo@custhelp.com).

SELECT COMMITTEE ON INTELLIGENCE

[Established by S. Res. 400, 94th Cong., 2d Sess.]

RICHARD BURR, North Carolina, Chairman  
MARK R. WARNER, Virginia, Vice Chairman

JAMES E. RISCH, Idaho  
MARCO RUBIO, Florida  
SUSAN COLLINS, Maine  
ROY BLUNT, Missouri  
JAMES LANKFORD, Oklahoma  
TOM COTTON, Arkansas  
JOHN CORNYN, Texas

DIANNE FEINSTEIN, California  
RON WYDEN, Oregon  
MARTIN HEINRICH, New Mexico  
ANGUS KING, Maine  
JOE MANCHIN III, West Virginia  
KAMALA HARRIS, California

MITCH McCONNELL, Kentucky, Ex Officio  
CHUCK SCHUMER, New York, Ex Officio  
JAMES INHOFE, Oklahoma, Ex Officio  
JACK REED, Rhode Island, Ex Officio

-----  
Chris Joyner, Staff Director  
Michael Casey, Minority Staff Director  
Kelsey Stroud Bailey, Chief Clerk

CONTENTS

-----  
SEPTEMBER 5, 2018

OPENING STATEMENTS

Burr, Hon. Richard, Chairman, a U.S. Senator from North Carolina. 1  
Warner, Mark R., Vice Chairman, a U.S. Senator from Virginia..... 3

WITNESSES

Sandberg, Sheryl, Chief Operating Officer, Facebook..... 6  
Prepared statement..... 9  
Dorsey, Jack, Chief Executive Officer, Twitter, Inc..... 19  
Prepared statement..... 21

SUPPLEMENTAL MATERIAL

Responses to Questions for the Record by:  
Sheryl Sandberg..... 68  
Jack Dorsey..... 133

OPEN HEARING ON FOREIGN INFLUENCE  
OPERATIONS' USE OF SOCIAL MEDIA  
PLATFORMS (COMPANY WITNESSES)

-----  
WEDNESDAY, SEPTEMBER 5, 2018

U.S. Senate,  
Select Committee on Intelligence,  
Washington, DC.

The Committee met, pursuant to notice, at 9:32 a.m., in Room G-50, Dirksen Senate Office Building, Hon. Richard Burr (Chairman of the Committee) presiding.

Present: Senators Burr, Warner, Risch, Rubio, Collins, Blunt, Lankford, Cotton, Wyden, Heinrich, King, Manchin, Harris, and Reed.

OPENING STATEMENT OF HON. RICHARD BURR, CHAIRMAN, A U.S. SENATOR FROM NORTH CAROLINA

Chairman Burr. I'd like to call the hearing to order. And I'd like to welcome our witnesses today: Jack Dorsey, chief executive officer at Twitter--Jack, welcome--and Sheryl Sandberg, chief operating officer at Facebook. I thank both of you for being here with us this morning.

Before I make my remarks, I want to say a few words about our colleague, our friend, and committee ex officio member Senator John McCain.

John could be blunt, and he could be direct, but when it came to committing himself to a cause that he believed in, John McCain was without equal. This Senate, this deliberative body, with its history and its traditions, will survive the passing of John McCain, but there can be no denying that the place is a little smaller without him. We will continue to do the important work we do here with passion, resolve, and a sense of purpose born from moral conviction. John would want that. In fact, he would insist on it from each of us.

My friends, if I can borrow the phrase: Arizona's loss is our loss, and our loss is America's loss. John McCain will be dearly missed, and as you can see, we have set his spot on the dais today.

Jack, Sheryl--as a committee, we've learned more about social media over the last 18 months than I suspect most of us ever thought we would in a lifetime. We've learned about social media's boundless potential for good and its ability to enable thoughtful and engaged interactions on a global scale.

But we've also learned about how vulnerable social media is to corruption and misuse. The very worst examples of this are absolutely chilling and a threat to our democracy: the founding ideal of different people from different beliefs and ideas all living peacefully under a single flag. The committee takes this issue very seriously and we appreciate the fact that Facebook and Twitter are represented here this morning with an equivalent and appropriate measure of seriousness.

The purpose of today's hearing is to discuss the role that social media plays in the execution of foreign influence operations. In the past, we've used terms like misinformation and divisive content to describe this activity.

Now as we go into our fourth and final hearing on this subject, I think it's important that we be precise and candid with our language, because that's what the significance of this threat demands. We need to be precise about the foreign actors we're talking about, we need to be precise about the consequences of not acting, and we need to be candid about where responsibility for solving this problem lies.

Two weeks ago your companies announced a series of successful disruptions that resulted in the removal of 652 Facebook pages, groups, and accounts, and 284 Twitter accounts based on their violating your company's standards of coordinated manipulation and inauthentic behavior. Google's own internal security teams did commendable work disrupting this influence operation and we would have valued the opportunity to speak with them at the appropriate level of corporate representation. Nevertheless, their efforts should be acknowledged.

In a departure from what we've all gotten a little accustomed to, this activity didn't come from Russia. It came from Iran. My instinct is to applaud the diligence of your security teams and credit you with taking the problem very seriously.

But I'm not sure your success is the big story here. As I understand it, a third-party security team was crucial to identifying the scope of the Iranian activity. And even more concerning is that more foreign countries are now trying to use your products to shape and manipulate American political

sentiment as an instrument of statecraft.

Jack, I was pleased when informed about your efforts to improve conversational health at Twitter. I think that kind of initiative can do a lot to improve the transparency of public discourse on your platform, and foreign influence operations thrive without transparency.

Sheryl, I fully support Facebook's hiring of the right security experts, building the necessary technologies and collaborating across law enforcement, commercial, cybersecurity, and social media company lines.

I think the observation that no one company can fight this on their own is spot on. Unfortunately, what I described as a national security vulnerability and an unacceptable risk back in November remains unaddressed. That risk and vulnerability was highlighted yet two weeks ago. Without question, positive things are happening. The collaboration, dedication, and resources and demonstrated willingness to work with us are critical and valued by every member of this committee.

It takes courage to call out a state actor and your companies have done that. But clearly this problem is not going away. I'm not even sure it's trending in the right direction. I will go back to what I said up front: we need to be candid about responsibility, and by that, I mean both the responsibility we have to one another--from one side of this dais to the other--as participants in this public policy discussion. And more importantly our shared responsibility to the American people.

Technology always moves faster than regulation, and to be frank, the products and services that enable social media don't fit neatly into the consumer safety or regulatory constructs of the past. The old definitions that used to differentiate a content publisher from a content facilitator are just not helpful here. I think that ambiguity has given rise to something of a convenient identity crisis, whereby judgments about what is and isn't allowable on social media are too episodic, too reactive, and too unrestricted. People are affected by the information your platforms channel to them. That channeling isn't passive or random. It's a function of brilliant algorithms and an incentive structure that prizes engagement. None of that is under attack here.

What is under attack is the idea that business as usual is good enough. The information your platform disseminates changes minds and hardens opinions. It helps people make sense of the world. When you control that or you influence a little of it, you're in a position to win wars without firing a shot. That's how serious this is.

We've identified the problem. Now it's time to identify the solution. Sheryl and Jack, I'm glad you decided to appear and your willingness to be part of the solution. I'm disappointed Google decided against sending out the right senior-level executive to participate in what I truly expect to be a productive discussion.

If the answer is regulation, let's have an honest dialogue about what that looks like. If the key is more resources or legislation that facilitates information sharing and government cooperation, let's get it out there. If it's national security policies that punish the kind of information and influence operations we're talking about this morning, to the point that they aren't even considered in foreign capitals, then let's acknowledge that. But whatever the answer is, we've got to do this collaboratively and we've got to do it now. That's our responsibility to the American people.

I'll offer a closing point. This is for the witnesses and the members alike. There are no unsolvable problems. There is only the will to do what needs to be done--or its absence.

With that, I turn to the Vice Chairman for any comments.

OPENING STATEMENT OF HON. MARK R. WARNER, VICE CHAIRMAN, A U.S.  
SENATOR FROM VIRGINIA

Vice Chairman Warner. Thank you, Mr. Chairman. And let me first of all echo your comments about our colleague and friend, John McCain. I hope we all take his advice to continue to put country first.

Welcome to the witnesses. Mr. Chairman has pointed out that today is an important public discussion. I am pleased that both Facebook and Twitter have sent their company's top leadership to address some of the critical public policy challenges. I look forward to a constructive engagement.

I'd say, though, that I am deeply disappointed that Google, one of the most influential digital platforms in the world, chose not to send its own top corporate leadership to engage this committee. Because I know our members have a series of difficult questions about structural vulnerabilities on a number of Google's platforms that we will need answers for: from Google Search, which continues to have problems surfacing absurd conspiracies; to YouTube, where Russian-backed disinformation agents promoted hundreds of divisive videos; to Gmail, where state-sponsored operatives attempted countless hacking attempts. Google has an immense responsibility in this space.

Given its size and influence, I would have thought that leadership at Google would have wanted to demonstrate how seriously it takes these challenges and actually take a leadership role in this important discussion. Unfortunately, they didn't choose to make that decision. But for the two companies that have chosen to constructively engage and to publicly answer some difficult and challenging questions, again, thank you.

Now, it would be an understatement to say that much has changed in the aftermath of the 2016 campaign. With the benefit of hindsight, it's obvious that serious mistakes were made by both Facebook and Twitter. You, like the Federal Government, were caught flat-footed by the brazen attacks on our election.

Even after the election, you were reluctant to admit there was a problem. I think in many ways it was pressure that was brought to bear by this committee that led Facebook, Twitter, and yes, Google to uncover the malicious activities of the Russian-backed internet Research Agency activities on each of your platforms.

Now each of you have come a long way with respect to recognizing the threat. We've seen important action by your companies to make political advertising more transparent--and we discussed this yesterday--by complying with the terms Senator Klobuchar and I put forward in the Honest Ads Act. In addition, as the Chairman mentioned, since last September you have identified and removed some bad actors from your platforms.

The bad news, I'm afraid, is that there's still a lot of work to do, and I'm skeptical that ultimately you'll be able to truly address this challenge on your own. I believe Congress is going to have to act.

First, on the disinformation front: Russia has not stopped. Russian-linked information warfare exists today. Just recently, we saw the two of you take action to take down suspected Russian operations. We also know Microsoft uncovered Russian attempts to hack political organizations and potentially several political campaigns.

The Russians also continue to infiltrate and manipulate American social media to hijack our national conversation.

Again, you've gotten better, and I'm pleased to see that you've begun to take action, but also the Russians are getting better as well. They have now become harder to track. Worse, now that the Russian playbook is out there, other adversaries, as we saw recently, like Iran, have joined the fray.

But foreign-based disinformation campaigns represent just a fraction of the challenge before you. In the same way that bots, trolls, fake pages, algorithmic gaming can be used to spread fake news, these same tools can be used to assist financial stock pumping fraud, to create filter bubbles and alternative realities, to incite ethnic and racial violence, and countless other misuses.

Imagine the challenge and damage to the markets if Ford's communications from the Fed Chairman were leaked online. Or consider the price of a Fortune 500 company's stock if a dishonest short seller was able to spread false information about the company's CEO or the effects of its products rapidly online.

Russian disinformation has revealed a dark underbelly of the entire online ecosystem, and this threatens to cheapen American discourse, weaken privacy, erode truth, and undermine our democracy on a previously unimagined scale. Worse, this is only going to get harder as we move into artificial intelligence, use of Deepfake technology.

During the 2016 election campaign, the Russians demonstrated how bad actors can effectively marry offensive cyber operations, including hacking, with information operations. I'm afraid that we're on the cusp of a new generation of exploitation, potentially harnessing hacked personal information, to enable tailored and targeted disinformation in social engineering efforts. That future should concern us all.

As someone who was involved in the tech industry for more than 20 years, I respect what this industry represents, and I don't envy the significant technical and policy challenges you face. But the size and reach of your platforms demand that we as policy makers do our job to ensure proper oversight, transparency, and protection for American users and our democratic institutions.

The era of the Wild West in social media is coming to an end. Where we go from here, though, is an open question. These are complicated technological challenges, and Congress has at times demonstrated that it still has some homework to do. I do think this committee has done more to understand the threat to our democracy posed by social media than any others, and I want to commend my colleagues on this committee for tackling this challenge in a bipartisan way.

As has been mentioned, this is our fourth public hearing on the subject, and we've met behind closed doors countless times with third-party researchers, with government officials, and with each of the platforms. We've done the work, and we're positioned to continue to lead in this space.

Again, as the Chairman has already indicated, today's hearing is not about gotcha questions or scoring political points. Our goal today is to begin to shape actual policy solutions which will help us tackle this challenge.

Now, I've put forth some ideas that I'd like to get your constructive thoughts on. For instance, don't your users have a right to know when they're interacting with bots on your platform? Isn't there a public interest in insuring more anonymized data is available to help researchers and academics identify the potential problems and misuse? Why are your terms of service so difficult to find and nearly impossible to read, much less understand? Why shouldn't we adopt ideas like data portability, data minimization, or first-party consent? And

after witnessing numerous episodes of misuse, what further accountability should there be with respect to the flawed advertising model that you utilize?

Now these are just some of our ideas. We have received a lot of positive feedback on some of these ideas from both experts and users. We've also been accused of trying to bring about the death of the internet. I'm anxious to hear your views on our proposals and suggestions your teams can bring to the table on this front.

We have to be able to find smart, thoughtful policy solutions that get us somewhere beyond the status quo, without applying ham-handed 20th-century solutions to 21st-century problems. At the same time, we should be mindful to adopt policies that do not simply entrench the existing dominant platforms.

These are not just challenges for our politics or our democracy. These threats can affect our economy, our financial system, and other parts of our lives. I'm hopeful that we can get there. I'm confident in American ingenuity. And I'm optimistic that Congress led by this committee in a bipartisan fashion can move this conversation forward.

I look forward to the discussion and appreciate the hearing being called. Thank you, Mr. Chairman.

Chairman Burr. I thank the Vice Chairman. At this time, I'd like to swear in our witnesses. If I could ask both of you to stand and raise your right hand?

Do you solemnly swear to give this committee the truth, the full truth and nothing but the truth so help you God?

[The witnesses answered in the affirmative.]

Please be seated. Ms. Sandberg, I'd like to recognize you first and then Mr. Dorsey for any opening statement you'd like to make. The floor is yours.

#### STATEMENT OF SHERYL SANDBERG, CHIEF OPERATING OFFICER, FACEBOOK

Ms. Sandberg. Thank you. Chairman Burr, Vice Chairman Warner, and members of this select committee, thank you for giving me the opportunity to speak with you today. My written testimony goes into more detail about the actions we're taking to prevent election interference on Facebook. But I wanted to start by explaining how seriously we take these issues and talk about some of the steps we're taking.

Free and fair elections are the foundation of any democracy. As Americans, they are part of our national identity and that's why it's incumbent upon all of us to do all we can to protect our democratic process. That includes Facebook. At its best, Facebook plays a positive role in our democracy, enabling representatives to connect with their constituents, reminding people to register and to vote, and giving people a place to freely express their opinions about the issues that matter to them.

However, we've also seen what can happen when our service is abused. As a bipartisan report from this committee said, Russia used social media as part of, and I quote: a comprehensive and multi-faceted campaign to sow discord, undermine democratic institutions and interfere in U.S. elections and those of our allies.

We were too slow to spot this and too slow to act. That is on us. This interference was completely unacceptable. It violated the values of our company and of the country we love. Actions taken show how determined we are to do everything we can do to stop this from happening.

The threat we face is not new. America has always confronted attacks from determined, well-funded opponents who want to undermine our democracy. What is new is the tactics

they are using. To stay ahead, we all need to work together, as Chairman Burr said: government, law enforcement, industry and experts from civil society. And that is why I'm grateful for the work this committee is doing.

At Facebook, we're investing in security for the long term. As our defenses improve, bad actors learn and improve too, and that's why security is never a finished job. We have more than doubled the number of people we have working in safety and security and we now have over 20,000 people and we are able to view reports in 50 languages, 24 hours a day.

Better machine learning and artificial intelligence have enabled us to be more proactive in finding abuse. In the first three months of 2018 alone, over 85 percent of the violent content we took down or added warning labels to was identified by our technology before it was reported. These are expensive investments, but that will not stop us because we know they are critical.

Our first line of defense is finding and shutting down fake accounts, the source of much of the inauthentic activity we see on Facebook. Authenticity matters because people need to trust that the content they're seeing is valid and they need to trust the connections they make. We are now blocking millions of attempts to register false accounts each and every day.

We're making progress on fake news. We're getting rid of the economic incentives to create it and we're limiting the distribution it gets on Facebook. We demote articles rated by third-party fact-checkers as false. We warn people who have shared them or who are about to share them, and we show them related articles to give them more facts.

We've also taken strong steps to prevent abuse and increase transparency in advertising. Today on Facebook, you can go to any page and see all the ads that page is running, even if they wouldn't be shown to you. For political and issue ads, you can also see who paid for the ads, how much was spent, and the demographics of the people who saw them.

We're also going to require people running large pages with large audiences in the United States to go through an authorization process and confirm their identity. These steps won't stop everyone who's trying to game the system, but they will make it a lot harder.

As these past few weeks and months have shown, this work is starting to pay off. In July, we removed 32 pages and accounts involved in coordinated, inauthentic behavior. In August, we removed 650 pages and accounts that originated in Iran, as well as additional pages and accounts from Russia. And just last week, we took down 58 pages and accounts from Myanmar, many of which were posing as news organizations.

We are focused, as I know you are, on the upcoming U.S. midterms and on elections around the world. Our efforts in recent elections from Germany, to Italy, to Mexico, to the Alabama special Senate election, show us that the investments we are making are yielding results. We also know, as Chairman Burr said, that we cannot stop interference by ourselves. We're working with outside experts, industry, partners and governments, including law enforcement, to share information about threats and prevent abuse.

We're getting better at finding and stopping our opponents, from financially motivated troll farms to sophisticated military intelligence operations. We don't have access to the intelligence governments have access to, so we don't always know exactly who is behind these attacks or their motives, and that's why we will continue working closely with law enforcement.

Chairman Burr, I want to thank you for your leadership. Vice Chairman Warner, I want to thank you for your white paper,

which has so many ideas on how we can work together to strengthen our defense. Senators, let me be clear, we are more determined than our opponents and we will keep fighting.

When bad actors try to use our site, we will block them. When content violates our policies, we will take it down. And when our opponents use new techniques, we will share them so we can strengthen our collective efforts.

Everyone here today knows that this is an arms race, and that means we need to be ever more vigilant. As Chairman Burr has noted, nothing less than the integrity of our democratic institutions, processes, and ideals is at stake. We agree, and we will work with all of you to meet this challenge.

Thank you.

[The prepared statement of Ms. Sandberg follows:]

[GRAPHICS NOT AVAILABLE IN TIFF FORMAT]

Chairman Burr. Thank you, Ms. Sandberg. Mr. Dorsey, the floor is yours.

STATEMENT OF JACK DORSEY, CHIEF EXECUTIVE OFFICER, TWITTER, INC.

Mr. Dorsey. Thank you Chairman Burr, Vice Chairman Warner and the committee for the opportunity--for the opportunity to speak on behalf of Twitter to the American people. I look forward to our conversation about the work we're doing to help protect the integrity of U.S. elections and elections around the world.

I am someone of very few words and typically pretty shy, but I realize how important it is to speak up now. If it's OK with all of you I'd like to read you something I personally wrote as I considered these issues. I'm also going to tweet this out now.

First, I want to step back and share our view of Twitter's role in the world. We believe many people use Twitter as a digital public square. They gather from all around the world to see what's happening and have a conversation about what they see. In any public space you will find inspired ideas and you'll find lies and deception--people who want to help others and unify, and people who want to hurt others and themselves, and divide.

What separates a physical and digital public space is greater accessibility and velocity. We're extremely proud of helping to increase the accessibility and velocity of a simple, free, and open exchange. We believe people would learn faster by being exposed to a wide range of opinions and ideas, and it helps make our Nation and the world feel a little bit smaller. We aren't proud of how that free and open exchange has been weaponized and used to distract and divide people and our Nation. We found ourselves unprepared and ill-equipped for the immensity of the problems that we have acknowledged: abuse, harassment, troll armies, propaganda through bots and human coordination, misinformation campaigns, and divisive filter bubbles. That's not a healthy public square. Worse, a relatively small number of bad faith actors were able to game Twitter to have an outsized impact.

Our interests are aligned with the American people and this committee. If we don't find scalable solutions to the problems we're now seeing, we lose our business and we continue to threaten the original privilege and liberty we were given to create Twitter in the first place.

We weren't expecting any of this when we created Twitter over 12 years ago. We acknowledge the real world negative consequences of what happened and we take the full responsibility to fix it. We can't do this alone and that's why

# Exhibit 29

**HEARING BEFORE  
THE UNITED STATES HOUSE OF REPRESENTATIVES  
PERMANENT SELECT COMMITTEE ON INTELLIGENCE**

June 18, 2020

Testimony of Nathaniel Gleicher  
Head of Security Policy, Facebook

**I. Introduction**

Chairman Schiff, Ranking Member Nunes, and members of the Committee, thank you for the opportunity to appear before you today. My name is Nathaniel Gleicher, and I am the Head of Security Policy at Facebook. My work is focused on addressing the adversarial threats we face every day to the security and integrity of our products and services. I have a background in both computer science and law, and before joining Facebook, I prosecuted cybercrime at the US Department of Justice and served as Director for Cybersecurity Policy at the National Security Council.

We recognize these are incredibly difficult and challenging times, and that's why it is more important than ever that people can have authentic conversations on our platforms about issues that matter to them, including COVID-19 public health issues, social and racial injustice, family and economic concerns, and the upcoming elections. This kind of authentic engagement promotes democracy and a more engaged and informed society.

We also know, however, that malicious actors are working to interfere with and manipulate these conversations, exploit our societal divisions, promote fraud, influence our elections, and delegitimize authentic social protest. Stopping these bad actors is one of our highest priorities, and we continue to work tirelessly to do so.

At Facebook, we believe in giving people a voice and building connection and community. By protecting authentic dialogue on our platforms, we're working to help connect people in a time when we need one another more than ever.

**II. Facebook's Election Integrity Efforts**

Facebook has made significant investments to help protect the integrity of elections—not only addressing threats we've seen on our platform in the past, but also anticipating new challenges, responding to new risks, and developing new tools that empower people to have a voice in their political process.

We have more than 35,000 people working on safety and security across the company, more than three times as many as we had in 2017. This includes nearly forty different teams focused on election work across Facebook's family of apps, including the team we have in place planning for the 2020 elections. We are also partnering with the federal government (including the Department of Homeland Security and the Federal Bureau of Investigation (FBI)), state

governments, other tech companies, researchers, and civil society groups to share information and stop malicious actors. For example, two days before the 2018 midterms, based on a tip from the FBI, we conducted a rapid investigation in a matter of hours and dismantled more than 100 accounts linked to the Russian Internet Research Agency. Since then, we've worked to improve our coordination with law enforcement on election-related matters and a host of newer concerns I'll discuss further below.

Over the past three years, we've worked to protect more than 200 elections around the world, including the 2018 midterms and elections in India and the European Union. Each election has presented its own unique challenges, and we're continuing to apply the lessons we learn so our defenses get stronger each time.

In the lead-up to the 2020 elections, we have been working to protect candidates and campaigns online. While we are careful not to divulge all of the steps we've taken to enhance security, we have launched Facebook Protect to further secure the accounts of elected officials, candidates, their staff, and others who may be targeted by hackers and foreign adversaries. Participants will be required to turn on two-factor authentication, and their accounts will receive enhanced monitoring for hacking, such as login attempts from unusual locations or unverified devices. If we discover an attack against one account, we will be able to review and protect other accounts affiliated with that same organization that are enrolled in our program.

We believe people should be able to understand easily why they're seeing ads, who paid for them, and what other ads that advertiser is running. That is why we have increased political and issue ad transparency. We introduced the ability to view a Page's active ads, regardless of the ads' targeted audience. We've added more information about who is behind certain Pages, including an "Organizations That Manage This Page" tab, which provides the Page's "Confirmed Page Owner," including the organization's legal name and verified city, phone number, or website. And all ads about social issues, elections, or politics on Facebook and Instagram in the US must be clearly labeled, including a paid-for-by disclosure from the advertiser at the top of the ad.

In addition, we launched the Ad Library to help people learn more about ads related to politics or issues that have run on Facebook or Instagram. The Ad Library houses ads for seven years and offers information about who saw the ad and its spend and impressions. The library also includes information about Pages, including a Page's history, the primary location of people who manage it, and advertiser spend information for certain political or issue-related ads. Users can also report ads from within the Ad Library.

Earlier this month we began labeling media outlets that are wholly or partially under the editorial control of their government. We're providing greater transparency into these publishers because they combine the influence of a media organization with the strategic backing of a state, and we believe people should know if the news they read comes from a publication that may be under the influence of a government. To ensure that we're equally transparent when it comes to paid content, we will begin labeling ads from these publishers later this year. And while state-controlled media outlets rarely advertise in the US, we've begun blocking ads from these outlets in the US out of an abundance of caution, to provide an extra layer of protection against various types of foreign influence in the public debate ahead of the 2020 election in November.

### **III. Inauthentic Behavior and Influence Operations**

Authenticity is the cornerstone of our community. We have invested significantly in combating inauthentic behavior, whether it takes the form of individual fake accounts or broader coordinated networks. Over the past several years, our team has grown to over 200 people with expertise ranging from open-source research to threat investigations, cyber security, law enforcement and national security, investigative journalism, engineering, product development, data science, and academic studies in disinformation.

Fake accounts are often behind harmful and misleading content, and we work hard to keep them off Facebook. Our technology enables us to stop millions of attempts to create fake accounts every day, and to detect and remove millions more, often within minutes after creation. Facebook disabled approximately 1.7 billion fake accounts between January and March of this year. The vast majority (over 99%) were identified proactively before receiving any report. And we have created tools to proactively identify fake accounts specifically targeting civic issues like elections.

In this extraordinary and difficult time, our work removing inauthentic behavior is more important than ever. And while the vast majority of expression on Facebook is authentic, we know that some bad actors try to use our platforms deceptively to provoke violence, engage in fraud, sow discord, or undermine the legitimacy of public debate. We have dedicated teams that proactively hunt for these threats, and we act swiftly when we find them.

When it comes to what we call “influence operations”—coordinated efforts to manipulate public debate for a strategic goal where fake accounts are central to the operation—we focus on two types of activity: 1) coordinated inauthentic behavior in the context of domestic, non-state campaigns, and 2) coordinated inauthentic behavior on behalf of a foreign or government actor. So far this year, we’ve taken down eighteen networks engaged in this sort of deceptive behavior, including three networks originating from Russia, two from Iran, and two based here in the United States. We report our enforcement actions in our monthly report on coordinated inauthentic behavior to make it easier for people to see the progress we’re making in one place.

We’ve also been monitoring to make sure bad actors are not able to interfere with conversations around the ongoing protests against injustice and detract from the important discussions about injustice and inequality happening across our nation. We recently identified and removed a series of accounts tied to two organized hate groups that we had previously banned from our platforms.

We are making progress rooting out this abuse, but it is an ongoing effort. We are committed to improving to stay ahead by building better technology; hiring more people; and working more closely with law enforcement, security experts, and other companies.

### **IV. Our Efforts to Support Voters**

An equally important part of our election integrity efforts is providing people with reliable, accurate information about elections in their area. We believe in the importance of taking proactive steps to support a more informed and engaged electorate. We also know that misinformation and influence operations are most virulent in information vacuums. This is why, to fight misinformation and encourage people to vote, we are creating a new Voter Information

Center to make sure voters have accurate and up-to-date information from their local, state, and federal election authorities, including how, when, and where to vote. We'll also be providing notifications to remind individuals to register to vote and reminders of local elections.

We believe in creating a space for people to have authentic conversations and speak about important issues, even if they may be expressing views we do not agree with. We will continue to stand for giving users a voice and erring on the side of free expression. Under our Community Standards, content that incites violence or causes harm is against our policies, regardless of the speaker. Our philosophy is that it is better to have discussions about difficult and divisive issues out in the open, especially when the stakes are so high. Ultimately, accountability for those in positions of power can only happen when their speech is scrutinized.

We recognize that the COVID-19 pandemic has caused new and unique challenges for voters, including fear and confusion around going to the polls in November, as well as changes to election dates, polling locations, and methods of voting. In this constantly evolving environment, we remain focused on working with election authorities to provide people with authoritative, geographically targeted voting information. For example, we have launched a new Vote By Mail in-product notification to people in states where there is no-excuse vote by mail or COVID-19 is considered a valid universal excuse. This notification links to authoritative information on how to request a ballot. We have also developed a notification to alert users if the date of their election has changed within a week of the original election date. And we are reviewing our policies to make sure we are appropriately taking into account the realities of voting in this context.

## **V. Supporting Our Community Through the COVID-19 Pandemic**

In the time since COVID-19 was declared a global public health emergency, we've been working to connect people to accurate information and taking aggressive steps to stop COVID-related misinformation and harmful content from spreading.

In January, we started displaying educational pop-ups in Facebook and Instagram connecting people to information from a wide range of health authorities, including the CDC, regional health authorities, and the WHO, when people search for COVID-19-related information. We also launched the COVID-19 Information Center, which is now featured at the top of News Feed on Facebook and includes real-time updates from national health authorities and global organizations. Through these efforts across Facebook and Instagram, we've directed more than 2 billion people to resources from health authorities—more than 350 million of whom clicked through to learn more. We're also giving millions in ad credits to health authorities so they can reach people with timely messages.

In addition to connecting people with accurate information from reliable sources, we're working to stop misinformation and harmful content from spreading on our platform. We remove COVID-19 related misinformation from Facebook and Instagram that could contribute to imminent physical harm, such as posts making false claims about cures, treatments, the availability of essential services, or the location and severity of the outbreak. We've also banned ads and commerce listings that imply a product guarantees a cure or prevents people from contracting COVID-19.

For other types of claims, like conspiracy theories about the origin of the virus, we continue to work with our network of independent fact-checking partners to debunk these claims. During the month of April alone, we displayed warnings on about 50 million posts related to COVID-19 on Facebook, based on around 7,500 articles by our independent fact-checking partners. When people saw those warning labels, 95% of the time they did not go on to view the original content. We have also removed hundreds of thousands of pieces of misinformation that could lead to imminent physical harm. Additionally, we've started showing messages in News Feed to connect people who have liked, reacted to, or commented on harmful misinformation about COVID-19 that we have since removed with information from authoritative sources.

As this pandemic evolves, we'll continue focusing on the most effective ways to keep misinformation and dangerous hoaxes about COVID-19 off our apps and ensure people have credible information from health experts to stay safe and informed.

## **VI. Conclusion**

We are proud of the progress we have made to protect authentic discourse on our platforms, but there is always more work to do. We are up against determined adversaries, and we will never be perfect, but we will continue our vital work to stop bad actors and give people a voice.

Thank you, and I look forward to answering your questions.

# Exhibit 30

**HEARING BEFORE  
THE UNITED STATES HOUSE OF REPRESENTATIVES  
COMMITTEE ON OVERSIGHT AND REFORM  
SUBCOMMITTEE ON NATIONAL SECURITY**

May 22, 2019

Testimony of Nathaniel Gleicher  
Head of Cybersecurity Policy, Facebook

**I. Introduction**

Chairman Lynch, Ranking Member Hice, and members of the Subcommittee, thank you for the opportunity to appear before you today. My name is Nathaniel Gleicher, and I am the Head of Cybersecurity Policy at Facebook. My work is focused on addressing the serious threats we face every day to the security and integrity of our networks and services. I have a background in both computer science and law; before coming to Facebook, I prosecuted cybercrime at the U.S. Department of Justice and built and defended computer networks.

Facebook cares deeply about protecting the integrity of the democratic process. We do not want anyone to use our tools to undermine elections or democracy. That is not what we stand for. We have dedicated significant resources to finding and removing malicious activity on our platforms and developing tools that help people have a voice in their political process. We are constantly learning—most recently from the 2018 midterm elections here in the United States, as well as from recent elections in India, Brazil, and Mexico, and in our preparations for European Parliamentary elections later this month. And we are applying what we learn to continue improving.

Our platforms are places where people can have authentic conversations about elections and other political topics because we believe this kind of engagement promotes democracy. We also know, however, that bad actors are working to interfere with those conversations and undermine our election integrity. We are taking steps to prevent election interference and combat coordinated inauthentic behavior, and we will continue to strengthen our efforts in these areas going forward.

**II. Facebook's Election Integrity Efforts**

Facebook has invested significantly in both the people and technology necessary to protect election integrity. We are not only addressing the threats we have seen on our platforms in the past, but also anticipating new challenges and responding to new risks.

To support these efforts, we have more than 30,000 people working on safety and security across the company, three times as many as we had in 2017. Our team reviews reported content in more than 50 languages, 24 hours a day. And we have nearly 40

different teams focused on election work across Facebook's family of apps, including the team we have in place planning for the 2020 elections.

In advance of the United States' midterm elections last year, we opened our first physical elections operation center at our headquarters in Menlo Park, California. The operation center leveraged experts from across the company—including from our threat intelligence, data science, software engineering, research, operations specialists, and legal teams. The purpose was to increase coordination and response time, to react immediately to any threats identified to our systems, and to reduce the spread of potentially harmful content. We have continued to build on this track record in 2019. We launched two new regional elections operation centers, in Singapore and Dublin, to assist with elections integrity monitoring in Southeast Asia, India, the European Union and elsewhere. We have a dedicated team focused on preparing for the United States' 2020 presidential election and will have an operation center set up for that effort as well.

We have also improved our machine learning capabilities, which allows us to be more efficient and effective in finding and removing violating behavior. We work closely with law enforcement, regulators, election commissions, other technology companies, researchers, academics and civil society groups to develop new and more advanced strategies to deal with these threats.

Our approach to this problem is multifaceted, and while our efforts are global, we also customize our work to individual countries, based on research and threat assessments that begin many months before ballots are cast. Our tactics include blocking and removing fake accounts; limiting the spread of false news and misinformation; bringing increased transparency to political advertising; and finding and removing bad actors from the platforms.

As noted in our Community Standards, “[e]very day, people come to Facebook to share their stories, see the world through the eyes of others, and connect with friends and causes. The conversations that happen on Facebook reflect the diversity of a community of more than two billion people communicating across countries and cultures and in dozens of languages, posting everything from text to photos and videos.” The vast majority of people who use Facebook comply with our terms and policies, but Facebook is aware that some individuals and bad actors attempt to create multiple or fake accounts.

Fake accounts are often behind harmful and misleading content, and we work hard to keep them off Facebook. Our technology helps us take action against millions of attempts to create fake accounts every day, and detect and remove millions more, often within minutes of creation. Facebook disabled approximately 2.1 billion fake accounts between January and September 2018. The vast majority—over 99% during this same time period—were identified proactively before receiving any report. And we have created new tools to proactively identify fake accounts specifically targeting civic issues like elections.

When it comes to false news, we follow a three-part framework to improve the quality and authenticity of stories in News Feed. First, we remove content that violates our Community Standards, which helps enforce the safety and security of the platform. Then, for content that does not directly violate our Community Standards, but still undermines the authenticity of our platform—such as clickbait or sensational material—we reduce its distribution in News Feed, so fewer people see it. The result is that lower-quality, less broadly trusted Pages—conservative and liberal alike—are getting less traffic than they did previously. And finally, we inform people by giving them more context regarding the information they see in News Feed. We have also continued to expand our third-party fact-checking program, which now includes 45 certified fact-checking partners who review content in 24 languages. Each partner is a signatory to the Poynters’ International Fact-Checking Network Code of Principles, the first principle of which is to be non-partisan.

We are also focused on political advertising. We believe people should be able to understand easily why they are seeing ads, who paid for the ads, and what other ads an advertiser is running. We also require election- or issue-related ads on Facebook and Instagram in the United States to be labeled clearly, including a paid-for-by disclosure from the advertiser at the top of the ad, and advertisers must confirm their identity before their ad can run, which helps ensure that foreign actors are not buying ads in United States elections. We place these ads in our Ad Library for seven years. In the Library, our users can find out how much was spent, how many times the political or issue ad was seen, as well as the demographics of who saw it.

### **III. Coordinated Inauthentic Behavior**

One area in which we have invested significant efforts is combating what we call “coordinated inauthentic behavior.” Coordinated inauthentic behavior is when networks of accounts, Pages or Groups work together to mislead others about who they are and what they are doing.

We ban this kind of behavior so people trust the connections they make on Facebook. And while we have made real progress, it is an ongoing challenge because the actors engaged in this behavior are determined and often well-funded. We have to improve constantly to stay ahead, including by building better technology and working more closely with law enforcement, security experts and other companies.

We combat coordinated inauthentic behavior in two ways. First, our expert investigators use skills brought from the worlds of cybersecurity research, law enforcement, and investigative reporting to find and take down the most sophisticated networks. To do so, they collaborate closely with our data science team, which uses machine learning and other advanced technologies to identify patterns of malicious behavior.

Second, we build technology to detect and remove automatically the most common threats. If expert investigations are looking for a needle in a haystack, our automated work is akin to shrinking that haystack. It reduces the noise in the search environment by removing unsophisticated threats. And it also makes it easier for our expert investigators

to corner the more sophisticated bad actors. Using these automated tools, we block millions of fake accounts every day, the vast majority at the point of creation, before they can do any harm.

This combination of expert and automated investigation and detection allows our platforms to adapt continually to make deceptive behaviors much more difficult and costly. And our efforts are having an impact. We have announced dozens of takedowns of coordinated inauthentic behavior across the world, from Asia to Europe to the Americas. And we are constantly following up on thousands of leads globally, including information shared with us by law enforcement, industry partners and civil society groups. For example, we received a tip from the FBI just 48 hours before the United States' midterm elections last year that allowed us to investigate and quickly take down a coordinated effort by foreign entities.

In the past month, we have removed two networks of coordinated inauthentic behavior emanating from Russia that focused on Austria, the Baltics, Germany, Spain, Ukraine and the United Kingdom. The individuals behind this activity frequently posted about local and political news, including topics like the military conflict in Eastern Ukraine, Russian politics, political news in Europe, politics in Ukraine and the Syrian civil war. Just last week, we removed additional Facebook and Instagram accounts, Facebook Pages, Groups and events involved in coordinated inauthentic behavior focused on Nigeria, Senegal, Togo, Angola, Niger and Tunisia, along with some activity in Latin America and Southeast Asia.

By continuing to develop smarter technologies, improving transparency, and enhancing our defenses, we are making the continual improvements we need to stay ahead of our adversaries and to protect the integrity of our platforms and our elections.

#### **IV. Our Efforts to Support Voters**

Election integrity is about more than just defending against threats. We at Facebook believe in the importance of taking proactive steps to encourage a more informed and engaged electorate. In 2018, for example, Facebook and Instagram helped an estimated 2 million people in the United States register to vote. We also supported our users' efforts to create their own voter registration drives to get their friends to vote. We helped voters find their polling places and reminded them to vote on Election Day. And we are building products that make it easier for people to find high-quality information during an election.

Another area of focus for Facebook has been protecting against the misuse of our platforms to intimidate voters or suppress participation, particularly amongst minority groups and people of color. Ahead of the 2018 midterms, we strengthened our policy prohibiting voter suppression under our Community Standards. The policy expressly bans threats of violence related to voting or voter registration, as well as misrepresentations about how to vote, such as claims that you can vote using an online app, and statements about whether a vote will be counted. Other misinformation related to voting—including false claims of polling place closures, long lines, and wait times—is

sent to third-party fact-checkers for review. And we are more proactive than ever in our work. Rather than wait for reports from our users, our teams now use trained algorithms to actively conduct sweeps tuned to identify violating content. In the weeks leading up to the United States' 2018 midterm elections, our team identified and removed 45,000 pieces of voter suppression content, over 90% of which we found before it was reported by any user.

Building a civically engaged community means building tools that help people participate in a thoughtful and informed way with the political process. And because Facebook is a platform for ideas, voices, and viewpoints across the political spectrum, we go to great lengths to ensure there is no bias in the way that we achieve that goal. We asked former Senator Kyl to lead a review related to identifying any bias in the work we do. The more users engage with the political process, the more they can ensure it reflects their values. This is an important part of feeling connected to our community and our democracy, and it is something we are increasingly focused on at Facebook.

## **V. Conclusion**

We are proud of our ongoing efforts to protect the integrity of our elections, but we know there is more to do. Security is an arms race—as we continue to improve our defenses, bad actors evolve their tactics. We will never be perfect, and we are up against determined adversaries, but we are committed to doing everything we can to strengthen our civic discourse and protect elections.

I look forward to answering any questions you may have.

# Exhibit 31

**HEARING BEFORE THE UNITED STATES HOUSE  
COMMITTEE ON VETERANS AFFAIRS**

November 13, 2019

Testimony of Nathaniel Gleicher  
Head of Security Policy, Facebook

**I. Introduction**

Chairman Takano, Ranking Member Roe, and members of the Committee, thank you for the opportunity to appear before you today. My name is Nathaniel Gleicher, and I am the Head of Security Policy at Facebook. My work is focused on addressing the serious threats we face every day to the security and integrity of our products and services. I have a background in both computer science and law; before coming to Facebook, I prosecuted cybercrime at the US Department of Justice and built and defended computer networks.

**II. Facebook's Efforts to Support Veterans**

Facebook supports the military and veteran community and is grateful for their service and the sacrifices made by veterans and their families. We are proud that thousands of veterans and active-duty military members use the Facebook family of apps to stay connected and share with their friends and loved ones. More than 900,000 users are part of the more than 2,000 active Facebook groups that have been created for veterans and their families, and 70% of the veteran and military groups on Facebook are for veteran or active duty spouses.

Veteran hiring is also an important focus for Facebook. Veterans currently hold senior roles at the company, and increasing the number of veterans working at Facebook is a critical part of our diversity initiatives. We offer a Military Skills Translator that helps veterans leverage their unique skills to find Facebook careers relevant to their military experience.

When veterans join our team, we provide dedicated resources so they can connect and share with one another to find opportunities for advancement, including internal programs for mentorship and support groups, and for the first time this year, we are hosting an internal Facebook Vets and Allies Leadership Summit. We are also launching a 12-month career development pilot program for veterans with a background in electrical engineering, mechanical engineering, or computer science in order to further the opportunities available to veterans at Facebook.

Veterans leave military service equipped with the traits and skills that provide a strong foundation for successful entrepreneurship, including leadership experience, attention to detail, dedication, and determination. We are pleased that veteran-owned small businesses use our services to connect with their customers and grow their businesses.

We also know that entrepreneurs with access to mentors are much more likely to start a business and to stay in business. This is why we have announced a new Partnership to Advance Veterans' Entrepreneurship (PAVE) with SCORE, the nation's largest network of volunteer expert business mentors. Our partnership with SCORE will provide education and mentoring to those in the veteran community who dream of becoming entrepreneurs. Through a mentor match program, we will connect potential veteran entrepreneurs with a cohort of SCORE's experienced business mentors who are also veterans. We will offer an educational toolkit, and in collaboration with SCORE, a veteran-focused series of workshops, both of which will help veterans with the skills, knowledge, and resources they need to launch a business. SCORE's veteran mentors will be available to attendees after the workshop to provide ongoing guidance throughout all stages of startup and growth.

In addition, our Military and Veterans Hub provides consolidated resources and tools for veterans to build their community, find job opportunities, and enhance digital skills. Last month, we hosted two free events to educate veterans and military families on using technology to grow their businesses and develop new skills.

We recognize the strain that military service places on servicemembers, veterans, and their families. That is why we partnered with the organization United Through Reading in May 2018 to host an event where servicemembers were able to use Facebook Portal, a smart device we offer that can be used for video calling, to record stories for their families to listen to when they cannot be there. We know that connections with family and loved ones are critical for servicemembers, whether deployed overseas or when they come home, and we want to be there for them along the way.

### **III. Fighting Fraud and Scams on Facebook**

Billions of people use our service to connect and share, and unfortunately some of them are intent on misusing it. We know how important it is to protect the people who use our services, and we have a combination of policies, processes, and technology to combat frauds and scams.

The idea behind Facebook is to help bring communities together in an authentic way. We believe that people are more accountable for their statements and actions when they use their authentic identities. As part of our commitment to authenticity, we have a series of policies to protect against misrepresentation, fraud, deception, spam, and inauthentic behavior. First, we require people to connect on Facebook using the name they go by in everyday life. Second, we do not allow people to misrepresent themselves on Facebook, use fake accounts, artificially boost the popularity of content, or engage in behaviors that otherwise violate our Community Standards. We prohibit users from impersonating or speaking for another person, and our policies require that users do not misuse our product by maintaining multiple Facebook profiles. Third, we work hard to limit the spread of spam or other content that abuses our platform, products, or features to artificially increase viewership or distribute content en masse for commercial gain. These policies are intended to create a space where our users can trust the people and communities with which they interact.

We enforce these policies through a combination of human review, automated detection technologies, and user reports, and we work hard to improve in all three areas. We have over 35,000 people across the company working on safety and security—more than three times as many as we had in 2017. In fact, our security budget today is greater than the entire revenue of our company at the time of our IPO earlier this decade. We assist law enforcement as they find and prosecute the scammers who engage in impersonation or other deceptive activities. We are constantly improving our technology as well. For example, in March 2018, we introduced new machine learning techniques that helped us take action against more than half a million accounts tied to financial scams on Facebook.

Fake accounts are often behind harmful and misleading content, and we work hard to keep them off Facebook. We took down over 2 billion fake accounts in the first quarter of this year alone, not including the millions of additional attempts to create accounts that our technology stops every day before they are created.

We know that user reports are another key component of identifying fraudulent and other prohibited behavior. Therefore, we continue to invest in educating our users and improving our reporting systems. We inform users about warning signs and abuse patterns to help them recognize when they may be a target for abuse. We are developing ways to discourage users from engaging in behaviors that play into the bad actors' aims (for example, warning against sending payments, compromising photos, or personal information). We have learned that users often have a gut instinct that something is not right when they encounter bad actors, so we are empowering users with easy-to-use reporting and self-remediation tools while encouraging them to report behavior they think is problematic.

On Instagram, we do not require users to use their real name when they register, but our policies require people to be authentic on our service—meaning that we do not allow people to misrepresent who they are or to mislead others. We use a combination of proactive technology and reporting to understand if an account violates these policies, and when we find violations, we take action. Our systems examine thousands of account attributes and focus on detecting behaviors that are very difficult for bad actors to fake, including their connections to others on our platform.

#### **IV. Combating Inauthentic Behavior**

We know that fraud, scams, and inauthentic behavior degrade the experience of our services and expose our users to risks of harm. Stopping this kind of abuse is a key priority as we work to make our services safer for people to connect and share. Our efforts to prevent inauthentic behavior have four components.

First, our expert investigators use their experience and skills in areas like cybersecurity research, law enforcement, and investigative reporting to find and take down the most sophisticated threats. To do so, they collaborate closely with our data science team, which uses machine learning and other advanced technologies to identify patterns of malicious behavior.

Second, we build technology to detect and automatically remove the most common threats. This reduces the noise in the search environment by removing unsophisticated threats, and it makes it easier for our expert investigators to corner the more sophisticated bad actors.

Third, we provide transparency and reporting tools so users can make informed choices when they encounter borderline content or content that we miss. This transparency extends to the application of our policies, which are detailed and public. And when we take down coordinated inauthentic behavior, we publicize these takedowns for all to see, and we provide information to third parties for them to review and share relevant data with researchers, academics, and others.

And fourth, we work closely with civil society, researchers, governments, and industry partners, so they can flag issues that they see and we can work quickly to resolve them. Engaging with these partners regularly helps us improve the efficacy of our techniques and learn from their experiences.

Using this combination of approaches, we continually adapt our platforms to make deceptive behaviors much more difficult and costly. When we conduct a takedown, we identify the tactics the bad actors used, and we build tools into our platforms to make those tactics more difficult at scale. Over time, we are making it harder for bad actors to operate and making our systems more secure and resilient. By continuing to develop smarter technologies, enhance our defenses, improve transparency, and build strong partnerships, we are making the constant improvements we need to stay ahead of our adversaries and to protect the integrity of our platforms.

We have also made real progress in curbing inauthentic engagement on Instagram. For example, we penalize accounts that distribute automated likes, comments, or follows in an attempt to expand their reach. Using machine learning, we can identify accounts that use third-party services to distribute inauthentic engagement. When a service uses an account to generate inauthentic activity, our tools can detect and remove that activity before it reaches the recipient. As our tools continue to remove inauthentic likes, follows, and comments, bad actors will have less incentive to use these methods. This will take time, but we are investing in this area for the long term.

## **V. Protecting Our Military and Veteran Users from Scams and Impersonation**

We recognize that individuals and groups that are considered trustworthy, like veterans, are more likely to be the targets of impersonation. This can occur on an individual basis—where a specific veteran is impersonated, such as in a so-called “romance scam.” Or it can happen at the organization level—where Facebook Pages or groups are created to impersonate veteran-related organizations. Protecting veterans on our site is something we take very seriously, and in addition to the steps I have already outlined above, we work to combat the increased risks of impersonation that uniformed personnel and veterans face.

We are testing new detection capabilities to help spot and remove accounts that pretend to be some of the most frequently impersonated members of the US military and veterans. We also are training our automated systems to look for certain techniques used by scammers to impersonate an individual, such as leaving out one letter of a person's name to make their impostor account look legitimate. If, during this process, we detect that an account may be impersonating such an individual, we flag it for human review. We are still testing these processes, but they have helped us more quickly detect the creation of impostor accounts and remove them shortly after their creation, often before people even see them.

When it comes to Pages that falsely represent themselves as belonging to real organizations, what we have found is that, unfortunately, these activities are not limited to veteran-related groups. In fact, the same bad actors sometimes create multiple Pages, some of which may impersonate veterans organizations, while others might impersonate organizations that focus on politically sensitive issues. That is why, to root out and remove these bad actors, we focus on patterns of behavior, not just content. Our approach is flexible enough to combat various types of impersonation, and when we develop tactics that prove effective with respect to one type of impersonation, we apply those same tactics to other types automatically.

To combat these inauthentic activities, our systems rely on signals about how the account was created and is being used, such as the use of suspicious email addresses, suspicious actions, or other signals previously associated with other fake accounts we have removed. Most of the accounts we currently remove are blocked shortly after their creation, before they can do any harm.

On Instagram, we are also using proactive technology to find and take action on potential scams, and we recently introduced the option for members of the community to let us know if they come across scams on our platform.

We have also worked to increase transparency. For example, we have changed the way users see information about Pages, so that if a Page is owned or run by a foreign actor, the country location of the people or organizations managing the Page is easily determined. This way, users can better assess whether the Page they're engaging with is legitimate. People can also see more information about accounts on Instagram that reach large audiences so they can evaluate the authenticity of the account, including the date the account joined Instagram, the country where the account is located, any username changes in the last year, and any ads the account is currently running.

Sometimes people fail to disclose the organization behind their Pages as a way to make others think that Page is run independently. We want to make sure Facebook is used to engage authentically, and that users understand who is speaking to them and what perspective they are representing. That is why we recently introduced a policy to require more accountability; if we find a Page that is concealing its ownership in order to mislead

people, we will require it to go through our business verification process and show more information about who is behind the Page in order for the Page to stay up.

We recognize our responsibility to work to make sure the veterans who use our platform are not being targeted or victimized. We also recognize that we can have a greater impact if we work in continued partnership with government, law enforcement, and civil society organizations. We work with law enforcement, including the FBI and the Department of Defense, to help find and prosecute the scammers who conduct these activities. We educate our users, including our veteran users, through videos and online safety guides in concert with civil society groups. And we work with the Department of Defense to help raise awareness among the military community about impersonation. For individuals and organizations most impacted by impersonation attempts, as well as for the Department of Defense, we have set up dedicated escalation channels for them to contact us when they learn of a new case of impersonation or targeting, to ensure that we can respond quickly.

## **VI. Conclusion**

We know that we are fighting against motivated adversaries in this space, and that we have to iterate and improve our approach to stay ahead. We are committed to doing just that. Although our efforts haven't been perfect, our commitment is producing results.

We also recognize the importance of working with government and outside groups who are engaged with us in this fight. We have strong relationships with veterans organizations and others working on these issues and look forward to strengthening those relationships as we go forward. We value the input and assistance these organizations provide as we work to keep veteran impersonation off of our platforms.

I appreciate the opportunity to be here today to hear your ideas and concerns, and I look forward to your questions.

# Exhibit 32

# **HEARING BEFORE THE UNITED STATES SENATE COMMITTEE ON COMMERCE, SCIENCE, & TRANSPORTATION**

January 17, 2018

Testimony of Monika Bickert  
Head of Product Policy and Counterterrorism, Facebook

## **INTRODUCTION**

Chairman Thune, Ranking Member Nelson, and distinguished members of the Committee, thank you for the opportunity to appear before you today. My name is Monika Bickert, and I am the head of Product Policy and Counterterrorism at Facebook. Prior to assuming my current role, I served as lead security counsel for Facebook. I am also a former prosecutor, having worked for a decade as an Assistant U.S. Attorney with the Department of Justice. We appreciate the Committee's hard work as it continues to seek more effective ways to combat extremism, crime, and other threats to our national security.

We take all of these threats very seriously. One of our chief commitments is to create and use innovative technology that gives people the power to build community and bring the world closer together. Keeping our community safe on Facebook is critical to this broader mission. We are proud that more than two billion people around the world come to Facebook every month to share with friends and family, to learn about new products and services, to volunteer or donate to organizations they care about, or help in a crisis. The promise of real connection, of extending the benefits of real world connections online, is at the heart of what we do and has helped us grow into a global company.

Being at the forefront of new technology also means being at the forefront of new legal, security, and policy challenges. My team and thousands of other Facebook employees around the world come to work every day to confront these challenges head on. Our goal is to ensure Facebook is a place where both expression and personal safety are protected and respected. We appreciate your commitment to these values as well in your roles as policymakers.

## **COUNTERING TERRORISM ON FACEBOOK**

I would like to focus my testimony today on the ways Facebook is addressing the challenge of terrorist propaganda and recruitment online.

On terrorist content, our view is simple: There is no place on Facebook for terrorism. Our longstanding policies, which are posted on our site, make clear that we do not allow terrorists to have any presence on Facebook. Even if they are not posting content that would violate our policies, we remove their accounts as soon as we find them. They simply are not allowed to use our services under any circumstances. We also remove any

content that praises or supports terrorists or their actions whenever we become aware of it, and when we uncover evidence of imminent harm, we promptly inform authorities.

We recognize the challenges associated with fighting online extremism, some of which I will outline in my comments today. We are committed to being part of the solution, and we are developing strategies built around both technology and human expertise to address these threats.

## **A. Using Technology to Identify and Remove Terrorist Content**

One of the challenges we face is identifying the small fraction of terrorist content posted to a platform used by more than two billion people every month. Our proactive efforts—specifically, the use of artificial intelligence (AI) and other automation—have become increasingly central to keeping this content off of Facebook. We currently focus our most cutting-edge techniques on combating terrorist content about ISIS, Al Qaeda, and their affiliates, and we are working to expand to other terrorist organizations. As we shared recently in a public blog post, 99% of the ISIS and Al Qaeda-related terror content that we remove from Facebook is detected and removed before anyone in our community reports it, and in some cases, before it goes live on the site. We do this primarily through the use of automated systems like photo and video matching and text-based machine learning. Once we are aware of a piece of terrorist content, we remove 83% of subsequently uploaded copies within one hour of upload.

Importantly, we do not wait for ISIS or Al Qaeda to upload content to Facebook before placing it into our internal detection systems. Rather, we use a variety of techniques, including consulting external experts, to track propaganda released by these groups and proactively insert it into our matching systems. Often, this means we are able to prevent its upload to Facebook entirely.

Because terrorists also adapt as technology evolves, we are constantly updating our technical solutions. I would like to share with you today several specific examples of the ways we are using technology to stay ahead of terrorist activity and combat terrorism online.

### **1. Image Matching and Language Understanding**

When someone tries to upload a terrorist photo or video, our systems look for whether the image matches a known terrorism photo or video. This means that if we previously removed an ISIS propaganda video, for example, we can work to prevent other accounts from uploading the same video to our site.

We also have started experimenting with using AI to understand text that potentially advocates for terrorism. We are working to develop text-based signals to detect praise or support of terrorist organizations. These signals will be incorporated into an algorithm that is in the early stages of learning how to detect similar posts.

## **2. Removing Terrorist Clusters**

We know from the many terrorism academics and experts we work with that terrorists tend to radicalize and operate in clusters. This offline trend is reflected online as well. As such, when we identify Pages, groups, posts, or profiles that support terrorism, we use AI to identify related material that may also support terrorism. As part of that process, we utilize a variety of signals, including whether an account is “friends” with a high number of accounts that have been disabled for terrorism, or whether an account shares the same attributes as a disabled account.

## **3. Identifying Repeat Offenders**

When we disable terrorist accounts, those account owners may try to create new accounts using different identities. We have become faster at using technology to detect new fake accounts created by repeat offenders, or recidivists. Through this work, we have been able to dramatically reduce the time that terrorist recidivist accounts are on Facebook.

## **4. Cross-Platform Collaboration**

Because we prohibit terrorists from maintaining a presence anywhere in the family of Facebook applications, we have begun work on systems that enable us to remove terrorist accounts across all of our platforms, including WhatsApp and Instagram. Given the limited data some of our applications collect as part of their service, this ability to share data helps immensely in keeping all of our applications safe.

These are some of our key tools, but there are other tools as well. Our ability to outline them here is, however, constrained by the need to avoid providing a roadmap to bad actors seeking to evade detection.

## **B. Human Expertise**

Identifying terrorist content often requires analyzing the relevant context, and we know we cannot rely on AI alone to identify and remove terrorist content. For example, a photo of an armed man waving an ISIS flag could be propaganda or recruiting material, or it could be an image in a major news story. To understand more nuanced cases, we need human expertise.

Our community of users helps us by reporting accounts or content that may violate our policies—including the small fraction that may be related to terrorism. Our content review teams around the world—which grew by 3,000 people last year—work 24 hours a day and in dozens of languages to review these reports. More broadly, by the end of 2018 we will more than double the number of people working on safety and security, including terrorism issues, from 10,000 to 20,000.

We also have significantly grown our team of counterterrorism specialists. Distinct from our content review teams, we have more than 180 highly trained people who are exclusively or primarily focused on preventing terrorist content from ever appearing on our platform and quickly identifying and removing it if it does. This group includes former academics who are experts on counterterrorism, former prosecutors and law enforcement agents, investigators and analysts, and engineers. Within this specialist team alone, we speak nearly 30 languages.

### **C. Partnering with Others**

We are proud of the work we have done to make Facebook a hostile place for terrorists. We understand, however, that simply working to keep terrorism off Facebook is an inadequate solution to the problem of online extremism, particularly because terrorists are able to leverage a variety of platforms. We believe our partnerships with others—including other companies, civil society, researchers, and governments—are crucial to combating this threat.

To this end, we have partnered with our industry counterparts to more quickly identify and slow the spread of terrorist content online. For example, in December 2016, we joined with Microsoft, Twitter, and YouTube to announce the development of a shared industry database of “hashes”—unique digital fingerprints for photos and videos—for content produced by or in support of terrorist organizations. The database now contains more than 40,000 hashes, and the consortium of companies has increased to include twelve companies.

This past summer, we formalized our relationship with industry partners and announced the Global Internet Forum to Counter Terrorism (GIFCT), an endeavor that focuses on knowledge sharing, support for counterterrorism work, and technical cooperation, as represented by the hash consortium. Already, this endeavor has brought together more than 68 technology companies over the course of international working sessions held on three continents. This effort gives structure to our existing and future areas of collaboration and fosters cooperation with smaller tech companies, civil society groups, academics, governments, and international bodies such as the EU and the UN.

We engage with governments and inter-governmental agencies around the world and we recently commissioned a research consortium led by the Brookings Institution and the Royal United Services Institute to examine how governments, tech companies, and civil society can work together to fight online extremism and radicalization. We have learned much through briefings from agencies in different countries about extremist organizations’ propaganda mechanisms. We also have participated in and benefited from efforts to support industry collaboration by organizations such as the National Counterterrorism Center (NCTC), the EU Internet Forum, the Global Coalition Against Daesh, and the UK Home Office.

In recent months, we have further expanded our partnerships with several organizations including Flashpoint, the Middle East Media Research Institute (MEMRI),

the SITE Intelligence Group, and the University of Alabama at Birmingham's Computer Forensics Research Lab. These organizations report Pages, profiles, and groups on Facebook that are potentially associated with terrorist groups. They also send us photo and video files associated with ISIS and Al Qaeda that they have located elsewhere on the internet. We check this information against our algorithms for file "matches," in order to remove or prevent upload of the files to Facebook in the first instance.

We appreciate the critical role that law enforcement plays in keeping people safe. Our legal and safety teams work hard to respond to legitimate law enforcement requests while fulfilling our responsibility to protect people's privacy and security. We have a global team that strives to respond within minutes to emergency requests from law enforcement. We provide the information that we can in response to law enforcement requests, consistent with applicable law and our policies. For example, in the first half of 2017, we provided information in response to more than 75% of the 1,864 requests for emergency disclosures that we received from U.S. law enforcement agencies.

## **PREVENTING RECRUITMENT THROUGH COUNTERSPEECH**

We believe that a key part of combating extremism is preventing recruitment by disrupting the underlying ideologies that drive people to commit acts of violence. That's why we support a variety of counterspeech efforts. Although counterspeech comes in many forms, at its core these are efforts to prevent people from pursuing a hate-filled, violent life or convincing them to abandon such a life.

Over the past three years, we have commissioned research on what types of counterspeech are the most effective at combating hate and violent extremism. Based on that research, we believe the credibility of the speaker is incredibly important. We have therefore partnered with non-governmental organizations and community groups around the world to empower positive and moderate voices. For example, two years ago, we worked with the Institute for Strategic Dialogue to launch the Online Civil Courage Initiative, a project that has engaged with more than 100 anti-hate and anti-extremism organizations across Europe. We also have worked with Affinis Labs to host hackathons in places like Manila, Dhaka, and Jakarta, where community leaders joined forces with tech entrepreneurs to develop innovative solutions to challenge extremism and hate online. Finally, we worked with EdVenture Partners to develop a peer-to-peer student competition called the Facebook Global Digital Challenge (P2P). This is a semester-long university course during which students build a campaign to combat extremism in their area, launch it, track its success, and then submit the results as part of a global competition. The University of Central Oklahoma recently implemented a student-led counterspeech program through P2P that uses social media to encourage people to challenge their beliefs and stereotypes. In less than three years, these P2P projects have reached more than 56 million people worldwide through more than 500 anti-hate and extremism campaigns created by more than 5,500 university students in 68 countries.

## **CONCLUSION**

In conclusion, let me reiterate our commitment to combating extremism on our platform. We have a responsibility to do all we can to combat these threats, and we are committed to improving our efforts.

Of course, companies like Facebook cannot do this without help. We will continue to partner with appropriate authorities to counteract these threats. By working together, business, government, and civil society can make it much harder for malicious actors to harm us, while simultaneously ensuring that people can express themselves freely and openly. I am here today to listen to your ideas and concerns, and I look forward to continuing this constructive dialogue.

# Exhibit 33

# HEARING BEFORE THE UNITED STATES SENATE COMMITTEE ON COMMERCE, SCIENCE, & TRANSPORTATION

September 18, 2019

Testimony of Monika Bickert

Vice President for Global Policy Management and Counterterrorism, Facebook

## **I. Introduction**

Chairman Wicker, Ranking Member Cantwell, and distinguished members of the Committee, thank you for the opportunity to appear before you today. My name is Monika Bickert, and I am the Vice President of Global Policy Management and Counterterrorism at Facebook. In that role, I lead our efforts related to Product Policy and Counterterrorism. Prior to assuming my current role, I served as lead security counsel for Facebook, working on issues ranging from children's safety to interactions with law enforcement. And before that, I was a criminal prosecutor with the Department of Justice for 11 years in Chicago and Washington, DC, where I prosecuted federal crimes including public corruption and gang violence.

On behalf of everyone at Facebook, I would like to express our sympathy and solidarity with the victims, families, communities, and everyone else affected by the recent terrible attacks across the country. In the face of such heinous acts, we remain committed to cooperating with law enforcement and standing with our community against hate and violence. We are thankful to be able to provide a way for those affected by the horrific recent attacks to communicate with loved ones, to organize events for people to gather and grieve, and to raise money to help support these communities as they begin to heal.

Facebook's mission is to give people the power to build community and bring the world closer together. We are proud that more than two billion people around the world come to Facebook every month to connect and share with one another. But people need to feel safe in order to build this community. That is why Facebook prohibits harmful conduct on its platform, including hate speech and inciting violence. Our goal is to ensure that Facebook is a place where both expression and personal safety are protected and respected.

We are not aware of any connection between our platform and the recent attacks, but we recognize that we all have a role to play in keeping our communities safe. At Facebook, we have strong policies and invest significant resources to protect our users on and offline.

## **II. Facebook's Policies Against Hate and Violence**

Facebook is committed to protecting our community by removing any content from our services that encourages real-world harm. Because harmful content can take many forms,

we have several policies in place to address these issues, all of which are published in our Community Standards, which define the content that is and is not allowed on our platform.

When we find content that violates our standards, we remove it. We invest in technology, processes, and people to help us identify violations and act quickly to mitigate any impact. There is always room for improvement, but we remove millions of pieces of content every year, much of it before any user reports it. We outline below several of the important steps that we take to prevent violence and keep our users safe.

**Prohibition Against Violence and Incitement:** We care deeply about our users and we want them to be safe. Therefore, it is critical to our mission to help prevent potential offline harm that may be related to content on Facebook. We remove content, disable accounts, and work with law enforcement when we believe there is a risk of physical harm or direct threats to public safety.

**Prohibition of Dangerous Individuals and Organizations:** In an effort to prevent and disrupt real-world harm, we do not allow any individuals or organizations that proclaim a violent mission, advocate violence, or are engaged in violence to have a presence on Facebook for any purpose, even if it appears benign. This includes organizations or individuals involved in the following:

- Terrorist activity, both domestic and international;
- Organized hate, including white supremacy and white nationalism;
- Human trafficking; and
- Organized violence or criminal activity.

We do not allow propaganda or symbols that represent any of these organizations or individuals to be shared on our platform unless they are being used to condemn or inform—for example, by media organizations. We do not allow content that praises any of these organizations or individuals or any acts committed by them. And we do not allow coordination of support for any of these organizations or individuals or any acts committed by them.

**No Promoting or Publicizing Crime:** We prohibit people from promoting or publicizing violent crime, theft, and/or fraud because we do not want to condone this activity and because there is a risk of copycat behavior. We also do not allow people to depict criminal activity or admit to crimes they or their associates have committed.

**Policies Against Coordinating Harm:** In an effort to prevent and disrupt real-world harm, we prohibit people from facilitating or coordinating future activity, criminal or otherwise, that is intended or likely to cause harm to people, businesses, or animals. People can draw attention to harmful activity that they may witness or experience as long as they do not advocate for or coordinate harm.

**Combatting Suicide and Self-Injury:** We also use and continue to develop tools and resources to proactively identify and help people who may be at risk of suicide or self-injury. We leverage pattern recognition technology to detect posts or live videos where someone might be expressing an intent to harm themselves. We also use artificial intelligence (AI) to prioritize the order in which our team reviews reported content relating to suicide or self-injury. This ensures we can get the right resources to people in distress and, where appropriate, we can more quickly alert first responders. And we remove content that encourages suicide or self-injury, including certain graphic imagery and real-time depictions that experts tell us might lead others to engage in similar behavior. We also work with organizations around the world to provide assistance and resources to people in distress.

**Cooperation with Law Enforcement:** Law enforcement plays a critical role in keeping people safe, and we have a long history of working successfully with law enforcement to address a wide variety of threats. As a former federal prosecutor, I know that this cooperation is vital. When we do receive reports or otherwise find content that violates our policies, we remove it. And we proactively reach out to law enforcement if we see a credible threat of imminent harm.

### **III. Facebook’s Efforts to Combat Violence and Hate**

Our efforts to combat violent and hateful content are focused in three areas: developing new technical capabilities for our products, investing in people, and building partnerships.

**Product Enhancements:** Facebook has invested significantly in technology to help meet the challenge of proactively identifying violent content, including through the use of AI and other automation. These technologies have become increasingly central to keeping hateful and violent content off of Facebook.

We use a wide range of technical tools to identify violent and hateful content. This includes hashes—or digital fingerprints—that allow us to find secondary versions of known bad content; text parsing; digital “fan-outs” to identify profiles, groups, and pages related to those we have identified as problematic; and more holistic machine learning that can assess all aspects of a post and score whether it is likely to violate our Community Standards.

We also know that bad actors adapt as technology evolves, and that is why we constantly update our technical solutions to deal with more types of content in more languages, and to react to the new ways our adversaries try to exploit our products. For example, in response to the tragic events in Christchurch, we made changes to Facebook Live to restrict users if they have violated certain rules—including our Dangerous Organizations and Individuals policy. We now apply a “one-strike” policy to Live: anyone who violates our most serious policies will be restricted from using Live for set periods of time—for example, 30 days—starting on their first offense. We have also updated our proactive detection systems and reduced the average time it takes for our AI to find a violation on Facebook Live to 12 seconds—a 90% reduction in our average detection time from a few

months ago. Being able to detect violations sooner means that in emergencies where every minute counts, we can assist faster.

**Investments in People:** We know that we cannot rely on AI alone to identify potentially violent content. Context often matters. To understand more nuanced cases, we need human expertise.

One of our greatest human resources is our community of users. Our users help us by reporting accounts or content that may violate our policies—including the small fraction that may be related to acts of violence. To review those reports, and to prioritize the safety of our users and our platform more generally, we have more than 30,000 people working on safety and security across the company and around the world. That is three times as many people as we had dedicated to such efforts in 2017. Our safety and security professionals review reported content in more than 50 languages, 24 hours a day.

We also have a team of more than 350 people at Facebook whose primary job is dealing with terrorists and other Dangerous Individuals and Organizations. This team includes language and cultural specialists, former law enforcement and intelligence professionals, and academics that have studied these groups and individuals for years. Many of them came to Facebook specifically because they are committed to the mission of keeping people safe.

This team was previously focused on counterterrorism, and we used our most sophisticated tools to predominantly combat ISIS, al-Qaeda, and their affiliates, which were recognized then as posing the greatest threats to our global community. Now, they lead our efforts against all people and organizations that proclaim or are engaged in violence. We are taking the initial progress we made in combatting content affiliated with ISIS, al-Qaeda, and their affiliates, and we are further building out techniques to identify and combat the full breadth of violence and extremism covered under our Dangerous Organizations policy.

**Partnerships:** We are proud of the work we have done to make Facebook a hostile place for those committed to acts of violence. We understand, however, that simply working to keep violence off Facebook is not an adequate solution to the problem of online extremism and violence, particularly because bad actors can leverage a variety of platforms. We believe our partnerships with other companies, civil society, researchers, and governments are crucial to combatting this threat. For example, our P2P Global Digital Challenge, which engages university students around the world in competitions to create social media campaigns and offline strategies to challenge hateful and extremist narratives, has launched over 600 counterspeech campaigns from students in 75 countries, engaged over 6,500 students, and reached over 200 million people. We're also partnering with Life After Hate, an organization founded by former violent extremists, to connect people who search for terms associated with white supremacy to resources focused on helping people leave behind hate groups.

Our work to combat violence is never complete. Individuals and organizations intent on violent acts come in many ideological stripes—and the most dangerous among them are deeply resilient. We know that bad actors will continue to attempt to skirt our detection with more sophisticated efforts, and we are dedicated to continuing to advance our work and share our progress.

#### **IV. Conclusion**

Facebook is committed to helping people build a vibrant community that encourages and fosters free expression. At the same time, we want to do what we can to protect our users from real-world harm and stop terrorists, extremists, hate groups, and any others from using our platform to promote or engage in violence. We recognize that there is always more work to do in combatting the abuse of our site by bad actors, but we are proud of the progress we have made over the last few years. We know that people have questions about what we are doing to continue that progress, and we look forward to working with this Committee, regulators, and others in the tech industry and civil society to continue working on these issues. I appreciate the opportunity to be here today, and I look forward to your questions.

# Exhibit 34

**HEARING BEFORE  
THE UNITED STATES SENATE JUDICIARY COMMITTEE  
SUBCOMMITTEE ON THE CONSTITUTION**

April 10, 2019

Testimony of Neil Potts  
Public Policy Director, Facebook

**I. Introduction**

Chairman Cruz, Ranking Member Hirono, and distinguished members of the Subcommittee, thank you for the opportunity to appear before you today. My name is Neil Potts, and I am a Director at Facebook with oversight of the development and implementation of Facebook's Community Standards, which serve as Facebook's rules for what types of content are allowed on our platform. I am a graduate of the United States Naval Academy and the University of Virginia School of Law. Prior to joining Facebook, I served as a ground intelligence officer in the United States Marine Corps and was deployed in support of Operation Enduring Freedom and Operation Iraqi Freedom.

Facebook's mission is to give people the power to build community and bring the world closer together. Over two billion people come to our platform every month to connect with friends and family, to discover what's going on in the world, to build their businesses, to volunteer or donate to organizations they care about, and to help those in need. Our users share billions of pictures, stories, and videos about their lives and their beliefs each day.

The diversity of viewpoints, expression, and experiences on our platform highlights much of what is best about Facebook. But it also presents challenges when deciding what content should and should not be allowed on our platform.

Facebook's most important responsibility is keeping people safe, both online and off. But we also strive to foster a diversity of viewpoints and experiences on our platform. To create a place that is safe for such a variety of people, we have to make hard decisions about what can and cannot be allowed on our platform.

We created our Community Standards to standardize our content removal decisions. Our Standards outline publicly and transparently what content is permissible. They apply around the world to all types of content and are designed to be applied consistently and fairly to a community that transcends regions, cultures, religions, and languages. At our scale, we are not always going to get the enforcement decision right. But I would like to state unequivocally that Facebook does not favor one political viewpoint over another, nor does Facebook suppress conservative speech. Our Community Standards have been carefully designed to ensure that content is reviewed in a neutral way, focused on what is necessary to keep our users safe. Our systems and human reviewers work in concert to identify and remove violent, hateful, or dangerous content.

But these decisions can be both far-reaching and novel: how to improve the quality of the discourse on a site as voluminous and varied as ours, how to keep hateful content off that site, and how to do so without hampering free expression. As Mark Zuckerberg noted in his recent op-ed, we should not make so many important decisions about speech on our own and everyone in the social media space should strive to do everything they can to keep the amount of harmful content to a minimum.

For our part, Facebook is creating an independent body so people can appeal our decisions. And we are working with governments on ensuring the effectiveness of our content review systems. But we need a standardized, industry-wide approach for determining the guidelines by which potentially harmful content is reviewed, and by which we assess issues as critical as election integrity, privacy, and data portability.

The rules of the Internet should reflect our society's values for a safe and open Internet. We care about updating these rules because we believe that technology should serve everyone, whatever their background, whatever their politics. Conversations like the ones we will have here today are an important part of making that belief a reality, and we appreciate the opportunity to take part in it.

I would like to begin by telling you more about our efforts to ensure that our content moderation policies are viewpoint neutral and designed to encourage dialogue and the free flow of ideas.

## **II. Content Moderation and Neutrality**

Our content policies are the centerpiece of our efforts to keep people safe. Our Community Standards and related policies work to balance our goals of giving people a place to express themselves genuinely while also promoting a welcoming and safe environment.

At the same time, we believe in embracing diverse views. Indeed, one of Facebook's foundational principles is to be a platform for diverse ideas. Suppressing content on the basis of political viewpoint or preventing people from seeing what matters most to them is directly contrary to Facebook's mission. We want Facebook to be a place where people can discover a greater diversity of news and information than they could otherwise. Therefore, unless we are confronted with a specific potential harm, we tend to err on the side of allowing content, even when some people find it objectionable or offensive.

Research shows that social media platforms provide more information diversity than traditional media ever has. A 2017 Reuters digital news report concluded that, on average, people who use social media, aggregators, and search engines experience more information diversity than non-users. Similarly, a Pew Research Center survey found that more than half of Facebook users report that there are a range of political beliefs among their Facebook friends.

Our Community Standards do not prohibit users from discussing controversial topics or supporting a debated point of view. Nor do they favor opinions on one end of the

political spectrum or the other. We believe that such discussion is critical to promoting greater understanding among members of our community.

But given the amount of content on our platform, content reviewers must respond to millions of reports each week from all over the world, and we do not always get it right. We know that there have been a number of high-profile content removal incidents affecting individuals across the political spectrum, and we are taking a variety of steps to respond to the concerns raised by this Subcommittee and others.

We want to make sure our community understands the systems and processes that lead to our content removal decisions. Transparency is the key to fostering that understanding, and as part of our annual Transparency Report, we publish a Community Standards Enforcement Report describing the amount and types of content we have taken action against, as well as the amount of content that we have proactively flagged for review. We currently publish our report every six months, but we soon expect to do so every quarter. In addition, we publish comprehensive guidelines to provide more clarity around where we draw lines on these complex and evolving issues. We hope that by sharing this information, we can encourage all stakeholders to contribute to an ongoing dialogue around our decisionmaking processes and help us improve our efforts to develop and enforce our standards.

We have also solicited external feedback on our content moderation policies from sources across the political spectrum. We have partnered with over 100 groups across the political spectrum, and we are continuing to expand our list of outside partner organizations to ensure we receive feedback on our content policies from a diverse set of viewpoints. The input we receive from these groups will help us to improve over time and ensure we can most effectively serve our diverse community.

For example, former Senator Kyl is gathering insights from members of Congress and a number of conservative groups and is assessing whether the company is unintentionally biased against conservative points of view. Senator Kyl and his team at Covington & Burling have talked to over 130 groups and individuals to understand how our policies and enforcement are affecting different people and communities. Having wrapped up the first phase of the project, which was focused on this external engagement, Senator Kyl and his team are now reviewing our external and internal policies. While conducting this review, Senator Kyl and his team have also been engaged in reviewing and providing insights into future policy changes under consideration. After Senator Kyl has reviewed our policies and internal guidelines, he and his team will share feedback and suggestions for improvements.

Another example of external feedback we have solicited is that of Laura Murphy, a national civil liberties and civil rights leader, who, as part of an independent civil rights audit, is coordinating with civil rights groups to help advise Facebook on how to empower users with a diversity of opinions while encouraging civil discourse. And Relman, Dane & Colfax, a respected civil rights law firm, is in the process of carrying out a comprehensive civil rights assessment of Facebook's services and internal operations.

We also created an appeals process for content that was removed from our platform as hate speech because we recognize that we sometimes make enforcement errors. We are working to extend this process further, by making appeals available not just for content that was taken down, but also for content that was reported and nonetheless left up, and by creating an independent oversight board of experts on free speech and safety to render binding and transparent decisions on these appeals. Through efforts like these, we will continue improving our systems and processes to correct for and minimize mistakes in the future.

And we are continuing our work to refine and enhance the quality of our machine learning, which is a first line of defense for content assessment on our platform. We hope that these improvements and safeguards will help ensure that Facebook remains a platform for a wide range of ideas and enables the broadest spectrum of free expression possible, while still keeping our space welcoming and safe for our entire community.

While we will continue to take steps on our own to improve, we hope that we have a broader discussion with the industry regarding decisions about what speech is harmful. People should be able to expect that companies will address these issues in a consistent way. We should have a broader debate about what we want as a society and how regulation can help. We believe Facebook has a responsibility to help address these issues, and we are looking forward to discussing them with lawmakers around the world, including during our discussion here today.

### **III. Terrorism, Violence, and Hate Speech**

While I know that we are here today to discuss our efforts to encourage a diversity of views and to ensure we remain politically neutral in our efforts to create a safe and welcoming environment for our community, I would also appreciate the opportunity to discuss our efforts to stamp out the use of our platform by terrorists and other extremists, particularly in light of the despicable acts perpetrated recently in Christchurch.

Since the terrorist attack, Facebook has been working closely with the New Zealand Police. At the same time, we have been working to understand how we can prevent such use in the future. Those efforts include exploring restrictions on who can go Live depending on factors such as prior Community Standards violations, working to improve our matching technology to detect and stop the spread of horrific viral videos, and developing methods to react faster when harmful content is video live-streamed.

More broadly, Facebook employs over 30,000 people across the country and around the world focused on safety and security, including those that block and remove terrorist and extremist accounts and their content. That group includes engineers who every day are building new, automated systems to identify and remove this material—often at upload, before it can be viewed by our community. And we have specific protocols in place to pass on threats of imminent harm to law enforcement as soon as we become aware of them.

We are also expanding our industry collaboration through the Global Internet Forum to Counter Terrorism (GIFCT), which we co-launched more than two years ago to help fight terrorism and extremism online alongside our peers at other technology companies, including Google, YouTube, Microsoft, and Twitter. The information made available through GIFCT allows smaller companies the ability to take advantage of our technology and tactics, even with fewer people and resources.

But hate can take many forms and none of it is permitted in our community. We disallow hate speech because it creates an environment of intimidation and exclusion that limits people's willingness to communicate and share with one another. In fact, Facebook rejects not just hate *speech*, but all hateful ideologies. That means that white supremacists are not allowed on our platform under any circumstances, and we have recently announced a ban on white nationalism and white separatism as well. We will therefore now use our Dangerous Organizations policy to remove from our platform praise, support, or representation of white supremacy, as well as of white nationalism or white separatism, because both ideologies are inextricably linked with white supremacy and with violence more generally. We have already banned more than 200 white supremacist groups because of our Dangerous Organizations policy.

We recognize the serious harm that hateful content can inflict in any community, including ours, and we continue to be committed to finding new and better ways to combat hate on Facebook.

## **V. Conclusion**

In closing, I want to reiterate our deep commitment to building a community that encourages and fosters free expression, as well as to stopping terrorists, extremists, and hate groups from using our platform to promote abhorrent ideologies. We want Facebook to be a place where individuals with diverse viewpoints can connect and exchange ideas. There is a lot more to do, but we are proud of the significant progress we have made over the last few years. Still, we know that people have questions about what we are doing to continue that progress, and we are looking forward to working with the members of this Committee, other policymakers, and others in the tech industry and civil society to continue the dialogue around these issues. I appreciate the opportunity to be here today, and I look forward to your questions.

# Exhibit 35

# Facebook Papers: 10 shocking revelations from the leaked documents

NoticiasFinancieras - English

## Search Details

---

Search Query: "joel kaplan" and remov! or "take down"  
Jurisdiction: FE

## Delivery Details

---

Date: November 17, 2021 at 2:47 PM  
Delivered By: Peter Romer-Friedman  
Client ID: GUPTAWESSLER  
Status Icons: 

10/26/21 NOTICIASFINANCIERAS - ENG. (Pg. Unavail. Online)

2021 WLNR 35035471

NoticiasFinancieras - English  
Copyright (c) 2021 ContentEngine, USA.

October 26, 2021

## Facebook Papers: 10 shocking revelations from the leaked documents

Nearly two months ago, The Wall Street Journal began publishing a series of reports based on tens of thousands of internal documents that a whistleblower named Frances Haugen turned over to the newspaper. "The Facebook files," as the stories were dubbed, revealed the extent to which the company was aware of the damage its platforms were doing to everything from the effort to vaccinate Americans to the self-esteem of teenagers.

Disinformation was spreading. Hate speech was rampant. People were even using Facebook to sell human organs. The leaked documents make clear that the company didn't much care to stop it, and in some cases, that it deliberately covered up internal research that revealed how toxic the social network had become.

Last Sunday, Ben Smith of The New York Times reported that days after Haugen appeared on 60 Minutes, she agreed to share the trove of documents with 17 other news outlets, provided they agreed to hold any news until a mutually agreed upon date. Those media outlets spent the next few weeks not only combing through the leaked information, but also conducting their own reporting on Facebook's practices. The embargo was lifted, and on Monday, the internet exploded with bombastic stories about the social media giant, many of them based on the documents provided by Haugen.

Here's what you may have missed:

### **1. Facebook ignored internal complaints about spreading posts with political misinformation leading up to the 2020 election**

According to a New York Times report, recent documents show that Facebook has repeatedly ignored internal complaints about political posts filled with misinformation and conspiracy theories from before and after the 2016 election.

Just days before Election Day last November, an employee triggered an internal alarm to inform team members that "comments with the most incendiary election disinformation were being amplified to appear at the top of comment sequences," according to the Times. Then, on Nov. 9, a Facebook data scientist messaged colleagues with a staggering statistic: 10 percent of American users posting political content claimed that Joe Biden's victory was fraudulent and that the process was rigged to prevent Donald Trump from returning to office. In addition, some of these posts appeared to be aimed at inciting violence.

### **2. Facebook didn't do enough to contain 'Stop the Steal' groups before the uprising: "Enforcement was fragmented"**

After protesters supporting Trump stormed the U.S. Capitol on Jan. 6, some employees complained about Facebook being ill-prepared to respond with the necessary agility. The New York Times recently reported that several posts from employees cited "dozens" of Stop the Steal groups pushing lies about the election that were active leading up to the uprising. "I have always felt that, on balance, my work has been meaningful and helpful to the world at large," one message said. "But honestly, this is a very dark day for me here."

An internal review in March, assessing how the company handles Stop the Steal groups, found that "enforcement was fragmented."

### **3. Facebook watched as QAnon conspiracy theories grew**

Long before the election, employees realized the dangers of radicalization at Facebook, the documents say, and years passed without substantial enough changes to slow the snowball effect. In the summer of 2019, one of the company's researchers created a fake account for an imaginary conservative woman living in North Carolina named Carol Smith, NBC News Previous Week reported. The 41-year-old's fictional profile had no photo, but many interests, including Fox News, parenting and Christianity. Within days, Facebook began recommending QAnon-related pages for "Smith." In less than a month, his feed "became a constant stream of misleading, polarizing, low-quality content," the researcher wrote."

### **4. Facebook "routinely makes exceptions for powerful actors when enforcing content policy"**

A data scientist pointed out that "final calls on content policy are routinely made by senior executives ... sometimes Mark Zuckerberg." They added that "it is unclear why executives would be consulted" and questioned "whether there was an unwritten aspect to our policies, namely to protect sensitive constituents." The analyst referred to "many" communications with colleagues on Facebook's content policy team, based in Washington, DC, who feel "pressured to ensure their recommendations are aligned with lawmakers' interests."

According to information obtained by Politico, the lobbying and government relations team overseen by former Republican operative **Joel Kaplan** regularly weighs in on communications-related issues when dealing with right-wing figures and ads from former President Donald Trump, as well as "the fallout from the George Floyd Protests in June 2020." Facebook says Kaplan's group is "just one of many" that Facebook consults in making content decisions.

### **5. Mark Zuckerberg gave in to Vietnam's censorship demands**

The Washington Post reported that in 2020 Mark Zuckerberg agreed to crack down on rhetoric critical of the Vietnamese government after the Communist Party in charge of the country asked him to. If he did not comply, Facebook risked losing the estimated \$1 billion in revenue generated by the company's presence in the Southeast Asian country. Facebook's own transparency report revealed the impact of the decision. The company blocked 834 posts from Vietnamese users in the first half of 2020, compared to more than 2,200 in the second half.

Zuckerberg reportedly defended the decision by arguing that completely depriving Vietnamese people of Facebook would be worse for free speech than censoring them. But according to advocates and activists interviewed by the Post, Facebook gave "the government almost total control over the platform."

### **6. Documents show Facebook did little to stop the spread of violent rhetoric surrounding the Ethiopian civil war**

For more than a year, Ethiopia has suffered through a turbulent civil war, and Facebook's neglect of the African nation has made things worse. Documents reviewed by American CNN show that the company has failed to equip local teams with the staff resources needed to navigate such a fragile period, despite several instances of employees warning the company about a variety of foreign organizations and armed groups spreading hate content and incitement to violence.

When Haugen came forward, she specifically called out "how poorly Facebook is handling places like Ethiopia" as one of her reasons for doing so, adding that "the raw version [of Facebook] that roams wild in most of the world has none of the things [related to online safety and curation] that make it palatable in the United States" and expressing fear for "many lives on the line".

Facebook has publicly highlighted its issues with Ethiopia as a problem and priority, but the company doesn't seem to be moving fast enough or with strong enough strategies. While, for example, Facebook watchdogs have recommended **removing** official accounts supporting the Fano militia - a group at the center of many controversies, including murder, looting and rape, according to CNN - other officials say individuals promoting Fano posts are still up through the.

In the summer of 2020, an employee shared an internal report that "found significant gaps" in how Facebook monitors events in Ethiopia, detects hate speech and flags misinformation. Still, Haugen argues that Facebook only offered "'even light language support' in two of the country's many native languages," as CNN reported. One researcher, Berhan Taye, wrote an open letter

implored Facebook to adequately equip its local team with people with enough cultural knowledge to properly respond to hours of footage created by millions of daily users in the area. Teye said little has changed in more than a year.

**7. Apple almost yanked Facebook and Instagram from the App Store because it wasn't doing enough to stop human trafficking in the Middle East**

Facebook was being used to buy and sell abused maids in the Middle East, a human trafficking violation flagged by officials that Facebook didn't do much to fix. The Wall Street Journal reported the issue in September, and the Associated Press followed up with a new report Monday. The situation got so bad, the media noted, that Apple threatened to pull Facebook and Instagram from the App Store. Facebook admitted in internal documents that it was "underestimating confirmed abusive activity," and the AP notes that it's still not hard to find ads from women to maids on the platform.

**8. Facebook allowed Arab hate content to spread on its platforms ... a lot**

In late 2020, Facebook realized it had a very real algorithm problem: only 40 percent of Arab hate content was being proactively detected. It was even worse on Instagram, which detected only 6% despite having 95% "more triggered hate speech violations" than Facebook in the Middle East and North America (MENA), according to an internal report created by a Facebook employee. This goes beyond posts and extends to online ads as well, according to the report, which cites "many" harmful ads targeting women and the LGBTQ community. These ads, however, were rarely flagged by Facebook in MENA territories. Meanwhile, Facebook was incorrectly detecting terrorist content across the region, resulting in the exclusion of non-violent Arabic content 77 percent of the time, according to a Politico report published Monday.

**9. Iraqi militias have been posting child nudity on rivals' Facebook pages**

Some supporters of Sunni and Shiite militias have been posting graphic images such as child nudity on their rivals' Facebook pages with the aim of getting those opponents' accounts shut down, Politico reported Monday. In another post reviewed by Politico, Islamic State fighters used a photo of Mark Zuckerberg to help a post applauding the deaths of 13 Iraqi soldiers that went unnoticed by the company's radar. It is unclear whether Facebook has done anything to respond to these specific incidents.

**10. Facebook has allowed anti-Muslim hate content to spread across India**

When religious protests flooded India, Facebook's largest market, in late 2019, "inflammatory content" aimed primarily at Muslims on Facebook increased 300 percent, the Wall Street Journal reported Saturday. Documents show that Facebook researchers recommended that the company **remove** one of two Hindu nationalist groups for posting hateful, anti-Muslim content - and that Facebook didn't listen. (The other was not deemed dangerous enough for **removal**, due to "political sensitivities," despite things like "misinformation claiming that the Quran calls for men to rape their female relatives." Facebook representative Andy Stone responded to the Journal with a statement about the company's "careful, rigorous, and multidisciplinary" banning processes.

Like the Ethiopian researchers, Indian colleagues called for more resources to detect and police users who spread hate, according to the Journal, which cited another report in which researchers flagged a different Hindu nationalist organization, the Bajrang Dal, for allegedly using Facebook's WhatsApp to "organize and incite violence." A spokesperson for the Bajrang Dal denied those claims to the Journal, before asking "If they say we broke the rules, why haven't they **removed** us?"

Politico reported on Monday documents from an internal Facebook presentation in which a data scientist made reference to an Indian politician who "regularly posted hate speech" but "was exempted by India's Public Policy team from normal punishment explicitly for political considerations." A Facebook spokesperson "would only go further by saying that this 'was not the only factor,'" the analyst wrote.

**---- Index References ----**

Company: Narragansett Bay Commission; Sunni International Limited; THE ASSOCIATED PRESS; APPLE INC.; P.O.L.I.C.Y. LIMITED; INSTAGRAM, INC.; CHRISTIANITY.COM; CABLE NEWS NETWORK, INC.; GRAHAM HOLDINGS COMPANY; POLITICO LLC; FACEBOOK, INC.; FOX NEWS NETWORK, LLC; HALO EXPLORATION LTD.; THE NEW YORK TIMES COMPANY

News Subject: (Civil Unrest (1CI11); Emerging Market Countries (1EM65); Global Politics (1GL73); Islam (1IS02); Major Corporations (1MA93); Religion (1RE60); Social Issues (1SO05); Top World News (1WO62); World Conflicts (1WO07))

Industry: (Internet (1IN27); Internet Media (1IN67); Online Social Media (1ON38))

Region: (Africa (1AF90); Asia (1AS61); East Africa (1EA80); Eastern Asia (1EA61); Ethiopia (1ET14); Far East (1FA27); India (1IN24); Indian Subcontinent (1IN32); Indo China (1IN61); Middle East (1MI23); Southeast Asia (1SO64); Southern Asia (1SO52); Vietnam (1VI02))

Language: EN

Other Indexing: (Wall Street Journal; Republican; Communist Party; Ethiopia; Islamic State; Bajrang Dal; India; NBC; Sunni; Associated Press; Apple; Policy; Instagram; Christianity; CNN; Washington Post; Politico; Facebook; Fox News; Fano; The New York Times) (Frances Haugen; Americans; Ben Smith; Joe Biden; Donald Trump; Carol Smith; Mark Zuckerberg; Mark Zuckerberg; Joel Kaplan; President Donald Trump; Berhan Taye; Andy Stone)

Keywords: (Giro); (abrir whatsapp); (ap facebook); (baixar facebook); (baixar facebook lite); (baixar instagram); (brir instagram); (close friends instagram); (como baixar whatsapp gb); (como cancelar conta do instagram); (como colocar senha no whatsapp?); (como postar no instagram pelo pc); (como saber quem visitou meu perfil no instagram grátis); (denúncias); (entrar no instagram pelo facebook); (estúdio de criação facebook); (EUA); (FAC); (Facebook); (Facebook adolescentes); (facebook apagão); (Facebook arquivos secretos); (Facebook ataque hacker); (Facebook caiu o que fazer?); (Facebook cookies); (facebook criar conta); (Facebook dados pessoais); (facebook denúncia); (Facebook denúncias Wall Street)

Word Count: 1818

---

End of Document

© 2021 Thomson Reuters. No claim to original U.S. Government Works.

**NewsRoom**

# Exhibit 36

**Get first dibs on all online Black Friday deals**  
Paid members shop 4 hours early.



**Become a member**  
\*Not available to trial members. While supplies last.



**yahoo!**  
**Help rid your phone of malicious apps.**  
Find them and delete them with Norton™ Security Online. FREE\* for 30 days.  
[Try it free!](#)



yahoo!finance



# Here's who is sitting behind Mark Zuckerberg and why they're there



**Ethan Wolff-Mann** · Senior Writer

April 11, 2018

**In this article:**

**Mark Zuckerberg**  
American Internet e...

**Joel Kaplan**  
VP Global Public Pol...

For hour after hour on Tuesday afternoon, Facebook (FB) CEO Mark Zuckerberg answered

**TRENDING**

**Audit: Governor improperly used COVID funds for salaries**

Associated Press · 4 min read



**Rittenhouse judge back in spotlight during jury instructions**

Associated Press · 4 min read



**Hillary Clinton Trolls Steve Bannon With Just 5 Words**

HuffPost · 1 min read



**'Vice presidents just don't break through.' Why are Kamala Harris' approval ratings lower than...**

USA TODAY · 11 min read



**Rittenhouse trial could be the 'pendulum swinging' back after George Floyd, expert says**

NBC News · 4 min read



video feeds. To Zuckerberg's left, in green, sat a Facebook star lobbyist Myriah Jordan, whose official title is public policy director. Jordan had previously worked in Sen. Richard Burr (R-NC)'s office where she was general counsel, and before that worked for the George W. Bush administration as special assistant for policy.



Myriah Jordan and Joel Kaplan, the people behind Mark Zuckerberg in the Senate. (Yahoo Finance screenshot)

On Zuckerberg's right sat Joel Kaplan, Facebook's VP of global public policy. Kaplan served as George W. Bush's deputy chief of staff, where he succeeded Karl Rove. Kaplan clerked for Supreme Court Justice Antonin Scalia and came to Facebook from Texas electric utility Energy Future Holdings.

### Wednesday at the House

Zuckerberg was back on Capitol Hill Wednesday morning, and the faces in the camera's direct view behind him changed somewhat. From left to right: Pearl Del Rosario, associate general counsel; Catlin O'Neill, public policy director; Joel Kaplan; Chris Herndon, public policy director.



Facebook Mark Zuckerberg on day two of his Capitol Hill rounds, in front of the Senate.

Grill, griddle, air fry & more. Shop now

### POPULAR



SoCal's cooler temps after mini-heatwave to last several days

KABC - Los Angeles



Uber Driver Realizes She's Driving Boyfriend's...

Ad • Rhyme Junkie



Coronavirus dashboard: Catch up fast

Axios



AccuWeather: Bright and brisk

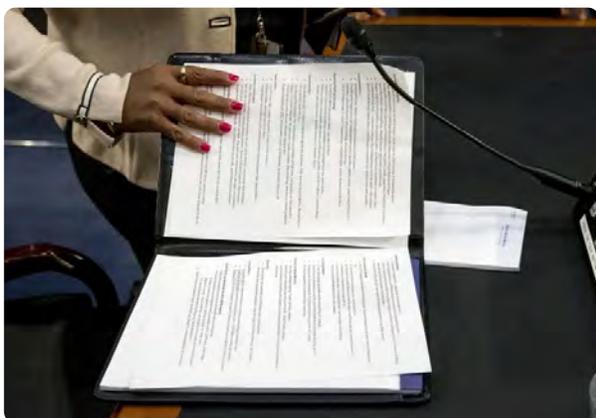
WABC - NY

Sign in

Mail

has not worked for the government. Herndon was the counsel for the Senate committee on commerce, science and transportation, the legislative director for former Rep. George Radanovich, and legislative counsel serving Rep. Patrick McHenry.

The faces behind Zuckerberg, doubtless familiar to many of the lawmakers present, illustrate the importance of government relations and lobbying efforts for large tech companies in Silicon Valley.



An aide to Facebook CEO Mark Zuckerberg closes a binder of notes left on the table as Zuckerberg takes a short break from testifying before a joint hearing of the Commerce and Judiciary Committees on

[More](#)

The CEO's talking points, left open on the desk for photographers to see, showed the careful prep work that went into Zuckerberg's polished performance that had him parrying almost all of the senators' jabs.

Fundstrat's Thomas Block, who has prepared witnesses for tough congressional hearings before, told Yahoo Finance that the government relations employees did a good job preparing Zuckerberg.

"He was well-prepared, had obviously had good practice sessions and importantly seemed to catch the right balance between personal poise yet respectful to the senators," said Block. "The market seemed to like performance."



### Rays OF Arozarena, Reds 2B India earn Rookie of Year honors

Associated Press



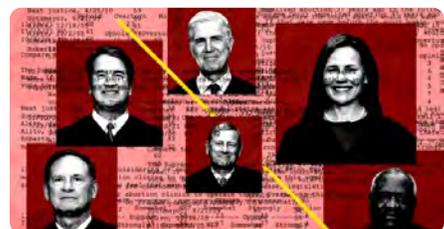
### Historic Figures Who Were Actually Photographed

Ad • Past Factory



### Grades from KU Jayhawks football's win over Texas Longhorns and looking ahead to TCU

Kansas City Star



### Is SCOTUS ready to cross public opinion on Roe?

The Week



### Ferris State, Grand Valley State make Division II playoffs; Albion in Division III tourney

Detroit Free Press

Sign in

Mail

Our goal is to create a safe and engaging place for users to connect over interests and passions. In order to improve our community experience, we are temporarily suspending article commenting

### Popular in the Community

**Factbox-How much prison time could shooter Kyle Rittenhouse...**

16 comments

**A Drizly drink guide for aficionados.**  
 sponsored by: Drizly

AdChoices

Sponsored



**\$188M Lottery Winner Loses All to Her Pastor**  
 Ad • Tripsided



**'Succession' Star Set to Tell Stories of 9/11 First Responders in Upcoming Series**  
 Military.com



**Browns cornerback Troy Hill suffers neck injury, taken to hospital for evaluation**  
 Akron Beacon Journal

### RECOMMENDED STORIES



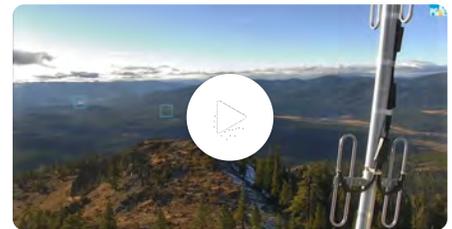
**BuzzFeed**  
**"Hogging" Is A Horrifying Sex Competition That Some Fraternities Engage In, And People Are Finally Horrifying.** [View Entire Post >](#)  
 1d ago



**Autoweek**  
**Mercedes Fires Off Protest against Max Verstappen, Red Bull After New Video Surfaces**  
 Mercedes asks for Right of Review of Hamilton-Verstappen incident at Brazil.  
 4h ago



**Ad • CapitalOne Shopping**  
**Before You Renew Amazon Prime, Read This**  
 Amazon Has Millions of Prime Subscribers — But Few Know About This Savings Trick



**PG&E tests AI cameras to spot wildfires in NorCal**  
 KGO — San Francisco



**Oscars Afterparty Dresses That'll Leave You in Awe**  
 Ad • POPSUGAR

The Columbus Dispatch

**'That's just lazy:' Dwayne Haskins called out by Pittsburgh Steelers' coaches: Report**  
 An NFL Network reporter said former Ohio State

# Exhibit 37



Facebook Legal\_Farhana <facebook\_farhana@muslimadvocates.org>

---

## Civil Rights Audit Update

1 message

---

Shaarik Zafar <shaarik@fb.com>

Tue, Dec 18, 2018 at 8:12 AM

To: Farhana Khera <farhana@muslimadvocates.org>, Naheed Qureshi <naheed@muslimadvocates.org>, Madihha Ahussain <madihha@muslimadvocates.org>

Dear Farhana, Naheed, and Farhana,

Good Morning.

I hope this email finds you well. I wanted to share an update on Facebook's civil rights audit. As Sheryl Sandberg notes in this [Newsroom Post](#), Facebook is committed to working with leading U.S. civil rights organizations such as Muslim Advocates to strengthen and advance civil rights on our service. In May, Facebook asked Laura Murphy, a respected civil rights and civil liberties leader, to guide the audit.

Today, after speaking with more than 90 civil rights organizations, Laura is providing an update on our progress. While the report indicates that Facebook has made some progress, the bottom line is that Facebook needs to do much more.

Please let me know if you have any additional questions or need any additional information.

Civil Rights Audit Update: <https://newsroom.fb.com/news/2018/12/civil-rights-audit/>

Warm Regards,

Shaarik

Shaarik Zafar

(Shah-Rik Zuh-fur)

**facebook | public policy**

[shaarik@fb.com](mailto:shaarik@fb.com)

# Exhibit 38



Facebook Legal\_Naheed <facebook\_naheed@muslimadvocates.org>

---

**Re: Follow-up**

1 message

---

**Shaarik Zafar** <shaarik@fb.com>

Wed, Mar 27, 2019 at 3:54 PM

To: Farhana Khera <farhana@muslimadvocates.org>, Monique Dorsainvil <monique@fb.com>

Cc: Monika Bickert <monika@fb.com>, Neil Potts <neilpotts@fb.com>, Naheed Qureshi

<naheed@muslimadvocates.org>, "madihha@muslimadvocates.org" <madihha@muslimadvocates.org>

Hi Farhana,

Is there a good time I can call you or folks on your team to discuss? I just wanted to clarify a few things about this specific policy update.

Many thanks as always.

Shaarik

---

**From:** Farhana Khera <farhana@muslimadvocates.org>

**Date:** Wednesday, March 27, 2019 at 9:05 AM

**To:** Monique Dorsainvil <monique@fb.com>

**Cc:** Monika Bickert <monika@fb.com>, Neil Potts <neilpotts@fb.com>, Shaarik Zafar <shaarik@fb.com>, Naheed Qureshi <naheed@muslimadvocates.org>, Madihha Ahussain <madihha@muslimadvocates.org>

**Subject:** Re: Follow-up

Thanks so much, Monique. How does FB define "white nationalism and separatism"?

Farhana

Sent from my iPhone

On Mar 26, 2019, at 10:54 PM, Monique Dorsainvil <monique@fb.com> wrote:

**[Shifting Sheryl to Bcc. Adding Monika Bickert, Neil Potts, & Shaarik Zafar]**

Dear Farhana -

Thank you for inquiring about the policy in more detail and asking these important follow-up questions.

The new policy will ban praise, support and representation of white nationalism and separatism, so it will focus on individual pieces of content (a post that says, "I'm not racist, I'm a white nationalist"). That said, this isn't the only policy implicated when we're talking about hateful groups and people.

Under our dangerous organizations policy, for example, we will remove hate figures and organizations – they aren't allowed to maintain a presence on the platform even if they're using Facebook or Instagram to post family pictures. We have a process for evaluating people and groups as hate figures and organizations, and we consider a number of different factors, among them organization of hate rallies and association with recognized hate groups. ACT for America doesn't currently meet our criteria for designation as a hate organization, but we did designate one of their local chapters, ACT for America Marlette.

As mentioned in a meeting with Muslim Advocates recently at our DC office, we expanded our credible violence policy such that we now remove content that encourages people to bring weapons to an event or location in order to intimidate or harass. I know this is something that Muslim Advocates specifically flagged to us as a trend your team was seeing on- and offline.

If you do see on or offline signals tied to ACT for America that we should look into, please let us know. New evidence is always something we want to take into account when making determinations about hate figures and organizations.

Thank you again for the follow up, Farhana. Please let me know if there is any additional context or information I can help provide.

Warm Regards,  
Monique

On Mar 26, 2019, at 9:07 PM, Farhana Khera <[farhana@muslimadvocates.org](mailto:farhana@muslimadvocates.org)> wrote:

Thank you!

Monique: I look forward to hearing from you.

Best,

Farhana

Sent from my iPhone

On Mar 26, 2019, at 7:24 PM, Sheryl Sandberg <[sheryl@fb.com](mailto:sheryl@fb.com)> wrote:

Thank you for reaching out.

Adding Monique to respond and share more information on this.

**From:** Farhana Khera <[farhana@muslimadvocates.org](mailto:farhana@muslimadvocates.org)>

**Sent:** Tuesday, March 26, 2019 4:12 PM  
**To:** Sheryl Sandberg <[sheryl@fb.com](mailto:sheryl@fb.com)>  
**Subject:** Follow-up

Dear Sheryl,

Many thanks again for reaching out with the policy news. I was thinking about our conversation and have a question: what would the policy say? Specifically, how does it define white nationalist/nationalism? Would it include anti-Muslim hate motivated groups and movements?

One example of an anti-Muslim hate group is ACT for America. ACT for America, which is the largest anti-Muslim hate group in the U.S. with 750,000 members, promotes hate and violence toward Muslims by spreading myths about Muslims seeking to bring Sharia law and that Muslims are inherently violent and disloyal Americans. They have overlap with anti-government and neo-Nazi groups and individuals and have organized hate rallies outside mosques and in other public spaces in recent years, seeking to further intimidate an already vulnerable community. The group was recently banned by Hyatt Hotels and cannot use its facilities for meetings or event.

Under the new policy, would ACT for America be banned from the FB and IG platforms?

If you or a member of your team could respond and help me understand the new policy, I would greatly appreciate it.

Many thanks again.

Best,  
Farhana

--

**Farhana Khara** | Muslim Advocates  
President & Executive Director  
[www.muslimadvocates.org](http://www.muslimadvocates.org)

-----

*Privileged/Confidential Information may be contained in this message. If you are not the intended recipient of this message (or responsible for delivery of the message to such person), you may not copy or deliver this message to anyone. In such case, you should destroy this message and kindly*

*notify the sender by reply email. Please advise immediately if you do not consent to Internet email for messages of this kind.*

*Privileged/Confidential Information may be contained in this message. If you are not the intended recipient of this message (or responsible for delivery of the message to such person), you may not copy or deliver this message to anyone. In such case, you should destroy this message and kindly notify the sender by reply email. Please advise immediately if you do not consent to Internet email for messages of this kind.*

*Privileged/Confidential Information may be contained in this message. If you are not the intended recipient of this message (or responsible for delivery of the message to such person), you may not copy or deliver this message to anyone. In such case, you should destroy this message and kindly notify the sender by reply email. Please advise immediately if you do not consent to Internet email for messages of this kind.*

# Exhibit 39



Facebook Legal\_Naheed <facebook\_naheed@muslimadvocates.org>

---

## Fwd: Sheryl -- Need your help

1 message

---

**Farhana Khera** <farhana@muslimadvocates.org>

Wed, May 1, 2019 at 8:19 PM

To: Naheed Qureshi <naheed@muslimadvocates.org>, Madihha Ahussain <madihha@muslimadvocates.org>

thoughts on how I should respond?

----- Forwarded message -----

From: **Sheryl Sandberg** <sheryl@fb.com>

Date: Wed, May 1, 2019 at 8:14 PM

Subject: Re: Sheryl -- Need your help

To: [farhana@muslimadvocates.org](mailto:farhana@muslimadvocates.org) <[farhana@muslimadvocates.org](mailto:farhana@muslimadvocates.org)>

Cc: Schuyler Milender <[schuyler@fb.com](mailto:schuyler@fb.com)>, Shaarik Zafar <[shaarik@fb.com](mailto:shaarik@fb.com)>, Catlin O'Neill (US Public Policy) <[catlinoneill@fb.com](mailto:catlinoneill@fb.com)>

Farhana,

Thank you for reaching out to me directly. We take threats of violence and hate speech very seriously, and I am so sorry to hear this has been Representative Omar's experience.

I am having my team do a careful review of the content that Rep. Omar has reported to us – for her accounts and her daughter's, on both Facebook and Instagram. We will remove anything that violates our Community Standards. To reduce the burden for Rep. Omar and her staff, we are also proactively reviewing the accounts for threats and hateful content.

My team is reaching out to hers so that we can talk through the steps we're taking, see how we can better support her, and build direct lines of communication so any issues get resolved quickly.

Thank you again for escalating this – we need to do better, and we will.

Sheryl

sheryl sandberg | chief operating officer | facebook

1 facebook way | menlo park, ca | 94025

[sheryl@fb.com](mailto:sheryl@fb.com)

---

**From:** Farhana Khera <[farhana@muslimadvocates.org](mailto:farhana@muslimadvocates.org)>

**Sent:** Wednesday, May 1, 2019 9:36 AM

**To:** Sheryl Sandberg

**Subject:** Sheryl -- Need your help

Dear Sheryl,

I hope you're doing well. I'm reaching out on an urgent matter and could really use your personal attention. I thank you in advance.

I'm writing to share concerns with you about the way in which Facebook and Instagram have been used to target Congresswoman Ilhan Omar because she is an immigrant, an African-American and one of the first Muslim women to become a member of Congress. She is receiving serious death threats on a daily basis and deserves an immediate response from Facebook.

As you know, President Trump recently tweeted a highly offensive video that juxtaposed footage from the 9/11 attacks with images of Rep. Omar and her words distorted and taken out of context, clearly implying that Rep. Omar somehow condoned the 9/11 attacks or possibly terrorism more generally. Unfortunately, though not surprisingly, this has led to a dramatic increase in the number of targeted attacks and threats against her. She is regularly receiving death threats on various platforms, including Facebook and Instagram, and now her children are being attacked and feel they are also in danger. **In fact, we have heard directly from Rep. Omar's office that her daughter's Instagram page is being flooded with hateful posts and threats targeting the Congresswoman.**

Per your team's request, Rep. Omar's staff and others are doing the best they can to report this abusive and hateful content when they see it, but they are completely overwhelmed. The sheer volume of hateful content and threats directed at the Congresswoman makes it impossible for any person or team to catalog. But more importantly, **it is completely inappropriate that the burden for addressing bigoted and hateful content on Facebook is often shifted to the victim of the attack.** This is Facebook's platform; it's Facebook's responsibility to remove this content.

Furthermore, in many instances, the content has not been removed when Rep Omar's staff has reported it -- even when the wording of the post mimics wording in Facebook's own examples of prohibited speech or content. It is also our understanding that a man who was recently charged with threatening to kill Rep. Omar was [permitted to post violent content on Facebook](#) for years without any restrictions.

Given the widespread attention to this by media outlets and government officials -- so much so that Speaker Nancy Pelosi had to call for increased security for Congresswoman Omar -- there must be more that Facebook can do to ensure that she can safely use your platform. Otherwise

inevitably, bigots and hate groups will win by successfully driving representatives of vulnerable communities off of Facebook and Instagram.

I hope that your team will take this seriously, and I look forward to hearing more from you about steps the company will take to address these concerns.

Thank you again in advance for your time and attention to this serious issue.

Best regards,  
Farhana

--

**Farhana Khera** | Muslim Advocates  
President & Executive Director  
[www.muslimadvocates.org](http://www.muslimadvocates.org)

-----

*Privileged/Confidential Information may be contained in this message. If you are not the intended recipient of this message (or responsible for delivery of the message to such person), you may not copy or deliver this message to anyone. In such case, you should destroy this message and kindly notify the sender by reply email. Please advise immediately if you do not consent to Internet email for messages of this kind.*

--

**Farhana Khera** | Muslim Advocates  
President & Executive Director  
[www.muslimadvocates.org](http://www.muslimadvocates.org)

-----

# Exhibit 40



Facebook Legal\_Naheed <facebook\_naheed@muslimadvocates.org>

---

## Fwd: Response to Muslim Advocates Email dated 2-25-2020

1 message

---

**Madihha Ahussain** <madihha@muslimadvocates.org>

Thu, Mar 19, 2020 at 12:11 PM

To: Scott Simpson <scott@muslimadvocates.org>, Eric Naing <eric@muslimadvocates.org>, "Erik W. Martinez Resly" <Erik@muslimadvocates.org>, Naheed Qureshi <naheed@muslimadvocates.org>

----- Forwarded message -----

From: **Shaarik Zafar** <shaarik@fb.com>

Date: Tue, Mar 17, 2020 at 7:56 PM

Subject: Response to Muslim Advocates Email dated 2-25-2020

To: Naheed Qureshi <naheed@muslimadvocates.org>

Cc: Lindsay Elin <lindsaye@fb.com>, Monique Dorsainvil <monique@fb.com>, Madihha Ahussain <madihha@muslimadvocates.org>, Farhana Khera <farhana@muslimadvocates.org>, Murphy Laura <laura@lwmurphy.com>

Dear Naheed,

I hope you and everyone at Muslim Advocates is keeping safe and healthy. Attached is a response from Kevin Martin to your February 25, 2020 email to Nick Clegg.

Best,

Shaarik

Shaarik Zafar

(Shah-Rik Zuh-fur)

**facebook | public policy**

[shaarik@fb.com](mailto:shaarik@fb.com)

--

**Madihha Ahussain** | Muslim Advocates

Special Counsel for Anti-Muslim Bigotry

202.492.2744

[www.muslimadvocates.org](http://www.muslimadvocates.org)



**Response to MA Letter - 2-25-2020.pdf**

101K

March 17, 2020

Dear Naheed,

I am responding to the email you sent to Nick Clegg on February 25, 2020.

We are sorry that Muslim Advocates did not attend the salon dinner Nick hosted last month. The focus of the discussion was on possible proactive regulation of the internet, including in the areas Mark Zuckerberg highlighted in his [Washington Post](#) and [Financial Times](#) op-eds: (1) content moderation; (2) data portability; (3) elections; and (4) privacy. The dinner was an opportunity for Nick and other policy team members to discuss these issues with leaders from the civil rights and progressive communities. We believe such feedback is invaluable; as such, we would still welcome your thoughts and insights.

Separately, we want to thank you for the specific points you raised in your note.

Regarding Facebook Events, we continue to believe that this is an important tool that allows our users to organize events, including social gatherings, political protests, and marches. With that said, your concern is an important one – events have the potential to be used in abusive and harmful ways. This is why – following our discussions with Muslim Advocates and other civil rights groups – we updated our [violence and incitement policy](#) based on the concerns you raised. The policy now bans “Statements of intent or advocacy, calls to action, or aspirational or conditional statements to bring weapons to locations, including but not limited to places of worship, educational facilities or polling places (or encouraging others to do the same).”

On hate speech – which we define as violent or dehumanizing speech, statements of inferiority, or calls for exclusion and/or segregation, based on protected characteristics – our policies strictly prohibit anti-Muslim, white supremacist, and hate group content. Additionally, we have invested in proactive detection so that we can find such content before people even report it to us and sometimes before anyone sees it. As we discussed with Muslim Advocates Special Counsel for Anti-Muslim Bigotry Madihha Ahussain in January, there are technical limitations to this process, namely because it is difficult for our AI systems to recognize context (e.g. whether a user is using a slur to attack someone or promote bigotry versus reappropriating or using it self-referentially). However, because of improvements in our detection systems, we now proactively detect 80% of the hate speech we remove before people report it to us, which is up from 60% over the past six months.

We are committed to continuing this work and being transparent about our efforts to combat hate. As a next step, when we share the fifth edition of the [Community Standards Enforcement Report](#) in May, we will share metrics on how we are doing at enforcing our policy against organized hate for the first time.

An additional point: our work to combat hate also goes beyond our policies. When someone searches for something related to hate and violent extremism in the United States, we point them to resources that help people leave behind hate groups in partnership with the organization Life After Hate. We have also more recently expanded this program to Australia in partnership with EXIT Australia, an organization focused on helping to redirect people away from hate in their local communities.

Regarding the NO BAN Act, we appreciate the importance of the issue. Our views have not changed: as we have said regarding earlier efforts to limit immigration on a country-specific basis, we believe that as a nation of immigrants, we all benefit from welcoming people from around the world to contribute to our society. And as [Mark has stated previously](#), “we all benefit when the best and brightest from around the world can live, work and contribute here.”

Finally, I want to address your point regarding our employees and consultants. We do not and will not tolerate harassment or discrimination in our workplace, nor do we allow hate figures or hate groups to have a presence on our platform. Moreover, in developing our policies – including our Community Standards – [we believe it is important to engage a range of stakeholders with diverse viewpoints and across the political spectrum](#).

Thank you again for your note. We value our relationship with Muslim Advocates. We appreciated the opportunity to speak with Madihha in January, including to discuss the issues Muslim Advocates Executive Director Farhana Khera raised with Mark following the dinner he hosted with civil rights leaders last November. We hope to continue to engage with you and your organization, including on ways to increase the online safety and security of all of our users.

Sincerely,



Kevin Martin  
Vice President, US Public Policy

CC: Laura Murphy

# Exhibit 41



## The transparency project

• This article is more than 1 year old

# Monetising hate: covert enterprise co-opts far-right Facebook pages to churn out anti-Islamic posts

Supported by



About this content

**Michael McGowan, Christopher Knaus and Nick Evershed**

Thu 5 Dec 2019 09:00 EST

A mysterious group has used some of Facebook's largest far-right pages to create a commercial enterprise that harvests anti-Islamic hate for profit and influences politics across the globe, a Guardian investigation has revealed.

For the past two years the Israel-based group has co-opted at least 21 organically grown far-right pages, using them to churn out thousands of coordinated posts to more than 1 million followers across four continents and funnelling audiences to a cluster of 10 advertisement-heavy websites to milk the traffic for profit.

The posts stoke deep hatred of Islam across the western world and influence politics in Australia, Canada, the UK and the US by amplifying far-right parties including Australia's [One Nation](#) and vilifying Muslim politicians such as US Democratic congresswoman Ilhan Omar.

The network has also targeted leftwing politicians at critical points in national election campaigns, posting false stories about the UK Labour leader, Jeremy Corbyn, and the Canadian prime minister, Justin Trudeau.

The revelations show how Facebook has failed to stop clandestine actors from using its platform to run coordinated disinformation and hate campaigns. The network uncovered by the Guardian has operated with relative impunity even since Mark Zuckerberg offered his apology to the US Senate after the [Cambridge Analytica](#) and [Russian interference scandals](#).

When the Guardian notified Facebook of its investigation, the company removed several pages and accounts “that appeared to be financially motivated”, a spokesperson said in a statement.

“These pages and accounts violated our policy against spam and fake accounts by posting clickbait content to drive people to off-platform sites.

“We don’t allow people to misrepresent themselves on Facebook and we’ve updated our inauthentic behaviour policy to further improve our ability to counter new tactics.

“Our investigations are continuing and, as always, we’ll take action if we find any violations.”

The Guardian’s investigation has revealed that the Israel-based group gains access to existing rightwing and far-right Facebook pages by approaching local administrators and offering to act as editors who could bring new content and increase reach.

Once they gain access, the Israeli administrators publish identical posts almost simultaneously to the network’s 21 Facebook pages, which have a combined 1 million followers around the globe. Queensland University of Technology researchers worked with the Guardian to confirm that the Facebook posts are being distributed by a single source across the 21 pages, probably using auto-scheduling software.

The network published 5,695 coordinated posts receiving 846,424 likes, shares or comments in October alone, Guardian analysis shows. In total, the network has published at least 165,000 posts and attracted 14.3m likes, shares or comments.

Australia’s first female Muslim senator, Mehreen Faruqi, felt the full force of the network in August last year, when 10 of its pages launched coordinated posts inciting their 546,000 followers to attack her for speaking in parliament against racism.

This prompted what Faruqi described as a “horrific feeding frenzy of racism, fake news and hate”.

She says the network represents a “new level of far-right organisation and coordination”.

“By allowing racist and misleading posts, social media giants like Facebook, Twitter and Instagram are profiteering from the proliferation of hate speech and abuse,” Faruqi said.

A spokesperson for Facebook told the Guardian: “Nobody can advocate or advertise hate or violence on Facebook and we remove any violations as soon as we become aware.”

In the UK, the London mayor, Sadiq Khan, who in May said he had been [forced to employ 24-hour police protection after repeated threats on social media](#), has been targeted by the network hundreds of times. The posts [falsely claimed Khan said terror attacks were “part and parcel of living in a big city” after the 2017 attack on Westminster](#) and that British people should “leave London if they do not want to experience a terror attack”. The posts have attracted abusive and violent comments.

Those behind the network have gone to great lengths to hide their identity. But [Guardian Australia’s investigation](#) has connected the operation to one known man in Tel Aviv, who goes by the username Ariel1238a.

# Exhibit 42



## Facebook

🕒 This article is more than **7 months old**

# Facebook leak underscores strategy to operate in repressive regimes

**Alex Hern** *UK technology editor*

🐦 @alexhern

Tue 23 Mar 2021 11.00 EDT

Facebook users are permitted to praise mass murderers and “violent non-state actors” in certain situations, according to internal guidelines that underline how the tech corporation is striving to operate in repressive regimes.

The leak also reveals that Facebook maintains a list of “recognised crimes” and instructs its moderators to distinguish between those and “crimes not recognised by FB” when applying the company’s rules.

The list is designed to avoid giving succour to countries where criminal law is considered incompatible with basic human rights. “We only recognise crimes that

cause physical, financial or mental injury to individual(s)” such as “theft, robbery and fraud, murder, vandalism [and] non-consensual sexual touching”, the guidelines say.

Crimes not recognised by Facebook include “claims about sexuality”, “peaceful protests against governments” and “discussing historical events/controversial subjects such as religion”. Facebook argues this is the only way it can function in countries where the rule of law is shaky.

But the revelation of its explicit decision to place itself above the law may cause friction with governments round the world. “One of the biggest problems is that Facebook has gone into every single country on the planet with no idea of the impact,” said Wendy Via, the co-founder and president of the US-based Global Project Against Hate and Extremism.

She described Facebook, which was founded in the US, as having “little language capability and zero cultural competency”, adding: “You can’t build secret rules if you can’t understand the situation.”

Even in the US, Facebook has struggled to deal with cultural changes. The documents give insight into how Facebook struggled to define and act against the far-right QAnon movement. Accounts associated with QAnon were [banned across the platform](#) in October 2020 after years of growing popularity and controversy.

Defining QAnon as a “violence-inducing conspiracy network”, the company now bans non-state actors that “are organised under a name, sign mission statement or symbol; AND promote theories that attribute violent or dehumanising behaviour to people or organizations that have been debunked by credible sources; AND have advocated for incidents of real-world violence to draw attention to or redress the supposed harms promoted in those debunked theories”, according to the leaked guidelines for moderators, which date from December 2020.

It highlights Facebook’s battle to function in some of the most autocratic regimes in the world. One exception to guidelines on terrorist content, for instance, allows users to praise mass murderers and “violent non-state actors”, a term describing designated militant groups engaged in civil wars that do not target civilians.

According to Facebook sources, the company recognised that in complex conflicts some violent non-state actors provided key services and engaged in negotiations with governments. Praise or support for violence by these groups is not allowed.

In a reference [to Myanmar](#), the Middle East and north Africa in the guidelines, Facebook’s global escalations team - a more elite group of moderators who are typically

directly employed by the company rather than outsourced - are told: “Allow content that praises violent non-state actors, unless it contains an explicit reference to violence.” Content “that discusses mass murders” is also allowed provided it is “discussion of the events leading up to a mass murder, even when such discussions take a favourable position towards the event or its perpetrator”.

An example of a legitimate comment is: “Where were the police? Why did it fall to this guy to try and restore order?” The policy was rolled out early in Myanmar and Syria and now applies globally, it is understood.

Facebook’s decision to set its own standard of behaviour above that of countries’ criminal legislation also applies in other areas of its moderation guidelines. In telling moderators how to police discussions on “regulated goods”, for instance, Facebook applies an international set of restrictions to items where national and local laws differ.

Cannabis cannot be bought, sold or traded on Facebook despite being legal in a number of regions but users can “admit” to smoking it and “promote” it. The same restrictions apply to alcohol, although alcohol stores, unlike cannabis retailers, are allowed to advertise to those over 18. All “non-medical drugs” are severely restricted on Facebook, overruling local legislation.

Facebook sources said the medical field had come to be more accepting of cannabis use to treat illnesses while “non-medical drugs” such as cocaine and heroin had no identified medical use.

Facebook’s policy of selectively applying national laws has been reflected by its public actions before. In February the BBC reported on Facebook Marketplace being used to facilitate [illegal sales of Amazonian land](#). According to the broadcaster, Facebook decided that “trying to deduce which sales are illegal would be too complex a task for it to carry out itself, and should be left to the local judiciary and other authorities”.

In the US, the company spent four years deflecting criticism for treating Donald Trump differently to other users and other world leaders. In summer 2020, Facebook refused to take action against the US president over a post declaring “when the looting starts, the shooting starts”. Its chief executive, [Mark Zuckerberg](#), said he considered the post a warning of state action rather than a threat that went against Facebook’s rules.

The same accusations of light-touch policing were made regarding how Facebook handled the QAnon movement. Until the platform declared its QAnon ban in October, the community had been largely unaffected by Facebook’s guidelines. Even after the ban, numerous QAnon-linked pages remained accessible on the site.

In 2017, a separate [leak of moderator documents to the Guardian](#) revealed that the company only enforced rules against Holocaust denial in a subset of countries where that misinformation was illegal.

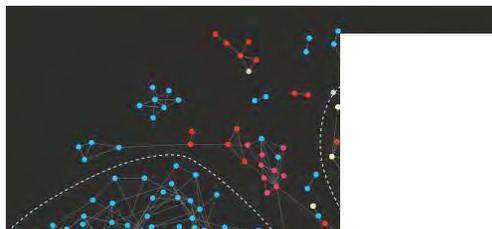
Rather than deciding based on the potential harm caused, Facebook focused on those places where the site was likely to face prosecution or be sued. In 2020, Facebook updated its policies to ban Holocaust denial on its platform around the world.

A Facebook spokesperson said: “We don’t allow anyone to praise violent actions and we remove content that represents or supports the organisations we ban under our policies. We recognise that in conflict zones some violent non-state actors provide key services and negotiate with governments - so we enable praise around those non-violent activities but do not allow praise for violence by these groups.

“We also maintain a list of crimes that we apply under these policies, but rather than breaking them down by country or region they are crimes that are recognised globally. Since we’re a global platform, we have a single set of policies about what we allow and apply them to every country and region. While we’ve made progress in our enforcement, we know there is always more to do.” The company had a process for national governments and courts to report content that they believed violated local law.

**The  
Guardian  
Masterclasses**

[Browse all →](#)



# Exhibit 43

Search

**U.S.**

**World**

**Business**

**Tech & Science**

**Culture**

**Autos**

**Sports**

**Health**

**Opinion**

**Experts**

**Education**

**Podcasts**

---

**U.S.**

# Facebook Has Failed to Stop Anti-Muslim Hate Groups, Despite Mark Zuckerberg Pledge

BY **MICHAEL EDISON HAYDEN** ON 4/20/18 AT 7:10 AM EDT

---



**W**hen Facebook CEO Mark Zuckerberg testified before Congress last week about his firm's privacy policies and the recent Cambridge Analytica scandal, he reported that hate groups were disallowed from his multibillion-dollar social network.

"We do not allow hate groups on Facebook, overall," Zuckerberg said. "So, if there's a group that their primary purpose, or a large part of what they do, is spreading hate, we will ban them from the platform overall."

But Zuckerberg has been saying that exact thing for several years without backing it up, Muslim advocacy groups allege. Anti-Muslim rhetoric and imagery is commonplace on the site, they claimed.

**[NEWSWEEK NEWSLETTER SIGN-UP >](#)**





Mark Zuckerberg testifies before Congress, on Capitol Hill, on April 11. Rights groups allege that Facebook has mishandled its approach to hate groups on the site.

CHIP SOMODEVILLA/GETTY IMAGES

Muslim Advocates, a legal advocacy group, presented the social media giant with a list of 26 different groups that they viewed as hate groups in December of 2017, but 24 of those remain active, they say. Scott Simpson, the Public Advocacy Director for that group, and Madihha Ahussain, their special counsel for anti-Muslim bigotry, told *Newsweek* they started meeting with Facebook four years ago about anti-Muslim groups and images being spread on the site.

Facebook repeated the same promise that hate groups are forbidden, according to Simpson and Ahussain. Simpson noted that the site took action after a

x

were not paying attention, similar content was ignored.

"This has been happening on Facebook and being done by Americans for a long time," Simpson says. "It feels like it's only because Russia was involved [that they noticed]. They're [sic] promises to remove hate groups stuck us as quite hollow."

**NEWSWEEK SUBSCRIPTION OFFERS >**



The cover photo of a Facebook group called Death to Islam. Researchers say that the social media giant has been slow to respond to the growth of such groups



Facebook to address hate groups using their platform since 2016, also expressed disappointment with its response to hate groups. Heidi Beirich, who leads the SPLC's Intelligence Project, told *Newsweek* that the United States remains behind its European counterparts in combatting hate speech on social media. Facebook has helped give greater legitimacy to controversial organizations like ACT for America, a self-described national security grassroots advocacy group that has been accused of promoting Islamophobia, according to Beirich.

"When we met with them, they said the same thing that Zuckerberg told Congress," Beirich said. "Facebook did nothing, and we started criticizing them publicly to get a response."

A spokesperson for Facebook directed *Newsweek* to its community standards on hate speech, which said that the platform "removes hate speech" that directly attacks people based upon "race, ethnicity, national origin, religious affiliation, sexual orientation, sex, gender, or gender identity, or serious disabilities or diseases."

The standards also stated that "organizations and people dedicated to promoting hatred against these protected groups are not allowed a presence on Facebook."





An anti-Trump protester is arrested by police after scuffling with anti-Sharia demonstrators during the March Against Sharia in Oceanside, California, on June 10, 2017.

SANDY HUFFAKER/AFP/GETTY IMAGES

## RELATED STORIES

• [Ford Spencer Event Linked to Attempted Murder](#)



But Act for America, which has over 160,000 likes on Facebook and is followed by more than 150,000 others, is a designated hate group, according to the Southern Poverty Law Center. Brigitte Gabriel, the group's founder, has argued that Muslims "cannot be loyal citizens of the United States." Billy Roper, an Arkansas-based neo-Nazi, organized a Batesville, Arkansas, rally for ACT for America's March Against Sharia in 2017. ACT for America made efforts to disavow Roper, but only after news about his inclusion in the controversial protest event spread.

"ACT for America has never, and will never, tolerate any bias, discrimination, or violence against anyone, based on their religion, gender, race, or political persuasion," Act for America told *Newsweek* in a statement.

In addition to larger groups, *Newsweek* pointed Facebook to a list of eight different smaller groups with names as explicit as Death to Islam that regularly promoted violent imagery directed at Muslims on Facebook. The groups remained up for years in some cases, despite being reported, the researcher says.



Muslim people, called for a new Christian crusade or showed images of the Quran being burned. Facebook claims that one of the groups was removed on March 16 and another on April 10. Others appear to have been removed after *Newsweek* reached out for comment about them.

One group that remains up is called Infidels United for Truth.

"Gun porn and 2<sup>nd</sup> amendment rights are encouraged, in fact, anything that ties into our way of life may be posted here," Infidels United for Truth group declares in its mission statement. The group once used the image of a knight in its cover photo including a statement declaring that a "final crusade" had begun. Today it posts "Proud American Infidel" with an assault rifle replacing the letter *F*. The group has over 2,700 members.

"Muslims are definitely being impacted by this content," Ahussain told *Newsweek* about the influence material found on social media potentially has on the culture at large. "Facebook is a global brand, and right now they're providing a space for hate."

x

# Exhibit 44

---

**Hateful Stereotypes**

1 message

**Shaarik Zafar** <shaarik@fb.com>

Mon, Sep 16, 2019 at 3:40 PM

To: Madihha Ahussain &lt;madihha@muslimadvocates.org&gt;

Cc: Georgina Fields &lt;georginabukenya@fb.com&gt;

Hi Madihha,

I'm writing to solicit your insight on how we address hateful stereotypes. Specifically, we have received feedback that our current policies do not go far enough in removing certain types of speech that have been weaponized to attack specific groups based on their protected characteristics. Often, such speech draws on tropes or stereotypes that are historically linked to intimidation, exclusion, or violence against these groups. We are currently examining whether there are stereotypes about racial, ethnic, religious, or other protected categories under our policies that don't currently violate, but that should be considered hateful in nature, with the goal of developing a well-grounded understanding of these types of stereotypes and creating a framework we can apply to content around the world to help us decide where to draw the line on what we remove and what we permit.

We have spent the past month talking to academic experts about this topic, and we would like to have a discussion with you to share some of our thinking and talk about options we are considering. My colleague Georgina Fields is helping lead this effort and can provide additional details.

Many thanks for your consideration,.

Shaarik

# Exhibit 45

---

**Facebook Policy Initiative**

1 message

**Georgina Fields** <georginabukenya@fb.com>

Wed, Sep 18, 2019 at 10:15 PM

To: "madihha@muslimadvocates.org" &lt;madihha@muslimadvocates.org&gt;

Cc: Shaarik Zafar &lt;shaarik@fb.com&gt;, Peter Stern &lt;pjstern@fb.com&gt;

Dear Madihha,

I hope my email finds you well.

I'm on the Product Policy team at Facebook, the group that drafts our [Community Standards](#) governing the scope of content we allow to be shared on the platform. As part of developing these standards, we regularly consult with experts and other stakeholders to get their views and provide visibility into our work.

I'm contacting you regarding a confidential project we now have in progress. As a result of our own analysis and external feedback, we have determined that our current policies may not go far enough in removing certain types of speech that have been used to attack specific groups based on their protected characteristics. Such speech may draw on tropes or stereotypes that are historically linked to intimidation, exclusion, or violence against these groups. We are currently examining this issue with the goal of developing a well-grounded understanding of these types of stereotypes and creating a framework we can apply to content around the world to help us decide where to draw the line on what we remove and what we permit.

We have spent the past month talking to academic experts about this topic, and based on their feedback we have developed some ideas for addressing harmful stereotypes. We are interested in your input and perspectives on:

- a. The approach we are considering;
- b. Stereotypes that target your community and how they appear online, including real world consequences/impact; and
- c. Factors we should consider to determine whether a stereotype is harmful – factors that help us identify the nature of the harm at issue and how we prioritize what is causing the harm

Below are some key questions we are thinking through:

- What background does the stereotype draw on?
- Who does the stereotype target or hit at?
- How does the stereotype work?
- What is the harm inflicted by the stereotype?

We would like to have a discussion with you to share some of our thinking and get your thoughts on this important issue. Are you available on **Wednesday September 25<sup>th</sup> at 9am PT/12pm ET**? Please let me know if you are interested and available and I can work out remaining logistics. If you have any questions, please do not hesitate to reach out.

Best regards,

Georgina

--

Georgina Bukenya Fields| [facebook](#)

Product Policy, Stakeholder Engagement

+1 650-709-5885

Learn more: "How does stakeholder engagement help us develop our Community Standards?"

# Exhibit 46

---

**Facebook Policies on Objectification of Public Figures**

1 message

**Kim Malfacini** <kmalfacini@fb.com>

Thu, Dec 12, 2019 at 5:43 PM

To: "madihha@muslimadvocates.org" &lt;madihha@muslimadvocates.org&gt;

Cc: Shaarik Zafar &lt;shaarik@fb.com&gt;

Dear Madihha,

I'm reaching out from Facebook's Content Policy team, which sets our Community Standards. I know that you've worked with many of my colleagues on these Standards and other Facebook policies and practices. We are in the process of revisiting our Standards related to harassment of public figures, and given your work, wondering if you have the time to connect and share your thoughts on how we can improve.

As background, our Standards on bullying and harassment permit open and critical discussion of public figures, including celebrities, journalists, politicians, and those who are featured in the news or have a large public audience based on their profession or activities. We do remove a great deal of content that targets public figures – including credible threats of violence, hate speech, and sexual or gendered cursing – yet we also allow much content that criticizes or objectifies, including commentary based on physical appearance or that which sexualizes public figures. We understand commentary that harasses public figures unrelated to their professional or public persona may perpetuate an environment of bullying and result in decreased participation by key voices. We are exploring whether and where our Standards should provide more protection for all or some public figures subject to such objectification, acknowledging that the removal of content is a blunt tool that does not tackle the often misogynistic roots of such commentary.

Would you have the time and interest in connecting either next week or early January?

Many thanks,

Kim Malfacini | [facebook](#)

Content Policy Manager, [Stakeholder Engagement](#)

# Exhibit 47



Facebook Legal\_Farhana <facebook\_farhana@muslimadvocates.org>

---

## Re: Thank you + next steps

1 message

---

**Shaarik Zafar** <shaarik@fb.com>

Tue, Dec 17, 2019 at 11:05 AM

To: Madihha Ahussain <madihha@muslimadvocates.org>

Cc: Monique Dorsainvil <monique@fb.com>, Lindsay Elin <lindsaye@fb.com>, Naheed Qureshi <naheed@muslimadvocates.org>, Farhana Khera <farhana@muslimadvocates.org>

Hi Madihha,

I'm writing to follow up on the examples of content Farhana shared with Mark. Initially, let me reiterate Mark's comment that he truly appreciated the opportunity to hear directly from Farhana and other civil rights leaders last month.

Our colleagues have finished a review of the materials, and we would like to schedule a meeting to discuss our findings. We'd also like to provide Muslim Advocates a briefing from our Product colleagues, who will discuss our efforts to proactively detect content including hate speech. And if possible, we'd appreciate hearing your perspectives on recent trends you're seeing when it comes to hate speech directed at Muslims (e.g. common words, phrases and images). Our Content Policy colleagues are seeking to refine some of our standards, and I know that would welcome your input.

Given the upcoming holidays, it probably makes sense to hold this meeting after the New Year. But I'd like to try and schedule it soonest. We're, of course, happy to host you (either in Menlo Park or DC). We could also do this by video chat. Let me know your preference, and dates in January that work for you and your colleagues.

Appreciatively,

Shaarik

---

**From:** Farhana Khera <farhana@muslimadvocates.org>

**Date:** Tuesday, November 5, 2019 at 1:55 PM

**To:** Mark Zuckerberg <mz@fb.com>

**Cc:** Sheryl Sandberg <sheryl@fb.com>, Lindsay Elin <lindsaye@fb.com>, Monique Dorsainvil <monique@fb.com>, Naheed Qureshi <naheed@muslimadvocates.org>, Madihha Ahussain <madihha@muslimadvocates.org>

**Subject:** Thank you + next steps

Dear Mark,

Thank you again for the invitation and for the opportunity to share our concerns directly with you. Your personal attention and engagement moving forward is important, and with that engagement, I am hopeful that our concerns will be addressed.

As we discussed last evening, Muslim Advocates has been closely tracking hate online and has been in dialogue with Facebook officials since 2012. We have found a disturbing rise in the use of dehumanizing and violent rhetoric and images directed at Muslims, often with the intent to stoke fear, hate and violence, in the U.S. and abroad. For our community, this is an emergency – lives are at risk.

I am heartened that you acknowledge and have affirmed Facebook's commitment to banning and removing dehumanizing and dangerous speech, but a gap remains between content policy and enforcement.

To address these concerns, Muslim Advocates requests that:

- You make a commitment to setting a goal of 100% proactive identification and removal of anti-Muslim hate content before it is even seen on the platform.
- You make a commitment to ensuring that the Events pages are not used and abused by hate actors to organize hate rallies targeting the Muslim community and that the company adopts a zero-tolerance policy for events that dehumanize people based on their religion or other immutable characteristics.

We also echo the requests of our civil rights colleagues seeking a re-evaluation of the political ads policy. Politicians should not be allowed to hide behind the ad policy to run ads that are false, foment hate and put lives in danger.

We also support the request of our civil rights colleagues seeking a permanent civil rights infrastructure to review proactively policies, products and services during development and before they are launched, as well as to address civil rights concerns going forward within the company.

We would like to work with you to meet these goals, including working with your engineering teams to educate them on common words, phrases and images used to demonize and dehumanize Muslims.

Thank you again for your time and attention and, most of all, for your leadership.

We look forward to working with you.

Best regards,

Farhana

P.S. I'm sharing an electronic version of the examples of hate content I shared on paper last evening, including posts by local and state politicians.

--

**Farhana Khera** | Muslim Advocates  
President & Executive Director  
[www.muslimadvocates.org](http://www.muslimadvocates.org)

-----



*Privileged/Confidential Information may be contained in this message. If you are not the intended recipient of this message (or responsible for delivery of the message to such person), you may not copy or deliver this message to anyone. In such case, you should destroy this message and kindly notify the sender by reply email. Please advise immediately if you do not consent to Internet email for messages of this kind.*

# Exhibit 48



Facebook Legal\_Farhana <facebook\_farhana@muslimadvocates.org>

---

## Re: Thank You + Next Steps

1 message

---

**Lindsay Elin** <lindsaye@fb.com>

Sat, May 5, 2018 at 10:14 AM

To: Farhana Khera <farhana@muslimadvocates.org>

Cc: Sheryl Sandberg <sheryl@fb.com>, Monique Dorsainvil <monique@fb.com>, Naheed Qureshi <naheed@muslimadvocates.org>

Thanks Farhana, these reflect the points I outlined in my email to you all yesterday. We're on the same page. Let's get started in crafting our next steps on the thread I started. Together, we'll make progress.

My very best,  
Lindsay

Sent from my iPhone

On May 4, 2018, at 9:24 PM, Farhana Khera <farhana@muslimadvocates.org> wrote:

Dear Sheryl,

Thank you again for the call yesterday. I particularly appreciated your willingness to have a candid and constructive dialogue. We appreciate your commitment to addressing our concerns and have already begun the process of following up with Lindsay.

We look forward to following up with you and your team on these key next steps:

1. Muslim Advocates will have the opportunity to review and provide input on any recommendations or suggestions made by Jon Kyl, with a focus on ensuring that the agenda of anti-Muslim hate groups is not disguised as "conservative viewpoints," and the Facebook team will not take any action on his recommendations before providing Muslim Advocates an opportunity to provide input.
2. Facebook will work towards hiring a senior level employee from the Muslim community with civil rights/countering violent extremism expertise who will be positioned in the company in such a way that s/he is able to advise on bigotry and counterterrorism discussions, policies, and practices within the company. This person would not be focused on outreach, but instead would be in a position to give input on both the company's public policy *and* Monika Bickert's policy work.
3. Facebook and Muslim Advocates will work together to coordinate an off-the-record discussion and training for senior level employees about the inappropriate and disproportionate impact of counterterrorism policies on Muslims in the US. This would include a presentation by our team and Mary McCord, former Assistant Attorney General for the National Security Division at the U.S. Department of Justice. You said that you will try to attend, but agreed that we could work with the team to schedule the training so that Monika Bickert and her team are present.
4. Facebook and Muslim Advocates will work together to explore organizing a convening focused on bigotry and that would bring together key stakeholders, advocates, and others to discuss best practices and strategies to counter hate and bigotry on social media platforms. (We envision this anti-hate convening to include hate against Muslim, Black, Jewish, LGBTQ, women and other vulnerable communities.)

I believe this is an accurate summary of our key takeaways and next steps. Please let me know if you had a different understanding of the call.

We look forward to working with you and your team to ensure Facebook is a safe and welcoming platform for all.

Thank you again.

Best regards,  
Farhana

--

**Farhana Khera**

| Muslim Advocates

President & Executive Director

[www.muslimadvocates.org](http://www.muslimadvocates.org)

-----



**Total and Complete Shutdown**  
How the Trump Administration is Working to Ban Muslims from the United States

[Download the new report](#)

TOTAL AND COMPLETE SHUTDOWN

*Privileged/Confidential Information may be contained in this message. If you are not the intended recipient of this message (or responsible for delivery of the message to such person), you may not copy or deliver this message to anyone. In such case, you should destroy this message and kindly notify the sender by reply email. Please advise immediately if you do not consent to Internet email for messages of this kind.*

# Exhibit 49



Facebook Legal\_Farhana &lt;facebook\_farhana@muslimadvocates.org&gt;

---

## A Second Update on Our Civil Rights Audit

1 message

---

**Monique Dorsainvil** <monique@fb.com>

Sun, Jun 30, 2019 at 6:47 PM

To: "farhana@muslimadvocates.org" <farhana@muslimadvocates.org>, Naheed Qureshi <naheed@muslimadvocates.org>

Cc: Shaarik Zafar <shaarik@fb.com>

Good Evening Farhana –

Quick follow up to your call with Sheryl. As you know, last May we kicked off a civil rights audit to better understand and address the civil rights implications of our policies, processes and products on the people who use our services.

As you know, the audit is being led by Laura Murphy, a highly respected civil rights and civil liberties advocate with support from the noted civil rights firm Relman, Dane & Colfax. During the first six months of the audit, Laura interviewed over 90 civil rights organizations to understand their concerns and identify key issues to analyze as part of the audit. Her first report, issued in December 2018, focused on our U.S. election-related work given the unique urgency around the November 2018 midterm elections.

**Today, Laura released a second progress report** that looks at four bodies of work that are of concern to the civil rights community:

- Content moderation and enforcement;
- Ads practices and targeting;
- Elections and civic engagement; and
- Civil rights accountability infrastructure that examines the longevity of the work.

Laura details the “meaningful progress” we’ve made, with new policies that protect against hate and harmful content and voter intimidation and suppression around upcoming elections and the 2020 Census. She also makes it clear where we need to do more, aptly noting that this is “a beginning, not an end.” I’ve attached a PDF of Laura’s full report here, as well as a summary that pulls directly from her report.

Civil rights and liberties issues that have been flagged by third party stakeholders have been an invaluable part of this process. Shaarik shared some of your team’s early feedback on the report. As we continue our work to advance and strengthen civil rights on Facebook, we look forward to more dialogue and partnership with you.

Warm Regards,  
Monique

monique dorsainvil | facebook | us public policy | monique@fb.com | 202.878.1044

---

 **CivilRightAudit\_Final[5].pdf**  
259K

# Exhibit 50



Facebook Legal\_Farhana <facebook\_farhana@muslimadvocates.org>

---

**(no subject)**

1 message

---

**Mark Zuckerberg** <mz@fb.com>

Wed, Nov 6, 2019 at 2:27 AM

To: "farhana@muslimadvocates.org" <farhana@muslimadvocates.org>

Cc: Sheryl Sandberg <sheryl@fb.com>, Nick Clegg <nclegg@fb.com>, Monique Dorsainvil <monique@fb.com>

Farhana,

Thanks for taking the time to join us for dinner yesterday. I appreciated your thoughts on addressing hate on our platform. This is an important focus for us, and it was useful to hear your perspective directly as we work to better understand the challenges and opportunities that come with protecting civil rights on our platform.

I'm grateful for your partnership with Sheryl to provide us with guidance and advice, and I plan to stay close to the work to follow our progress.

Mark

# Exhibit 51



Facebook Legal\_Farhana &lt;facebook\_farhana@muslimadvocates.org&gt;

---

**Facebook VP of Civil Rights announcement**

1 message

**Sheryl Sandberg** <sheryl@fb.com>

Mon, Jan 11, 2021 at 12:55 PM

To: "farhana@muslimadvocates.org" &lt;farhana@muslimadvocates.org&gt;

Cc: Lindsay Elin &lt;lindsaye@fb.com&gt;, Monique Dorsainvil &lt;monique@fb.com&gt;, Maui Orozco &lt;maui@fb.com&gt;, Claire Choi &lt;clairechoi@fb.com&gt;, Shaarik Zafar &lt;shaarik@fb.com&gt;

Farhana,

Happy New Year - I hope you and your loved ones are staying safe and healthy.

Since last June, when we announced that we would be creating a senior civil rights role, we have been focused on fulfilling our commitment to continue the important work that was started through the audit. On that note, we are announcing today that Roy L. Austin, Jr. will join Facebook as the VP of Civil Rights and Deputy General Counsel. We will be publishing our blog post at 10am PT– we'd appreciate it if you held any public comments until after then.

I am thrilled to welcome Roy and look forward to working with him as he develops and oversees our civil rights accountability efforts. His role will be incredibly significant for us and for the entire tech industry.

As you may know, Roy joins us from the law firm of Harris, Wiltshire & Grannis LLP, where he was a partner specializing in criminal defense and civil rights law. He brings with him over 25 years of experience working as both a civil rights lawyer and advocate, having begun his career as an honors trial attorney with the Criminal Section of the Civil Rights Division of the US Department of Justice.

While we are still at the beginning of our journey to strengthen and advance civil rights at every level of our company, we are excited that this announcement brings us one step closer. We are truly grateful for the guidance and insights from you, Naheed, and other civil rights leaders who have played a crucial role in evolving Facebook's products and policies for the better.

We look forward to continuing this work together at a time when it matters now, more than ever.

Yours,  
Sheryl

sheryl sandberg | chief operating officer | facebook

1 facebook way | menlo park, ca | 94025

[sheryl@fb.com](mailto:sheryl@fb.com)

# Exhibit 52

## Facebook ignored racial bias research, employees say

Researchers said the company ignored their work and then stopped them from pursuing topics related to bias altogether.



— Mark Zuckerberg; Sheryl Sandberg. Getty Images

July 23, 2020, 3:29 PM EDT

**By Olivia Solon**

In mid-2019, researchers at Facebook began studying a new set of rules proposed for the automated system that Instagram uses to remove accounts for bullying and other infractions.

What they found was alarming. Users on the Facebook-owned Instagram in the United States whose activity on the app suggested they were Black were about 50 percent more likely under the new rules to have their accounts automatically disabled by the moderation system than those whose activity indicated they were white, according to two current employees and one former employee, who all spoke on the condition of anonymity because they weren't authorized to talk to the media.

The findings were echoed by interviews with Facebook and Instagram users who said they felt that the platforms' moderation practices were discriminatory, the employees said.

The researchers took their findings to their superiors, expecting that it would prompt managers to quash the changes. Instead, they were told not share their findings with co-workers or conduct any further research into racial bias in Instagram's automated account removal system. Instagram ended up implementing a slightly different version of the new rules but declined to let the researchers test the new version.

It was an episode that frustrated employees who wanted to reduce racial bias on the platform but one that they said did not surprise them. Facebook management has repeatedly ignored and suppressed internal research showing racial bias in the way that the platform removes content, according to eight current and former employees, all of whom requested anonymity to discuss internal Facebook business.

The lack of action on this issue from the management has contributed to a growing sense among some Facebook employees that a small inner circle of senior executives – including Chief Executive Mark Zuckerberg, Chief Operating Officer Sheryl Sandberg, Nick Clegg, vice president of global affairs and communications, and [Joel Kaplan](#), vice president of global public policy – are making decisions that run counter to the recommendations of subject matter experts and researchers below them, particularly around hate speech, violence and racial bias, the employees said.

Facebook did not deny that some researchers were told to stop exploring racial bias but said that it was because the methodology used was flawed.

Alex Schultz, Facebook's vice president of growth and analytics, said research and analyses on race are important to Facebook but is a “very charged topic” and so needs to be done in a rigorous, standardized way across the company.

“There will be people who are upset with the speed we are taking action,” he said, adding that “we’ve massively increased our investment” in understanding hate speech and algorithmic bias.

“We are actively investigating how to measure and analyze internet products along race and ethnic lines responsibly and in partnership with other companies,” Facebook spokeswoman Carolyn Glanville added, noting that the company established a team of experts last year, called Responsible AI, focused on “understanding fairness and inclusion concerns” related to the deployment of artificial intelligence in Facebook products.

# Reporting and moderation

One key source of tension for Facebook comes from the way its automated system moderates hate speech.

Facebook has policies prohibiting hate speech that attacks people based on “protected characteristics” including race, ethnicity, religion, gender or sexual orientation. It relies on user reports and automated content moderation tools to identify and remove this speech.

In an [effort to be neutral](#), the company’s hate speech policies treat attacks on white people or men in exactly the same way as it treats comments about Black people or women, an approach that employees said does not take into account the historical context of racism and oppression.

“The world treats Black people differently from white people,” one employee said. “If we are treating everyone the same way, we are already making choices on the wrong side of history.”

**New audit finds Facebook has done little to combat hate speech**



Employees said that this policy means the company’s automated content moderation tools proactively detect far more hate speech targeting white people than it does hate speech targeting Black people, even if the hate speech targeted at Black people is widely considered more offensive -- a hypothesis supported by academics and the company’s own internal research..

The company has conducted internal research that showed that Facebook users in the United States from both sides of the political spectrum find attacks against traditionally marginalized groups including Black and Hispanic people to be more upsetting than attacks against groups that have not traditionally been marginalized including men and white people – even when the same type of language is used. So “white people are trash” is generally considered less offensive than “Black people are scum,” but Facebook’s policies treat them the same. Data presented at Facebook policy meetings, [including one attended by Vanity Fair in fall 2018](#), shows that users are more upset by attacks against women than they are by attacks against men.

This inequity is reflected in the levels of hate speech that is reported versus taken down automatically. According to a chart posted internally in July 2019 and leaked to NBC News, Facebook proactively took down a higher proportion of hate speech against white people than was reported by users, indicating that users didn’t find it offensive enough to report but Facebook deleted it anyway. In contrast, the same tools took down a lower proportion of hate speech targeting marginalized groups including Black, Jewish and transgender users than was reported by users, indicating that these attacks were considered to be offensive but Facebook’s automated tools weren't detecting them.

The employee who posted the chart to Workplace, the internal version of Facebook, said that the findings showed that Facebook’s proactive tools “disproportionately defend white men.”

Facebook spokeswoman Ruchika Budhraj said Wednesday that the company has since early 2018 considered treating different groups differently, [as reported by Vanity Fair in February 2019](#), but that it is “very difficult to parse out who is privileged and who is marginalized globally” and so the company has not changed its policies.

## Roadblocks and hurdles

The episodes detailed by the current and former employees add to growing scrutiny from both Facebook critics and the company's own workers over how seriously it takes allegations of racial bias on its platforms. The company is in the midst of a major advertiser boycott that was sparked in part by social justice groups that believe it has not done enough to protect users from discrimination.

Meanwhile, the social media giant is also under fire from Republican politicians who say it has a liberal tilt and unfairly censors conservative voices.

Zuckerberg has tried to maintain that the platform is politically neutral and an advocate for free speech while also declining to make major changes. On Tuesday, The Wall Street Journal

reported that Facebook was [creating new teams to study racial bias on its platforms](#).

## Recommended

---

### TECH NEWS

**Activision Blizzard employees walk out over report CEO knew of rape allegation**

---

### SECURITY

**British news website was hacked to control readers' computers, report says**

Facebook employees who were already working on that topic say that for years the company disregarded their work and often instructed them to stop their research.

At around the same time as the Instagram episode, several pieces of research exploring race and racial bias on Facebook and Instagram were summarized and presented in a document to Zuckerberg and his inner circle, known as the M-Team.

The team responded by instructing employees to stop all research on race and ethnicity and not to share any of their findings with others in the company, according to two current and one ex-employee.

Schultz, who said he was part of the M-Team at the time, did not recall the specific communication, but said that some research was stopped over ethics and methodology concerns.

Other attempts to study racial and social bias or oppression on the platform were stopped at the internal research review process, two current and three former employees said. Researchers, many of whom have conducted academic research of societal biases, were told they were not allowed to ask users questions about their racial identity, according to four sources.

Without permission to ask users questions about racial identity, researchers – including those who conducted the Instagram study – relied on a proxy for race called “[multicultural affinity](#),” which categorized users for advertising purposes based on their behavior according to their “affinity” for African American, Asian American or Hispanic people in the United States.

While the current and former employees acknowledged this is not a perfect proxy for race, they had few other options for attempting to understand racial bias on the platform. They were also frustrated by the idea that the company was comfortable in delineating users on the basis of “ethnic affinity” for advertising purposes but not for research purposes.

“Leadership wanted a standard and consistent approach to avoid biased, incorrect and irresponsible work and are proud we set up a project to do that,” Glanville said.

After a ProPublica investigation in 2016, Facebook prohibited advertisers from targeting housing, employment and credit ads [based on what was then called “ethnic affinity”](#) to “prevent potential discrimination through ads,” Glanville said.

It’s not the first time Facebook executives have been accused of ignoring internal research highlighting problems on the platform. A team at Facebook delivered a presentation in 2018 showing that Facebook’s algorithms were driving people apart by showing users increasingly divisive content, [The Wall Street Journal reported in May](#), but senior executives including Zuckerberg shelved the research.

Facebook responded to the article by pointing to its “research to understand our platform’s impact on society so we continue to improve.”

## **'This is not a new issue'**

Whether Facebook takes that research into account has become a subject for discussion on the company's internal message boards. One engineer shared data showing the slant of Facebook's moderation practices and offered a pointed criticism of the company.

“This is not a new issue. This has been going on for years. People smarter, harder working, more patient, and more professional than I have fought to address it, only to be shut down by myopic focus on bad metrics,” the engineer wrote, according to screenshots of a post on the company’s internal message boards shared with NBC News. “I’ve seen people be driven insane as leadership ignores them or outright shuts them down and commits us, again and again, to doubling down on this same path.”

The engineer quit the company the same day, according to the leaked post and to two current employees, over the leadership’s lack of action on this issue and accused Zuckerberg of making misleading statements about the company’s handling of hate speech.

“For months I’ve wrestled with myself, tried to convince myself that the work was definitely good, that it was all worth it – but I can’t,” he wrote. “The issues are too glaring, the failures of leadership too grievous. I’ve lost too much sleep wondering how many people having an awful day I’ve hurt just a little bit more by silencing their opportunity to vent with their friends, or how many other tiny injustices I’ve inflicted in the course of following orders.”

The engineer did not respond to several requests for comment.

“The mere fact we have this research, and continue to find the best way to conduct this and similar research, is because we are trying to understand,” Facebook said.

These revelations echo the findings of an external civil rights audit that Facebook commissioned in 2018 and was published this month. [The audit report revealed that the company has not done enough to protect users from discrimination](#), falsehoods and incitement to violence.

“I don’t think they understand civil rights,” said NAACP president Derrick Johnson, who was among the civil rights leaders to meet with Zuckerberg and Sandberg in the week the audit was released. “They have a blind spot to the needs to protect people and unfortunately, far too often, they conflate issues related to civil rights with partisanship. Defeating hate isn’t a partisan question.”

---

## Get the Morning Rundown

Get a head start on the morning's top stories.

Enter your email

[SIGN UP](#)

---

THIS SITE IS PROTECTED BY RECAPTCHA  
[PRIVACY POLICY](#) | [TERMS OF SERVICE](#)



Olivia Solon



Olivia Solon is a senior reporter on the tech investigations team for NBC News.

---

# Exhibit 53

July/August 2019 (<https://washingtonmonthly.com/magazine/july-august-2019/>)

# What Your Data Is Really Worth to Facebook

And why you deserve a cut.

by Robert J. Shapiro (<https://washingtonmonthly.com/people/robert-j-shapiro/>)

---

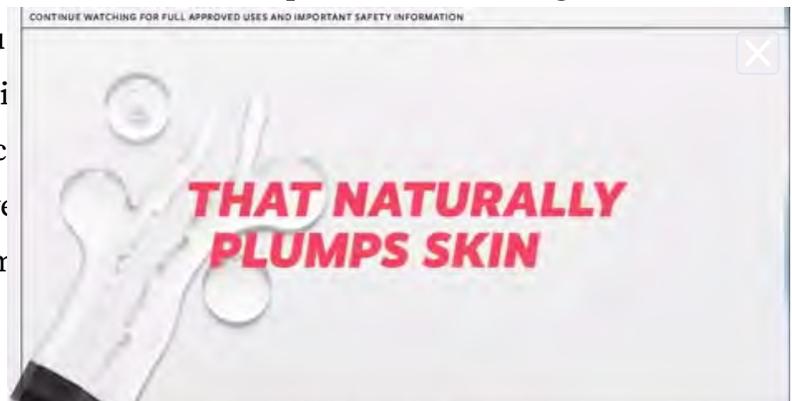
MAGAZINE (<https://washingtonmonthly.com/magazine/july-august-2019/>)

Americans who use the internet—85.5 percent of us—have made a tacit bargain with Facebook, Google, MasterCard, Verizon, and most other sites and products we use regularly. We get access to these companies' services, and they get to scoop up, analyze, and sell our personal information. Few people question this setup, perhaps because most of us assume that our data isn't worth much.

But that assumption is wrong.

Earlier this year, my colleague Siddhartha Aneja and I published a deep-dive study into the value of the personal information that every major website sells access to. It's a complicated problem. Much of the value comes from advertising revenue, disclosed in annual reports and SEC filings by public companies. But we also had to determine how much of that ad revenue is derived specifically from the micro-targeting that user data makes possible, as well as how much the companies spent to gather, analyze, and market user profiles. In the end, we calculated that internet companies earned an average of \$202 per American internet user in 2018 from personal data. We believe that's a conservative estimate.

The value reflects the extraordinarily varied and detailed data that companies collect. Google collects not only the personal information you reveal when you search, but also the information you reveal when you use any of its products, from Maps, the Chrome browser, Google Pay—or apps across its ecosystem. Facebook gathers all the data crumbs you leave whenever you use its services, plus whatever you do on subsidiaries like Instagram and Messenger.



on data-derived profits. But Amazon's public records show that its earnings from user data likely more than doubled between 2016 and 2018. Beyond the major platforms, hundreds of other companies take part in the burgeoning personal data business. Our study also explored the revenues from digital advertising earned by smaller internet services, ranging from Snapchat and Spotify to internet media holding companies such as IAC, which owns Match.com, the Daily Beast, and Investopedia.

For a general sense of the value of people's personal data to these companies, we started with digital advertising revenue. In 2018, Facebook earned an average of roughly \$110 in ad revenue per American user. This calculation, however, ignores what it costs to collect, analyze, and market user data. According to the balance sheet on file with the SEC, Facebook earned \$55.8 billion worldwide in 2018, virtually all of it from targeted advertising. Facebook also reported that relevant costs came to \$20.6 billion. That implies that the value of its users' personal information was equivalent to \$35.2 billion, or 63 percent of Facebook's earnings.

In other cases, determining a company's data-related costs is less straightforward. Google's cost data, for example, is embedded in the balance sheets for Alphabet, the holding company that also includes Google Fiber, GV (former Google Ventures), CapitalG, Waymo, and Google Deep Mind, as well as the suite of Google-branded internet services.

Given these issues, we developed a proxy to distinguish the value of personal information to the online platforms and the costs to gather and monetize those data. We relied on a careful study by three business school economists who analyzed certain aspects of the AdChoices program created by the online advertising industry. In 2010, AdChoices announced that anyone could opt out of all targeted online ads by registering at a special website. While relatively few internet users opted out, the researchers found that those who did not opt out earned more than comparable targeted ones. This suggests that 5 percent of the profits derived from the personal information used to target those users.

Since targeted online advertising generated \$108.6 billion in 2018, we estimate that the profits derived from American internet advertising last year, for the 279.7 million Americans used the internet last year, after costs, came to an average of \$202 per

---

Imagine the profits General Motors could achieve if it didn't have to pay for the steel it uses to build cars. Like GM, online companies should pay their users for the valuable raw materials they provide.

---



and detailed. Algorithms track and save data on what we search for, what we write in emails and messages, what we buy, and everything else we do online, whether on our phones or laptops. Not only do the algorithms then build up a basic profile based on gender, age, ethnicity, and so on; they also determine our individual interests, likes and dislikes, family background, political leanings, sexual orientation, and much more. Everything we reveal online is fair game.

As the software for data mining and targeting has advanced, the revenue from digital ads and the consequent value of the data used to target them have risen rapidly. Our study found that from 2016 to 2018, the value of the information Google mined from Americans grew 40 percent; for Facebook, 85 percent; and for the latecomer Amazon, 312 percent. Overall, the value internet companies derive from Americans' personal data increased almost 54 percent. At that rate, the number will reach \$127.9 billion in four years. Adjusting for the estimated increase in the number of Americans using the internet, people's personal data will be worth an average of \$434 per American user in 2022.

Given how profitable these data operations are, the practice is sure to spread, and the commercial, social, and other uses of our personal data—and the related side effects—will proliferate. In response, we can try to regulate it, but we shouldn't be surprised when tech companies figure out how to deflect or defeat such regulation.

Instead of regulation, then, we should consider a more direct economic response. Imagine the profits General Motors could achieve if it didn't have to pay for the steel it uses to build cars. Like GM, online companies should pay their users for the valuable raw materials they provide.

Behind this proposal is the principle that people have a property interest in their personal information, or at least in the wealth generated by that information. This theory does not depend on any particular position on privacy. Rather, it comes directly from John Locke's analysis of the origins of property, which are embodied in the U.S. Constitution. Locke said that a person can create property by mixing his or her labor with materials from nature, because each of us has personal ownership of our own bodies and

and, therefore, of whatever we produce by using our personal information online companies gather, and so it meets Locke's test for personal property. Some lead you about its value to them, either you're a suc

Congress should recognize people's property rights net companies do so as well. It's true that the struct



Just as Facebook's value to any individual increases as more people use it, so the value of any individual's personal data to Facebook and its advertisers increases as Facebook gathers and analyzes data from millions of other users.

In other words, internet companies and their users both contribute to the commercial value of the personal profiles that drive digital advertising. A straightforward solution is thus to require the companies to share the profits from those operations with users on a fifty-fifty basis. Of course, asking internet companies to write a check to every individual user would be impossibly inefficient. Instead, each company could write a single check to the government, and the government could distribute the proceeds to every household based on the number of its internet users. So, in 2022, a family of four internet users would receive \$868 in payment for their personal data. The era of free riding for online companies would be over. Corporations have gotten rich by exploiting our data. It's time for them to share the wealth.

## Support Nonprofit Journalism

---

If you enjoyed this article, consider making a donation to help us produce more like it. The *Washington Monthly* was founded in 1969 to tell the stories of how government really works — and how to make it work better. More than fifty years later, the need for incisive analysis and new, progressive policy ideas is clearer than ever. As a nonprofit, we rely on support from readers like you.

YES, I'LL MAKE A DONATION

---

**Robert J. Shapiro** (<https://washingtonmonthly.com/people/robert-j-shapiro>)

(<https://twitter.com/robshapiro>)

*Robert J. Shapiro, a Washington Monthly contributor, is a Senior Lecturer and  
Fellow at the McDonough School of Business at Georgetown University and  
Secretary of Commerce for Economic Affairs under*



# Exhibit 54

**Facebook under fire**

# The case against Mark Zuckerberg: Insiders say Facebook's CEO chose growth over safety

The SEC has been asked to probe whether his iron-fisted management style, described in newly released documents and by insiders, led to disastrous outcomes.

By [Elizabeth Dwoskin](#), [Tory Newmyer](#) and [Shibani Mahtani](#)

October 25, 2021 | Updated October 25, 2021 at 3:34 p.m. EDT



## CORRECTION

A previous version of this article incorrectly described the content of a blog post by Guy Rosen, Facebook’s vice president for integrity, and of congressional testimony by the firm’s CEO, Mark Zuckerberg. Rosen wrote in the blog post that the White House had missed its vaccination goals, not that Facebook had missed its own goals. And Zuckerberg testified that the company removes 94 percent of the hate speech it finds before a human reports it, not just that it removes 94 percent of the hate speech it finds. The article has been corrected.

Late last year, Mark Zuckerberg faced a choice: Comply with demands from Vietnam’s ruling Communist Party to censor anti-government dissidents or risk getting knocked offline in one of Facebook’s most lucrative Asian markets.

In America, the tech CEO is a champion of free speech, reluctant to remove even malicious and misleading content from the platform. But in Vietnam, upholding the free-speech rights of people who question government leaders could have come with a significant cost in a country where the social network earns more than \$1 billion in annual revenue, according to a 2018 estimate by Amnesty International.

So Zuckerberg personally decided that Facebook would comply with Hanoi’s demands, according to three people familiar with the decision, speaking on the condition of anonymity to describe internal company discussions. Ahead of Vietnam’s party congress in January, Facebook significantly increased censorship of “anti-state” posts, giving the government near-total control over the platform, according to local activists and free-speech advocates.

Zuckerberg’s role in the Vietnam decision, which has not been previously reported, exemplifies his relentless determination to ensure Facebook’s dominance, sometimes at the expense of his stated values, according to interviews with more than a dozen former employees. That ethos has come under fire in a series of whistleblower complaints filed with the U.S. Securities and Exchange Commission by former Facebook product manager Frances Haugen.

While it’s unclear whether the SEC will take the case or pursue action against the CEO personally, the allegations made by the whistleblower represent arguably the most profound challenge to Zuckerberg’s leadership of the most powerful social media company on Earth. Experts said the SEC — which has the power to seek depositions, fine him and even remove him as chairman — is likely to dig more deeply into what he knew and when. Though his direct perspective is rarely reflected in the documents, the people who worked with him say his fingerprints are everywhere in them.

In particular, Zuckerberg made countless decisions and remarks that demonstrated a hard-line devotion to free speech. Even in Vietnam, the company says that the choice to censor is justified “to ensure our services remain

Haugen references Zuckerberg’s public statements at least 20 times in her SEC complaints, asserting that the CEO’s singular power and unique level of control over Facebook mean he bears ultimate responsibility for a litany of societal harms. Her documents appear to contradict the CEO on a host of issues, including the platform’s impact on children’s mental health, whether its algorithms contribute to polarization and how much hate speech it detects around the world.

For example, Zuckerberg testified last year before Congress that the company removes 94 percent of the hate speech it finds before a human reports it — but internal documents show that its researchers estimated that the company was removing less than 5 percent of hate speech on Facebook. In March, Zuckerberg told Congress that it was “not at all clear” that social networks polarize people, when Facebook’s own researchers had repeatedly found that they do.

The documents — disclosures made to the SEC and provided to Congress in redacted form by Haugen’s legal counsel —

**Unprecedented times call for unlimited access.**

**Get one year for \$40**



In her congressional testimony, Haugen repeatedly accused Zuckerberg of choosing growth over the public good, an allegation echoed in interviews with the former employees.

“The specter of Zuckerberg looms in everything the company does,” said Brian Boland, a former vice president of partnerships and marketing who left in 2020 after coming to believe that the platform was polarizing society. “It is entirely driven by him.”

A Facebook spokeswoman, Dani Lever, denied that decisions made by Zuckerberg “cause harm,” saying the claim was based on “selected documents that are mischaracterized and devoid of any context.”

“We have no commercial or moral incentive to do anything other than give the maximum number of people as much of a positive experience as possible,” she said. “Like every platform, we are constantly making difficult decisions between free expressions and harmful speech, security and other issues, and we don’t make these decisions inside a vacuum — we rely on the input of our teams, as well as external subject matter experts to navigate them. But drawing these societal lines is always better left to elected leaders which is why we’ve spent many years advocating for Congress to pass updated Internet regulations.”

Facebook has previously fought efforts to hold Zuckerberg personally accountable. In 2019, as the company was facing a record-breaking \$5 billion fine from the Federal Trade Commission for privacy violations related to Cambridge Analytica, a political consultancy that abused profile data from tens of millions of Facebook users, Facebook negotiated to protect Zuckerberg from direct liability. Internal Facebook briefing materials revealed the tech giant was willing to abandon settlement talks and duke it out in court if the agency insisted on pursuing the CEO.

The current chair of the SEC, Gary Gensler, has said he wants to go much harder on white-collar crime. Experts said Gensler is potentially likely to weigh the Haugen complaint as he looks toward a new era of corporate accountability.

Zuckerberg “has to be the driver of these decisions,” said Sean McKessy, the first chief of the SEC’s whistleblower office, now representing whistleblowers in private practice at Phillips & Cohen. “This is not a typical public company with checks and balances. This is not a democracy, it’s an authoritarian state. ... And although the SEC doesn’t have the strongest track record of holding individuals accountable, I certainly could see this case as being a poster child for doing so.”

Zuckerberg, who is 37, founded Facebook 17 years ago in his college dorm room, envisioning a new way for classmates to connect with one another. Today, Facebook has become a conglomerate encompassing WhatsApp, Instagram and a hardware business. Zuckerberg is chairman of the board and controls 58 percent of the company’s voting shares, rendering his power virtually unchecked internally at the company and by the board.

An ownership structure that gives a single leader a lock on the board’s decision-making is “unprecedented at a company of this scale,” said Marc Goldstein, head of U.S. research for the proxy adviser Institutional Shareholder Services. “Facebook at this point is by far the largest company to have all this power concentrated in one person’s hands.”

Zuckerberg has long been obsessed with metrics, growth and neutralizing competitive threats, according to numerous people who have worked with him. The company’s use of “growth-hacking” tactics, such as tagging people in photos and buying lists of email addresses, was key to achieving its remarkable size — 3.51 billion monthly users, nearly half the planet. In Facebook’s early years, Zuckerberg set annual targets for the number of users the company wanted to gain. In 2014, he ordered teams at Facebook to grow “time spent,” or each user’s minutes spent on the service, by 10 percent a year, according to the documents and interviews.

In 2018, Zuckerberg defined a new metric that became his “north star,” according to a former executive. That metric was MSI — “meaningful social interactions” — named because the company wanted to emphasize the idea that engagement was more valuable than time spent passively scrolling through videos or other content. For example, the company’s algorithm would now weight posts that got a large number of comments as more “meaningful” than likes, and would use that information to inject the comment-filled posts into the news feeds of many more people who were not friends with the original poster, the documents said.

Even as the company has grown into a large conglomerate, Zuckerberg has maintained a reputation as a hands-on manager who goes deep on product and policy decisions, particularly when they involve critical trade-offs between preserving speech and protecting users from harm — or between safety and growth.

Politically, he has developed hard-line positions on free speech, announcing that he would allow politicians to lie in ads and at one time defending the rights of Holocaust denialists. He has publicly stated that he made the final call in the company’s most sensitive content decisions to date, including allowing President Donald Trump’s violence-inciting post during the George Floyd protests to stay up, despite objections from thousands of employees.

And his capacity for micromanagement is vast: He personally chose the colors and layout of the company’s “I got vaccinated” frames for user profile pictures, according to two of the people.

But the former employees who spoke with The Post said his influence goes far beyond what he has stated publicly, and is most felt in countless lesser-known decisions that shaped Facebook’s products to match Zuckerberg’s values — sometimes, critics say, at the expense of the personal safety of billions of users.

Ahead of the 2020 U.S. election, Facebook built a “voting information center” that promoted factual information about how to register to vote or sign up to be a poll worker. Teams at WhatsApp wanted to create a version of it in Spanish, pushing the information proactively through a chat bot or embedded link to millions of marginalized voters who communicate regularly through WhatsApp. But Zuckerberg raised objections to the idea, saying it was not “politically neutral,” or could make the company appear partisan, according to a person familiar with the project who spoke on the condition of anonymity to discuss internal matters, as well as documents reviewed by The Post.

Ultimately, the company implemented a whittled-down version: a partnership with outside groups that allowed WhatsApp users to text a chat bot if they saw potential misinformation or to text a bot built by the organization Vote.org to get voting info.

“WhatsApp did not propose pushing information to all users, which is not how WhatsApp works,” said spokeswoman Christina LoNigro.

When considering whether to permit increased censorship in Vietnam, one former employee said, Zuckerberg’s line in the sand regarding free speech seemed to be constantly shifting. Warned that catering to a repressive regime could harm Facebook’s global reputation, according to one of the people, Zuckerberg argued that going offline entirely in Vietnam would cause even greater harm to free speech in the country.

After Zuckerberg agreed to increase censorship of anti-government posts, Facebook’s transparency report shows that more than 2,200 posts by Vietnamese users were blocked between July and December 2020, compared with 834 in the previous six months. Pro-democracy and environmental groups, meanwhile, have become a target of government-led mass reporting campaigns, the documents and interviews show, landing people in jail for even mildly critical posts.

In April 2020, Zuckerberg appeared to shoot down or express reservations about researchers’ proposals to cut down on hate speech, nudity, graphic violence and misinformation, according to one of the documents. The pandemic was in its early days and coronavirus-related misinformation was spreading. The researchers proposed a limit to boosting content the news-feed algorithm predicts will be reshared, because serial “reshares” tended to correlate with misinformation. Early tests showed limiting this could reduce coronavirus-related misinformation by up to 38 percent, according to the document.

“Mark doesn’t think we could go broad,” said Anna Stepanov, the director giving the readout from the Zuckerberg meeting, about the CEO’s response to the proposal to change the algorithm. “We wouldn’t launch if there was a material trade-off with MSI.”

Zuckerberg was a bit more open to a proposal to allow algorithms to be slightly less precise in what the software deemed to be hate speech, nudity and other banned categories — enabling it to delete a broader array of “probable violating content” and potentially reducing such harmful material by as much as 17 percent. But he only supported it as a “break the glass” measure, to be used in emergency situations such as the Jan. 6 insurrection, the documents said. Account demotions — which would have preemptively limited accounts that algorithms predicted were most likely to promote misinformation or hate — were off the table.

Facebook's Lever says "probable violating" proposals were not break the glass measures and the company did implement them across categories such as graphic violence, nudity and porn, and hostile speech. Later, it also implemented the algorithm change fully for political and health categories that are in place today.

The Wall Street Journal first reported on the document's existence.

The document that finally reached Zuckerberg was carefully tailored to address objections that researchers anticipated he would raise. For each of the nine suggestions that made their way up the chain, the data scientists added one row to list how the proposals would affect three areas he was known to care about: free speech, how Facebook is viewed publicly and how the algorithm change might affect MSI.

One former employee involved in that proposal process said those who worked on it were deflated by Zuckerberg's response. The researchers had gone back and forth with leadership for months on it, changing it many times to address concerns about clamping down on free speech.

Zuckerberg, said a former executive, "is extremely inquisitive about anything that impacts how content gets ranked in the feed — because that's the secret sauce, that's the way this whole thing keeps spinning and working and making profits."

"People felt, it was Mark's thing, so he needs it to be successful. It needs to work," the person added.

In 2019, those in the company's civic integrity division, a roughly 200-person team that focused on how to mitigate harms caused by the platform, began to hear that Zuckerberg himself was becoming very worried about "false positives" — or legitimate speech being taken down by mistake. They were soon asked to justify their work by providing estimates of how many "false positives" any integrity-related project was producing, according to one of the people.

"Our very existence is fundamentally opposed to the goals of the company, the goals of Mark Zuckerberg," said another person who quit. "And it made it so we had to justify our existence when other teams didn't."

“Founder-CEOs have superpowers that allow them to do courageous things. Mark has done that time and again,” Samidh Chakrabarti, the former head of the company’s civic integrity unit, who quit recently, tweeted this month. “But the trust deficit is real and the FB family may now better prosper under distributed leadership.”

Even as Facebook is facing perhaps its most existential crisis to date over the whistleblower documents, lately Zuckerberg’s attention has been elsewhere, focused on a push toward virtual-reality hardware in what former executives said was an attempt to distance himself from the problems of the core Facebook platform, known internally as the Big Blue app. The company is reportedly even considering changing its name to align better with his vision of a virtual-reality-driven “metaverse.” Facebook has said it doesn’t comment on rumors or speculation.

The former employees said it was also not surprising that the document trove contains so few references to Zuckerberg’s thoughts. He has become more isolated in recent years, in the face of mounting scandals and leaks (Facebook disputes his isolation). He primarily communicates decisions through a small inner circle, known as the Small Team, and a slightly bigger group of company leaders known as M-Team, or Mark’s team. Information that gets to him is also tightly controlled, as well as information about him.

Even criticizing Zuckerberg personally can come with costs. An engineer who spoke with The Post, and whose story was reflected in the documents, says he was fired in 2020 after penning an open letter to Zuckerberg on the company’s chat system, accusing the CEO of responsibility for protecting conservatives whose accounts had been escalated for misinformation.

One document, a 2020 proposal that indicates it was sent to Zuckerberg for review — over whether to hide like counts on Instagram and Facebook — strongly suggests that Zuckerberg was directly aware of some of the research into harmful effects of the service. It included internal research from 2018 that found that 37 percent of teenagers said one reason that they stopped posting content was because wanting to get enough like counts caused them “stress or anxiety.”

(The like-hiding study, named Project Daisy, was also reported by the Journal. In 2021, the company ultimately did offer an option to hide likes on Instagram, but not on Facebook. Facebook says it didn’t implement Project Daisy because a test showed mixed results for people’s well-being and that the 2018 study used in the presentation “cannot be used to show that Instagram causes harm because the survey wasn’t designed to test that, nor does the data show it.”)

# Exhibit 55



[\(https://muslimadvocates.org/\)](https://muslimadvocates.org/)

JUNE 30, 2019

Issues: [Corporate Accountability \(https://muslimadvocates.org/issues/corporate-accountability/\)](https://muslimadvocates.org/issues/corporate-accountability/), [Fighting Bigotry \(https://muslimadvocates.org/issues/fighting-bigotry/\)](https://muslimadvocates.org/issues/fighting-bigotry/)

## Muslim Advocates: Facebook Does Not Take Hate Content Seriously

[Press Release](#)

SHARE →

### *Civil Rights Audit Shows Need for Board-Level Change*

WASHINGTON, DC – The following is a statement from **Madihha Ahussain, Muslim Advocates' special counsel for anti-Muslim bigotry**, on the release of Facebook's second update on its civil rights audit. Muslim Advocates, along with Color of Change, Center for Media Justice and many other partners [urged Facebook to conduct this audit \(https://www.cmcj.org/press-releases/2019/06/30/muslim-advocates-urges-facebook-to-conduct-civil-rights-audit/\)](https://www.cmcj.org/press-releases/2019/06/30/muslim-advocates-urges-facebook-to-conduct-civil-rights-audit/) [\(https://muslimadvocates.org/2018/05/muslim-advocates-applauds-facebook-announcement-of-civil-rights-audit/\)](https://muslimadvocates.org/2018/05/muslim-advocates-applauds-facebook-announcement-of-civil-rights-audit/). After the first audit update was made public by Facebook in December 2018, Muslim Advocates and more than 30 organizations [called for board-level changes \(https://muslimadvocates.org/2018/12/muslim-advocates-responds-to-facebook-civil-rights-audit-update-stands-by-demands-for-board-reforms/\)](https://muslimadvocates.org/2018/12/muslim-advocates-responds-to-facebook-civil-rights-audit-update-stands-by-demands-for-board-reforms/) at the company to ensure accountability:

**“We appreciate that Facebook has acknowledged its role in undermining elections and voting rights, especially those of people of color, and is attempting to make progress on those fronts. However, this latest audit update shows that on issues regarding content moderation and the increased threat of white nationalist violence, the company has failed to take meaningful action. The murder of 51 Muslims in Christchurch broadcast all over the world on Facebook Live, made it clear that this is a life and death matter—still, the company has yet to take serious action to protect our community. Importantly, the audit process will not be successful if Facebook does not take seriously and implement the audit team’s recommendations for improving content moderation.**

**In addition, instead of building a permanent, board and staff-level civil rights infrastructure with the expertise needed to address this crisis, Facebook has chosen to take perfunctory half-steps all while anti-Muslim bigots and white nationalists continue to use the company’s platforms to organize and spread hatred and bigotry. Further, the burden still remains on victimized community members to report content and hope that the company will address the problem. Facebook’s piecemeal approach to these issues will not result in long-term solutions, and the time has come for the company to honor its commitment to fix these problems.**

**Facebook’s announcement that it will convert an ad hoc, interdepartmental collaboration of current staff tasked with addressing civil rights concerns into a permanent configuration will not result in meaningful change. It is clear th**

**FACEBOOK'S LEADERSHIP CONTINUES TO FAIL ON THIS FRONT. THE UPDATE TODAY confirms that demands for reforms to Facebook's board are still necessary, including:**

- Mark Zuckerberg stepping down as board chair,
- Sheryl Sandberg stepping down from the board,
- Increased diversity on the board and,
- A board-level civil rights expert and ombudsman.

**If Facebook has the capability to proactively remove content that violates its policies such as child pornography or ISIS-inspired speech and rhetoric, then it has the capability to remove anti-Muslim and white nationalist content just as aggressively. It is just choosing not to do so. There is no more time for cosmetic half-measures. Bold, structural change is needed now and that must start with Facebook's board."**

*Muslim Advocates is a national civil rights organization working in the courts, in the halls of power and in communities to halt bigotry in its tracks. We ensure that American Muslims have a seat at the table with expert representation so that all Americans may live free from hate and discrimination.*

###

June 30, 2019 6:06 pm

[Press Release](#)

## SHARE THIS ARTICLE:

<https://www.muslimadvocates.org/press-releases/facebook-does-not-take-hate-content-advocates-demands-reforms-to-board-that-will-take-hate-content-off-boards>

# Exhibit 56



ADAM MAIDA

DOUG BOCK CLARK SECURITY 01.16.2018 06:00 AM

## Meet Antifa's Secret Weapon Against Far-Right Extremists

Megan Squire is an intelligence operative of sorts, passing along information to those who might put it to real-world use, like Antifa—who can weaponize it.

**THE EMAIL ARRIVED** just as Megan Squire was starting to cook Thanksgiving dinner. She was flitting between the kitchen, where some chicken soup was simmering, and her living room office, when she saw the subject line flash on her laptop screen: “LOSer Leak.” Squire recognized the acronym of the League of the South, a neo-Confederate organization whose leaders have called for a “second secession” and the return of slavery. An anonymous insider had released the names, addresses, emails, passwords, and dues-paying records of more than 4,800 members of the group to a left-wing activist, who in turn forwarded the information to Squire, an expert in data mining and an enemy of far-right extremism.

Fingers tapping across the keyboard, Squire first tried to figure out exactly what she had. She pulled up the Excel file’s metadata, which suggested that it had passed through several hands before reaching hers. She would have to establish its provenance. The data itself was a few years old and haphazardly assembled, so Squire had to rake the tens of thousands of information-filled cells into standardized sets. Next, she searched for League members near her home of Gibsonville, North Carolina. When she found five, she felt a shiver. She had recently received death threats for her activism, so she Googled the names to find images, in case those people showed up at her door. Then she began combing through the thousands of other names. Two appeared to be former South Carolina state legislators, one a firearms industry executive, another a former director at Bank of America.

Once she had a long list of people to investigate, Squire opened a database of her own design—named Whack-a-Mole—which contains, as far as anyone can tell, the most robust trove of information on far-right extremists. When she cross-checked the names, she found that many matched, strengthening her belief in the authenticity of the leak. By midafternoon, Squire was exchanging messages via Slack with an analyst at the Southern Poverty Law Center, a 46-year-old organization that monitors hate groups. Squire often feeds data to the SPLC, whose analysts might use it to provide information to police or to reveal white supremacists to their employers, seeking to get them fired. She also sent several high-profile names from the list back to the left-wing activist, who she knew might take more radical action—like posting their identities and photos online, for the public to do with what it would.<sup>1</sup>

WIRED-26-02

CREATE. CONNECT. CONDU. MAST.

FEATURING:

ZEYNEP TUFEKCI  
ALICE GREGORY  
VIRGINIA HEFFERNAN  
STEVEN JOHNSON  
DOUG BOCK CLARK

# WIRED

# THE GOLDEN AGE OF FREE SPEECH

SPECIAL ISSUE:  
TECH, TURMOIL,  
AND THE  
NEW CENSORSHIP  
P. 50

FEBRUARY 2018 | CAN WE TALK?

Squire, a 45-year-old professor of computer science at Elon University, lives in a large white house at the end of a suburban street. Inside are, usually, some combination of husband, daughter, two step-children, rescue dog, and cat. In her downtime she runs marathons and tracks far-right extremists. Whack-a-Mole, her creation, is a set of programs that monitors some 400,000 accounts of white nationalists on Facebook and other websites and feeds that information into a centralized database. She insists she is scrupulous to not break the law or violate Facebook's terms of service. Nor does she conceal her identity, in person or online: "We shouldn't have to mask up to say Nazis are bad. And I want them to see I don't fit their stereotypes—I'm not a millennial or a 'snowflake.' I'm a peaceful white mom who definitely doesn't like what they're saying."

Though Squire may be peaceful herself, among her strongest allies are "antifa" activists, the far-left antifascists. She doesn't consider herself to be antifa and pushes digital activism instead of the group's black-bloc tactics, in which bandanna-masked activists physically attack white supremacists. But she is sympathetic to antifa's goal of silencing racist extremists and is unwilling to condemn their use of violence, describing it as the last resort of a "diversity of tactics." She's an intelligence operative of sorts in the battle against far-right extremism, passing along information to those who might put it to real-world use. Who might weaponize it.

As day shifted to evening, Squire closed the database so she could finish up cooking and celebrate Thanksgiving with her family and friends. Over the next three weeks, the SPLC, with help from Squire, became comfortable enough with the information to begin to act on it. In the shadowy world of the internet, where white nationalists hide behind fake accounts and anonymity is power, Whack-a-Mole was shining a searchlight. By mid-December, the SPLC had compiled a list of 130 people and was contacting them, to give them a chance to respond before possibly informing their employers or taking legal action. Meanwhile, the left-wing activist whom Squire had separately sent data to was preparing to release certain names online. This is just how Squire likes it. Hers is a new, digitally enabled kind of vigilante justice. With no clear-cut rules for just how far a citizen could and should go, Squire has made up her own.

“ I’m the old lady of activism,” says Megan Squire, a professor of computer science at Elon University. JOÃO CANZIANI

**SQUIRE GREW UP** near Virginia Beach in a conservative Christian family. She has been involved in left-leaning movements since she was 15, when her high school environmental club took a trip to protest the pollution from an industrial pig farm. “I loved the activist community,” she says, “and saying things we weren’t supposed to say.” After getting degrees in art history and public policy from William & Mary, she became interested in computers and took a job as a secretary at an antivirus software company, working her way up to webmaster. She eventually got a PhD in computer science from Nova Southeastern University in Florida and moved to North Carolina to work at startup companies before landing a job teaching at Elon. Between classes she could often be spotted around town waving signs against the Iraq War, and in 2008 she went door to door campaigning for Barack Obama. But Obama’s failure, in her view, to live up to his rhetoric, compounded by the Great Recession, was “the turning point when I just threw in the towel on electoral politics,” she says. She plunged into the Occupy movement, coming to identify as a pacifist-anarchist, but she eventually became disillusioned with that as well when the movement’s “sparkle-fingers” utopianism, as she puts it, failed to generate results. In 2016, she cast a vote for the Green Party’s Jill Stein.

---

### **Dig Deeper With Our Longreads Newsletter**

Sign up to get our best longform features, investigations, and thought-provoking essays, in your inbox every Sunday.

Your email

Enter your email

SUBMIT

By signing up you agree to our [User Agreement](#) and [Privacy Policy & Cookie Statement](#)

Donald Trump's campaign, though, gave Squire a new sense of mission: "I needed to figure out what talents I had and what direct actions I could do." When a mosque in the nearby city of Burlington was harassed by a local neo-Confederate group called Alamance County Taking Back Alamance County, she decided to put her skills to use. ACTBAC was using Facebook to organize a protest against the opening of the mosque, so Squire began scraping posts on the page that threatened to "kick Islam out of America." She submitted her findings to the SPLC to get ACTBAC classified as a hate group, and to the North Carolina Department of the Secretary of State, which started an investigation into the group's tax-exempt nonprofit status. She also organized a counterprotest to one of the group's rallies, and it was at this event and others like it where she first became acquainted with the black-clad antifa activists. She was impressed. "They were a level of mad about racism and fascism that I was glad to see. They were definitely not quiet rainbow peace people." Over the following months, she began feeding information to some of her new local antifa contacts. As white pride rallies intensified during 2017's so-called Summer of Hate—a term coined by a neo-Nazi website—Squire began to monitor groups outside of North Carolina, corresponding with anonymous informants and pulling everything into her growing Whack-a-Mole database. Soon, in her community and beyond, antifa activists could be heard whispering about a new comrade who was bringing real, and potentially actionable, data-gathering skills to the cause.

The first big test of Whack-a-Mole came just before the white supremacist Unite the Right rally in Charlottesville on Saturday, August 12. In the weeks before, because of her database, Squire could see that nearly 700 white supremacists on Facebook had committed to attend the rally, and by perusing their posts, she knew they were buying plane tickets and making plans to caravan to Charlottesville. Her research also showed that some of them had extensive arrest records for violence. She sent a report to the SPLC, which passed it on to Charlottesville and Virginia law enforcement. She also called attention to the event on anarchist websites and spread the word via "affinity groups," secret peer-to-peer antifa communication networks.

---

"Antifa was a level of mad about racism and fascism that I was glad to see. They were definitely not quiet rainbow peace people."

---

The night before the rally, Squire and her husband watched in horror on the internet as several hundred white supremacists staged a torch-lit march in Charlottesville to protest the removal of a statue of Robert E. Lee, chanting "Jews will not replace us!" The next morning, the couple got up at 5 am and drove more than 150 miles through rain and mist to Virginia. At a crowded park, she met with a half-dozen or so activists she knew from North Carolina, some of them antifa, and unfurled a banner for the Industrial Workers of the World. (She'd joined the Communist-inspired labor organization in December 2016, after witnessing what she considered its well-organized response to KKK rallies in North Carolina and Virginia.) Just before 10 am, the white supremacists began marching into Emancipation Park, a parade of Klansmen, neo-Nazis, militia members, and so-called alt-right adherents, armed with everything from homemade plexiglass shields to assault weapons. Squire screamed curses at the white supremacists by name—she knew them because she had their information on file in Whack-a-Mole and had memorized their faces. At one point, a group of clergy tried to blockade the white supremacists, and Squire linked arms with other activists to protect them. A petite woman, she was pushed aside

by men with plexiglass shields. Fights broke out. Both sides blasted pepper spray. Squire put on a gas mask she'd been carrying in a backpack, but the pepper spray covered her arms, making them sting.

After the police finally separated the combatants, Squire and dozens of other counterprotesters took to Fourth Street in triumph. But then, a gray Dodge Challenger tore down the street—and rammed into their backs. The driver, who had marched with the white nationalists and was later identified as James Alex Fields, missed Squire by only a few feet. She stood on the sidewalk, weeping in shock, as the fatally injured activist Heather Heyer lay bleeding in the street.

Recounting the event months later, Squire began to cry. “I had all this intelligence that I hadn’t used as effectively as I could have. I felt like I’d wasted a chance that could have made a difference.” When she returned home, she threw herself into expanding Whack-a-Mole.

Squire, center, marches through the streets of Asheboro, North Carolina, to protest the KKK. DANIEL HOSTERMAN

**ONE MORNING IN** December, I visited Squire in her small university office. She had agreed to show me the database. First she logged onto a foreign server, where she has placed Whack-a-Mole to keep it out of the US government’s reach. Her screen soon filled with stacks of folders nested within folders: the 1,200-plus hate groups in her directory. As she entered command-line prompts, spreadsheets cascaded across the screen, each cell representing a social media profile she monitors. Not all of them are real people. Facebook says up to 13 percent of its accounts may be illegitimate, but the percentage of fakes in Squire’s database is probably higher, as white nationalists often hide behind multiple sock puppets. The SPLC estimates that half of the 400,000-plus accounts Squire monitors represent actual users.

Until Whack-a-Mole, monitoring white nationalism online mainly involved amateur sleuths clicking around, chasing rumors. Databases, such as they were, tended to be cobbled together and incomplete. Which is one reason no one has ever been able to measure the full reach of right-wing extremism in this country. Squire approached the problem like a scientist. “Step one is to get the data,” she says. Then analyze. Whack-a-Mole harvests most of its data by plugging into Facebook’s API, the public-facing code that allows developers to build within Facebook, and running scripts that pull the events and groups to which various account owners belong. Squire chooses which accounts to monitor based on images and keywords that line up with various extremist groups.

Most of the Whack-a-Mole profiles contain only basic biographical sketches. For more than 1,500 high-profile individuals, however, Squire fills out their entries with information gleaned from sources like the SPLC, informers, and leaks. According to Keegan Hankes, a senior analyst at the SPLC, Squire's database "allows us to cast a much, much wider net. We're now able to take a much higher-level look at individuals and groups."

In October, after a man fired a gun at counterprotesters at a far-right rally in Florida, SPLC analysts used Squire's database to help confirm that the shooter was a white nationalist and posted about it on their blog. Because so much alt-right digital data vanishes quickly, Whack-a-Mole also serves as an archive, providing a more permanent record of, say, attendees at various rallies. Squire's database has proven so useful that the SPLC has begun laying the groundwork for it to feed directly into its servers.

"I don't have any moral quandaries about this. I know I'm following rules and ethics that I can stand up for." MARK PETERSON/REDUX

**WHEN SQUIRE SENDS** her data to actual citizens—not only antifa, but also groups like the gun-toting Redneck Revolt—it gets used in somewhat less official ways. Before a neo-Nazi rally in Boston this past November, Squire provided local antifa groups with a list of 94 probable white nationalist attendees that included their names, Facebook profiles, and group affiliations. As one activist who goes by the pseudonym Robert Lee told me, "Whack-a-Mole is very helpful. It's a new way to research these people that leads me to information I didn't have." He posts the supposed identities of anonymous neo-Nazis and KKK members on his blog, Restoring the Honor, which is read by journalists and left-wing activists, and on social media, in an effort to provoke the public (or employers) to rebuke them.

Lee is careful, he says, to stop short of full-on doxing these individuals—that is, publicizing more intimate details such as home addresses, emails, and family photos that would enable electronic or even real-world harassment against them. Squire says that's why she feels comfortable sending him information. Of course, once a name is public, finding personal information is not that hard. In the digital age, doxing is a particularly blunt tool, one meant to terrorize and threaten people in their most private spaces. Celebrities, private citizens, left-wing activists, and Nazis have all been doxed. The tactic allows anonymous hordes of any persuasion to practice vigilante justice on anyone they deem evil, problematic, or just plain annoying. As the feminist videogame developer and activist Zoe Quinn, who has been doxed and brutally harassed online, has written: "Are you calling for accountability and reform, or are you just trying to punish someone—and do you have any right to punish anyone in the first place?"

Squire has been doxed herself. Pictures of her home, husband, and children have been passed around on racist websites. She has received death threats and terrorizing voicemails, including one that repeated “dirty kike” for 11 seconds. Elon University has fielded calls demanding she be fired. On Halloween, Confederate flags were planted in her yard. Still, though Squire fears for her family’s safety, she keeps going. “I’m aware of the risks,” she says. “But it seems worth it. That’s what taking a stand is.”

Members of Berkeley’s antifascist group block an Infowars reporter from covering a rally. MARK PETERSON/REDUX

After Charlottesville, Squire considered, in her anger and grief, publicly releasing the entire Whack-a-Mole database. It would have been the largest-ever doxing of the far right. But she worried about the consequences of misidentification. Instead, she worked with her regular partners at the SPLC and activists she trusts. At one point the SPLC contacted a university about a student whom Squire had identified as a potentially violent member of the League of the South. The university did not take action, and she thought about tossing the student’s name to the ever-ravenous social media mobs. But here too, she reasoned that when you have someone’s life at your fingertips, you need rules. If the university wasn’t willing to act, then neither was she. It was, for her, a compromise, an attempt to establish a limit in a national moment pointedly lacking in limits.

Critics might still argue that public shaming of the kind Squire promotes constitutes a watered-down form of doxing, and that this willingness to take matters into their own hands makes Squire and her cohort no better than vigilantes. As David Snyder, executive director of the First Amendment Coalition, says of Squire’s work: “Is it ethical to digitally stalk people? It may not be. Is it legal? Probably, as long as she doesn’t hack into their accounts and she’s collecting information they post publicly on an open platform like Facebook.” But he warns that limiting speech of anyone, even white supremacists, starts down a slippery slope. “Political winds can shift across time. Liberals who might cheer at a university limiting neo-Nazi speech also have to worry about the flip side of that situation when someone like Trump might penalize them in the future.”

As far as Squire is concerned, there’s a clear difference between protected speech and speech that poses an imminent threat to public safety. “Richard Spencer yelling about wanting a white ethno-state after events like Charlottesville—it’s hard to argue that kind of speech doesn’t constitute danger.”

---

## Related Stories

---

### BUSINESS

#### Myanmar's Internet Disrupted Society—and Fueled Extremists

DOUG BOCK CLARK

---

### NATIONAL AFFAIRS

#### Neo-Nazis Face a New Foe Online and IRL: the Far-Left Antifa

EMMA GREY ELLIS

---

### SECURITY

#### Alt-Right Chat Logs Are Key to Charlottesville Lawsuits

NITASHA TIKU

---

Ultimately, Squire sees her work as a type of “fusion center”—a government term for a data center that integrates intelligence from different agencies—for groups combating white nationalism. And she admits that she is outsourcing some of the ethical complexities of her work by handing her data off to a variety of actors. “But it’s the same as how Facebook is hypocritical in claiming to be ‘just a platform’ and not taking responsibility for hate. Every time we invent a technology to solve a problem, it introduces a bunch more problems. At least I’m attentive to the problems I’ve caused.” Squire sees herself as having to make difficult choices inside a system where old guidelines have been upended by the seismic powers of the internet. White nationalists can be tracked and followed, and therefore she believes she has a moral obligation to do so. As long as law enforcement keeps “missing” threats like James Alex Fields, she says, “I don’t have any moral quandaries about this. I know I’m following rules and ethics that I can stand up for.”

After Charlottesville, some white supremacist groups did find themselves pushed off certain social media and hosting sites by left-wing activists and tech companies wary of being associated with Nazis. These groups relocated to platforms like the far-right Twitter clone Gab and Russia’s Facebook-lite VK. Squire sees this as a victory, believing that if white nationalists flee to the confines of the alt-right echo chamber, their ability to recruit and organize weakens. “If the knowledge that we’re monitoring them on Facebook drives them to a darker corner of the internet, that’s good,” she asserts.

That doesn’t mean Squire won’t follow them there. She has no plans to stop digitally surveilling far-right extremists, wherever they may be. After Jason Kessler, the organizer of the Unite the Right rally, was unverified on Twitter, he joined VK. His first post read, “Hello VK! I’d rather the Russians have my information than Mark Zuckerberg.” The declaration was quickly scooped up by Squire. She had already built out Whack-a-Mole to track him there too.

## The Free Speech Issue

- **Tech, Turmoil, and the New Censorship:** Zeynep Tufekci explores how technology is upending everything we thought we knew about free speech.
- **“Nice Website. It Would Be a Shame if Something Happened to It.”:** Steven Johnson goes inside Cloudflare's decision to let an extremist stronghold burn.
- **Please, Silence Your Speech:** Alice Gregory visits a startup that wants to neutralize your smartphone—and un-change the world.

- **The Best Hope for Civil Discourse on the Internet ... Is on Reddit:** Virginia Heffernan submits to [Change My View](#).
- **6 Tales of Censorship:** What it's like to be suspended by Facebook, blocked by Trump, and more, [in the subjects' own words](#).

**Doug Bock Clark** ([@dougbockclark](#)) wrote about [Myanmar's digital revolution](#) in issue 25.10. His first book, [The Last Whalers](#), comes out in July.

<sup>1</sup> **Correction appended, 1/22/2018, 2:58 PM EDT:** A previous version of this story incorrectly stated that Squire sent names from the LOSer Leak spreadsheet to another contact. She only sent them back to the person she received the spreadsheet from.

*This article appears in the February issue. [Subscribe now](#).*

*Listen to this story, and other WIRED features, on the [Audm app](#).*

# Exhibit 57



(<https://muslimadvocates.org/>).

OCTOBER 16, 2019

Issue: [Corporate Accountability \(https://muslimadvocates.org/issues/corporate-accountability/\)](https://muslimadvocates.org/issues/corporate-accountability/)

## Muslim Advocates Demands that Zuckerberg Address Facebook's Anti-Muslim Problem

[Press Release](#)

SHARE ↗

### *Ahead of Zuckerberg's Georgetown Speech on Thursday, Muslim Advocates Urges Facebook to End False Ad Policy*

WASHINGTON, DC – The following is a statement issued today from **Muslim Advocates** (<https://www.muslimadvocates.org/>) **Executive Director Farhana Khera** responding to Facebook's [newly-codified policy \(https://newsroom.fb.com/news/2019/09/elections-and-political-speech/\)](https://newsroom.fb.com/news/2019/09/elections-and-political-speech/) allowing politicians to lie in their ads, as well as a report that Facebook CEO Mark Zuckerberg [held private meetings with pundits who have spread anti-Muslim bigotry \(https://www.politico.com/news/2019/10/14/facebook-zuckerberg-conservatives-private-meetings-046663\)](https://www.politico.com/news/2019/10/14/facebook-zuckerberg-conservatives-private-meetings-046663):

“Facebook’s decision to broadcast false, hateful ads from politicians not only threatens democracy, it also threatens the personal safety of American Muslims, immigrants and other vulnerable communities.

Facebook’s decision has already had real life and death consequences. Facebook has [run thousands of ads \(https://www.cnn.com/2019/08/06/politics/trump-invasion-facebook-ads/index.html\)](https://www.cnn.com/2019/08/06/politics/trump-invasion-facebook-ads/index.html) from the Trump campaign warning of an immigrant ‘invasion’— language that was echoed by white nationalist mass murderers like the Christchurch shooter and the El Paso shooter. Additionally, at a time when American Muslims are facing a wave of bigotry, the Trump campaign [ran multiple, false ads \(https://muslimadvocates.org/wp-content/uploads/2019/10/Screen-Shot-2019-10-15-at-1.22.48-PM.png\)](https://muslimadvocates.org/wp-content/uploads/2019/10/Screen-Shot-2019-10-15-at-1.22.48-PM.png) calling two Muslim members of Congress ‘anti-Israel, anti-AMERICAN and pro-terrorist,’ contributing to an environment where these members of Congress now receive death threats on a regular basis.

people never making anyone available for a meeting with advocates representing communities directly targeted by these hateful and false ads, Mark Zuckerberg instead has held private meetings (<https://www.politico.com/news/2019/10/14/facebook-zuckerberg-conservatives-private-meetings-046663>), with right-wing media personalities with a history of amplifying anti-Muslim hate. Let's be clear: the people Zuckerberg dined with and sought counsel from are not just standard-issue conservative pundits, they are bigots who have voiced and amplified dangerous, white nationalist, anti-Muslim hate, including:

- **Ben Shapiro** saying that Arabs (<https://twitter.com/benshapiro/status/25712847277?lang=en>), 'like to bomb crap and live in open sewage' and falsely claiming (<https://www.politifact.com/punditfact/statements/2014/nov/05/ben-shapiro/shapiro-says-majority-muslims-are-radicals/>), that a majority of Muslims are anti-American radicals.
- **Brent Bozell** giving a keynote speech at a conference (<https://www.splcenter.org/hatewatch/2017/10/02/despite-major-setbacks-anti-muslim-hate-group-act-america-kicks-its-annual-conference-today>), hosted by ACT for America, an anti-Muslim extremist group so extreme that it was recently disinvited from Trump's own Mar-a-Lago resort.
- **Byron York** penning an op-ed (<https://www.washingtonexaminer.com/obama-has-himself-to-blame-for-muslim-problem>), that tried to legitimize the anti-Muslim 'birther' conspiracy theory against President Barack Obama.
- **Tucker Carlson** saying on his cable news show ([https://twitter.com/ndrew\\_lawrence/status/1148761751414087680](https://twitter.com/ndrew_lawrence/status/1148761751414087680)), that Rep. Ilhan Omar is 'living proof that the way we practice immigration has become dangerous to this country' and warning that 'no country can import large numbers of people who hate it and expect to survive.'
- **Hugh Hewitt** using his radio show to broadcast anti-Muslim stereotypes (<https://www.mediamatters.org/hugh-hewitt/hugh-hewitt-osu-usc-football-game-its-probably-last-football-game-well-ever-get-see>) and amplify people who said that Islam is antithetical to the American values system (<https://www.hughhewitt.com/dennis-prager-and-hugh-on-still-the-best-hope/>).

Groups like Muslim Advocates have spent years asking Zuckerberg to take meaningful action to stop the dangerous, violent hate speech that still thrives on Facebook and have been met with excuses and half-measures. Meanwhile, he has opened his doors and broken bread with people who have spread anti-Muslim hate.

And the problem isn't just the rampant hate content, the dishonest ads and the meetings to appease conservatives. The massacre of 51 people in two Christchurch mosques was broadcast on Facebook. Further, the company knowingly tapped known anti-Muslim politician Jon Kyl to author its anti-conservative bias audit.



# Exhibit 58

October 30, 2017

Mr. Mark Zuckerberg, Chief Executive Officer  
Ms. Sheryl Sandberg, Chief Operating Officer  
Facebook, Inc.  
1 Hacker Way  
Menlo Park, CA 94025

Dear Mr. Zuckerberg and Ms. Sandberg,

We, the undersigned civil rights, interfaith, and advocacy organizations write to express our deep concern regarding ads, pages, and hateful content on your platform used to divide our country, and in particular, to promote anti-Muslim, anti-Black, anti-immigrant, and anti-LGBTQ animus. We thank you for recent meetings with some of our organizations representing communities that were directly affected by the material on your platform. We appreciate that senior members of your team—including you, Ms. Sandberg—have facilitated these meetings, and we hope that these conversations are the beginning of a serious and ongoing dialogue. Now, it is necessary for Facebook to take critical steps to address the bigotry and discrimination generated on your platform.

As you know, we do not yet have access to all the divisive content targeting communities we represent; therefore, we are only able to cite to the few examples that were leaked to the media.

For example, Russian operatives set up misleading accounts impersonating or posing as American individuals and groups on Facebook to promote Russian propaganda during the American election season. Reports indicate that a Russian Facebook account called “SecuredBorders” posed as a group of US citizens concerned about the increased number of refugees in America. This fake account not only promoted anti-immigrant messaging online, but also managed to organize an in-person anti-refugee rally in Twin Falls, Idaho in August 2016.<sup>1</sup>

In addition, a Facebook page entitled “United Muslims of America” was an imposter account traced back to Russia<sup>2</sup>—the real United Muslims of America is a California-based interfaith organization working at the local level to promote dialogue and political participation.<sup>3</sup> The imposter account smeared political candidates and

---

<sup>1</sup> Geoffrey Smith, “Russia Orchestrated Anti-Immigrant Rallies in the U.S. via Facebook Last Year,” *Fortune*, Sept. 12, 2017, *available at* <http://fortune.com/2017/09/12/russia-orchestrated-anti-immigrant-rallies-in-the-u-s-via-facebook-last-year/>.

<sup>2</sup> Dean Obeidallah, “How Russian Hackers Used My Face to Sabotage Our Politics and Elect Trump,” *The Daily Beast*, Sept. 27, 2017, *available at* <https://www.thedailybeast.com/how-russian-hackers-used-my-face-to-sabotage-our-politics-and-elect-trump>.

<sup>3</sup> United Muslims of America “About” page, *available at* <http://www.umanet.org/about-us>.

promoted political rallies aimed at Muslim audiences.<sup>4</sup> In another example, the Internet Research Agency in Russia promoted an anti-Muslim rally thousands of miles away in Houston, Texas where individuals protested outside of a mosque.<sup>5</sup> Additional reports indicate that Facebook offered its expertise to a bigoted advocacy group by creating a case study testing different video formats, and advising on how to enhance the reach of the group's anti-refugee campaign in swing states during the final weeks of the 2016 election.<sup>6</sup> These examples of content on Facebook were not only harmful, but also used to rile up supporters of President Trump.

Furthermore, it has been reported that Russian operatives purchased Facebook ads about Black Lives Matter—some impersonating the group and others describing it as a threat.<sup>7</sup> This included ads that were directly targeted to reach audiences in Ferguson, Missouri and Baltimore, Maryland. CNN reports that the Russian Internet Research Agency used these ads in an attempt to amplify political discord and create a general atmosphere of incivility and chaos.<sup>8</sup> This included a fake ad containing an image of an African-American woman dry-firing a rifle, playing on the worst stereotypes regarding African-Americans as threatening or violent.<sup>9</sup>

We were alarmed to see your platform being abused to promote bigotry, and especially disappointed that it has taken media exposure and congressional oversight to give a degree of transparency into your practices. It is important to keep in mind that pervasive bigotry has long existed on your platform, and the Russian operatives

---

<sup>4</sup> Obeiallah, *supra* note 1.

<sup>5</sup> Tim Lister & Clare Sebastian, "Stoking Islamophobia and secession in Texas - from an office in Russia," CNN Politics, Oct. 6, 2017, *available at* <http://www.cnn.com/2017/10/05/politics/heart-of-texas-russia-event/index.html>.

<sup>6</sup> Melanie Ehrenkranz, "Facebook Reportedly Used Anti-Muslim Ad as Test Case in Video Formats," Gizmodo, Oct. 18, 2017, *available at* <https://gizmodo.com/facebook-reportedly-used-anti-muslim-ad-as-test-case-in-1819645900>.

<sup>7</sup> Adam Entous, Craig Timberg, & Elizabeth Dwoskin, "Russian operatives used Facebook ads to exploit America's racial and religious divisions," The Washington Post, Sept. 25, 2017, *available at* [https://www.washingtonpost.com/business/technology/russian-operatives-used-facebook-ads-to-exploit-divisions-over-black-political-activism-and-muslims/2017/09/25/4a011242-a21b-11e7-ade1-76d061d56efa\\_story.html?tid=sm\\_tw&utm\\_term=.e49cecc1a834](https://www.washingtonpost.com/business/technology/russian-operatives-used-facebook-ads-to-exploit-divisions-over-black-political-activism-and-muslims/2017/09/25/4a011242-a21b-11e7-ade1-76d061d56efa_story.html?tid=sm_tw&utm_term=.e49cecc1a834).

<sup>8</sup> Dylan Byers, "Exclusive: Russian-bought Black Lives Matter ad on Facebook targeted Baltimore and Ferguson," CNN Media, Sept. 28, 2017, *available at* <http://money.cnn.com/2017/09/27/media/facebook-black-lives-matter-targeting/index.html>.

<sup>9</sup> Adam Entous, Craig Timberg, & Elizabeth Dwoskin, "Russian Facebook ads showed a black woman firing a rifle, amid efforts to stoke racial strife," The Washington Post, Oct. 2, 2017, *available at* [https://www.washingtonpost.com/business/technology/russian-facebook-ads-showed-a-black-woman-firing-a-rifle-amid-efforts-to-stoke-racial-strife/2017/10/02/e4e78312-a785-11e7-b3aa-c0e2e1d41e38\\_story.html?utm\\_term=.aa2267a2f46c](https://www.washingtonpost.com/business/technology/russian-facebook-ads-showed-a-black-woman-firing-a-rifle-amid-efforts-to-stoke-racial-strife/2017/10/02/e4e78312-a785-11e7-b3aa-c0e2e1d41e38_story.html?utm_term=.aa2267a2f46c).

simply exploited the hateful content and activity already present. We are concerned about how a platform like Facebook's could operate without appropriate safeguards that take into account how it could be manipulated to further sow divisions in our society.

As a company and social network platform whose mission is "to give people the power to build community and bring the world closer together,"<sup>10</sup> we hope that you understand the gravity of this hateful rhetoric and behavior. During a time when anti-Muslim, anti-Black, anti-LGBTQ, and anti-immigrant sentiment has swept the nation, it is more important than ever for companies like yours to take an unequivocal stance against bigotry.

Over the years, many of us have raised concerns about how your platform may have a negative impact on our communities, with disappointing results. For example, we have requested that you address attacks on African Americans and Muslims, organizing by hate groups, and the censorship of Black, Arab, Muslim, and other marginalized voices. As a result of the pervasive presence and organizing by hate groups on your platform—some could not exist as national level entities without it—we have repeatedly requested that you convene a gathering with civil rights organizations to discuss appropriate and strategic responses. While you were unable to sufficiently respond to the concerns raised above, Facebook participated in and organized events that stigmatized Muslims and other communities such as a recent convening called "Tech Against Terrorism."

Though in the past you have displayed a willingness to listen to our concerns, we have yet to see meaningful change. It is our hope that recent developments will mark a new chapter in Facebook's commitment to protecting the rights of all who use your platform.

As we continue this important dialogue, we urge you to:

1. Fully disclose to the public all of the ads, pages, events, accounts, and posts you have traced back to Russian operatives targeting African American, LGBTQ, and Muslim communities. In particular, we believe that Facebook has a special responsibility to notify those individuals and organizations who have been impersonated or misrepresented.
2. Bring on an independent third-party team to conduct a thorough and public audit of the civil rights impact of your policies and programs, as well as how the platform has been used by hate groups, political entities, and others to stoke racial or religious resentment or violence. Other leading companies in the

---

<sup>10</sup> Facebook "About" page, February 4, 2004, *available at* [https://www.facebook.com/pg/facebook/about/?ref=page\\_internal](https://www.facebook.com/pg/facebook/about/?ref=page_internal).

industry like Airbnb have made the decision to conduct such an assessment, and we hope you will follow their lead.

3. Regularly convene a new working group of a diverse group of civil rights organizations working to counter bigotry, and solicit input on policies and processes from this group. And, integrate addressing hate into Facebook's corporate structure by:
  - a. Assigning a board committee with responsibility for assessing management efforts to stop hate groups, state actors, and individuals engaged in hate from using your platform and tools;
  - b. Assigning a senior manager who is a member of Facebook's Executive Team with authority to oversee addressing hate company-wide and name that person publicly and employing staff with expertise in this area to vet advertisements and develop process and procedures the address this issue; and,
  - c. Creating a committee of outside advisors with expertise in identifying and tracking hate who will be responsible for producing an annual report on the effectiveness of steps taken by Facebook.
4. Develop, with input from diverse civil rights groups and experts, and make public a clear process for how Facebook:
  - a. Reviews content constituting hate speech;
  - b. Reviews efforts to use Facebook as a platform to stoke identity-based, racial, or religious resentment or violent actions; and,
  - c. Responds to complaints about content that reasonably creates fear and chills speech on Facebook.
5. Make public detailed information regarding training and support for anti-immigrant, anti-Muslim, anti-black, and anti-LGBTQ organizations, including the monetary value of these services; and establish a fund to provide grants to organizations combating hatred and bigotry.

Thank you in advance for your consideration. Please contact Naheed Qureshi at [naheed@muslimadvocates.org](mailto:naheed@muslimadvocates.org) with any questions.

We look forward to your reply.

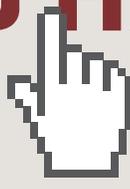
Sincerely,

Arab American Institute (AAI)  
Asian Americans Advancing Justice | AAJC  
Center for Media Justice

Center for New Community  
Color of Change  
CREDO  
Human Rights Campaign (HRC)  
The Leadership Conference on Civil and Human Rights  
League of United Latin American Citizens (LULAC)  
MoveOn.org  
Muslim Advocates  
NAACP  
NAACP Legal Defense and Educational Fund, Inc. (LDF)  
National Center for Lesbian Rights  
National Hispanic Media Coalition  
National LGBTQ Task Force  
National Sikh Campaign  
Sikh Coalition  
Southern Poverty Law Center

# Exhibit 59

**CLICK HERE TO  
END HATE**



**Anti-Muslim Bigotry Online  
& How to Take Action**

**Published May 2014**

Muslim Advocates is a national legal advocacy and educational organization working on the frontlines of civil rights to protect freedom for Americans of all faiths, through legal advocacy, policy engagement, and civic education, and by serving as a legal resource to promote the full and meaningful participation of Muslims in American public life.

**Muslim Advocates**

*[www.muslimadvocates.org](http://www.muslimadvocates.org)*

*[info@muslimadvocates.org](mailto:info@muslimadvocates.org)*

© All rights reserved.

The quotes, posts, and screenshots that appear in this report have been dated and sourced as accurately as possible. The number of likes, followers, views, or other statistics related to pieces of content included in this report are current as of April 22, 2014, unless otherwise indicated. Please note that content or links may have since been modified, moved, or deleted, as content online and on social media platforms in particular evolve and change. The issues raised by the hateful content referenced in this report, however, remain a constant challenge in need of understanding and confrontation.

Dear Friend:

In the summer of 2012 an anti-Islam video denigrating Prophet Muhammad (P.B.U.H.) entitled *The Innocence of Muslims* was uploaded to YouTube. From that time until February 2014, the film had been viewed over one million times, and thousands of hateful comments about Islam and Muslims had been posted in response. The film also sparked demonstrations around the globe, in Egypt and in other Muslim-majority nations. In the United States, the film's content raised questions about the permissibility of such hateful content and offensive depictions on the Internet, particularly on widely accessible social media platforms.

At the same time, Muslim Advocates heard from concerned American Muslims asking what could be done to counter hateful content online. As part of our program to combat anti-Muslim hate, we began to explore the issue and soon realized that this video was just one of many examples of online hate. While *The Innocence of Muslims* did not explicitly encourage violence towards Muslims, there are countless other examples online that do—making Internet hate a growing challenge that affects the everyday lives of American Muslims and, indeed, all Americans.

The Internet is a powerful tool, connecting the world and bringing instant information to anyone with a screen and keyboard. And while much progress and good is carried out through websites, blogs, and social media channels, in some cases, these very same outlets provide a platform for hate and threaten the rights, dignity, and safety of innocent Americans.

In the last few years, the number of Americans with an unfavorable view of Islam has grown and they now form a majority. During this same time, hate crimes and employment discrimination motivated by anti-Muslim bias have spiked and remain at disturbingly high levels. In addition, many politicians and public figures have used their profile and influence to spread fear and encourage violence against an entire group of people simply because of their faith. These voices are amplified on social media and help create a space for others to echo and build upon anti-Muslim sentiments and hate, and in turn foster an environment where it is acceptable, for some, to engage in acts of violence and discrimination.

This groundbreaking report documents the scope of anti-Muslim hate online, and offers tools for American Muslims and all Americans who reject fear and hate to report abusive content to Internet companies and to engage in effective counterspeech. In addition, the report explains Internet company policies and the limitations of the law to combat online hate. Finally, the report provides recommendations for Internet companies to ensure their platforms create safe communities online.

With these tools and resources, we can make our communities safer from bigotry and hate. It is my hope that *Click Here to End Hate: Anti-Muslim Bigotry Online & How to Take Action* will educate parents, students, youth, community leaders, activists, Internet companies, and policy makers about this emerging challenge and empower them to take the steps necessary to address it.

Thank you for reading.

**Farhana Khera**  
President & Executive Director  
Muslim Advocates

# Table of Contents

- Executive Summary ..... **01**
- Introduction ..... **05**
- What Anti-Muslim Hate Looks Like: The Hate Feed ..... **07**
  - Online Hate by Public Officials ..... **08**
  - Speech by Hate Groups & Anti-Muslim Activists ..... **11**
  - Online Hate by Individuals..... **18**
- What the Law Says ..... **22**
- What Internet Companies Say About Hateful Content ..... **24**
- What Users Can Do..... **26**
  - Report Hateful Content ..... **27**
  - Engage in Counterspeech..... **32**
- Conclusion & Recommendations ..... **36**
- Endnotes ..... **38**

# Executive Summary

The Internet has fundamentally changed the way we communicate and consume information. A significant part of that transformation has been through social media. As of 2013, almost 75% of Internet users were active on social media. While the Internet and social media have provided the opportunity for more efficient communication and community building, they have also given a platform to those who purvey bigotry and hatred.

In particular, broader society has seen a significant increase in anti-Muslim hate. As public opinion polls as recent as 2010 indicate, a majority of Americans have a negative view of Islam. Evidence of that hate is further seen in opposition to mosque construction and expansion, employment discrimination against American Muslims, anti-Muslim rhetoric from public officials, and hate crimes such as vandalism of mosques, violence, and threats of violence. It should not be surprising, then, that anti-Muslim bigotry has found a strong voice on the Internet and social media.

## Online Hate by Public Officials

Perhaps the most troubling form of anti-Muslim hate is that conveyed by public officials—the same people we entrust with the responsibility to uphold and enforce our laws, including freedom and equality for Americans of all faiths. Perpetrators range from members of congress to state and local politicians. They suggest American Muslims are somehow less American than other Americans and make negative statements on social media, which in turn provide a forum for constituents to add vitriol. Sometimes they even encourage violence, such as a Tennessee county commissioner who last year posted a photo of a man peering down the site of a shotgun with one eye closed, captioned “How to Wink at a Muslim.”

## Speech by Hate Groups & Anti-Muslim Activists

Hate groups have also built a strong online presence. As of 2010, there were an estimated 11,500 hate-related sites, including websites, social network pages, and micro-blogs. Many anti-Muslim hate groups identified by the Southern Poverty Law Center use the Internet and social media to

spread their destructive agendas. One of the larger hate groups, Stop Islamization of America, has a Facebook page with over 18,000 members and helped organize a campaign against Park51, a proposed Muslim community center in lower Manhattan.

Individual activists, some of whom are associated with hate groups, cultivate their own brand of anti-Muslim hate. Infamous personalities, such as Pamela Geller, Brigitte Gabriel, and others, use their online following to spread hate and misinformation about Islam.

### **Online Hate by Individuals**

Individuals without a public personality also contribute heavily to the flood of anti-Muslim hate on social media. For example, a map posted on Facebook showing the distribution of mosques in America prompted one individual to comment “let them put one in upstate south carolina and we wil [sic] burn it down.” Another posting of an image of two women walking down the street wearing headscarves, one of which had an American flag print in celebration of Independence Day, prompted two users to comment that they would choke her with the scarf.

### **What the Law Says**

People often refer to comments like those described above as “hate speech,” when the comments denigrate a person’s race, religion, ethnicity, national origin, sexual orientation, or disability. Both within and outside of the law, hate speech does not have a universal definition. However, the challenge is often not how to define hate speech but how to treat it under the law and by social media platforms that some users employ to promote hate.

The starting point for understanding how online hate can be addressed is the First Amendment to the U.S. Constitution; however, it applies only to actions and restrictions imposed by the government, not private entities such as Internet and social media companies. In addition, in the overwhelming majority of cases, what many people consider hate speech is protected by the First Amendment. Certain exceptions to the broad free speech protections of the First Amendment do exist, but in relation to what might be called hate speech, the exceptions are very narrow.

### **What Internet Companies Say About Hateful Content**

Because the First Amendment limits only government restrictions on speech, virtually all social media companies have created terms of service agreements or user policies that address hateful or abusive speech. For example, Facebook is committed to creating a safe and respectful community online and has an explicit policy prohibiting hate speech. YouTube similarly does not permit hate speech. Twitter currently maintains a more permissive policy that prohibits users from publishing “direct, specific threats of violence against others.”

## What Users Can Do

Although the law provides few remedies to victims of hate speech, there are important steps they and others who reject bigotry can take to address online hate. The two most effective responses are reporting hateful content to the social media companies on whose platforms the hate speech appears and engaging in counterspeech.

This report provides step-by-step instructions on how to report content that violates social media companies' policies. Although reported content will not always be removed from social media platforms, user reporting helps inform companies about offensive content online and also holds Internet companies accountable to their policies.

The other effective way to address hate speech is through "counterspeech." The courts and civil society have long encouraged more speech as a response to offensive speech. When offensive, hateful content appears on a website or social media platform, a common and effective response employs the tradition of counterspeech.

This report cites several effective uses of counterspeech, including a classic example that occurred in 2012, after *Newsweek* published a controversial cover story with the headline "Muslim Rage."

## Conclusion & Recommendations

Given today's widespread use of the Internet, all Americans should remain actively engaged and vigilant to prevent our freedom of speech from being abused. This report makes several recommendations for addressing online hate:

- Social media users should learn about user policies and reporting tools to report hateful content, and consider opportunities to engage in counterspeech. If users have been the target of threats, they should report them to law enforcement immediately.
- Faith and civic leaders and organizations should share this report and engage with colleagues, members, and interfaith partners in their communities about issues of online hate.
- Parents and students should engage school administrators about their concerns with the use of the Internet and social media platforms and the impact on their child at school and immediately inform school administrators about bullying in school. Also, they should learn about the school's policies on cyberbullying or Internet use at school or during school hours in the event that a threatening or harmful situation involving other students arises. Parents and students can visit the U.S. Department of Education website at [www.ed.gov](http://www.ed.gov) for more information about bullying.

- Internet companies should:
  - Develop and maintain an understanding of sensitivities that relate to American Muslims and other communities targeted by hate groups;
  - Track and record the frequency at which reports are based on hateful content, particularly as it relates to a person's faith;
  - Affirmatively state company policy on hate speech and threatening speech;
  - Continue to enhance tools designed for reporting content;
  - Review all content reported by users to determine whether content violates company policies; and
  - Promptly notify users who have reported content violations of the outcome of the company's review and provide a clear explanation of the evaluation process used by the company.

Finally, the White House should convene a national-level dialogue on hate against religious communities and invite Internet companies to participate in discussions addressing online hate.

# INTRODUCTION



*“If there is even one more act of Muslim terrorism, it is then time for Americans to start slaughtering Muslims in the streets, all of them.”*

**@PatDollard**

*“Yes, they’re evil. Let’s kill them all.”*

**@ErikRush**

Hate and threats of violence directed at Muslims have disturbingly become all too common in the United States. Since the September 11, 2001 attacks on the World Trade Center and Pentagon, anti-Muslim bigotry and hate have infected many facets of our culture, from media coverage to political discourse to social media.

In 2010, nearly a decade after 9/11, a Public Religion Research Institute study found that 49 % of Americans believe the values of Islam are incompatible with the American way of life,<sup>1</sup> and 53% of Americans say their opinion of Islam is either “not too favorable” (22%) or “not favorable at all” (31%).<sup>2</sup> This societal anti-Muslim sentiment has coincided with an increase in the number of acts of violence and discrimination targeting American Muslims, including hate crimes, opposition to mosques, reports of employment discrimination, and anti-Muslim rhetoric by public officials.

**49%**

of Americans believe the values of Islam are incompatible with the American way of life

**Americans’ opinion of Islam:**

**22%**

not too favorable

**31%**

not favorable at all

Anti-Muslim sentiment came to a head in the summer of 2010, as media outlets provided daily, and sometimes seemingly nonstop, coverage of the growing opposition to Park51, a proposed Muslim community center in lower Manhattan, which critics associated with the World Trade Center site. Widespread media coverage of the controversy, coupled with bigoted statements by public officials, conveyed to American Muslims that their entire faith was being blamed for the acts of a criminal few. It also demonstrated how purveyors of anti-Muslim hate could command public and media attention for months.<sup>3</sup> Perhaps more disturbingly, while they had once resided primarily in the remote reaches of the blogosphere, television, and radio, they had now secured a platform in both mainstream media and social media.

The power of the Internet has fundamentally changed how we consume information. There was a time when people expressed their hatred in private or within social circles, but the Internet has dramatically changed the way we share ideas and interact with others. In fact, social media has become the most effective online tool to convey viewpoints and information rapidly. An increasing number of Internet users are active on social media—73% as of 2013.<sup>4</sup> The ubiquitous use of social media through computers, phones, and tablets has created opportunities for groups to rapidly generate and proliferate hate, without time for reflection and collective processing. Hateful and inaccurate information can become more potent as it is amplified and permanently stored online. Thus, the use of the Internet presents a new paradigm for our nation's unique and long-cherished commitment to religious freedom and the fundamental right to express oneself.<sup>5</sup>

The free speech legal doctrines that protect the protester on a public street corner rarely apply in the online context, since forums such as Facebook, Twitter, and YouTube are controlled by private companies, not the government. As a result, these Internet companies often have their own policies that govern content on their platforms, including limitations on hateful and abusive speech, and they enforce compliance with those policies.

This report highlights examples of the many different forms of hate that are found online. Although the law will rarely require that material be removed from the Internet, there are important steps that Internet users can take to respond effectively to hate speech online: namely, reporting hateful and abusive speech to Internet companies and countering offending speech with speech that challenges the message of hate. This report also walks readers through the reporting process for leading social media platforms and provides specific examples of counterspeech that have been used to respond to hateful speech. When done right, both reporting and counterspeech can be effective methods to combat online hate.

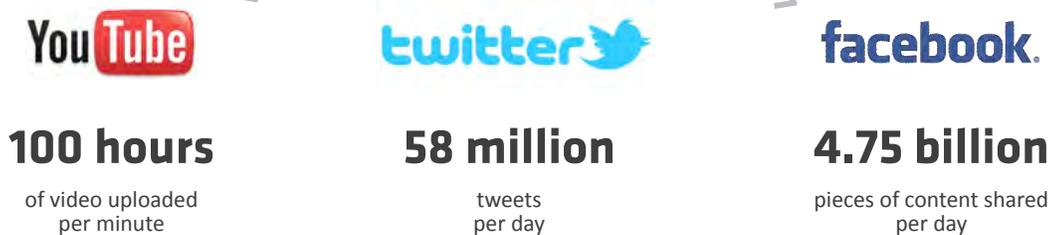
This report focuses on anti-Muslim content found on Facebook, YouTube, and Twitter because they are three of the largest social media platforms in the U.S. today. However, there are many websites and platforms in use, all rising and falling in popularity, and all with their share of users and posts expressing hateful or bigoted views. This report highlights some prominent examples of anti-Muslim animus online, with the goal of empowering users to respond to such views regardless of site, application, or platform.

**This report is designed to be a guide for:**

- Anyone who uses the Internet and social media platforms to communicate with friends and colleagues;
- Leaders of mosques or other faith and civic organizations that use social media sites to publicize events and share updates;
- Parents who have children who use the Internet and social media; and
- Students in middle school, high school, or college using social media for daily interactions with their peers.

# WHAT ANTI-MUSLIM HATE ONLINE LOOKS LIKE: THE HATE FEED

Every minute 100 hours of video are uploaded to YouTube,<sup>6</sup> and every day there is an average of 58 million tweets<sup>7</sup> and about 4.75 billion pieces of content shared on Facebook.<sup>8</sup> Given the staggering amount of content created, uploaded, or posted online, it is impossible for social media companies to proactively review each piece of content found on their platforms. In addition, the mass accessibility of social media sites makes it difficult to know exactly how many pieces of anti-Muslim hate are transmitted every second of every day. But we do know, even anecdotally, that the problem exists in many different forms.



Some of the most problematic perpetrators of online hate are public officials, hate groups and anti-Muslim activists, and private individuals. The following pages include examples of their hateful content.

## Online Hate by Public Officials

We have entrusted public officials with the responsibility to uphold and enforce our laws, including freedom and equality for Americans of all faiths. In recent years, however, public officials have engaged in offensive and dangerously misinformed dialogue about Islam and Muslims. In 2011, U.S. Representative Peter King (R-NY), then-Chair of the U.S. House Committee on Homeland Security, held a series of hearings that were intended to further stoke suspicion of American Muslims as a threat to our nation's security.<sup>9</sup> The next year, U.S. Representatives Michele Bachmann (R-MN), Trent Franks (R-AZ), Louie Gohmert (R-TX), Thomas Rooney (R-FL), and Lynn Westmoreland (R-GA), requested that the State, Homeland Security, Defense, and Justice Departments investigate American Muslims working within those agencies, calling into question their loyalty to the United States.<sup>10</sup> In 2013, U.S. Senator Rand Paul (R-KY) alleged that Muslims have waged a "worldwide war on Christianity" and that "Christians should be prepared for war."<sup>11</sup>

When public officials make bigoted statements, particularly on their own social media pages or accounts, their comments can be viewed by hundreds of thousands of people instantly. Such rhetoric and sentiment shapes public opinion, sending a clear message that it is appropriate to demonize—and even engage in an act of violence against—a group of Americans simply because of their faith.

The following are some examples of how public officials use social media to promote anti-Muslim views.

## Barry West

**Barry West**, a county commissioner in Coffee County, Tennessee, posted the adjacent image and caption in April of 2013.

The post suggests that Muslims should be targeted and shot. When asked about the image, Commissioner West said: “I’m prejudiced against anyone who’s trying to tear down this country, Muslims, Mexicans, anybody.”<sup>12</sup> Apart from the obvious bigotry underlying the sweeping statement that people of the Islamic faith or of Mexican national origin are trying to hurt America, his post was particularly troubling for Muslims in Tennessee, who have witnessed a string of hate crimes targeting their community in recent years.<sup>13</sup> The Islamic Center of Murfreesboro in Rutherford County, Tennessee, which has faced severe opposition to its construction and development, including repeated vandalism of signs on its property, arson, and a bomb threat, expressed concerns that Commissioner West’s post incites further hatred and violence against American Muslims.<sup>14</sup>

facebook.



### DOCUMENTING HATE TO EDUCATE

In February 2011, **protesters gathered outside the Yorba Linda Community Center in Orange County, California**, the location of a Muslim charity event. During the rally, Councilwoman Deborah Pauly made a number of anti-Muslim and threatening comments, including that she knew “quite a few Marines who [would] be very happy to help these terrorists to an early meeting in paradise.”<sup>15</sup> Protesters also used hateful and inflammatory language to denigrate Prophet Muhammad<sup>16</sup> and Islam such as “Muhammad was a child molester, Muhammad was a pervert . . . Muhammad was a fraud . . . Muhammad was a false prophet.” The protest and comments created fear and intimidated the men, women, and children walking past the protest to enter the event hall. Subsequently, the Greater Los Angeles Area office of the Council on American-Islamic Relations (CAIR-LA) uploaded a video entitled “Hate Comes to Orange County” on YouTube to inform people about Pauly’s statements and the protest. This is an example of how to turn an incident of hate into an opportunity to educate others.



YouTube

Hate Comes to Orange County

815,556

1,844 5,474

# Scott Desjarlais

Also in Tennessee, U.S. Representative **Scott Desjarlais (R-TN)** posted on Facebook his “deep” concerns regarding approval of the Islamic Center of Murfreesboro’s cemetery in his district. The negative sentiment Rep. Desjarlais directed at the mosque’s facility provided a convenient opportunity for others to use his Facebook page as a place to display their bigotry.



**Scott Desjarlais**  
January 24 · 🌐

Like Page

Friends, I have received numerous calls over the last couple of weeks regarding the Murfreesboro mosque cemetery. Although this is a state issue, I am deeply concerned over the impact it might have on our community. Unfortunately the Tennessee Religious Freedom Act, passed by the TN General Assembly, may have played a key role in allowing this cemetery to be approved. There is a difference between legislation that would protect our religious freedoms and legislation that would allow for the circumvention of laws that other organizations comply with on a daily basis.



**Murfreesboro mosque cemetery approved**  
The Rutherford County Board of Zoning Appeals approved the Islamic Center of Murfreesboro cemetery request Wednesday night.  
THE TENNESSEAN

Like · Comment · Share

125 people like this.

22 shares

**Gary Gill** What's next? Sharia law?  
January 24 at 10:30am · Like · 6

## facebook.

These are just a few examples of the views expressed in response to Representative Desjarlais’ post:



**Douglas Smith** YUP< Sharia law around the corner, but it will be hard to enforce with true Tennesseans, as far as the cemetery, isn't there a dump near the VA?  
January 24 at 10:33am · Like · 6

**Bethany Martin** Why did the state allow a mega mosque to begin with. They are hubs for t\*rr\*rism. Something needs to be done about those t\*rr\*r training camps around the country. There is one near Oak Ridge.  
January 24 at 10:37am · Edited · Like · 6

**Paul Ballard** If you people would read the Quran you would know a lot of what they believe in is illegal in the United States. They don't like Christian. They want to take over the world. The mosque and the muslim's and Islam and the cemetery should not be in the United States Of America. Scott and all American's better wake up.  
January 24 at 11:11am · Like · 6

**Chad Johnson** islam is not a religion, and they dont bury their dead correctly and it could have adverse effects on the water tables and be a health issue...I advise we litigate this out until they cant afford to build it, should be no problem finding lawyers to do that.  
January 24 at 12:07pm · Like

**John Crotty** Wrong, Don. you are being LIED to. Muhammed is the "perfect human example" according to Haddith. So, a raping murdering, illiterate pedophile is their "example". You need to educate yourself as to what this "religion" really says  
January 24 at 2:01pm · Like · 3

# Speech By Hate Groups & Anti-Muslim Activists

Hate groups were among the Internet’s earliest users,<sup>17</sup> and today their presence online is unwavering. There were an estimated 11,500 hate-related sites including websites, social network pages, chat forums, and micro-blogs in 2010.<sup>18</sup> The Southern Poverty Law Center, which tracks hate groups, has identified a number of active anti-Muslim hate groups,<sup>19</sup> many of which have used the Internet and social media platforms to spread their destructive agendas.

## Stop Islamization of America

**Stop Islamization of America (SIOA)**<sup>20</sup> has propagated fear and falsehoods about Islam and Muslims since its formation in 2009. One of the group’s early initiatives involved a highly publicized campaign in New York opposing Park51, a Muslim community center in lower Manhattan.<sup>21</sup> More recently, SIOA ran a series of anti-Muslim ads on public transportation in major cities including New York, San Francisco, and Washington, D.C. One ad read: “In any war between the civilized man and the savage, support the civilized man. Support Israel. Defeat Jihad.”<sup>22</sup>



Stop Islamization of America

facebook.

Group: **18,238** Members

Page: **18,492** Likes | **1,508** Talking about



**1,153** Followers

SIOA’s Facebook page recently linked to a blog post by activist Pamela Geller (see adjacent image), discussing a Muslim woman’s lawsuit against a gym that would not allow her to wear a headscarf while exercising. In response, users made degrading comments.



**Stop Islamization of America** shared a link. Like Page  
March 20 · 🌐

**New Mexico Muslima Sues Planet Fitness for Headgear Safety Rules**  
Another day, another Muslim supremacist lawsuit. Obviously head gear is prohibited in this gym because it presents a safety hazard. But people's safety be damned. Islam abrogates everyone and everything....

Like · Comment · Share

👍 25 people like this.  
↪ 5 shares

**Phillip F. Formicola** Fat fugly dog...  
March 20 at 5:34pm · Like · 👍 2

**Michael Keller** stealth jihad  
March 20 at 6:52pm · Like · 👍 1

**Kathy Spurgeon** Sick of these whiners aways b\*tching about something! Get the H out of our country if it doesn't suit you!  
March 20 at 6:58pm · Like · 👍 1

**William Bush** You won't need headgear, if you don't have a head.  
Forum for Middle East Understanding has released a current article on human slaughter by Muslims, for purposes of Islamo-cannibalism:... [See More](#)  
March 20 at 7:47pm · Like

**Mike Heins** The religion of hatred is at it again  
March 20 at 9:52pm · Like · 👍 1

**Andrew Edward Briseno** Never hire a stinking bag scum....  
March 21 at 1:53am · Like

## United States Defense League

United States Defense League (USDL) was founded in 2012 with a mission to “educate and unite Americans on understanding Islam and exposing Sharia Law for the inhumane treatment of women, honor killings, teaching Islam in public schools and other stealth ways it is creeping in to our society.”<sup>23</sup>



United States Defense League

facebook.

22,964 Likes

6,959 Talking about

The page has become a repository for anti-Muslim views, including genocidal references to Muslims. Below are examples of comments by individual users on USDL's Facebook page:



## The Counter Jihad Report

www.counterjihadreport.com

A blog entitled, “The Counter Jihad Report,” with over 990,000 hits since 2011, has countless posts filled with anti-Islam and anti-Muslim ideas. The Counter Jihad Report Facebook page states that “**Islam is at war with Western Civilization**” and calls upon followers to educate themselves, share what they have learned and “get involved.”<sup>24</sup>



In a blog post titled “No Common Ground,” one of many discussing opposition to the Islamic Center of Murfreesboro in Tennessee, the author states: “**The barbaric ideology of Islam can no longer be tolerated in America, and we must facilitate its change or its self-destruction through direct ideological and philosophical confrontations.**”<sup>25</sup> Opponents of the mosque filed a private lawsuit to block the Center's construction, arguing that Islam is not a religion. The U.S.

Department of Justice later intervened to enforce the Religious Land Use and Institutionalized Persons Act, a federal law that protects religious institutions from unduly burdensome land use regulations.

## Bare Naked Islam

www.barenakedislam.com

A blog named “Bare Naked Islam,” which is hosted by WordPress.org<sup>26</sup> and has over 51 million reported hits<sup>27</sup> since 2008, states that it is designed to show readers and viewers the “dark side of Islam.”<sup>28</sup>



### ONLINE HATE GOES BEYOND THE WEB

In January of 2013, law enforcement authorities planned to offer heightened protection for Muslims taking part in “Texas Muslim Capitol Day” at the state Capitol in Austin after being notified of threats made on the notorious anti-Islam blog Bare Naked Islam.<sup>29</sup> Threats included statements such as the ones to the right.

In November of 2011, Bare Naked Islam was criticized for allowing individuals to make comments threatening mosques, particularly a mosque in Falls Church, Virginia. For example, one individual claiming to have issues with the mosque wrote, “I want Muslim blood on my hands.”

A big bunch of muzzies all in one place eh?? Why not give em a warm Texas welcome . . . How do you Americans say? LOCK AND LOAD!

Call out the texas militia and kill or capture all participants. What in hell is going on in texas?

Screw Moderation!! Every One of them should be looking over his/her shoulder.

Comments posted on [barenakedislam.com](http://barenakedislam.com)

## Blogs and websites dedicated to spreading anti-Muslim hate

www.jihadwatch.org  
 freedomdefense.typepad.com  
 atlasshrugs2000.typepad.com  
 muslimsagainstsharia.blogspot.com  
 www.actforamerica.org

The following are examples of well-known anti-Muslim activists with a significant online presence through various web pages they use to gather supporters and spread hate.

## Pamela Geller & Atlas Shrugs

Pamela Geller is a well-known figure in anti-Muslim activist circles. Geller founded “Atlas Shrugs,” a blog she uses to voice hateful conspiratorial views about Islam and Muslims.<sup>30</sup> In 2010, she partnered with fellow anti-Muslim activist, Robert Spencer, to lead SIOA. Through her work with SIOA, Geller became known as the public face of opposition to the Park51 community center in New York.<sup>31</sup> She has also made many appearances on Fox News to comment on Islam, Sharia (i.e., Islamic religious law), and the supposed threat they pose to American values.<sup>32</sup>



*Pamela Geller*

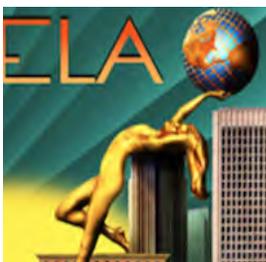
**facebook.**

78,968 Likes

35,151 Talking about

**twitter**

41,496 Followers



*Atlas Shrugs*

**twitter**

13,216 Followers

### Anti-Muslim Hater Geller’s Post Inspires Plot to Bomb Mosque

Robert James Talbot, Jr., created a Facebook page called American Insurgent Movement (AIM) and sought to recruit like-minded people interested in “walking away from [their lives] . . . to stop the regime.”<sup>33</sup> He used the page to solicit supporters, discuss what he planned to do, and to share his hateful opinions. After Pamela Geller posted information on her blog about construction plans for a new mosque in Memphis, Tennessee,<sup>34</sup> AIM linked to the post on its Facebook page, describing it as a “mission”:



On March 27, 2014, FBI agents arrested Talbot in Texas for allegedly plotting to use explosives and weapons to blow up mosques and other buildings.<sup>35</sup>

## Brigitte Gabriel & ACT! for America

Brigitte Gabriel is the founder of ACT! for America and the author of two controversial books portraying Islam as a threat to America, *Because They Hate: A Survivor of Islamic Terror Warns America* and *They Must Be Stopped: Why We Must Defeat Radical Islam and How We Can Do It*.<sup>36</sup> Gabriel believes that all



Brigitte Gabriel

Muslims are radical, and devout Muslims are terrorists.<sup>37</sup> *The New York Times* has said about Gabriel: “She presents a portrait of Islam so thoroughly bent on destruction and domination that it is unrecognizable to those who study or practice the religion.”<sup>38</sup>



ACT! For America

Gabriel has used her Twitter account to talk about Islam as a threat and the diverse support for ACT! for America, as shown in the images to the right.



facebook.

83,998 Likes  
50,924 Talking about

ACT! for America was founded in 2007 and purports to defend Western civilization, “as opposed to the authoritarian values of Islamofascism, such as the celebration of death, terror, and tyranny.”<sup>39</sup> ACT! for America claims to have over 875 chapters around the country with 279,000 members. The group actively grows its base, including hosting a series of meetings and trainings about best practices and communicating anti-Muslim messages.<sup>40</sup> ACT! for America also participates in many leading conferences and Tea Party events around the country to reach broader audiences.<sup>41</sup>



YouTube

Person at ACT! for America Table in Fla. Brags of Desecrating Quran

9,534  
24 38

A video uploaded to YouTube captures on audio an individual at an ACT! for America information table in Florida stating in part:

“Their foot baths, I love pissing in them . . . The Qur’an makes worthless toilet paper. It just kind of scratches my ass a little bit.”<sup>42</sup>

## Pastor Terry Jones of Stand Up America

Pastor Terry Jones of Stand Up America declared the 2010 anniversary of 9/11 “International Burn a Koran<sup>43</sup> Day.”<sup>44</sup> President Barack Obama, U.S. military leadership, and U.S. State Department officials all condemned his plans,<sup>47</sup> and the fire department in Gainesville, Florida, refused to give him a permit for the event.<sup>46</sup> While his plans for 2010 were eventually called off, Jones again advocated for a worldwide “burning of Korans” in 2012 and proceeded to organize events in various cities around the country. One of these instances, which concluded with a burning ceremony involving the Qur’an and an image of Prophet Muhammad, was captured on video and uploaded to YouTube.<sup>47</sup>

### ISLAM’S HOLY BOOK

Muslims believe that the holy book of Islam, the Qur’an, contains the word of God, so any attempt to desecrate it is viewed as extremely offensive and threatening to Muslims all over the world. In fact, many Muslims believe that desecrating any holy book is offensive.



Worldwide Burning of Korans and Muhammad by Dr. Terry Jones

69,605

381 likes 724

1,175 comments

The video has been viewed over 69,000 times and has nearly 1,200 comments, including “Muslims should not be allowed in America, they are terrorist,” “muslim mudafuckas should carry a terrorist prevention bracelet with a GPS on it everytime you enter the civilized west,” “burn them and burn them all!” and “Its high time we end them before they end us.”

- Ryan Rich** 5 months ago *in reply to Dax Santos*  
Fuck mecca, mekkah, or meco, however you spell that SHIT. Ain't nobody trying to go there and see a fucking rock and a bunch of zombies praying to it. And you dax santos, since non-muslims are not allowed in mecca, muslim mudafuckas should carry a terrorist prevention bracelet with a GPS on it everytime you enter the civilized west. Why should we be tolerant to the intolerant muslim rats, rouches, pigs, animals, cavemen that don't even let their women drive??? fuck them, don't let them in LOL
- Ryan Rich** 7 months ago  
cristians are not allowed in Saudia Anibia, Muslims should not be allowed in America, they are terrorist
- Suko Dan** 1 year ago  
burn them and burn them all!
- bary1234** 1 year ago  
Religions are poison. These idiotic sick superstitious cults have dragged humanity down for too long. Its high time we end them before they end us.

### REVISITING THE INNOCENCE OF MUSLIMS

In the film, which dramatizes the life of Prophet Muhammad,<sup>48</sup> he is portrayed “as a child of uncertain parentage, a buffoon, a womanizer, a homosexual, a child molester and a greedy, bloodthirsty thug.”<sup>49</sup>

Depictions, portraits, or images of the Prophet Muhammad are considered disrespectful and traditionally prohibited in Islam.



This image has been modified from its original format.

## ANTI-MUSLIM HATE ON FACEBOOK

facebook.

Examples of Facebook pages that have been created to spread anti-Muslim bigotry.



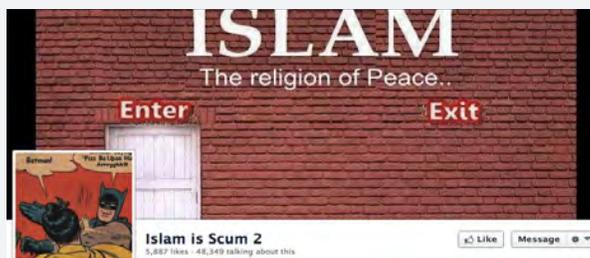
**Allah Sucks**  
9,516 Likes | 2,603 Talking about



**Anti-Islam Alliance**  
21,137 Likes | 892 Talking about



**Ban Islam and Sharia Law Worldwide**  
10,412 Likes | 33 Talking about



**Islam is Scum 2**  
5,887 Likes | 48,349 Talking about

As of July 17, 2013.

## Online Hate by Individuals

Individuals are often inspired to spread hate after engaging or interacting with anti-Muslim activists and groups online.

### Erik Rush

In the immediate aftermath of the Boston Marathon bombings in 2013, before the perpetrators had been identified, frequent Fox News contributor Erik Rush posted tweets blaming Muslims for the attacks and declared, “**Let’s kill them all.**” Within seconds the tweets reached his 12,000-plus Twitter followers, though Rush later tweeted that his remarks were sarcastic.<sup>50</sup>



Even if these statements have little effect when uttered as the opinion of a private individual, statements coming from a TV media correspondent undoubtedly have greater impact and can encourage others to act on a hateful message.



### Pat Dollard

Immediately after a deadly shooting at Fort Hood, Texas, on April 2, 2014, a conservative documentary filmmaker and former Breitbart News contributor, Pat Dollard, called for Americans to “**start slaughtering Muslims in the streets**” on Twitter.<sup>51</sup>



Despite pressure from fellow Twitter users, Dollard’s tweet has not since been removed.

#### ANTI-MUSLIM HATE ON TWITTER

##### HASHTAGS

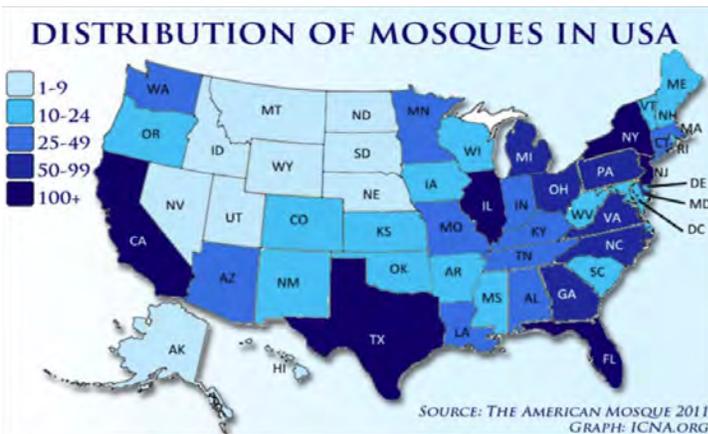
- #bansharia
- #bantheburqa
- #banmosques
- #ihatemuslims

##### HANDLES

- @killmuslims
- @BanSharia
- @ihateislam
- @creepingsharia
- @jihadwatchRS
- @MuslimsSuck

**facebook.**

Threats to mosques and holy sites have also appeared online. For example, in response to a photo posted on a Facebook user’s page depicting the distribution of mosques in America, one individual wrote “let them put one in upstate south carolina an **we wil [sic] burn it down.**”



- 

**Doug Williams** Biggest state by sq mi south of Alaska, 26 million people, and hey it's a free country, you can come in illegally, move from state to state without a passport.....but we might not be free much longer  
Like · Reply · ♡ 3 · March 5 at 6:23am
- 

**Rovia Tourist** I agree its a Cult  
Like · Reply · ♡ 3 · March 4 at 6:24pm
- 

**Mike Pearson** let them put one in upstate south carolina an we wil burn it down.  
Like · Reply · ♡ 6 · March 4 at 5:50pm
- 

**Carman Defendthe Constitution** does it concern others as it does me, that the position of the states with the most mosques are key to a MAJOR terrorist attack.....northeast.....southeast.....texas.....california.....illinois.....there aren't enough people in the upper plain states for them to mess with.....this should be a wake up call to all.....this administration has let them infiltrate our own government too.....  
Like · Reply · ♡ 2 · March 6 at 6:22am
- 

**Diane Johnson** I don't understand why Texas has the most of them  
Like · Reply · ♡ 4 · March 4 at 5:38pm
- 

**MiddleEast ForJesus** Due to Islams brutality, it should not be recognized as a religion at all. It is a political machine meant to conquer the whole world and rule with Sharia Law. Those who voted for Obama and the Democratic party got what they

**facebook.**

The photo below was posted on a Facebook page and depicted a violent attack in Mecca, Saudi Arabia, where millions of Muslims travel every year to perform Hajj, or pilgrimage—one of the five core acts of faith for adherents of Islam. Comments such as “One of the best solutions to solve a worse threat,” “I wish,” and “**shoulda been a nuke**” were left in response.



- 

**Omega Jin** ▸ Allah Sucks  
December 19, 2012

Like · Comment · Share

15 people like this.

76 shares
- 

**Omega Jin** ONE OF THE BEST SOLUTIONS TO SOLVE A WORSE THREAT....  
December 19, 2012 at 9:06am · Like · ♡ 6
- 

**George Smith** I wish!!  
December 19, 2012 at 1:31pm via mobile · Like · ♡ 1
- 

**Philip K. Eyrich** Allah! So that's the Mecca-nism for peace!  
December 19, 2012 at 2:28pm · Like
- 

**Christafari Baqe** Peace n love gift 4rm america  
December 19, 2012 at 5:56pm · Like
- 

**Brent Ireland** shoulda been a nuke  
December 19, 2012 at 10:31pm · Like
- 

**Thomas Lind** very nice

## ATTACKS ON MUSLIMS, MOSQUES, AND ISLAMIC INSTITUTIONS

According to the latest FBI hate crimes statistics, the number of attacks on Muslims, mosques, and Islamic institutions throughout the country has spiked to alarming levels since 9/11. Twenty-eight hate crimes targeting American Muslims were reported in 2000, and just one year later that number increased to 481.<sup>52</sup>

While the number of hate crimes reported declined after 2001, they began to rise again in 2010, increasing by 50% in the past few years.<sup>53</sup> Hate crime rates are now 5 times greater than before 9/11.

In addition, since 2010, opposition to mosques has also grown, often resulting in vandalism or arson. In 2012 alone, during the month of Ramadan, when Muslims all over the world refrain from food and drink until after sunset, a man vandalized a sign in front of a mosque in North Smithfield, Rhode Island, and a suspected arson attack burned the Islamic Society of Joplin in Missouri to the ground. Just one month later, a fire was deliberately set in the prayer area of the Islamic Center of Toledo in Ohio, the third largest mosque in the U.S. These incidents came on the heels of a tragic shooting in Oak Creek, Wisconsin, where a white supremacist opened fire on worshippers at a Sikh gurdwara, killing six people and injuring many others.

2000

**28**

hate crimes reported

2001

**481**

hate crimes reported

### facebook.

The photo below was posted on a Facebook page entitled, “**Ban Islam,**” and solicited input from followers about a young Muslim woman wearing a headscarf with the American flag printed on it to celebrate Independence Day. In response, Facebook users threatened violent attacks on the young woman for wearing the headscarf. For example, one user said: “I’d be in the news for snatchin it off her head.” **Two users commented that they would choke the young woman with the scarf she was wearing.**



**Ban Islam**  
Like This Page · 2 hours ago

to our American members: what would you do if you saw this?

Like · Comment · Share

65 people like this.

20 shares

- Dave Gee** thats utter disrespect!!!  
2 hours ago · Like · 6
- Pat St-Pierre** ?????  
2 hours ago · Like · 1
- Bender Bot** Id give her a towel and rip that flag off her head. She wouldnt do anything about it.  
2 hours ago via mobile · Like · 4
- Ganit Bas Noach** I'd be in the news for snatchin it off her head.  
2 hours ago · Like · 9
- Elijah Abascal** Wow...that is infuriating.  
2 hours ago via mobile · Like · 2
- Jaina Proudmoore** Choke the bitch with it!  
2 hours ago · Like · 6
- Jordan Stransky** Spartan kick her twat  
2 hours ago via mobile · Like · 6
- Neil Murphy** snatch it and half her greasy hair off with it....  
2 hours ago · Like · 3
- Ben Turner** choke the fucking cunt with it  
2 hours ago · Like · 12

### HIJAB (HEADSCARF)

Some Muslim women wear the *hijab, or headscarf*, as a form of modesty and refrain from exposing their hair in public. Therefore, asking a Muslim woman who wears the *hijab* to remove it would be considered disrespectful. Furthermore, purposefully removing a woman’s headscarf or threatening to remove it would be an offensive, intimidating, and violent act.

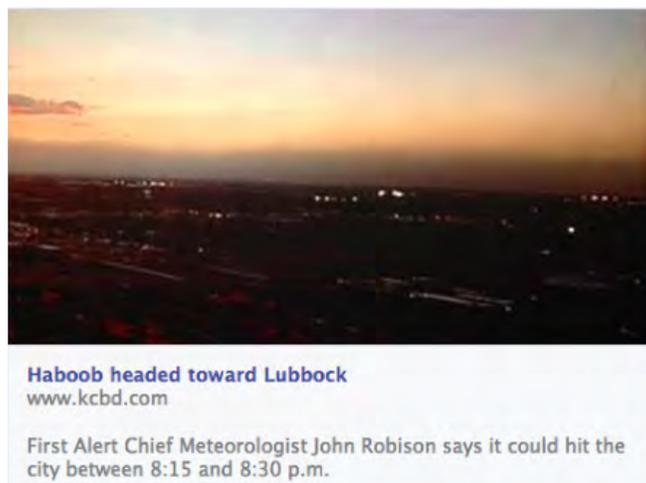
## facebook.

In response to a post on the Facebook page “Islam is Scum 2” regarding the Islamic holiday known as Eid al-Adha, which traditionally involves slaughtering animals for meat to be shared with family, friends, and those in need, one user wrote the following comment: **“The only blood I wanna see is that of a Muslims pouring from there black necks.”**



## facebook.

In Texas, a local news channel posted on its Facebook page that a *haboob*, or severe duststorm, was approaching Lubbock.<sup>55</sup> The word *haboob* is derived from an Arabic term that means “wind.”<sup>56</sup> The announcement was met with a number of bigoted comments including: “Since when do we need to apply a Muslim vocabulary to a good ole AMERICAN dirt storm??” and “It’s called a dust storm . . . Texas is not a rag head country.”<sup>57</sup>



### OSA at Islamic Mosque Little Rock

On September 14, 2012, a group of 20-30 individuals protested outside a mosque in Little Rock, Arkansas during the congregation’s Friday prayer. A video of their meeting after visiting the mosque can be found on YouTube.<sup>56</sup> The video included statements describing Islam as a “slavish” and “bondage” religion, as well as a declaration that the group has “got to nail this” religion and show Muslims that Christianity is special.

## VIRTUAL BECOMES REAL: BULLYING OF MUSLIM STUDENTS

There are real-life consequences to propagating hate on the Internet. When school children use social media websites to bully their classmates online, a phenomenon referred to as cyberbullying, it can aggravate tensions on school campuses and in classrooms. For example, Muslim high school students of Somali descent in Minnesota were targeted by another student who created a Facebook group called “I hate the Somalians [sic] at Tech High.” Unfortunately, this came as no surprise to some of the students since it was not uncommon for students to make disparaging remarks about their Muslim classmates.<sup>58</sup>

In another instance, a Muslim high school student was subjected to repeated bullying by classmates, including threats of violence on Facebook. Neither police nor school staff took action when she reported the harassing activity, and she was later attacked by the same students, suffering a concussion and bruising. One of her attackers later bragged about the incident on Facebook.<sup>59</sup>

# WHAT THE LAW SAYS

*“Congress shall make no law ... abridging the freedom of speech, or of the press ... ”*

## **First Amendment to the U.S. Constitution**

The starting point for understanding how online hate can be addressed is the First Amendment to the U.S. Constitution; however, it applies only to actions and restrictions imposed by government entities. The First Amendment prohibits Congress from making any law that interferes with freedom of speech and it has been interpreted to apply to all levels of government. Even when speech is offensive or disfavored, it will most likely be protected by the Constitution. Since the First Amendment was enacted in 1791, courts have generally been reluctant to create exceptions that chip away at its protections, particularly with regard to hate speech. For example, in 1977 the U.S. Supreme Court ruled that Skokie, Illinois, home to the highest per capita number of Holocaust survivors outside of Israel at the time,<sup>60</sup> could not stop a “Nazi parade” from marching through the streets simply because of the content of its message.<sup>61</sup> In a later case, the Court noted that it cannot permit the government to impose special prohibitions on those who express disfavored views.<sup>62</sup>

While most forms of public expression are afforded robust protection, the right to free speech is not absolute.<sup>63</sup> Narrowly defined exceptions to First Amendment protections<sup>64</sup> include: false statements of fact in limited circumstances<sup>65</sup> (e.g., libel<sup>66</sup>), obscenity,<sup>67</sup> child pornography,<sup>68</sup> and commercial speech.<sup>69</sup> The exceptions most relevant to hate speech are highlighted below:

### **Incitement**

The First Amendment protects speech that abstractly advocates for the use of force or violence, unless that speech is “directed to inciting or producing imminent lawless action” and is “likely to incite or produce such action.”<sup>70</sup> For example, speech that advocates for evading a mandatory military draft that results in people actually breaking the law is not protected by the First Amendment.

Not all cases, however, are this clear. Take, for instance, *The Innocence of Muslims*, a short video maligning the Prophet Muhammad that went viral.<sup>71</sup> A court has not considered whether the film constitutes incitement under First Amendment law, but some argue that the film’s production and dissemination suggest “the aim was not just to air offensive views, but to do so in such a way as to ignite precisely the violence that in fact ensued.”<sup>72</sup>

### **“Fighting Words”**

Another exception to the First Amendment, which is related to but distinct from incitement, applies to “fighting words,” which the Supreme Court has defined as speech that “tend[s] to incite an immediate breach of the peace” by provoking a violent reaction.<sup>73</sup> The subtle distinction between inciting speech and fighting words lies in the speaker’s intent: inciting speech causes others to perform unlawful acts while fighting words are intended to cause one who hears the words to react to the speaker. For example, speech that contains deeply abusive language, is exchanged face-to-face, and is likely to provoke a violent reaction will generally be considered unprotected speech under the “fighting words” exception.

### **Threats**

First Amendment protections are not afforded to true threats, or declarations of “intention to inflict punishment, loss, or pain on another, or to injure another by the commission of some unlawful act.”<sup>74</sup> The Supreme Court, however, has stated that threats *cannot* be punished if a reasonable person would understand them as obvious hyperbole.<sup>75</sup> With this exception, threatening messages sent online or via social media platforms can be prosecuted under the law if the recipient reasonably believes that the sender intends to put him or her at risk of harm.

#### **THREATS ONLINE**

If you have received a threat online and believe that **someone is attempting to harm you in any way**, report it to law enforcement immediately. Simply flagging or reporting the content online is not sufficient.

In sum, when speech falls under one of the specific exceptions listed above, it may be actionable.

### **WHAT IS HATE SPEECH?**

Hate speech is difficult to define, both within and outside of the law. Some define it broadly as speech that marginalizes an individual or a group of people. Others define it more specifically as speech that incites harm or prejudicial action against someone because of his or her race, religion, ethnicity, national origin, sexual orientation, or disability. However, even without a clear, universally accepted definition, hate speech is easily identifiable in many instances. The challenge with hate speech is often not how to define it but rather how it is treated under the law and by the social media platforms that some users employ to promote hate.

# WHAT INTERNET COMPANIES SAY ABOUT HATEFUL CONTENT

For a few reasons, online hate speech falls outside the First Amendment exceptions described in the previous section. For one, although the First Amendment prohibits certain government action that curtails speech, it does not stop private entities or companies from restricting speech. As a result, virtually all social media companies have created terms of service agreements or user policies that address hateful or abusive speech. They have also developed ways to monitor and remove content that violates their policies. These companies strongly believe in the free marketplace of ideas inspired by First Amendment principles, but they are also committed to user safety.

Internet companies have differing user policies. For example, as shown on the following page, Facebook is committed to creating a safe and respectful community online and has an explicit policy prohibiting hate speech. Its policy does “not permit individuals or groups to attack others based on race, ethnicity, national origin, religion, sex, gender, sexual orientation, disability or medical condition.”<sup>76</sup> Similarly, YouTube does not permit hate speech.<sup>77</sup> In addition, Twitter currently maintains a more permissive policy that prohibits users from publishing “direct, specific threats of violence against others.”<sup>78</sup>



## Hate speech

We encourage free speech and try to defend your right to express unpopular points of view, but we don't permit hate speech.

Hate speech refers to content that promotes violence or hatred against individuals or groups based on certain attributes, such as:

- race or ethnic origin
- religion
- disability
- gender
- age
- veteran status
- sexual orientation/gender identity

There is a fine line between what is and what is not considered to be hate speech. For instance, it is generally okay to criticize a nation-state, but not okay to post malicious hateful comments about a group of people solely based on their race.<sup>79</sup>

In addition, even if First Amendment protections governed online speech, most instances of hate speech would not fall under the narrow exceptions described above. Some online speech may be extremely offensive, but only rarely is it likely to incite unlawfulness or tend to cause a reader to respond with violence. Arguably, such speech is threatening but does not rise to the level of a "true threat" that will cause someone to reasonably believe he or she is in danger. Furthermore, the anonymity of many Internet users presents a practical limitation: if we don't know who the speakers are, we cannot hold them accountable.



## Hate speech

Facebook does not permit hate speech, but distinguishes between serious and humorous speech. While we encourage you to challenge ideas, institutions, events, and practices, we do not permit individuals or groups to attack others based on their race, ethnicity, national origin, religion, sex, gender, sexual orientation, disability or medical condition.<sup>80</sup>



**Violence and Threats:** You may not publish or post direct, specific threats of violence against others.<sup>81</sup>

### PROTECTING MINORS: "ERASER LAW"

Some states have passed legislation that address very limited circumstances surrounding online speech. For example, California recently passed a law that would require Internet companies to take down something a minor has posted online if that minor requests it. This "eraser law" is set to go into effect in 2015.<sup>82</sup>

## WHAT USERS CAN DO

Although the law provides few remedies to victims of hate speech, there are important steps they and others who reject bigotry can take to address online hate. The two most effective responses are reporting hateful content to the social media companies on whose platforms the hate speech appears and engaging in counterspeech.

# Report Hateful Content

At any given minute, there are millions of people all over the world using the Internet and social media, sharing billions of pieces of content. Internet companies are not able to review all content before it is uploaded or posted. Instead, they rely on their users to report content to them if they believe it violates the companies' policies. Even if a user is not certain that a piece of content violates a policy, the user is encouraged to report it anyway, and many of the large Internet companies have designated teams to review the reported content and determine if it complies with their policies. Although reported content will not always be removed from social media platforms, user reporting helps inform companies about offensive content online and also holds Internet companies accountable to their policies.

Facebook, YouTube, and Twitter have their own reporting mechanisms, some of which are described, step-by-step, on the following pages.

## facebook.

If users see something they believe to be offensive or in violation of Facebook's Community Guidelines, the company suggests users report it and provides resources on how to do so.



**Reporting Abuse**

If you see something on Facebook that you believe violates our terms, you should report it to us. Please keep in mind that reporting a piece of content does not guarantee that it will be removed from the site.

Because of the diversity of our community, it's possible that something could be disagreeable or disturbing to you without meeting the criteria for being removed or blocked. For this reason, we also offer personal controls over what you see, such as the ability to hide or quietly cut ties with people, Pages, or applications that offend you.

- 1 The first step is to click on the arrow on the top right corner of the post and select the **"Report/Mark as Spam"** option.



- 2 Once that option is selected, users have the option to **"Undo"** or **"Report"** the content as abusive to Facebook.

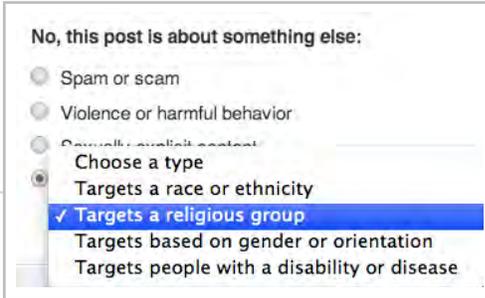


- 3 When **"Report"** is selected, users have the option to explain why they are reporting the content to Facebook: **"Is this post about you or a friend?"** Users may select **"Hate Speech"** as the reason for why the post is being reported.

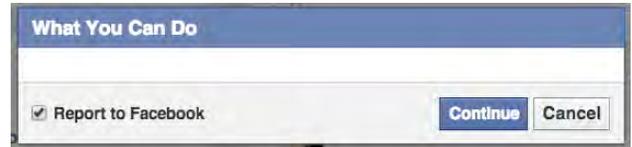


A screenshot of the Facebook reporting dialog. The title is "Is this post about you or a friend?". There are two main sections: "Yes, this post is about me or a friend:" and "No, this post is about something else:". Under the "Yes" section, there are radio buttons for "I don't like this post", "It's harassing me", and "It's harassing a friend". Under the "No" section, there are radio buttons for "Spam or scam", "Violence or harmful behavior", "Sexually explicit content", and "Hate speech". A separate box on the right titled "No, this post is about something else:" contains radio buttons for "Spam or scam", "Violence or harmful behavior", "Sexually explicit content", and "Hate speech", along with a "Choose a type" dropdown menu. At the bottom, there is a question "Is this your intellectual property?" and "Continue" and "Cancel" buttons.

4 Users also have the option to further explain what **type of hate speech** the post includes.



5 The final step is to select “**Report to Facebook**”.



Facebook has produced an infographic that lays out the process for reporting, and displays a wide variety of content that may be reported. This infographic is available on Facebook’s website.<sup>83</sup>



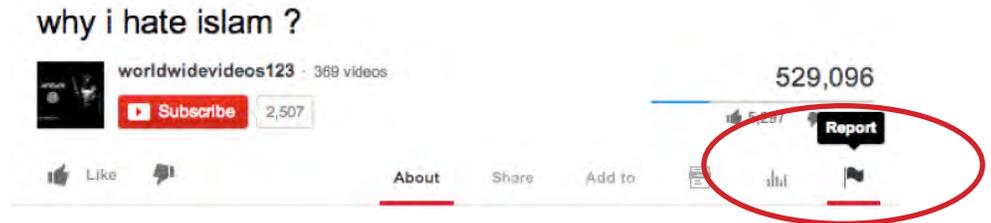
**FACEBOOK TAKES A CLOSER LOOK**

Facebook has recently taken a closer look at how people use reporting to resolve concerns with problematic posts. It has created and tested new user experiences that are designed to meet people’s concerns about the content they see and empower them to engage with those creating the content. Facebook reports that with these new experiences, people are ten times more likely to send a message to someone posting status updates they do not like. Furthermore, people who say their needs are met by Facebook’s reporting Teams are significantly more likely to send a message (42%) than report the status update to Facebook (17.7%). According to their own research, Facebook is helping 3.9 million people resolve disputes every week with social resolution tools that allow people to engage others about a piece of content that bothers them. For example, when one person confronts another about an embarrassing photo, the photo is removed or a conversation is started about 85% of the time. In addition, 90% of the people contacted by these messages feel positive or neutral about the person who sent the message. While this data focuses heavily on content that people see in their News Feed, and not on content that exists outside of their networks, it demonstrates Facebook’s commitment to understanding and addressing hate online without extraneously limiting content.<sup>84</sup>



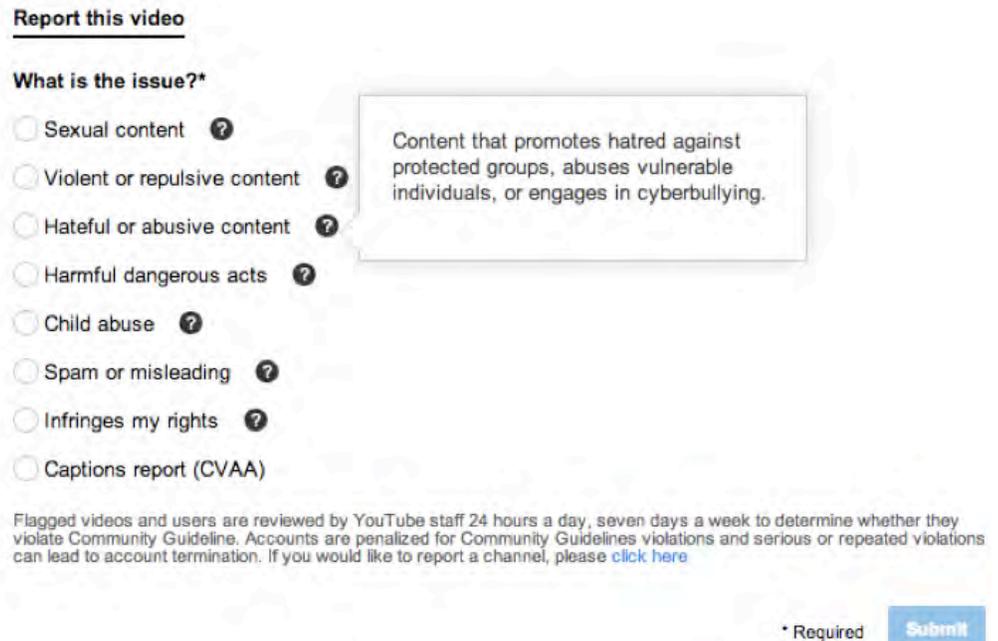
1

To report a video on YouTube, users should click on the flag icon in the bottom right corner of a video.



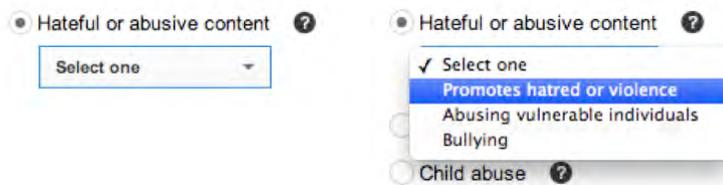
2

Users can select from a list of options to describe why the video is being reported.



3

After selecting “Hateful or abusive content,” users have the opportunity to further explain how the content is hateful.



4

Finally, users are asked to provide the timestamp and any additional details about the video to complete the report. This is an opportunity to explain in further detail why the content is offensive and a violation of YouTube’s policy.





- 1 To report abusive content on Twitter, users should go to the Help page and locate the section entitled, “Policies & Violations,” and then select the option for “**How to report violations.**”



- 2 Next, users should find the section relating to abusive behavior and violent threats. When reporting abusive behavior and violent threats, users have the option to report content, or learn more about Twitter’s policies and procedures.

#### **Abusive behavior and violent threats**

When reporting abusive behavior on Twitter, please provide the following:

- Description of problem, including length of time the abusive behavior has been happening
- Tweet URLs (to find the exact link of a Tweet, please review [this article](#))
- Tweet text (copy and paste the text of the Tweet into the form)
- Your email address

**Please note:** If you believe you may be in danger, please contact your local law enforcement authority in addition to reporting the content to Twitter so that the situation can also be addressed offline.

To report abusive behavior on Twitter, [click here](#).

For more information about Twitter’s abusive behavior policy, [click here](#).

For more information about reporting abusive behavior on Twitter, [click here](#).

3

After clicking the link provided to report content, users are directed to a form that asks for information pertaining to the offensive content, including when the problem began, the frequency of occurrences, and a link to the content being reported.

## I'm reporting an abusive user

Please fill out all the fields below so we can review your report.

For more information and resources on dealing with abusive users both on the internet and on Twitter, please review [this article](#).

- How can we help?
- Someone on Twitter is posting my private information.
  - Someone on Twitter is being abusive.
  - Someone on Twitter is sending me violent threats.

What username is causing the issue?

@

(e.g. @safety)

Please provide links to the Tweets you are reporting as evidence so that we can investigate. To find the exact link of a Tweet, please review [this article](#). You'll need to provide at least one direct link to the content you're reporting; more links are helpful to establish patterns.

### Tweet I am reporting

Link to Tweet

[Report another Tweet](#)

- What are you reporting?
- I think the user has multiple accounts they are using to directly @reply me and others.
  - This user keeps sending me @replies and I don't want to receive them.
  - This user is saying really offensive things, but is not sending me @replies.

Have you already blocked the person(s) involved?

- Yes
- No

How long ago did this begin?

- 24 hours ago
- Few days ago
- About a week ago
- About a month ago
- More than a month ago

How many times has this happened?

Further description of problem

Please provide as much detail as possible surrounding your issue. We are unable to accept attachments or screenshots related to your report. Please only provide links to exact Tweets or Twitter accounts.

Your full name

- I understand that Twitter may provide third parties, for example the reported user, with details of this report, such as the reported Tweet. Your contact information, like your email address, will not be disclosed.

Twitter username

@

Once the reporting process on Facebook, YouTube, or Twitter is complete, users will receive a response indicating the content they reported was either removed or not removed because it did not violate the company's policies. If you have reported content and it was not removed, contact Muslim Advocates and let us know about it.

## Engage in Counterspeech

*“If there be time to expose through discussion the falsehood and fallacies, to avert the evil by the processes of education, **the remedy to be applied is more speech, not enforced silence.**”<sup>85</sup>*

United States Supreme Court case *Whitney v. California*

Both legally and culturally, the country favors free expression. Bad speech should be countered with good speech, and false speech with truthful speech. The courts and civil society have long encouraged more speech as a response to offensive speech. When offensive, hateful content appears on a website or social media platform, a common and effective response is counterspeech.

The following are examples of effective counterspeech<sup>86</sup> campaigns in response to bigotry online.



### #myNYPDfile

In February 2012, the Associated Press published online the documents supporting its prior reporting that the New York Police Department (NYPD) has been spying on Muslims in New York and throughout the Northeast.

On Twitter, users responded with humor, mocking the ill-advised, blanket surveillance program.

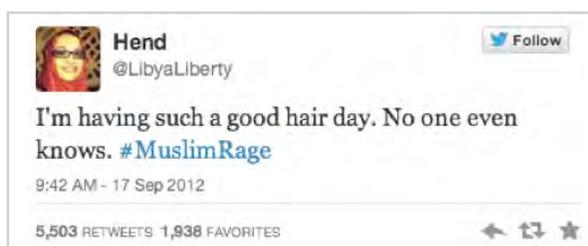




## #MuslimRage

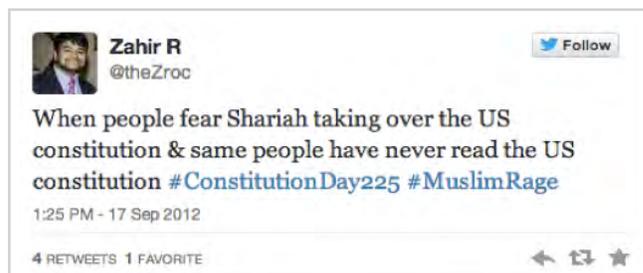
Shortly after protests broke out all over the world in response to *The Innocence of Muslims*, the American news media questioned why the film sparked such a violent response.<sup>87</sup> *Newsweek* published a cover story written by a Dutch-Somali critic of Islam, Ayaan Hirsi Ali, titled “Muslim Rage” with a photo depicting a group of angry Muslim men. The magazine also invited its Twitter followers to discuss the cover using the Twitter hashtag “#MuslimRage.”<sup>88</sup>

While the poorly chosen cover and hashtag perpetuated the stereotype of the angry, violent Muslim man, it became the subject of ridicule for many Twitter users. Soon users responded *en masse* by poking fun at the hashtag:



This week's Newsweek cover, on newsstands & the iPad today: #MuslimRage! Ayaan Hirsi Ali writes on how she survived it [pic.twitter.com/QPnIRtf9](http://pic.twitter.com/QPnIRtf9)

Reply Retweet Favorite More



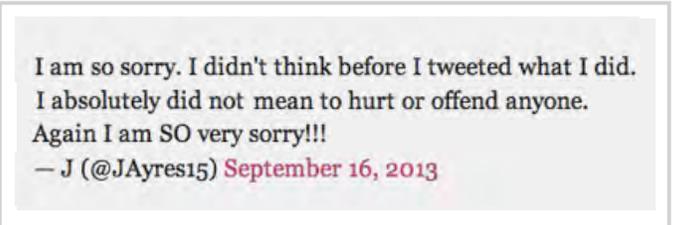
# Miss America Twitterstorm



When the winner of the Miss America 2014 pageant, Indian-American Nina Davaluri, was announced, Twitter users inundated the network with hateful tweets associating her with terrorism and al-Qaeda<sup>89</sup>:



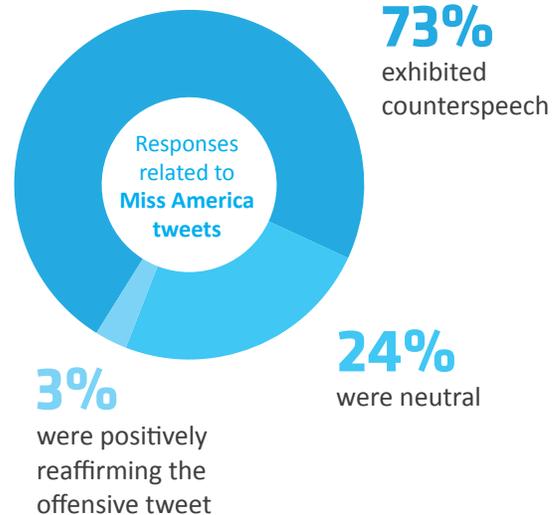
Other Twitter users quickly began engaging in counterspeech, causing some to apologize for their statements, as displayed below:



## Twitter Digs Deeper



Based on a quick scan of tweets related to Miss America shortly after her win was announced, Twitter noted that out of a small sample of 573 responses 73% exhibited counterspeech, 24% were neutral, and 3% were positively reaffirming the offensive tweet.<sup>90</sup> While none of Twitter's research is conclusive, it provides anecdotal evidence of the power in counterspeech. An example of this is described below in more detail.



@DallasRobinson8 tweeted the following:



However, due to reactions by people all over the world to his tweet, @DallasRobinson8 finally began to realize the hurtful nature of his tweet:



After being publicly shamed in international media, @DallasRobinson8 celebrated the coverage:

@DallasRobinson8 finally apologized to Miss America two days after his initial tweet:



The examples above demonstrate the **power in counterspeech** and how it can be used on social media platforms to change the course of dialogue.

# CONCLUSION & RECOMMENDATIONS

Our country's Founding Fathers could not have contemplated a nation where the speech of a single individual could be amplified throughout the country instantaneously, and echoed by others within seconds. But even though the speech of our time may be different from theirs, there is no doubt that free speech remains a bedrock principle of our society. Given today's widespread use of the Internet, all Americans should remain actively engaged and vigilant to prevent our freedom of speech from being abused.

**To address hate online, Muslim Advocates encourages and recommends that you do the following:**

**1) Learn About User Policies:**

Review the terms of service agreements or user policies for sites and platforms that you are using or about which you are concerned;

**2) Know & Use the Reporting Tools:**

Familiarize yourself with the tools that sites have put in place for reporting hateful content and use them if you believe something violates a company's guidelines;

**3) Respond to Hate with Effective Counterspeech:**

Consider opportunities to engage in counterspeech, using the examples highlighted above as a model for what you can do when you encounter hate speech online; and,

**4) Report Threats to Law Enforcement:**

If you have been the target of threats, report them to law enforcement immediately.

---

**Additional recommendations:**

**Parents and Students:**

- Engage school administrators about your concerns with the use of the Internet and social media platforms and the impact on your child at school;
- Immediately inform school administrators about bullying in school;
- Learn about the school's policies on cyberbullying or Internet use at school or during school hours in the event that a threatening or harmful situation involving other students arises; and,
- Visit the U.S. Department of Education website at [www.ed.gov](http://www.ed.gov) for more information about bullying.

**Leaders of Organizations:**

- If your organization has been a target of threats, inform law enforcement immediately;
- Share this report and engage your colleagues and members about the issues of hate online using the resources provided in this report; and,
- Create opportunities to engage with interfaith partners in your community and educate them and others about these issues.

**Internet Companies:**

- Develop and maintain an understanding of sensitivities that relate to American Muslims and other communities targeted by hate groups;
- Track and record the frequency at which reports are based on hateful content, particularly as it relates to a person's faith;
- Affirmatively state company policy on hate speech and threatening speech;
- Continue to enhance tools designed for reporting content;
- Review all content reported by users to determine whether content violates company policies; and
- Promptly notify users who have reported content violations of the outcome of the company's review and provide a clear explanation of the evaluation process used by the company.

**Policy Makers:**

- The White House should convene a national-level dialogue on hate against religious communities and invite Internet companies to participate in discussions addressing online hate.

**SHARE YOUR STORIES WITH US**

Let us know about examples of online hate so we can continue to monitor hate directed at the Muslim community. We also want to hear about your successes in reporting content or using counterspeech as a response to online hate.

# ENDNOTES

- <sup>1</sup> ROBERT P. JONES & DANIEL COX, PUB. RELIGION RESEARCH INST., OLD ALIGNMENTS, EMERGING FAULT LINES: RELIGION IN THE 2010 ELECTION AND BEYOND 17 (2010), *available at* <http://publicreligion.org/site/wp-content/uploads/2011/06/2010-Post-election-American-Values-Survey-Report.pdf>.
- <sup>2</sup> ABU DHABI GALLUP CENTER, RELIGIOUS PERCEPTIONS IN AMERICA: WITH AN IN-DEPTH ANALYSIS OF U.S. ATTITUDES TOWARD MUSLIMS AND ISLAM 7 (2009), *available at* [http://www.abudhabigallupcenter.com/File/144335/WorldReligion\\_Report\\_en-US\\_final.pdf](http://www.abudhabigallupcenter.com/File/144335/WorldReligion_Report_en-US_final.pdf).
- <sup>3</sup> *See, e.g.*, Bobby Ghosh, *Islamophobia: Does America Have a Muslim Problem?*, TIME, Aug. 30, 2010, <http://content.time.com/time/magazine/article/0,9171,2011936,00.html>.
- <sup>4</sup> *Social Networking Fact Sheet*, PEW RESEARCH INTERNET PROJECT, <http://www.pewinternet.org/fact-sheets/social-networking-fact-sheet/> (last visited Apr. 18, 2014).
- <sup>5</sup> ABRAHAM H. FOXMAN & CHRISTOPHER WOLF, VIRAL HATE 59 (Palgrave Macmillan 2013).
- <sup>6</sup> YouTube Statistics, YOUTUBE, <http://www.youtube.com/yt/press/statistics.html> (last visited Apr. 4, 2014).
- <sup>7</sup> Twitter Statistics, STATISTIC BRAIN, <http://www.statisticbrain.com/twitter-statistics/> (last visited Apr. 4, 2014).
- <sup>8</sup> Dan Noyes, *The Top 20 Valuable Facebook Statistics – Updated February 2014*, ZEPHORIA (Feb. 19, 2014), <http://zephoria.com/social-media/top-15-valuable-facebook-statistics/>.
- <sup>9</sup> Jordy Yager, *Lawmaker Announces Second Hearing Into Muslim-American Radicalization*, THE HILL, June 9, 2011, *available at* <http://thehill.com/homenews/house/165697-lawmaker-announces-second-muslim-radicalization-hearing->.
- <sup>10</sup> Lauren Fox, *Michele Bachmann Sticks To Accusations About Muslim Brotherhood*, U.S. NEWS & WORLD REP., July 19, 2012, *available at* <http://www.usnews.com/news/articles/2012/07/19/michele-bachmann-sticks-to-accusations-about-muslim-brotherhood>.
- <sup>11</sup> Dean Obeidallah, *Rand Paul’s Muslim-Bashing Speech*, THE DAILY BEAST, Oct. 14, 2013, <http://www.thedailybeast.com/articles/2013/10/14/rand-paul-s-hate-speech-sounded-just-like-al-qaeda.html>.
- <sup>12</sup> Nick Wing, *Barry West, Tennessee County Commissioner, Draws Backlash For ‘How To Wink At A Muslim’ Post*, HUFFINGTON POST, (May 1, 2013, 12:28 p.m.), [http://www.huffingtonpost.com/2013/05/01/barry-west-tennessee-muslims\\_n\\_3193600.html](http://www.huffingtonpost.com/2013/05/01/barry-west-tennessee-muslims_n_3193600.html).
- <sup>13</sup> Heidi Hall, *Middle TN Commissioner’s Facebook Post Frightens Muslims*, THE TENNESSEAN, May 1, 2013, <http://www.tennessean.com/article/20130501/NEWS02/305010108/Middle-TN-commissioner-s-Facebook-post-frightens-Muslims>.
- <sup>14</sup> Wing, *supra*, note 12.
- <sup>15</sup> CAIR LA, *Hate Comes to Orange County*, YOUTUBE (Mar. 2, 2011), <https://www.youtube.com/watch?v=NutFkykjmbM>.
- <sup>16</sup> Muslims customarily wish “peace and blessings” upon the mention of the name of the Prophet Muhammad.
- <sup>17</sup> Jason Chan et al., *The Internet and Hate Crime: Offline Spillovers from Online Access 2* (NET Inst., Working Paper No. 13-02, 2014), *available at* [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2335637](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2335637).
- <sup>18</sup> Steve Lohr, *Online Hate Sites Grow With Social Networks*, N.Y. TIMES BITS BLOG (Mar. 16, 2010, 9:28 AM), <http://bits.blogs.nytimes.com/2010/03/16/online-hate-sites-grow-with-social-networks/>.

- <sup>19</sup> List of Active Anti-Muslim Groups, SOUTHERN POVERTY LAW CENTER, <http://www.splcenter.org/node/3502/activegroups> (last visited Apr. 4, 2014).
- <sup>20</sup> SIOA is also known as the American Freedom Defense Initiative and it was founded as the U.S. branch of Stop Islamisation of Europe. Nathan Lean, *Expose the Islamophobia Industry*, N.Y. DAILY NEWS, July 9, 2012, <http://www.nydailynews.com/opinion/expose-islamophobia-industry-article-1.1109263>.
- <sup>21</sup> Profile of Pamela Geller, SOUTHERN POVERTY LAW CENTER, <http://www.splcenter.org/get-informed/intelligence-files/profiles/pamela-geller> (last visited Apr. 4, 2014).
- <sup>22</sup> Alex Davies, *Extreme Anti-Islam Ads Are Now Running On San Francisco's Buses*, BUS. INSIDER, Mar. 13, 2013, <http://www.businessinsider.com/anti-islam-ads-run-on-san-francisco-buses-2013-3>.
- <sup>23</sup> About Section of United States Defense League's (USDL) Facebook Page, FACEBOOK, <https://www.facebook.com/USDefenseLeague/info> (last visited Apr. 18, 2014).
- <sup>24</sup> Facebook Page for The Counter Jihad Report, FACEBOOK, <https://www.facebook.com/counterjihadreport> (last visited Apr. 24, 2014).
- <sup>25</sup> Justin O. Smith, *No Common Ground*, THE COUNTER JIHAD REPORT (Sept. 1, 2012), <http://counterjihadreport.com/2012/09/01/no-common-ground/>.
- <sup>26</sup> Note that WordPress.org is different from WordPress.com. WordPress.com has terms of service and allows people to report abusive content, however it does not have control over sites powered by WordPress.org as indicated on their website. *Dispute Resolution & Reporting*, WORDPRESS.COM, <http://en.support.wordpress.com/disputes/> (last visited Apr. 23, 2014).
- <sup>27</sup> This number is based on the figure reported on the website. BARE NAKED ISLAM, <http://www.barenakedislam.com> (last visited Apr. 23, 2014).
- <sup>28</sup> About Section of Bare Naked Islam's Webpage, BARE NAKED ISLAM, <http://www.barenakedislam.com/about/> (last visited Apr. 24, 2014).
- <sup>29</sup> *Threats Prompt Additional Security Measures for Texas Muslim Event*, NEWS 92 FM, Jan. 31, 2013, <http://news92fm.com/322713/threats-prompt-additional-security-measures-for-texas-muslim-event/>.
- <sup>30</sup> WAJAHAT ALI ET AL., CENTER FOR AM. PROGRESS, FEAR, INC. 89–90 (2011), available at <http://www.americanprogress.org/wp-content/uploads/issues/2011/08/pdf/islamophobia.pdf>.
- <sup>31</sup> *Id.* at 70.
- <sup>32</sup> SOUTHERN POVERTY LAW CENTER, *supra* note 21.
- <sup>33</sup> Amago, *Robert James Talbot Jr.: Radical-Right Terrorist Sought to Blow-up Mosques, Was A Fan of Pamela Geller*, LOONWATCH.COM (Apr. 3, 2014), <http://www.loonwatch.com/2014/04/robert-james-talbot-jr-radical-right-terrorist-sought-to-blow-up-mosques-was-a-fan-of-pamela-geller/>.
- <sup>34</sup> Pamela Geller, *Target Memphis: Another Massive Mega-Mosque Compound in Middle America*, PAMELA GELLER, ATLAS SHRUGS (Feb. 28, 2014), <http://pamelageller.com/2014/02/target-memphis-another-massive-mega-mosque-compound-middle-america.html/>.
- <sup>35</sup> Caitlin Dickson, *Far-Right Texas Terrorist Planned Murder And Robbery Spree in the Name of 'Liberty'*, THE DAILY BEAST, Apr. 1, 2014, <http://www.thedailybeast.com/articles/2014/04/01/far-right-texas-terrorist-planned-murder-and-robbery-sprees-in-the-name-of-liberty.html>.
- <sup>36</sup> Ryan Lenz, *Acting Out*, INTELLIGENCE REP., Fall 2011, available at <http://www.splcenter.org/get-informed/intelligence-report/browse-all-issues/2011/fall/acting-out>.

<sup>37</sup> *Id.*

<sup>38</sup> Laurie Goodstein, *Drawing U.S. Crowds With Anti-Islam Message*, N.Y. TIMES, Mar. 7, 2011, <http://www.nytimes.com/2011/03/08/us/08gabriel.html>.

<sup>39</sup> About Section of ACT! for America's Facebook Page, FACEBOOK, <https://www.facebook.com/actforamerica/info> (last visited Apr. 18, 2014).

<sup>40</sup> ALI ET AL., *supra* note 30, at 67.

<sup>41</sup> *Id.* at 67–68.

<sup>42</sup> CAIRtv, *Person at ACT! for America Table in Fla. Brags of Desecrating Quran*, YOUTUBE (Apr. 5, 2010), <https://www.youtube.com/watch?v=Xn5UfW6GOc4>.

<sup>43</sup> Note that the generally accepted spelling for Islam's holy book is "Qur'an," and not "Koran," which is used in Pastor Terry Jones' materials.

<sup>44</sup> Lynn Waddell, *Florida's Quran-Burning Pastor*, THE DAILY BEAST, Sept. 7, 2010, <http://www.thedailybeast.com/articles/2010/09/07/terry-jones-pastor-who-want-to-burn-qurans.html>.

<sup>45</sup> Ewen MacAskill et al., *Pastor Terry Jones Calls Off Qur'an Burning*, GUARDIAN, Sept. 10, 2010, <http://www.theguardian.com/world/2010/sep/10/pastor-terry-jones-quran-burning>.

<sup>46</sup> Waddell, *supra* note 44.

<sup>47</sup> StandUpAmericaNow, *Worldwide Burning of Korans and Muhammad by Dr. Terry Jones*, YOUTUBE (Apr. 28, 2012), <https://www.youtube.com/watch?v=tZk8do68JwE>.

<sup>48</sup> Robert Mackey & Liam Stack, *Obscure Film Mocking Muslim Prophet Sparks Anti-U.S. Protests in Egypt and Libya*, N.Y. TIMES THE LEDE BLOG (Sept. 11, 2012, 7:25 PM), <http://thelede.blogs.nytimes.com/2012/09/11/obscure-film-mocking-muslim-prophet-sparks-anti-u-s-protests-in-egypt-and-libya/>.

<sup>49</sup> Adam Nagourney, *Origins of Provocative Video Are Shrouded*, N.Y. TIMES, Sept. 12, 2012, <http://www.nytimes.com/2012/09/13/world/middleeast/origins-of-provocative-video-shrouded.html>.

<sup>50</sup> Katherine Fung, *Erik Rush, Conservative Columnist, Makes Muslim Joke After Boston Marathon Explosions*, HUFFINGTON POST (Apr. 15, 2013, 6:05 PM), [http://www.huffingtonpost.com/2013/04/15/erik-rush-boston-marathon-muslims\\_n\\_3087642.html](http://www.huffingtonpost.com/2013/04/15/erik-rush-boston-marathon-muslims_n_3087642.html).

<sup>51</sup> Christopher Zara, *Pat Dollard Twitter Backlash: 'Slaughter Muslims' Tweet Called Hate Speech, Or Was It A Joke?*, INT'L BUS. TIMES (Apr. 3, 2014, 1:46 PM), <http://www.ibtimes.com/pat-dollard-twitter-backlash-slaughter-muslims-tweet-called-hate-speech-or-was-it-joke-1567081>.

<sup>52</sup> See FED. BUREAU OF INVESTIGATION, HATE CRIME STATISTICS 7 (2000), *available at* <http://www.fbi.gov/about-us/cjis/ucr/hate-crime/2000/hatecrime00.pdf>; FED. BUREAU OF INVESTIGATION, HATE CRIME STATISTICS 9 (2001), *available at* <http://www.fbi.gov/about-us/cjis/ucr/hate-crime/2001/hatecrime01.pdf>.

<sup>53</sup> See FED. BUREAU OF INVESTIGATION, HATE CRIME STATISTICS (2010), *available at* <http://www.fbi.gov/about-us/cjis/ucr/hate-crime/2010/tables/table-1-incidents-offenses-victims-and-known-offenders-by-bias-motivation-2010.xls>; FED. BUREAU OF INVESTIGATION, HATE CRIME STATISTICS (2011), *available at* <http://www.fbi.gov/about-us/cjis/ucr/hate-crime/2011/tables/table-1>; FED. BUREAU OF INVESTIGATION, HATE CRIME STATISTICS (2012) *available at* [http://www.fbi.gov/about-us/cjis/ucr/hate-crime/2012/tables-and-data-declarations/1tabledatadecpdf/table\\_1\\_incidents\\_offenses\\_victims\\_and\\_known\\_offenders\\_by\\_bias\\_motivation\\_2012.xls](http://www.fbi.gov/about-us/cjis/ucr/hate-crime/2012/tables-and-data-declarations/1tabledatadecpdf/table_1_incidents_offenses_victims_and_known_offenders_by_bias_motivation_2012.xls).

<sup>54</sup> Apuritan, *OSA at Islamic Mosque Little Rock*, YOUTUBE (Sept. 16, 2012), <https://www.youtube.com/watch?v=YgxUHD0qxSo>.

<sup>55</sup> Dean Obeidallah, *Texans Attack ‘Muslim Weather’*, THE DAILY BEAST, Mar. 17, 2014, <http://www.thedailybeast.com/articles/2014/03/17/texans-attack-muslim-weather.html>.

<sup>56</sup> Dan Satterfield, *NWS Use of the Word Haboob Sets off Firestorm In West Texas*, AM. GEOPHYSICAL UNION’S DAN’S WILD WILD SCIENCE JOURNAL (Mar. 14, 2014), <http://blogs.agu.org/wildwildscience/2014/03/14/nws-use-of-the-word-haboob-upsets-some-in-west-texas/>.

<sup>57</sup> Obeidallah, *supra* note 55.

<sup>58</sup> Ambar Espinoza, *Somali Population, Cultural Tension Rising In St. Cloud*, MINN. PUB. RADIO, Mar. 15, 2010, <http://www.mprnews.org/story/2010/03/15/st-cloud-tensions>.

<sup>59</sup> CAIR CAL., *GROWING IN FAITH 17* (2013), available at <http://ca.cair.com/downloads/GrowingInFaith.pdf>.

<sup>60</sup> Douglas Belkin, *Holocaust Survivors’ Protest Still Echoes in Illinois Suburb*, WALL ST. J., Apr. 18, 2009, <http://online.wsj.com/news/articles/SB124001198935030861>.

<sup>61</sup> *Nat’l Socialist Party of America v. Village of Skokie*, 432 U.S. 43, 44 (1977).

<sup>62</sup> *R.A.V. v. City of St. Paul*, 505 U.S. 377, 391 (1992).

<sup>63</sup> *Gitlow v. New York*, 268 U.S. 652, 666 (1925).

<sup>64</sup> “There are certain well-defined and narrowly limited classes of speech, the prevention and punishment of which have never been thought to raise any Constitutional problem. These include the lewd and obscene, the profane, the libelous, and the insulting or ‘fighting’ words—those which by their very utterance inflict injury or tend to incite an immediate breach of the peace. It has been well observed that such utterances are no essential part of any exposition of ideas, and are of such slight social value as a step to truth that any benefit that may be derived from them is clearly outweighed by the social interest in order and morality.” *Chaplinsky v. New Hampshire*, 315 U.S. 568, 571–72 (1942).

<sup>65</sup> *Gertz v. Robert Welch, Inc.*, 418 U.S. 323 (1974).

<sup>66</sup> *N.Y. Times v. Sullivan*, 376 U.S. 254 (1964). Note that courts have also held that libel directed against religious or racial groups does not create an actionable offense – “group libel” is different from libel directed toward a particular person or entity, which is actionable under the law. FOXMAN & WOLF, *supra* note 5, at 62; *Who Can Sue For Defamation*, DIGITAL MEDIA LAW PROJECT, <http://www.dmlp.org/legal-guide/who-can-sue-defamation> (last visited Apr. 24, 2014).

<sup>67</sup> *Miller v. California*, 413 U.S. 15 (1973).

<sup>68</sup> *New York v. Ferber*, 458 U.S. 747 (1982).

<sup>69</sup> *Cent. Hudson Gas & Electric Corp. v. Pub. Serv. Comm’n of N.Y.*, 447 U.S. 557 (1980).

<sup>70</sup> *Brandenburg v. Ohio*, 395 U.S. 444, 447 (1969).

<sup>71</sup> On February 26, 2014, Google removed *The Innocence of Muslims* from YouTube pursuant to a court order by the U.S. Court of Appeals for the Ninth Circuit in *Garcia v. Google, Inc.*, No. 12-57302, 2014 U.S. App. LEXIS 3694, at \*24 n.9 (9th Cir. 2014), *appeal docketed*, No. 12-57302 (9th Cir. Mar. 13, 2014). In *Garcia*, Cindy Lee Garcia alleged copyright infringement of her performance in the film because it had been partially dubbed over with anti-Muslim statements. The page for the former video indicates that Google disagrees with the Court’s copyright ruling and will appeal the decision. StandUpAmericaNow, *Innocence of Muslims Movie Trailer*, YOUTUBE, <https://www.youtube.com/watch?v=mjoa3QazVv8> (last visited Apr. 24, 2014).

<sup>72</sup> Sarah Chayes, *Inciting Violence Can Cross the Line*, N.Y. TIMES ROOM FOR DEBATE BLOG (Mar. 6, 2013, 7:47 PM), <http://www.nytimes.com/roomfordebate/2013/03/05/in-free-speech-a-line-between-offputting-and-illegal-inciting-violence-is-not-protected-speech>.

<sup>73</sup> *Chaplinsky v. New Hampshire*, 315 U.S. 568, 572 (1942).

<sup>74</sup> BLACK'S LAW DICTIONARY 769 (5th Ed. 1983); *Watts v. U.S.*, 394 U.S. 705 (1969); *R.A.V. v. City of St. Paul*, 505 U.S. 377 (1992).

<sup>75</sup> *Watts*, *supra* note 73, at 708. See EUGENE VOLOKH, FIRST AMENDMENT AND RELATED STATUTES 166 (3rd Ed. 2008).

<sup>76</sup> *Facebook Community Standards*, FACEBOOK, <https://www.facebook.com/communitystandards> (last visited Apr. 22, 2014).

<sup>77</sup> *Hate Speech*, YOUTUBE, <https://support.google.com/youtube/answer/2801939> (last visited Apr. 22, 2014).

<sup>78</sup> *The Twitter Rules*, TWITTER, <https://support.twitter.com/articles/18311-the-twitter-rules> (visited Apr. 22, 2014).

<sup>79</sup> YOUTUBE, *supra* note 77.

<sup>80</sup> FACEBOOK, *supra* note 76.

<sup>81</sup> TWITTER, *supra* note 78.

<sup>82</sup> Newsdesk, *California "Eraser Law" Lets Minors Remove Embarrassing Online Content*, PBS NEWSHOUR'S THE RUNDOWN BLOG (Sept. 25, 2013, 5:21 PM), <http://www.pbs.org/newshour/rundown/california-eraser-law-lets-minors-remove-embarrassing-online-content/>.

<sup>83</sup> Facebook Safety, *What Happens After Your Click "Report"*, FACEBOOK, (JUNE 19, 2012, 8:05 AM), <https://www.facebook.com/notes/facebook-safety/what-happens-after-you-click-report/432670926753695>.

<sup>84</sup> Facebook, Inc., April 2014.

<sup>85</sup> *Whitney v. California*, 274 U.S. 357, 377 (1927).

<sup>86</sup> Counterspeech has been an effective way of responding to hate for all types of communities. For example, a UCLA student, Alexandra Wallace, posted an incendiary video about her fellow Asian students that were being disruptive in the library during the school's final exam period. The video went viral on social media (although the original has since been removed) and soon other students were posting parody videos that quickly became popular. One video titled "Ching Chong! Asians in the Library Song (Response to UCLA's Alexandra Wallace)" featured a catchy mock-love song and had more than 160,000 views in just one day. Erica Goldberg, *The Power of Parody and Counter-Speech: Student Reaction to Alexandra Wallace's Rant Video*, FOUND. FOR INDIVIDUAL RIGHTS IN EDUC., <http://www.thefire.org/the-power-of-parody-and-counter-speech-student-reaction-to-alexandra-wallaces-rant-video/> (last visited Apr. 24, 2014). Today, the video has over 5 million views on YouTube while duplicates of Wallace's original video have significantly less views. Jimmy Wong, *Ching Chong! Asians in the Library Song (Response to UCLA's Alexandra Wallace)*, YOUTUBE (Mar. 15, 2011), <https://www.youtube.com/watch?v=zulEMWj3sVA> (indicating 5,125,500 views as of Apr. 24, 2014).

<sup>87</sup> David Kirkpatrick, *Newsweek's 'Muslim Rage' Cover Mocked Online*, N.Y. TIMES THE LEDE BLOG (Sept. 17, 2012, 7:52 PM), <http://thelede.blogs.nytimes.com/2012/09/17/newsweeks-muslim-rage-cover-mocked-online/>.

<sup>88</sup> *#MuslimRage and 6 Other Social Media Blunders of 2012*, THE GLOBE AND MAIL (Dec. 19, 2012, 2:13 PM), <http://www.theglobeandmail.com/news/muslimrage-and-6-other-social-media-blunders-of-2012/article6044093/>.

<sup>89</sup> Ann Oldenburg, *Miss America Nina Davuluri Brushes Off Racist Remarks*, USA TODAY, Sept. 16, 2013, <http://www.usatoday.com/story/life/people/2013/09/16/miss-america-nina-davuluri-brushes-off-racist-remarks/2819533/>.

<sup>90</sup> Twitter, Inc., April 2014.

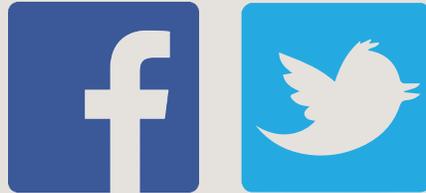
### **Acknowledgements**

This report could not have been possible without the dedication, commitment, and passion of the Muslim Advocates staff, particularly the lead author, Madihha Ahussain, who worked tirelessly on the report with the guidance and support of Mohamed Sabur, Junaid Sulahry, Adil Haq, and consultant Fatima Khan.

Muslim Advocates also extends its deep gratitude to Facebook and Twitter for the research they have shared on these issues.

Finally, Muslim Advocates extends its sincere thanks and appreciation to all the advocates, philanthropists, government officials, parents, community leaders, and concerned Americans who have worked to address hate in their schools, cities, and the country. It is because of your persistence and courage that Americans are aware of these issues, and it is with your voices that together, we will create a nation free of bigotry and hate.

Follow Us:



[www.muslimadvocates.org](http://www.muslimadvocates.org)

# Exhibit 60

The truth will not reveal itself.

SUPPORT OUR WORK TODAY

TO PROTECT AND SLUR

# American cops have openly engaged in Islamophobia on Facebook, with no penalties

by Will Carless and Michael Corey | June 27, 2019

*Part three of a series. Read parts [one](#) and [two](#).*



“WELL, LOOK WHO THE DEMS HAVE AS A DEPUTY CHAIR!”

The [message](#) by Richard Crites, a sheriff’s deputy in Missouri, starts off like so many political posts on Facebook. Then there’s the kicker:

“A RAGHEAD MUSLIM.”

In New Jersey, prison guard Joseph Bonadio posted repeated insults about the Prophet Muhammad and shared [memes](#) of roasting pigs with the message “Happy Ramadan.” In Georgia, retired cop Claude Stevens Jr. railed against Muslims for months, posting [conspiracy theories](#) and [Islamophobic memes](#).

They are among dozens of current and former American law enforcement officers whom Reveal from The Center for Investigative Reporting identified as members of Facebook groups dedicated to Islamophobia. With names such as “Veterans Against islamic Filth,” “PURGE WORLD-WIDE (The Cure for the Islamic disease in your country)” and “Americans Against Mosques,” these groups serve as private forums to share bigoted messages about Muslims, and they have proven attractive for cops.

Reveal’s yearlong investigation found police officers across the country belonging to a [wide spectrum of extremist groups](#) on Facebook, such as Confederate groups filled with racist memes and conspiracies and

groups run by the [anti-government militias](#) Oath Keepers and Three Percenters. Islamophobic behavior was notably brazen. While officers shared slur-filled jokes about African Americans, Latinos and the LGBTQ community behind the walls of closed groups, anti-Muslim comments often were posted on public pages for all to see.

“The problem with law enforcement officials engaging in this type of behavior is that it’s probably influencing the way in which they police in their communities,” said Madihha Ahussain, special counsel for anti-Muslim bigotry at the civil rights group Muslim Advocates. “If they hold these biases towards Muslims, we’re very deeply concerned about the ways in which that manifests itself when it comes to being a first responder or being somebody who is investigating crimes against Muslims.”

The findings come as hate crimes against American Muslims continue at [historically high levels](#). Muslim places of worship across the country have been [set on fire](#) and had their [windows broken](#). Islamophobes have left [slabs of bacon](#) and scrawled [graffiti](#) on the doorsteps of mosques. Muslims have been [shot](#), [stabbed](#) and had their religious garments [ripped off](#). They’ve been [shouted at](#), [kicked](#), [threatened](#) and [spit on](#).

Islamic centers and places of worship across the country also have boosted security since the horrific attacks against two mosques in Christchurch, New Zealand, in March, often asking local cops to stand guard during services.

Muslim Americans long have been the targets of discriminatory polic-

ing, most notably in New York City in the years after the 9/11 attacks. In 2018, the New York Police Department settled the last of three major lawsuits in which it was accused of spying on the local Muslim community for more than a decade, infiltrating mosques and creating a team of informants with the help of the CIA.

We notified nearly 150 departments about their officers' behavior on Facebook and membership in extremist groups. Some departments launched immediate investigations, and one detective in Houston was fired for posting racist memes about African Americans, in violation of department policy.

However, other departments were unbothered by their officers' social media activity. Some police leaders were angry that we even asked them about it.

Not a single department has said it disciplined an officer for Islamophobic posts or membership in an anti-Islam group.

**'This group is for those who wish to speak out about the evils of Islam'**



We were able to identify cops in these groups by writing software to scour Facebook for connections between users who belonged to both extremist and law enforcement groups on the platform, then verifying the identities and professions of active-duty and retired officers. (Read more about our methodology [here](#).)

Through that search, we found people such as Crites, a sworn member of the Lawrence County Sheriff's Office in Missouri.

In addition to his 2018 “raghead Muslim” comment, which he used to introduce a news story about then-Minnesota Rep. Keith Ellison, Crites was a member of three different extremist Facebook groups, including one called “[STOP OBAMA AND CRONIES : RADICAL LEFTIES, ISLAMISTS, MEDIA LIES](#),” which we joined. Inside the group, which was full of [Islamophobic](#) content, we saw Crites posting several times, including writing, “Stop Obama stop the Muslims.”



**Richard Crites**

May 23 · Yahoo · 🌐



WELL, LOOK WHO THE DEMS HAVE AS A DEPUTY CHAIR! A RAGHEAD MUSLIM. BOY THAT PARTY REALLY SUCKS NOW.



YAHOO.COM

**Democrats can — and must — unite in November, says party deputy chair Ellison**

👍👎 5

3 Comments 3 Shares

👍 Like

🔗 Share



██████████ And don't forget racist. He pretty much has all the Dim values covered

Like · 8w

👍 1

Lawrence County Sheriff Brad DeLay said Crites is a volunteer deputy but carries a gun and has arrest powers. Asked about Crites' activity on Facebook, DeLay said he's never heard any concerns from the community about his deputy's work.

"I'm looking at disciplinary records now, and there aren't any complaints," he said.

DeLay wouldn't provide us with those records, and Crites didn't respond to numerous calls for comment.

Joseph Bonadio is a senior corrections officer for the New Jersey Department of Corrections. He also was a member of a group called "Infidel Brotherhood Worldwide."

Islamophobic groups often use the word "infidel" as a dog whistle to attract people with similar views on Islam. Facebook is full of "infidel" groups, including "Any islamist insults infidels, I will put him under

my feet,” “The Infidel Den – Anti Islam Coalition” and “Infidel Elite – Against Islam, by the Pen and/or Sword,” all of which count law enforcement officers as members.

Inside these groups, members often traffic in disproven theories that Muslims are invading the United States and plan to impose Sharia law and that this “Muslimification” already has happened across much of Europe.

Often, though, members just express their disgust with a religion practiced by about a quarter of the world’s population.

“The rabies that is islam being passed down from deluded parent to deluded and brainwashed child,” reads a [typical civilian comment](#) in “Infidel Brotherhood Worldwide.”

Bonadio, who works at the Adult Diagnostic and Treatment Center, a prison in Woodbridge Township, New Jersey, hasn’t actually posted in the group. Instead, he posted openly anti-Muslim content on his public Facebook wall:

- “Known fact Jesus is better then (sic) goat FUCKER Muhammad,” he [posted](#) in 2015.
- “I love the smell of bacon on Ramadan ... Smells like America,” reads a meme he [posted](#) in May, at the beginning of the Muslim holy month of Ramadan.
- “[Happy Ramadan](#),” he posted the same day, captioning a photo of a pig being roasted over a barbecue.

In addition to posting anti-Muslim content, Bonadio poked fun at the LGBTQ community, especially transgender people. He also has posted memes more than once that depict former first lady Michelle Obama as a man and questioned whether white Americans should be blamed for bringing slavery to the country.

After we sent screenshots of Bonadio's Facebook activity to the New Jersey Department of Corrections, a spokesperson sent the following statement: "We are aware of the allegations referenced. These allegations will be investigated and appropriate disciplinary action will be taken, if warranted."

Bonadio did not respond to a call for comment.

Many working police officers were careful to hide their identities on Facebook, using pseudonyms, not listing their place of work or sometimes claiming to work in nonexistent jobs. An officer in Chicago, for example, listed his job as "Bent Over at City of Chicago." Several cops used variations of their real names, such as Texas State Trooper Kevin Lashlee, who called himself "KD Lash" on Facebook and posted in a group containing racist, homophobic, anti-Semitic and Islamophobic content.

But retired law enforcement officers were far more brazen.

Inside hate groups on Facebook, police officers trade racist memes, conspiracy theories and Islamophobia  
The American militia movement, a breeding ground for hate, is pulling in cops on Facebook

These police officers were members of extremist groups on Facebook

---

Claude Stevens Jr., who retired from the Waynesboro Police Department in Georgia in 2015, since has joined at least six closed anti-Muslim groups, including “DEATH TO ISLAM UNDERCOVER” and another named “Rage against the veil.”

Stevens’ personal Facebook page was awash with anti-Islamic memes, and he’s actively commented in at least two of the closed groups. For example, he wrote under a video of Islamic immigrants in Germany, “The Prophet Muhammad eat’s (sic) dog shit and is a follower of Satan/Allah” in March 2017.

When reached for comment, Stevens initially was defensive of his views. He called Islam “evil” and said America needs to be extremely wary of Muslim immigrants, who he claims seek to impose Sharia law in a Christian nation. However, he claimed that as a police officer, he always treated people fairly, no matter what their religion.

Asked how he could treat all people equally while at the same time posting about how Muslims are “filthy” and “animals,” he paused and said: “I would have to concede to you that I probably have to back off on my words and look at it differently.”

As a transit officer with the New York Police Department, John Intranuovo policed a city that's home to more than 600,000 Muslims. Now that he's retired, he has used a group called "Stop the War on Christianity and White America" to rail against Muslims.

Intranuovo had a simple reaction to a post about former President Barack Obama endorsing Amir Malik of the Council on American-Islamic Relations, who was seeking election to the Minnesota House of Representatives in 2018. "No muslims," he wrote. In another comment, Intranuovo called Muslims "evil people."





Intranuovo also was a member of two more anti-Muslim Facebook groups: “The Infidel Den – Anti Islam Coalition” and “THE VOICE OF THE AMERICAN INFIDELS,” neither of which allowed us to join, but

both of which contained openly anti-Islam sentiment in their public descriptions.

"This group is for those who wish to speak out about the evils of Islam. All members of this group want Islam removed from America," reads the public description for "THE VOICE OF THE AMERICAN INFIDELS," which can be viewed by anybody on Facebook.

'These are law enforcement officers who are sworn to protect us pledge, to turn around the social media behemoth, Facebook first promised to ban white nationalist and white supremacist content, then followed up by ousting several prominent purveyors of anti-Muslim rhetoric, including Milo Yiannopoulos and Laura Loomer. But anyone hoping these moves would mark an end to widespread hate speech on the platform was disappointed.

---

Earlier this year, Facebook announced a big push against hate speech.





Facebook CEO Mark Zuckerberg makes the keynote speech at F8, Facebook's developer conference, on April 30 in San Jose, Calif. CREDIT: Tony Avelar/Associated Press



pushing Facebook and other social media companies to take hate speech more seriously.

“Facebook provides a platform and a space where people feel like they can say these things,” she said.

That’s particularly true when it comes to hate speech directed against Muslims, Squire said. Islamophobia on Facebook can be a gateway to other forms of intolerance, she said.

The majority of U.S. hate crimes motivated by religious bias are anti-Semitic, and Reveal’s investigation found plenty of anti-Semitic activity in private groups. But the public nature of the Islamophobic activity on the platform resonates with Squire’s observation from years of monitoring Facebook: that anti-Muslim hate speech is “the last accepted form of bigotry in America.”

*Researchers Daneel Knoetze and Michael Dailey contributed to this story. It was edited by Andrew Donohue and Matt Thompson.*

*Will Carless can be reached at [wcarless@revealnews.org](mailto:wcarless@revealnews.org), and Michael Corey can be reached at [mcorey@revealnews.org](mailto:mcorey@revealnews.org). Follow Carless on Twitter: [@willcarless](https://twitter.com/willcarless).*



**WILL CARLESS**

✉ [wcarless@revealnews.org](mailto:wcarless@revealnews.org)

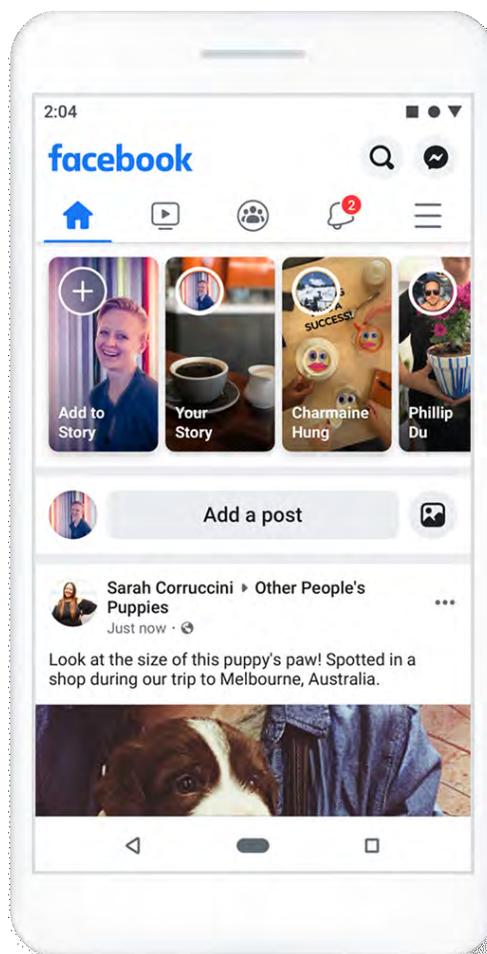
# Exhibit 61

The Facebook company is now Meta. Learn More.



# Let's find more that brings us together.

The Facebook app helps you connect with friends, family and communities of people who share your interests. Connecting with your friends and family as well as discovering new ones is easy with features like Groups, Watch and Marketplace.



[Go to Facebook app](#)

# Exhibit 62

# The Detroit News

---

## POLITICS

# Tlaib not cowed by 'hateful' threats, behavior

**Melissa Nann Burke** The Detroit News

Published 12:02 a.m. ET Jan. 27, 2019 | Updated 9:04 a.m. ET Jan. 28, 2019

*Washington* — The death threats started on U.S. Rep. Rashida Tlaib's first day of orientation in Congress and haven't stopped.

Her office said the Detroit Democrat received around 60 threats in the two weeks following her swearing-in this month.

That same day, she made national headlines after issuing a profane cry at a Washington party to "impeach the mother (expletive)," referring to President Donald Trump.

One of the first two Muslim women elected to the U.S. House, Tlaib also has been the target of anti-Muslim slurs on social media, false internet articles, hoax memes and fake Twitter accounts posing as the freshman lawmaker.

In the past week, colleagues reprimanded a Florida commissioner for saying on Facebook that Tlaib could "become a martyr and blow up Capitol Hill."

"My mere existence here is causing people to say some very hateful and racist comments," said Tlaib, the first Palestinian-American woman to serve in Congress.

The 42-year-old former environmental justice lawyer has renounced the attacks as hate speech that "absolutely has no place in our politics." Tlaib has also suggested Trump's divisive rhetoric is at least in part responsible for threats to harm her.

She ran for office because "people like us deserve a seat at the table." That seat has now propelled Tlaib to a national profile and prompted messages of both support and condemnation. Her mission remains unchanged.

"Girls, we have a new Congress. We not only look differently, but we speak differently," Tlaib told the Women's March in Detroit on Jan. 19, promising to fight for women on the House floor, in the courts and in the streets.

"They will try to shush us. They will try to tell us to be quiet, or this is just not how we're supposed to do things here. ... You all are fueling us to speak louder and very clearly. And the whole nation knows exactly how I feel."

### **Threats 'across the spectrum'**

Tlaib had a few family members serving as her security detail at the march inside the Charles H. Wright Museum of African American History. She said she feels safer at home in Michigan's 13th District than at other events.

"Here, I feel like my whole community protects me. I always worry about my staff and my family more than I worry about myself," Tlaib said in an interview.

"But it's unprecedented, not only myself, but the other women — the new members in Congress — to deal with threats all of us have received. It shows how much violence is being promoted from the White House."

Tlaib isn't the only member of Michigan's congressional delegation to receive death threats.

U.S. Attorney Matthew Schneider of the Eastern District of Michigan said threats against elected officials happen "across the spectrum, across the country."

"We take these, all of them, very seriously. The FBI is specially assigned to be on alert for these. It's not a joking matter, and we're going to follow up on all of them," Schneider said.

"People think that they can be anonymous whether they use email or Snapchat or Facebook. That's really not the case. Law enforcement has tools to identify that, and we've done that on several occasions — whether they're threats to members of Congress or threats to our schools."

The House sergeant at arms has said threatening incidents and communications against House members more than doubled from 902 in 2016 to more than 2,000 in 2017, according to news reports.

A Southgate man, Dennis Downey, awaits sentencing after pleading guilty last year to one count of communicating a threat to injure another after he phoned the Washington office of U.S. Rep. Debbie Dingell, D-Dearborn, saying he would kill "all of you."

Court records say law enforcement traced the call and arrested Downey, who admitted to placing it.

It's unclear whether charges have been brought yet in relation to the threats against Tlaib. Spokesman Denzel McCampbell said Tlaib's office is working with all levels of law enforcement to ensure the threats against her are taken seriously.

### **'It's a sensitive time'**

"I can empathize. We get death threats regularly," said U.S. Rep. Andre Carson, a Muslim and former police officer who has served in Congress since 2009.

Carson represents the Indianapolis area and has a security detail from the local sheriff's department when he does events in his district, he said. Last year, officials secured a restraining order against an individual who threatened one of Carson's staffers, he said.

"It's a sensitive time. Folks are upset. They are looking for a boogeyman or woman to place their blame on, and you look at a woman like Rashida who makes folks uncomfortable. She represents the 'changing of America,' as it were," Carson said.

"You have people who are still sexist, and Islamaphobes who can't stand to see women in power, women in authority. To be a woman and a Muslim, that doubles the offense for them and doubles the suspicion. She represents all that they're afraid of."

National coverage of Tlaib's call to impeach Trump this month drew a flurry of angry calls to the 13th District Democratic Party — at least 100 over 10 days from area codes around the country, said Jonathan Kinloch, the party chairman for the district.

"What is wrong with your people in Michigan?" one caller grouched in a voicemail. "Rag heads like that shouldn't be in Congress."

Many callers insulted Muslims and Palestinians, engaged in name-calling and suggested Tlaib be removed from office. The episode and the threats to Tlaib illustrate how polarized the country has become, Kinloch said.

"The threshold has been lowered in terms of tolerance and acceptability for the vile discourse taking place," Kinloch said. "It's just unfortunate. Trump's normalizing it, and those who choose to get into the squalor with him."

### **Memories of Congress shooting**

Republican Rep. John Moolenaar of Midland said he communicated to Tlaib that he "in no way" agreed with her remarks about impeaching Trump, urging decorum in Congress and respect for the office of the president.

"I'm not saying in any way she deserves that kind of treatment, even though her comments were very offensive. It's two separate things," Moolenaar said of the threats against her.

"It's unacceptable for her to be treated that way, and I'm sorry she's experiencing that."

Moolenaar, who like Tlaib is a former state lawmaker, said nothing ever justifies threats or intimidation of a public servant. "That's terrible," he said.

Moolenaar was with other GOP lawmakers practicing for the Congressional Baseball Game in June 2017 when a gunman opened fire, wounding four people including Rep. Steve Scalise of Louisiana and Oakland County native Matt Mika.

Gunman James Hodgkinson died following a shootout with police. He was later identified as a Bernie Sanders supporter who once posted on Facebook that "Republicans are the Taliban of the USA."

"Having been in a situation where people on the field that day were targeted because of their political views, that's a very serious problem," Moolenaar said. "Anyone who threatens the livelihood or lives of people deserves consequences for that."

*mburke@detroitnews.com*

*Staff Writer Sarah Rahal contributed.*

# Exhibit 63

—ANONYMOUS WHISTLEBLOWER DISCLOSURE—

[REDACTED]

SEC Office of the Whistleblower  
Via Online Portal & FedEx

- Re: Supplemental Disclosure of Securities Law Violations by Facebook, Inc. (NASDAQ: FB), SEC ICR [REDACTED]

**Facebook misled investors and the public about equal enforcement of its terms given that high-profile users are "whitelisted" under its "XCheck" program.**

To the SEC Office of the Whistleblower:

1. The instant letter is one of multiple disclosures related to the above-captioned matter. Our anonymous client is disclosing original evidence showing that **Facebook, Inc. (NASDAQ: FB)** has, for years past and ongoing, violated U.S. securities laws by making **material misrepresentations and omissions in statements to investors and prospective investors**, including, *inter alia*, through filings with the SEC, testimony to Congress, online statements and media stories.
2. **Summary.** In particular, despite reassuring investors and the public that it enforces its terms and policies in a "fair and consistent" way, and that its "XCheck" (pronounced "Cross Check") program only provides "additional review" for high-visibility users (e.g., celebrities and high-paying advertisers), this is a material misstatement and/or omission. In fact, XCheck functions in practice as a "whitelister" for privileged users, furthering harmful content and violation of terms and causing significant and long-term risks to Facebook and its investors.
3. **Facebook's Material Misrepresentations and Omissions Include Mark Zuckerberg's Sworn Testimony to Congress.**

Whistleblower Aid is a U.S. tax-exempt, 501(c)(3) organization, EIN 26-4716045.

<https://WhistleblowerAid.org> — Anonymously via Tor Browser: <http://WBAidLw4sqwv7h2.com/>  
Contact via SecureDrop or Tor: <http://whistlebloweraid.securedrop.org/tor/onion> — via Signal App: [REDACTED]

4. For example, on October 28, 2020, Mark Zuckerberg testified before the U.S. Senate, and when Senator Mike Lee asked:

*"[D]o you state before this committee, for the record, that you always apply your terms of service equally to all of your users?" (emphasis added)*

5. Mark Zuckerberg responded:

*"I certainly don't think we have any intentional examples where we're trying to enforce our policies in a way that is anything other than fair and consistent." (emphasis added)*

6. Further, Mark Zuckerberg testified:

*"Incitement of violence is against our policy and there are not exceptions to that, including for politicians." (emphasis added)*

7. Likewise, on November 17, 2020, Mark Zuckerberg testified before the Senate:

*"We took our responsibility for protecting the integrity of this election seriously . . . we worked hard to apply those policies fairly and consistently."<sup>3</sup> (emphasis added)*

8. This follows Mark Zuckerberg's testimony before the U.S. House of Representatives in 2018, and when Rep. McMorris-Rodgers asked:

*"And what is Facebook doing to ensure that its users are being treated fairly and objectively by content reviewers?" (emphasis added)*

9. Mark Zuckerberg testified:

*" . . . we take a number of steps to make sure that none of the changes that we make are targeted in any kind of biased way. . . . I agree that this is a serious issue . . . we make a relatively small percent of mistakes in content review . . . I wouldn't extrapolate from a few examples to assuming that the overall system is biased." (emphasis added)*

<sup>1</sup><https://www.wire.com/blog/transcript/tech-ceos-senate-testimony-transcript-october-28/>

<sup>2</sup><https://www.wire.com/blog/transcript/tech-ceos-senate-testimony-transcript-october-28/>

<sup>3</sup><https://www.judiciary.senate.gov/imo/media/doc/zuckerberg%20testimony.pdf>

<sup>4</sup>[https://energycommerce.house.gov/sites/ideмокoats.energycommerce.house.gov/files/documents/20180411\\_FCH%20Facebook%20Transparency%20and%20Use%20of%20Consumer%20Data.pdf](https://energycommerce.house.gov/sites/ideмокoats.energycommerce.house.gov/files/documents/20180411_FCH%20Facebook%20Transparency%20and%20Use%20of%20Consumer%20Data.pdf)

10. In March and May 2021, Mark Zuckerberg and Facebook continued to represent:

***"people . . . want to know that when platforms remove harmful content, they are doing so fairly and transparently."***<sup>73</sup> (emphasis added)

*"We strive to enforce our policies consistently . . . **Our Community Standards apply to all content, and we assess everyone under those Standards. When we identify or learn of content that violates our policies, we remove that content regardless of who posted it** . . .*

*Facebook's Terms and Policies are available here:*

*<https://www.facebook.com/policies>. Facebook's Community Standards are available at <https://www.facebook.com/communitystandards/>. Both are global and apply to all accounts on Facebook."<sup>74</sup> (emphasis added)*

11. Facebook Has Made Misstatements in Securities Filings and Related Records.

12. For example, Facebook has repeatedly represented its "transparency," "integrity," and "visibility," including in its filed 10-K statements in January 2021<sup>75</sup> and January 2020<sup>76</sup> and its 10-Q statement in July 2021,<sup>77</sup> as well as quarter results conference calls in 2021<sup>78</sup> and July 2020, stating to investors and the public:

***"[We] also have clear community standards and guidelines that we enforce fairly . . ."***<sup>79</sup> (emphasis added)

13. In its Notice of Annual Meeting and Proxy Statement in 2021,<sup>80</sup> it also emphasized:

*"We publish quarterly Community Standards Enforcement Reports that track our progress on enforcing our content policies . . . We regularly publish Transparency Reports to give our community visibility into how we enforce policies . . ."*<sup>81</sup>

14. Facebook Has Made Statements in its Public Pages and Guidelines.

15. Facebook's "Cross Check" page and policies represented since at least 2018:

<sup>73</sup><https://docs.house.gov/meetings/IF/IF16/20210326/1114074/HHRG-117-IF16-Website-ZuckerbergM-20210326-011.pdf>

<sup>74</sup><https://docs.house.gov/meetings/IF/IF16/20210326/1114074/HHRG-117-IF16-Website-ZuckerbergM-20210326-03004.pdf>

<sup>75</sup><https://sec.report/Document/10001326801-21-000014/>.

<sup>76</sup><https://www.sec.gov/Archives/edgar/data/1326801/000132680120040013/fb-12312018x10k.htm>.

<sup>77</sup><https://sec.report/Document/10001326801-21-000049/>.

<sup>78</sup>[https://x21.g4cdn.com/329690738/files/doc\\_financials/2020/q4/FB-Q4-2020-Conference-Call-Transcript.pdf](https://x21.g4cdn.com/329690738/files/doc_financials/2020/q4/FB-Q4-2020-Conference-Call-Transcript.pdf)

<sup>79</sup>[https://x21.g4cdn.com/329690738/files/doc\\_financials/2020/q2/Q2'20-FB-Follow-Up-Call-Transcript.pdf](https://x21.g4cdn.com/329690738/files/doc_financials/2020/q2/Q2'20-FB-Follow-Up-Call-Transcript.pdf), see also

<https://about.fb.com/news/2018/07/working-to-keep-facebook-safe/>.

<sup>80</sup><https://www.sec.gov/Archives/edgar/data/1326801/000132680121000032/bxscprnk2021definitivexpx.htm>.

***"We want to make clear that we remove content from Facebook, no matter who posts it, when it violates our standards. There are no special protections for any group . . ."***<sup>17</sup> (emphasis added)

See also: "If someone posts something that breaks our Standard and their page was Cross-Checked, we would still remove that content from Facebook after double-checking this was the correct decision."<sup>18</sup>

16. Continuing through June 2021, after Facebook's "independent Oversight Board" upheld the decision to suspend Donald Trump's account and requested that Facebook, among other things, "act quickly on posts made by influential users that pose a high probability of imminent harm," Facebook stated:

*"For content that will likely be seen by many people, we may employ a cross check system to help ensure that we are applying our policies correctly . . . **Our Community Standards apply around the world to all types of content and are designed so they can be applied consistently and fairly** to a community that transcends regions, cultures, and languages . . . We employ an additional review, called our cross check system, to help confirm we are applying our policies correctly for content that will likely be seen by many people . . . **We want to make clear that we remove content from Facebook, no matter who posts it, when it violates our Community Standards.** There is only one exception — and that is for content that receives a newsworthiness allowance . . . Cross check simply means that we give some content from certain Pages or Profiles additional review . . ." (And when asked to report on error rates and thematic consistency of determinations made through the Cross Check process, Facebook responded: "it is not feasible to track this information."<sup>19</sup> (emphasis added)*

17. In committing to an "independent Oversight Board," Facebook represented:

*"we have created and empowered a new group to exercise independent judgment over some of the most difficult and significant content decisions . . . they are truly autonomous in their exercise of independent judgment."<sup>20</sup>*

<sup>17</sup> <https://about.fb.com/news/2018/03/working-to-keep-facebook-safe/>

<sup>18</sup> <https://about.fb.com/wp-content/uploads/2018/07/Facebook-to-Freedom-Index-10-07-181.pdf>

<sup>19</sup> <https://about.fb.com/wp-content/uploads/2021/05/Facebook-Responses-to-Oversight-Board-Recommendations-in-Trump-Case.pdf>; see also

<https://oversightboard.com/news/2266/24558/6409-oversight-board-asks-former-president-trump-to-suspend-its-own-website-if-it-cannot-impose-penalty> (Oversight Board decision regarding Donald Trump).

<sup>20</sup> <https://about.fb.com/news/2021/05/creating-the-oversight-board/>

18. In addition, Facebook's Community Standards state:

**"Our Community Standards apply to everyone, all around the world, and to all types of content."**<sup>177</sup>

19. Facebook also advertises "Commitment to Transparency," stating:

*"We're also launching a redesign of our Transparency Center to make it easier for people to find what they need. Our Transparency Report also includes the Community Standards Enforcement Report for Q1 of 2021, which provides data on how we take action against violating content across our platforms."<sup>178</sup>*

*"We publish regular reports to give our community visibility into how we enforce our policies."<sup>179</sup>*

*"This is why we have the Facebook Community Standards and Instagram Community Guidelines, which define what is and is not allowed in our community."<sup>180</sup>*

20. Turning to its "Transparency Center," Facebook has represented its "consistent" enforcement since at least 2017 up through at least the summer of 2021:

**"Facebook's review teams are trained to ensure that their content decisions are accurate and consistent . . . we may employ additional reviews for high-visibility content that may violate our policies . . . This process, which we refer to as cross-check, means that our review teams will assess this content multiple times . . . It also helps us verify that when content violates our policies, including from public figures or popular Pages, we consistently remove it."**<sup>181</sup> (emphasis added)

*"We remove content that goes against our policies . . ."<sup>182</sup>*

<sup>177</sup> <https://www.facebook.com/communitystandards/>

<sup>178</sup> <https://about.fb.com/news/2021/05/transparency-report-q1-2021/>

<sup>179</sup> <https://transparency.fb.com/data/?from=idge%3A%2F%2Ftransparency.facebook.com%2F>

<sup>180</sup> <https://transparency.fb.com/data/community-standards-enforcement>

<sup>181</sup> <https://transparency.fb.com/enforcement/detecting-violations/reviewing-high-visibility-content-decisions/>

<sup>182</sup> <https://transparency.fb.com/enforcement/missing-action/>

"If your content goes against the Facebook Community Standards or Instagram Community Guidelines, the Facebook company will remove it."<sup>24</sup>

21. However, these documents, including the Community Standards Enforcement Reports,<sup>25</sup> do not explain that in practice, the "XCheck" or "Cross-Check" system effectively "whitelists" high-profile and/or privileged users, enabling them to violate Facebook's terms, as shown by the enclosed documents.

22. Facebook's Records Confirm That Facebook's Statements Were False.

23. As the enclosed internal Facebook records show, Facebook's statements were false. For example, Facebook has confirmed:

"over the years, many XChecked pages, profiles and entities have been exempted from enforcement."<sup>26</sup> (emphasis added)

*In 2020, Cross Check entities were shielded from the majority of Integrity actions (there are 109 daily xcheck exempted actions and 90 actions per daily without xcheck protection).*<sup>27</sup>

"over the years, many XChecked people & entities have been exempted from enforcement. That means, for a select few members of our community, we are not enforcing our policies and standards. Unlike rest of our community, these people can violate our standards without any consequences . . . Since we currently review less than 10% of Checked content . . . without optimizing list of people XChecked, it would require significant investment in staffing (>10X increase)."<sup>28</sup> (emphasis added)

*"This opens us up to a few different legal liabilities ( caveat: I am not a lawyer). We currently apply XChecks on official government figures, but not on candidates . . . definitely more prevalent on the local or state level . . . this creates legal liability wrt campaign finance."*<sup>29</sup>

*"X-Check, like all components, has a cost and a benefit to the company. . . The Cost of X-Check can be quantified by bad VPVs. This is the count of*

<sup>24</sup><https://transparency.fb.com/en/commen/faking-actions/taking-down-violating-content/>

<sup>25</sup>See e.g., <https://upload.fo.com/docs/2021/05/community-standards-enforcement-report-q1-2021/>

<sup>26</sup> [REDACTED] Whistleblong, p. 1

<sup>27</sup> See [REDACTED] Adding Civic Affairs to Xcheck Document, p. 11

<sup>28</sup> [REDACTED] Misake Revelation, p. 7.

<sup>29</sup> [REDACTED] Integrity Ideas to Fight Racial Injustice Document, p. 3.

News accruing to content that should have been removed, but the removal was blocked by X-Check.”<sup>20</sup>

“All together there are 229K confirmed Civic entities (per 07/25 data), 180k are protected by XCheck. . . . There are another 19M entities in probably Civic list (per 07/25 data), 757K are protected by XCheck. . . .”<sup>21</sup>

“On June 1, a video containing NCII (non-consensual intimate imagery), was posted to the Instagram account and Facebook page associated with global . . . star . . . **A delete action was blocked at scaled support and escalated to . . . XCheck queues where it remained over a weekend. . . . to that time, it amassed 56 Million views, video was XChecked, leading to longer review time and therefore more BVPV. . . . Safety OS doesn't have permissions to override XCheck.**”<sup>22</sup> (emphasis added)

“**We are exempting certain people and businesses from our policies and standards, at various stages of integrity lifecycle – exemptions from detection, strike accrual and enforcement. . . . This undermines our fairness and legitimacy efforts; creates legal and compliance risks for the company. . . . Based on an initial company-wide audit, this problem is pervasive across the country. . . . Why is this a problem? Exempting (aka whitelisting) specific people and entities creates numerous legal, compliance, PFI risks for the company and harms our community. . . .**”<sup>23</sup> (emphasis added)

**24. Facebook Has Publicly Admitted This is a Material Issue.**

25. In its public securities filings (e.g., 10-K,<sup>24</sup> 10-Q,<sup>25</sup> and Proxy Statement<sup>26</sup>) and other records, Facebook has conceded:

“We are making significant investments in . . . content review efforts to combat misuse of our services. . . . Any of the foregoing developments may negatively affect user trust and engagement, harm our reputation and brands, require us to change our business practices in a manner adverse to our business, and adversely affect our business and financial results.”

<sup>20</sup> XCheck Get Well, p. 1.

<sup>21</sup> Adding Civic Users to Xcheck Document, p. 4.

<sup>22</sup> Mistake prevention incident list, p. 14.

<sup>23</sup> The “Whistle” Problem, multiple pages.

<sup>24</sup> <https://sec.report/Document/0001325801-21-000314/>.

<sup>25</sup> <https://sec.report/Document/0001325801-21-000349/>.

<sup>26</sup> <https://www.sec.gov/Archives/edgar/data/1325801/000132580121000032/facebook2021definitivprox.htm>.

"Our brands may also be negatively affected by . . . decisions or recommendations regarding content . . ."

"Our advertising revenue can also be adversely affected by a number of other factors, including: . . . reductions of advertising by marketers due to our efforts to implement or enforce advertising policies that protect the security and integrity of our platform."

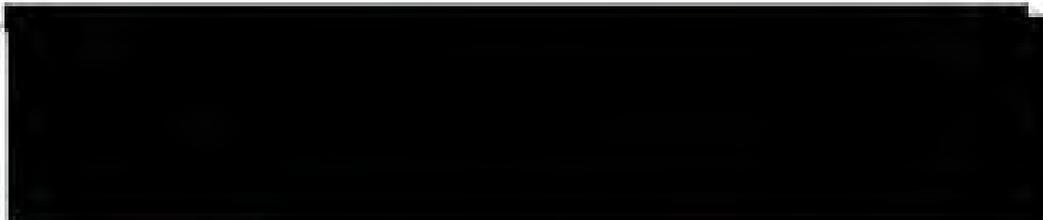
". . . the substance or enforcement of our community standards, the actions of our users, the quality and integrity of content shared on our platform, or the actions of other companies that provide similar services to ours, has in the past, and could in the future, adversely affect our reputation."

26. Likewise, Facebook's Community Standards (Stakeholder Engagement) confirm:

"Given the impact of our Community Standards on society, it's critical for us to create a policy development process that's not only inclusive and based on expert knowledge, but also transparent. We know from talking to hundreds of stakeholders that coming up our policy-making process helps build trust. The more visibility we provide, the more our stakeholders are likely to view the Community Standards as relevant, legitimate, and based on consent."<sup>10</sup>

27. **Role for the SEC.** The SEC is charged with enforcing the laws that protect investors in public companies like Facebook. Facebook's investors care about misrepresentations and omissions by Mark Zuckerberg and other Facebook executives because consistent and fair applications of its policies, or lack thereof, and integrity and transparency matter to users and advertisers, and therefore affect Facebook's advertising revenue and corporate profits. Further, some shareholders would not want to invest in the company if they knew the truth about Facebook's special treatment for high-profile users.

28.



<sup>10</sup> [https://www.facebook.com/communitystandards/stakeholder\\_engagement](https://www.facebook.com/communitystandards/stakeholder_engagement)



Report government and corporate wrongdoing.  
Without breaking the law.

[Redacted]

29. [Redacted]

30. Whistleblower Aid is a non-profit legal organization that helps workers report their concerns about violations of the law safely, lawfully, and responsibly. We respectfully request the SEC's assistance ensuring that our client never faces actual or threatened retaliation.

31. We plan to continue supplementing this disclosure with additional information and evidence. Our client would be happy to meet with investigators at your convenience. Please feel free to contact us using the information below.

32. We are representing an anonymous whistleblower who is making the above disclosures solely for reporting the suspected violation of laws as outlined.

Sincerely,

John N. Tye, Attorney at Law  
Chief Disclosure Officer

[Redacted]

Andrew Bakaj, Attorney at Law  
Of Counsel

[Redacted]

— ANONYMOUS WHISTLEBLOWER DISCLOSURE —

REDACTED FOR CONGRESS

Karl Kronenberger, Attorney at Law  
Kronenberger Rosenfeld, LLP

Enclosures:

██████████  
██████████ "Whitelist" Problem  
██████████ Mistakes prevention incident list some XCheck

Other internal Facebook documents –

██████████ Mistake Prevention XCheck (Cross Check) Get Well  
██████████ XCheck (Cross Check) Get Well Plan  
██████████ Whitelist Where We Are  
██████████ Integrity Ideas To Fight Racial Injustice  
██████████ Cross Check  
██████████ Whitelisting  
██████████ XCheck (Cross Check) Get Well  
██████████ Adding Civic Users to XCheck  
██████████ Civic Actors  
██████████ XCheck (Cross Check)  
██████████ Cross Check Wiki  
██████████ Mistake Prevention for XCheck Exemption  
██████████ Political Influence in Content Policy  
██████████ Comparing the effects of misinfo  
██████████ White List contradicts Facebook stated principles

REDACTED FOR CONGRESS

— ANONYMOUS WHISTLEBLOWER DISCLOSURE —

# Exhibit 64

FACEBOOK FILES —

# Facebook AI moderator confused videos of mass shootings and car washes

Executive concerns of “over-enforcement” let hate speech through, report says.

TIM DE CHANT - 10/18/2021, 9:30 AM



**Enlarge** / Facebook CEO Mark Zuckerberg testifying before Congress in April 2018. It wasn't his only appearance in DC this decade.

---

Facebook CEO Mark Zuckerberg sounded an optimistic note three years ago when he wrote about the progress his company was making in automated moderation tools powered by artificial intelligence. "Through the end of 2019, we expect to have trained our systems to proactively detect the vast majority of problematic content," he **wrote** in November 2018.

But as recently as March, internal Facebook documents reveal the company found its automated moderation tools were falling far short, removing posts that were responsible for only a small fraction of views of hate speech and violence and incitement on the platform. The posts removed by AI tools only accounted for 3–5 percent of views of hate speech and 0.6 percent of views of violence and incitement.



Join Ars Technica and

## Get Our Best Tech Stories

DELIVERED STRAIGHT TO YOUR INBOX.

SIGN ME UP

Will be used in accordance with our [Privacy Policy](#).

While that's up from 2 percent of hate speech views two years ago, according to documents turned over to The [Wall Street Journal](#) by whistleblower Frances...



### FURTHER READING

Facebook "is tearing our societies apart," whistleblower says in [interview](#)

SUBSCRIBE

SIGN IN

the... in order of magnitude but that they might then hit a ceiling beyond which further advances would be difficult.

"The problem is that we do not and possibly never will have a model that captures even a majority of integrity harms, particularly in sensitive areas," he wrote. "Recent estimates suggest that unless there is a major change in strategy, it will be very difficult to improve this beyond 10-20% in the short-medium term."

To arrive at these estimates, Facebook takes a sample of posts, applies its AI moderation tools to them, and then asks human moderators to assess the AI's accuracy. It then uses that fraction to estimate how much hate speech or violence and incitement is missed platform-wide.

Advertisement

...actually take 100 violations for that group to accrue its five strikes,” one data scientist said in a 2020 note that was reported by [BuzzFeed](#) and WSJ.

## Differing statistics

Facebook’s internal view of its AI moderation tools appears far more pessimistic than what it reports to the public. Part of that is because what it reports internally and what it’s telling the public are subtly, though entirely, different. In public statements, Facebook has disclosed the percent of hate speech discovered by AI before users report it, which is a very high number, 98 percent. The problem is, there are many cases where hate speech goes unreported.

Company spokesperson Andy Stone told WSJ that figures about posts removed do not include other actions the platform takes, such as decreasing the reach of suspect content. In that context, he said, policy violating content is decreasing in prevalence and is what the company judges itself by.

Facebook has said it’s gotten better about finding hate speech on its platform, [claiming](#) that it proactively removed 15 times more in 2020 than in 2017. That figure obscures some key details, though. “We ask, what’s the numerator? What’s the denominator? How did you get that number? And then it’s like crickets,” Rashad Robinson, president of the civil rights group Color of Change, told WSJ. “They won’t ever show their work.”

## Harder to report

Today, Facebook’s AI tools may be catching more content before users report it, because two years ago, Facebook intentionally made it harder for users to file reports. A side effect of that was that the AI tools were now able to catch more posts before they were finally reported by users.

“We may have moved the needle too far,” one of the report’s authors said of the extra hurdles users must go through to report posts that may violate the site’s policies. Stone, the Facebook spokesperson, told the WSJ that the company had removed some though not all of the barriers.



### FURTHER READING

Facebook’s latest “apology” reveals security and safety disarray

Facebook has a strong profit motive to automate more of its moderation. Human moderators cost the company \$104 million in 2019, according to WSJ, and three-quarters of that was paying people to respond to user reports. That year, Facebook made it a goal to “reduce \$ cost of total hate review capacity by 15%,” one document says.

---

What's more, WSJ reports that Facebook at the time also tweaked its algorithm in a way that led it to ignore more user reports.

## AI confusion

Facebook's internal documents reveal just how far its AI moderation tools are from identifying what human moderators were easily catching. Cockfights, for example, were mistakenly flagged by the AI as a car crash. "These are clearly cockfighting videos," the report said. In another instance, videos livestreamed by perpetrators of mass shootings were labeled by AI tools as paintball games or a trip through a carwash.

If the situation sounds grim in the US or among English-speaking countries, it appears far worse elsewhere. In Afghanistan, for example, the company said in reports that it lacks a dictionary of slurs in the country's various languages. As a result, Facebook estimates that it identified just 0.23 percent of hate speech posted on the platform in Afghanistan.

Internal reports show that Facebook's users would rather the company take a more aggressive approach to enforcing policy violations for hate speech and violence and incitement, even if it means removing a higher number of innocent posts. In a survey, users from around the world said inaccurate content removals were the least of their concerns and told Facebook that hate speech and violence should be its highest priority. In the US, more users felt inaccurate removals were an issue but that hate speech and violence were still voted the top problem.

Still, Facebook's leadership has been more concerned with taking down too many posts, company insiders told WSJ. As a result, they said, engineers are now more likely to train models that avoid false positives, letting more hate speech slip through undetected.

---

### FURTHER READING

Algorithms shouldn't be protected by Section 230, Facebook whistleblower tells Senate

---

READER COMMENTS 130

SHARE THIS STORY

---

**TIM DE CHANT**

Tim De Chant covers technology, policy, and energy at Ars. He has written for Wired, The Wire China, and

# Exhibit 65



Broken Promises



May 21, 2020

## White Supremacist Groups Are Thriving on Facebook



Facebook says hate groups aren't allowed on the platform. But white supremacists are using the social network to build their movement.

[Click here to download the full report \(https://www.techtransparencyproject.org/sites/default/files/Facebook-White-Supremacy-Report.pdf\)](https://www.techtransparencyproject.org/sites/default/files/Facebook-White-Supremacy-Report.pdf) »

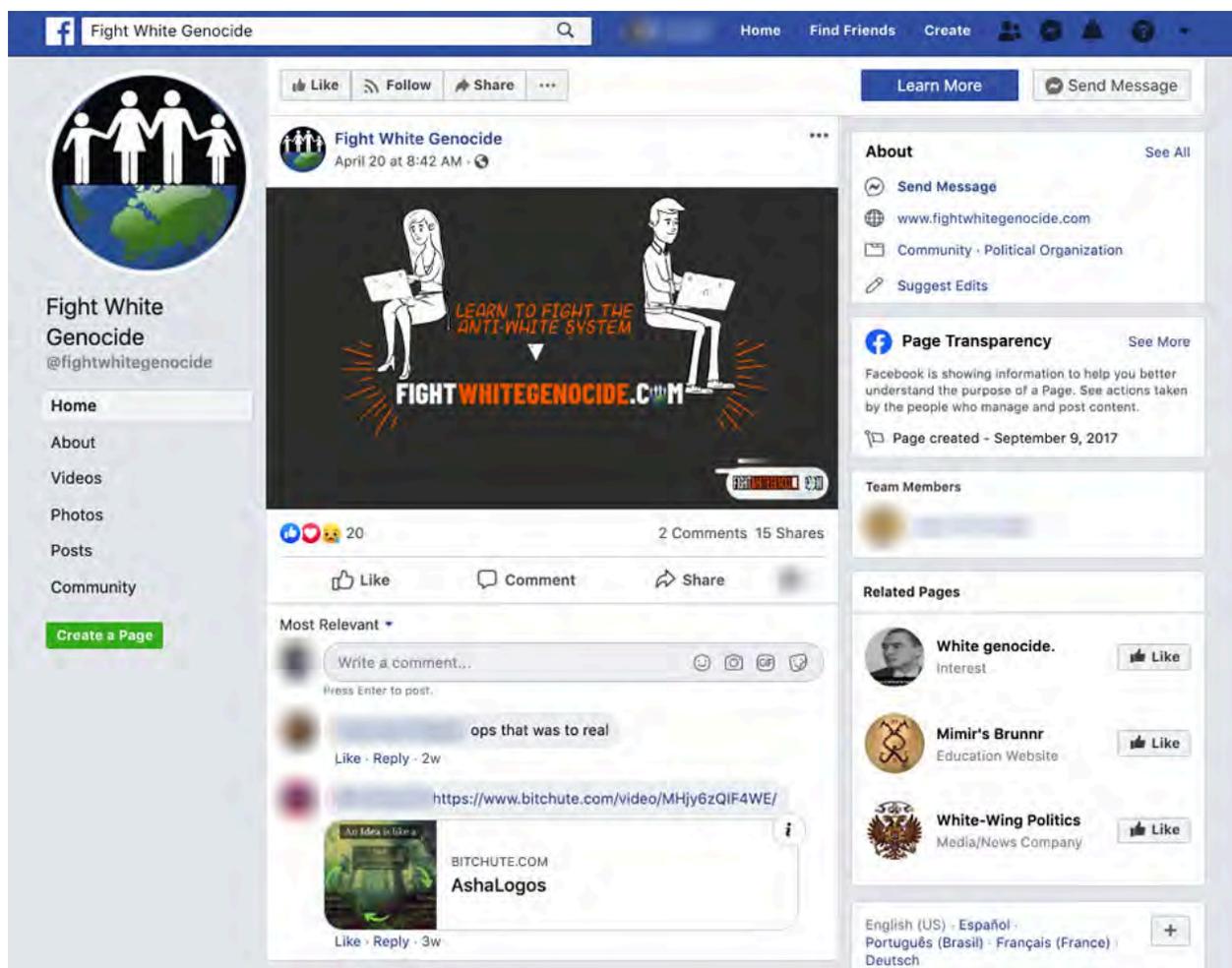
[Click here to download data on the hate group websites \(https://www.techtransparencyproject.org/sites/default/files/SPLC-and-ADL-hate-groups.xlsx\)](https://www.techtransparencyproject.org/sites/default/files/SPLC-and-ADL-hate-groups.xlsx) »

Dozens of white supremacist groups are operating freely on Facebook, allowing them to spread their message and recruit new members, according to a Tech Transparency Project (TTP) investigation, which found the activity is continuing despite years of promises by the social network that it bans hate organizations.

TTP recently documented how online extremists, including many with white supremacist views, are using Facebook to plan for a militant uprising dubbed the "boogaloo." (<https://www.techtransparencyproject.org/articles/extremists-are-using-facebook-to-organize-for-civil-war-amid-coronavirus>) as they stoke fears that coronavirus lockdowns are a sign of rising government repression. But TTP's latest investigation reveals Facebook's broader problems with white supremacist groups, which are using the social network's unmatched reach to build their movement.

The findings, more than two years after Facebook hosted an event page for the deadly "Unite the Right" rally in Charlottesville, Virginia, cast doubt on the company's claims that it's effectively monitoring and dealing with hate groups. What's more, Facebook's algorithms create an echo chamber that reinforces the views of white supremacists and helps them connect with each other.

With millions of people now quarantining at home and vulnerable to ideologies that seek to exploit people's fears and resentments about Covid-19, Facebook's failure to remove white supremacist groups could give these organizations fertile new ground to attract followers.



Facebook's Community Standards prohibit hate speech ([https://www.facebook.com/communitystandards/hate\\_speech](https://www.facebook.com/communitystandards/hate_speech)) based on race, ethnicity, and other factors because it "creates an environment of intimidation and exclusion and in some cases may promote real-world violence." The company also bans hate organizations ([https://www.facebook.com/communitystandards/dangerous\\_individuals\\_organizations](https://www.facebook.com/communitystandards/dangerous_individuals_organizations)). Since the Charlottesville violence, Facebook has announced the removal of specific hate groups and tightened restrictions on white extremist content on the platform.

"We do not allow hate groups on Facebook, overall," CEO Mark Zuckerberg told Congress (<https://www.washingtonpost.com/news/the-switch/wp/2018/04/11/transcript-of-zuckerbergs-appearance-before-house-committee/>), in April 2018. "So, if – if there's a group that – their primary purpose or – or a large part of what they do is spreading hate, we will ban them from the platform, overall."

To test those claims, TTP conducted searches on Facebook for the names of 221 white supremacist organizations that have been designated as hate groups by the Southern Poverty Law Center (SPLC) and the Anti-Defamation League (ADL), two leading anti-hate organizations.

The analysis found:

- Of the 221 designated white supremacist organizations, more than half—51%, or 113 groups—had a presence on Facebook.
- Those organizations are associated with a total of 153 Facebook Pages and four Facebook Groups. Roughly one third of the organizations (34) had two or more Pages or Groups on Facebook. Some had Pages that have been active on the platform for a decade.
- Many of the white supremacist Pages identified by TTP were created by Facebook itself. Facebook auto-generated them as business pages when someone listed a white supremacist or neo-Nazi organization as their employer.
- Facebook’s “Related Pages” feature often directed users visiting white supremacist Pages to other extremist or far-right content, raising concerns that the platform is contributing to radicalization.
- One of Facebook’s strategies for combatting extremism—redirecting users who search for terms associated with white supremacy or hate groups to the Page for “Life After Hate,” an organization that promotes tolerance—only worked in 6% (14) of the 221 searches for white supremacist organizations.
- In addition to the hate groups designated by SPLC and ADL, TTP found white supremacist organizations that Facebook had explicitly banned in the past. One known as “Right Wing Death Squad” had at least three Pages on Facebook, all created *prior* to Facebook’s ban.



(<https://www.techtransparencyproject.org/articles/hate-pages>).

*TTP created a visualization to illustrate how Facebook's Related Pages connect white supremacist groups with each other and with other hateful content. To view this interactive feature, [click here](https://www.techtransparencyproject.org/articles/hate-pages) (<https://www.techtransparencyproject.org/articles/hate-pages>).*

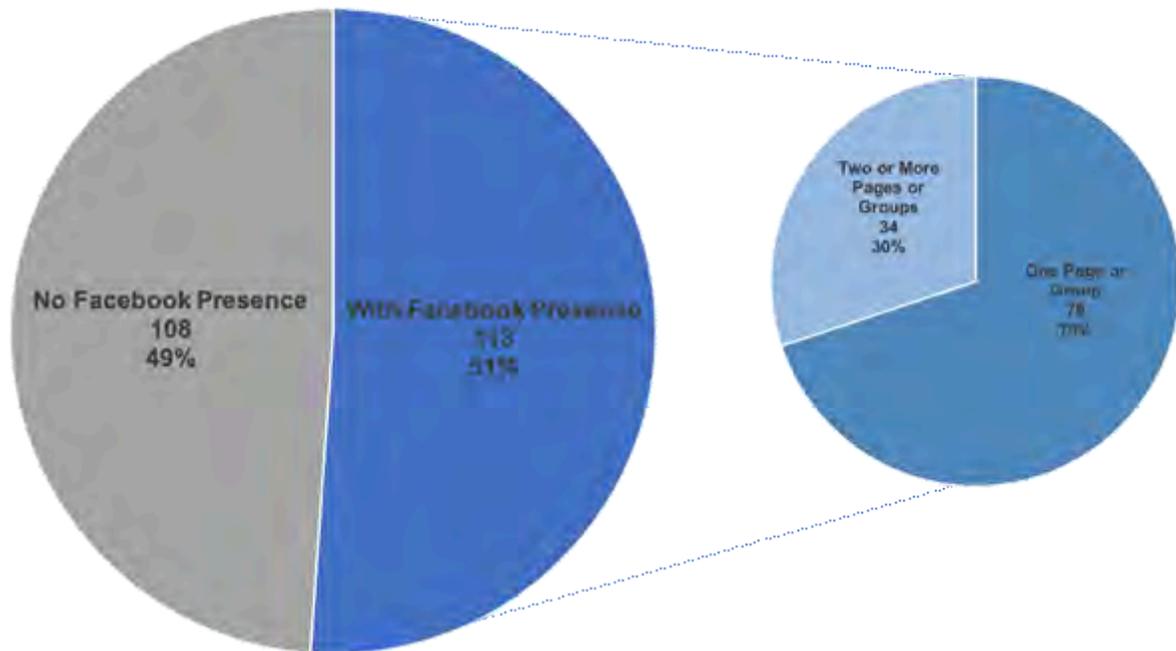
### **Facebook is Creating Pages for Hate Groups**

TTP examined the Facebook presence of 221 hate groups affiliated with white supremacy. The groups were identified via the Anti-Defamation League’s (ADL) [Hate Symbols Database](https://www.adl.org/hate-symbols) (<https://www.adl.org/hate-symbols>) and the Southern Poverty Law Center’s (SPLC) [2019 Hate Map](https://www.splcenter.org/hate-map) (<https://www.splcenter.org/hate-map>), an annual census of hate groups operating in the U.S.

TTP used ADL’s glossary of white supremacist terms and movements to identify relevant groups in the Hate Symbols Database. With the SPLC Hate Map, TTP used the 2019 map categories of Ku Klux Klan, neo-Confederate, neo-Nazi, [neo-völkisch](https://www.splcenter.org/fighting-hate/extremist-files/ideology/neo-volkisch) (<https://www.splcenter.org/fighting-hate/extremist-files/ideology/neo-volkisch>), racist skinhead, and white nationalist to identify relevant groups. Of the 221 groups identified by TTP, 21 were listed in both the ADL and SPLC databases.

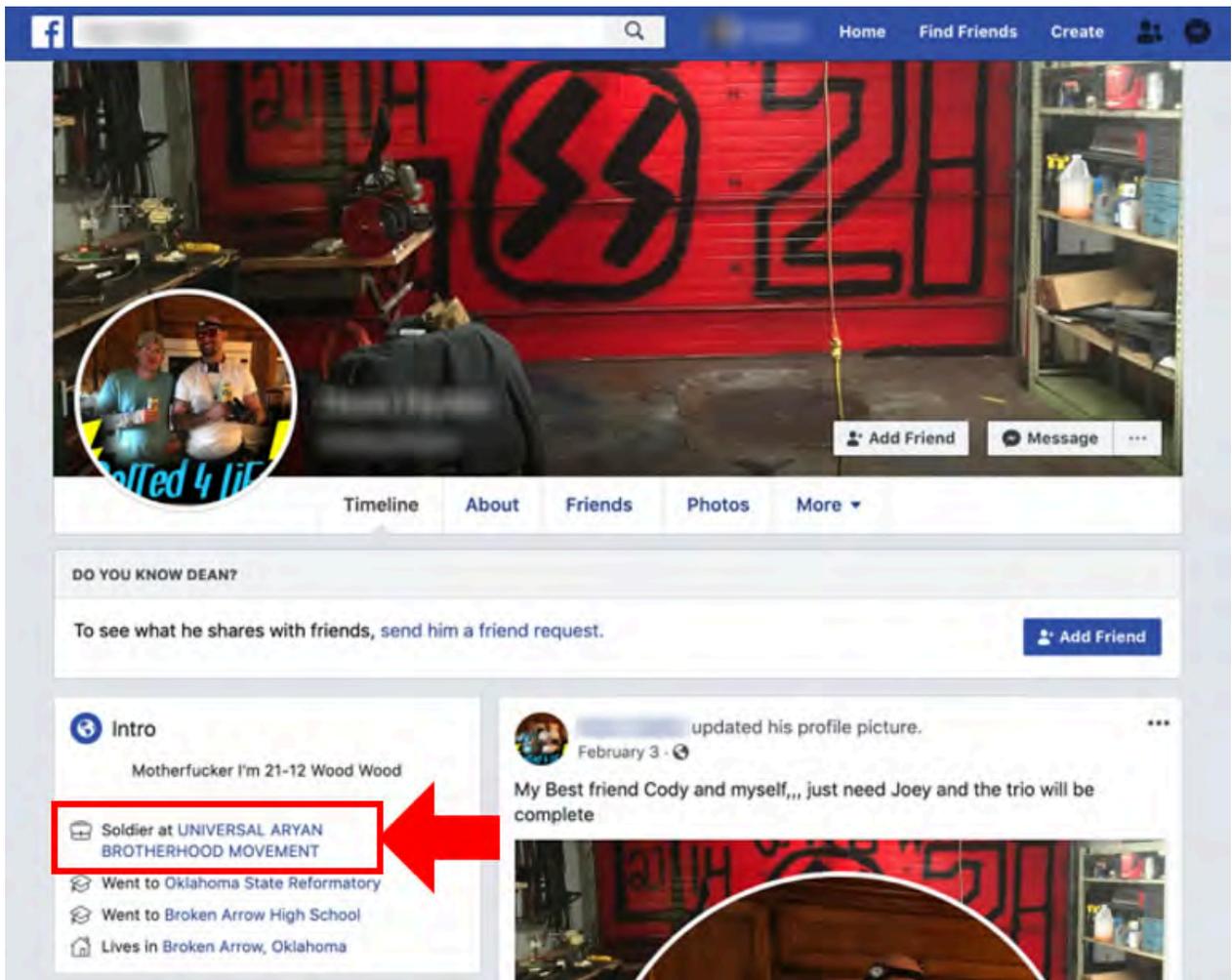
TTP found that 51% (113) of the organizations examined had a presence on Facebook in the form of Pages or Groups. Of the 113 hate groups with a presence, 34 had two or more associated Pages on Facebook, resulting in a total of 153 individual Pages and four individual Groups.

## White Supremacist Groups on Facebook



Roughly 36% (52 Facebook Pages and four Facebook Groups) of the content identified was created by users. One user-generated Page (<https://www.facebook.com/Arktos/>), for a group designated as white nationalist by SPLC had more than 42,000 "likes" on Facebook and has been active since 2010.

The remaining 64% of the white supremacy content identified by TTP involved Pages that had been auto-generated by Facebook. These Pages are automatically created by Facebook when a user lists a job in their profile that does not have an existing Page. When a user lists their work position as "Universal Aryan Brotherhood Movement," for instance, Facebook generates a business page for that group.



Since the publication of this report, Facebook has removed 137 of the 153 white supremacist Pages identified by TTP, including all but two of the auto-generated Pages. All of the Facebook Groups identified by TTP, however, remained active.

The auto-generation problem has existed for some time (<https://www.bbc.com/news/technology-48217827>). In April 2019, an anonymous whistleblower filed a Securities and Exchange Commission (SEC) petition (<https://www.whistleblowers.org/wp-content/uploads/2019/05/Facebook-SEC-Petition-2019.pdf>), regarding extremism on the platform and Facebook's practice of auto-generating business pages for terrorist and white supremacist groups. Some of these Facebook-generated Pages gained thousands of "likes," giving a way for the groups to identify potential recruits, according to the whistleblower.

One of the auto-generated hate group Pages with the most "likes" in TTP's analysis was for the Council of Conservative Citizens, an SPLC-designated white nationalist group. The group made headlines in 2015 after an online manifesto linked to white supremacist Dylann Roof referenced the organization (<https://www.theatlantic.com/politics/archive/2015/06/council-of-conservative-citizens-dylann-roof/396467/>); Roof opened fire at a historically black church in South Carolina, killing nine people. Facebook's auto-generated Page for the Council of Conservative Citizens included a description of the group's white supremacist affiliations, complete with a direct link to their website.

Facebook's role creating Pages for organizations like these undermines claims by the company that it bars hate groups (<https://docs.house.gov/meetings/JU/JU00/20190409/109266/HHRG-116-JU00-Wstate-PottsN-20190409.pdf>).

*"Our rules have always been clear that white supremacists are not*

*allowed on our platform  
under any circumstances."*

*– Neil Potts, Facebook public policy director*

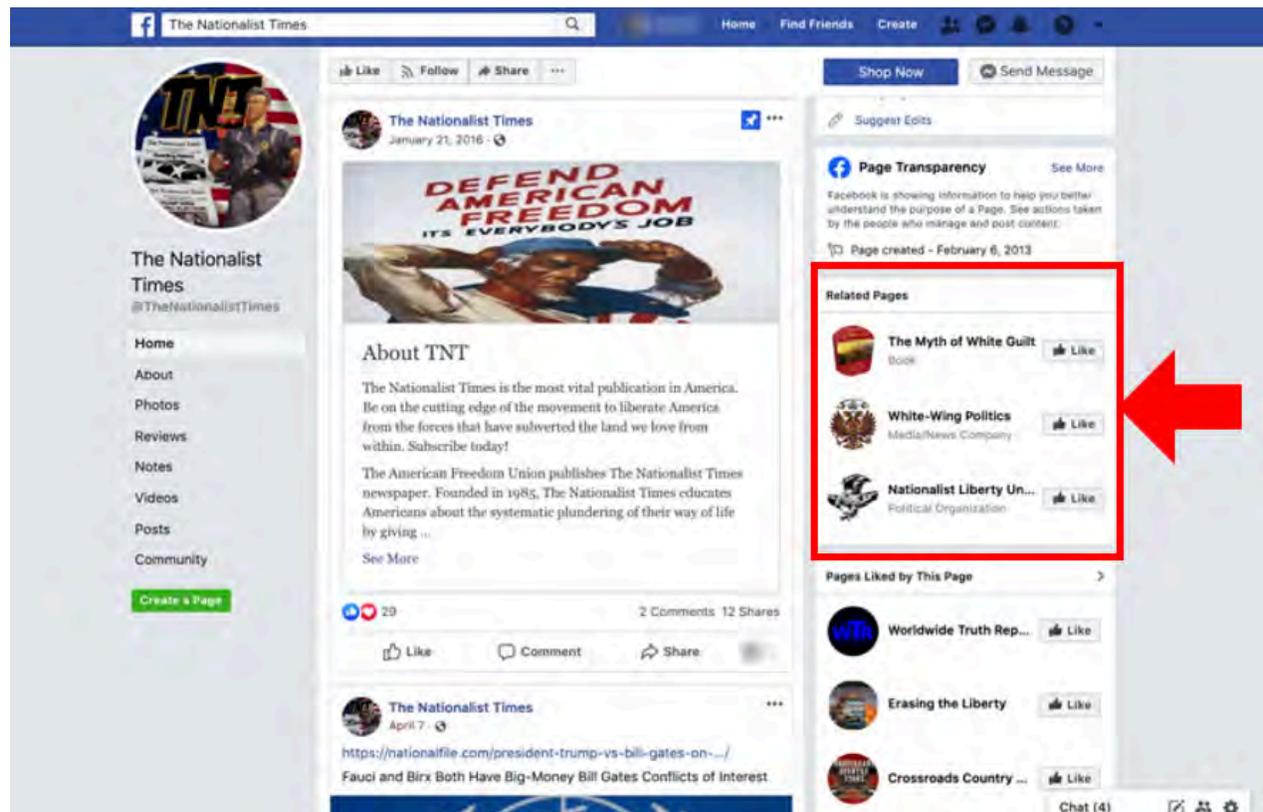
#### Related Pages: Facebook's Extremist Echo Chamber

The TTP review highlights flaws in Facebook's content moderation system, which relies heavily on artificial intelligence (AI) and Facebook users to report problematic content to human moderators for review (<https://www.npr.org/2019/07/01/737498507/for-facebook-content-moderators-traumatizing-material-is-a-job-hazard>).

Relying on users to identify objectionable material doesn't work well when the platform is designed to connect users with shared ideologies, experts have noted, since white supremacists are unlikely to object to racist content they see on Facebook. "A lot of Facebook's moderation revolves around users flagging content. When you have this kind of vetting process, you don't run the risk of getting thrown off Facebook," according to SPLC research analyst Keegan Hanks (<https://www.theguardian.com/technology/2017/jul/31/extremists-neo-nazis-facebook-groups-social-media-islam>).

Artificial intelligence, which Facebook has touted for years as the solution to identifying and removing bad content, also has limitations when it comes to hate speech (<https://www.barrons.com/articles/facebook-artificial-intelligence-hate-speech-51558724564>). AI can miss deliberate misspellings; manipulation of words to include numbers, symbols, and emojis; and missing spaces in sentences. Neo-Nazis, for example, have managed to avoid detection through simple measures like replacing "S" with "\$." (<https://psmag.com/ideas/neo-nazi-hate-speech-foiling-algorithms>).

At the same time, Facebook's algorithms can create an echo chamber of white supremacy through its "Related Pages" feature, which suggests similar Pages to keep users engaged on a certain topic. TTP's investigation found that among the 113 hate groups that had a Facebook presence, 77 of them had Pages that displayed Related Pages, often pointing people to other extremist or right-wing content. In some cases, the Related Pages directed users to additional SPLC- or ADL-designated hate groups.

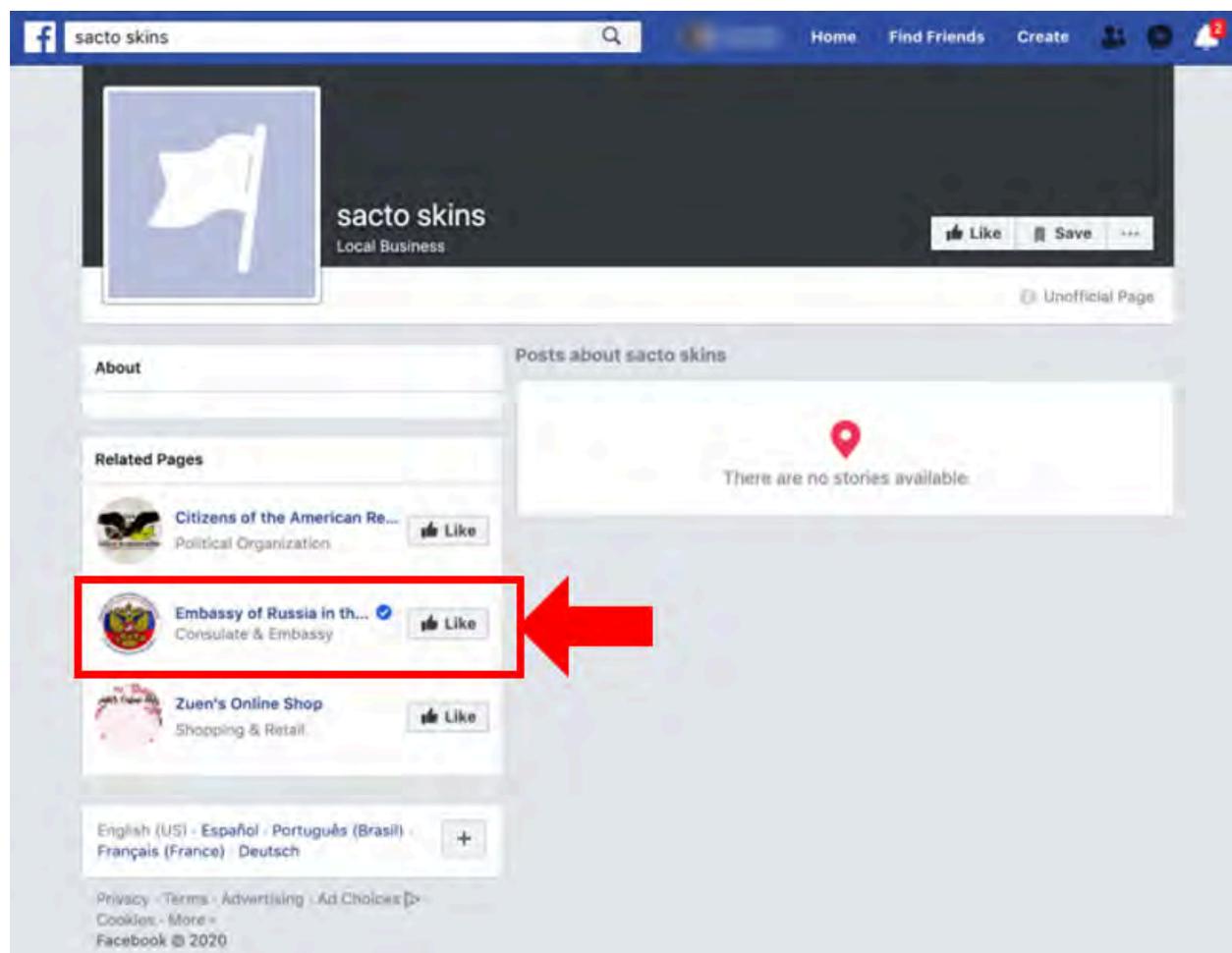


For example, TTP found that the user-generated Page for Nazi Low Riders, an [ADL-listed hate group](https://www.adl.org/resources/profiles/nazi-low-riders) (<https://www.adl.org/resources/profiles/nazi-low-riders>), showed Related Pages for other groups associated with white supremacy. The top recommendation was another user-generated Page called "Aryanbrotherhood." (By omitting the space between the two words, the Page may have been trying to evade Facebook's AI systems, as discussed above.) The Aryan Brotherhood is "the oldest and most notorious racist prison gang in the United States," [according to ADL](https://www.adl.org/education/references/hate-symbols/aryan-brotherhood) (<https://www.adl.org/education/references/hate-symbols/aryan-brotherhood>).

The Aryanbrotherhood Facebook Page in turn displayed Related Pages for more white supremacist ideologies, some of them making reference to "peckerwoods," [a term associated with racist prison and street gangs](https://www.adl.org/education/references/hate-symbols/peckerwood) (<https://www.adl.org/education/references/hate-symbols/peckerwood>).

The Related Pages listed on the [user-generated Page of American Freedom Union](https://www.facebook.com/TheNationalistTimes) (<https://www.facebook.com/TheNationalistTimes>), an SPLC-designated white nationalist group, included a link to a Page for the book "[White Identity: Racial Consciousness in the 21st Century](https://www.facebook.com/Whiteldentity/?ref=py_c)," ([https://www.facebook.com/Whiteldentity/?ref=py\\_c](https://www.facebook.com/Whiteldentity/?ref=py_c)). The book was authored by Jared Taylor, who [runs the website for American Renaissance](https://www.thedailybeast.com/cheats/2016/01/10/white-nationalists-campaigning-for-trump) (<https://www.thedailybeast.com/cheats/2016/01/10/white-nationalists-campaigning-for-trump>), another SPLC-designated white nationalist group.

Facebook's algorithms even pick up on links between organizations that may not be obvious to others. For example, the [auto-generated Page](https://www.facebook.com/pages/sacto-skins/109545472400512) for Sacto Skins (<https://www.facebook.com/pages/sacto-skins/109545472400512>), a short form of the [SPLC-designated racist hate group](https://www.splcenter.org/fighting-hate/intelligence-report/2015/active-racist-skinhead-groups) Sacto Skinheads (<https://www.splcenter.org/fighting-hate/intelligence-report/2015/active-racist-skinhead-groups>), included a Related Page recommendation for Embassy of Russia in the United States. A recent investigation by *The New York Times* found that [Russian intelligence services](https://www.nytimes.com/2020/03/10/us/politics/russian-interference-race.html?referringSource=articleShare) (<https://www.nytimes.com/2020/03/10/us/politics/russian-interference-race.html?referringSource=articleShare>) are using Facebook and other social media to try to incite white supremacists ahead of the 2020 election.



This web of white supremacist Pages surfaced by Facebook's algorithms is not new. The non-profit Counter Extremism Project, in a [2018 report about far-right groups on Facebook](#)

([https://www.counterextremism.com/sites/default/themes/bricktheme/pdfs/The\\_Far\\_Right\\_on\\_Facebook.pdf](https://www.counterextremism.com/sites/default/themes/bricktheme/pdfs/The_Far_Right_on_Facebook.pdf)), identified multiple white supremacist and far-right Pages by following the Related Pages feature.

### Banned Groups Persist

Facebook's Community Standards have included rules against hate speech for years, but in the past three years the company has expanded its efforts.

One significant change came quietly in 2017, following mounting [reports about white supremacist activity on Facebook](https://www.forbes.com/sites/rebeccaheilweil/2017/07/18/facebook-removes-only-a-fraction-of-hate-groups-flagged-by-activists/#4ef2cdde2711) (<https://www.forbes.com/sites/rebeccaheilweil/2017/07/18/facebook-removes-only-a-fraction-of-hate-groups-flagged-by-activists/#4ef2cdde2711>). The company didn't publicly announce a policy change, but the Internet Archive shows that in mid-July, it added "organized hate groups" to the "Dangerous Organizations" section of its Community Standards. (The change can be seen from [here](https://web.archive.org/web/20170629012605/https://www.facebook.com/communitystandards/#dangerous-organizations) (<https://web.archive.org/web/20170629012605/https://www.facebook.com/communitystandards/#dangerous-organizations>) to [here](https://web.archive.org/web/20170726012723/https://www.facebook.com/communitystandards/#dangerous-organizations) (<https://web.archive.org/web/20170726012723/https://www.facebook.com/communitystandards/#dangerous-organizations>),) The company did not, however, specify how it would define such hate groups.



Unite the Right rally participants preparing to enter Lee Park in Charlottesville, Virginia on August 12, 2017. Photo by Anthony Crider.

(<https://www.splcenter.org/hatewatch/2017/07/26/neo-nazi-misfits-join-unite-right>). According to one media report, Facebook only pulled the listing [the day before the rally](https://www.businessinsider.com/facebook-removed-unite-the-right-charlottesville-rally-event-page-one-day-before-2017-8) (<https://www.businessinsider.com/facebook-removed-unite-the-right-charlottesville-rally-event-page-one-day-before-2017-8>), in which one woman was killed and more than a dozen others injured when a white supremacist [drove into a crowd of counter-protestors](https://www.nytimes.com/2019/06/28/us/james-fields-sentencing.html) (<https://www.nytimes.com/2019/06/28/us/james-fields-sentencing.html>), in Charlottesville.

Amid the ensuing public outcry, Facebook announced removals of a [number of hate groups](https://www.theguardian.com/technology/2017/aug/16/daily-stormer-forced-dark-web-reddit-facebook-ban-hate-groups) (<https://www.theguardian.com/technology/2017/aug/16/daily-stormer-forced-dark-web-reddit-facebook-ban-hate-groups>) including White Nationalists United and Right Wing Death Squad.

Facebook scrambled again in early 2019 following the Christchurch attack, in which a gunman used Facebook to stream the massacre of 51 people at a pair of mosques in New Zealand. As the killings made headlines around the world, the company said it would [ban "white nationalist" content](https://www.theguardian.com/technology/2019/mar/27/facebook-white-nationalism-hate-speech-ban) (<https://www.theguardian.com/technology/2019/mar/27/facebook-white-nationalism-hate-speech-ban>), along with the previously banned category of white supremacy. Facebook Chief Operating Officer Sheryl Sandberg also said a handful of hate groups in

Despite the policy update, Facebook didn't immediately take down an event page for the "Unite the Right" rally, which SPLC had [tied to neo-Nazis](#)

Australia and New Zealand would be banned (<https://about.instagram.com/blog/announcements/sheryl-sandbergs-statement-on-new-zealand-shooting>).

Two months after the New Zealand attack, however, *BuzzFeed News* found that extremist groups Facebook claimed to have banned were still on the platform (<https://www.buzzfeednews.com/article/janelytynenko/facebook-white-nationalist-ban-evaded>). Later that year, *The Guardian* identified multiple white nationalist Pages on Facebook (<https://www.theguardian.com/technology/2019/nov/21/facebook-white-nationalists-ban-vdare-red-ice>) but said the company “declined to take action against any of the pages identified.” Online extremism expert Megan Squire told BuzzFeed, “Facebook likes to make a PR move and say that they’re doing something but they don’t always follow up on that.”

Research suggests there continues to be a gap between Facebook’s public relations responses and the company’s enforcement of its own policies. A recent report by TTP (<https://www.techtransparencyproject.org/articles/broken-promises-year-later-christchurch-attack-videos-still-on-facebook>) found that videos of the Christchurch attack continued to circulate on the platform a year later, despite Facebook’s vow to remove them.

Since 2017, Facebook announced removals of at least 14 white supremacist and white nationalist groups in the U.S. and Canada, according (<https://thehill.com/policy/technology/437844-facebook-bans-white-nationalist-groups-after-criticism>), to (<https://www.theverge.com/2018/10/30/18045410/facebook-bans-proud-boys-far-right-extremist-group-gavin-mcinnis>), media (<https://www.theguardian.com/technology/2017/aug/16/daily-stormer-forced-dark-web-reddit-facebook-ban-hate-groups>), reports (<https://observer.com/2017/08/charlottesville-facebook-removes-racist-pages/>), tallied (<https://techcrunch.com/2017/08/16/hatespeech-white-supremacy-nazis-social-networks/>) by TTP. (Only one of these groups, Vanguard America, is included in the TTP’s review of 221 white supremacist groups named by the SPLC and ADL.) Of the 14 groups, four continue to have an active presence on Facebook: Awakening Red Pill, Wolves of Odin, Right Wing Death Squad, and Physical Removal.

TTP identified three user-generated Pages for Right Wing Death Squad that are currently active on Facebook. All (<https://www.facebook.com/RightWingDS/>), three (<https://www.facebook.com/RealRightWingDeathSquad/>), Pages (<https://www.facebook.com/RightWingDeathSquadsAssemble>) identified by TTP were created before the Unite the Right rally and were never removed by Facebook.

The Right Wing Death Squad Pages include extremist language as well as references to the ["boogaloo,"](https://www.adl.org/blog/the-boogaloo-extremists-new-slang-term-for-a-coming-civil-war) (https://www.adl.org/blog/the-boogaloo-extremists-new-slang-term-for-a-coming-civil-war), the term used by extremists to reference a coming civil war. Some of the Right Wing Death Squad Pages brand themselves as anti-globalist, a term often considered a [dog whistle for anti-Semitism](https://www.theatlantic.com/politics/archive/2018/03/the-origins-of-the-globalist-slur/555479/) (https://www.theatlantic.com/politics/archive/2018/03/the-origins-of-the-globalist-slur/555479/).

In March 2020, Facebook announced the [removal of a network of white supremacists linked to the Northwest Front](https://www.bloomberg.com/news/articles/2020-03-25/facebook-removes-network-of-white-supremacist-accounts?sref=VDXBDEF) (https://www.bloomberg.com/news/articles/2020-03-25/facebook-removes-network-of-white-supremacist-accounts?sref=VDXBDEF), an SPLC-designated hate group that has been called ["the worst racists" in America](https://www.politico.com/magazine/story/2015/07/northwest-front-americas-worst-racists-119803) (https://www.politico.com/magazine/story/2015/07/northwest-front-americas-worst-racists-119803). Facebook's director of counterterrorism Brian Fishman said the action came after the group, which had been banned for years, [tried to "reestablish a presence" on the platform](https://www.motherjones.com/politics/2020/03/facebook-just-revealed-its-secret-strategy-for-taking-down-hate-groups/) (https://www.motherjones.com/politics/2020/03/facebook-just-revealed-its-secret-strategy-for-taking-down-hate-groups/). TTP, however, found that the auto-generated Page for Northwest Front was not removed and that searches for the group's name on Facebook still fail to trigger the company's re-direct effort to Life After Hate.

Facebook also said it [removed a network of accounts linked to the VDARE](https://about.fb.com/news/2020/05/april-cib-report/) (https://about.fb.com/news/2020/05/april-cib-report/), an [SPLC-designated white nationalist group](https://www.splcenter.org/fighting-hate/extremist-files/group/vdare) (https://www.splcenter.org/fighting-hate/extremist-files/group/vdare), and individuals associated with a similar website called The Unz Review, in April 2020. Facebook said the group had engaged in "suspected coordinated inauthentic behavior ahead of the 2020 election," and described VDARE's anti-immigrant focus without mentioning its link to white nationalism. According to Facebook, the network spent a total of \$114,000 on advertising through the platform.

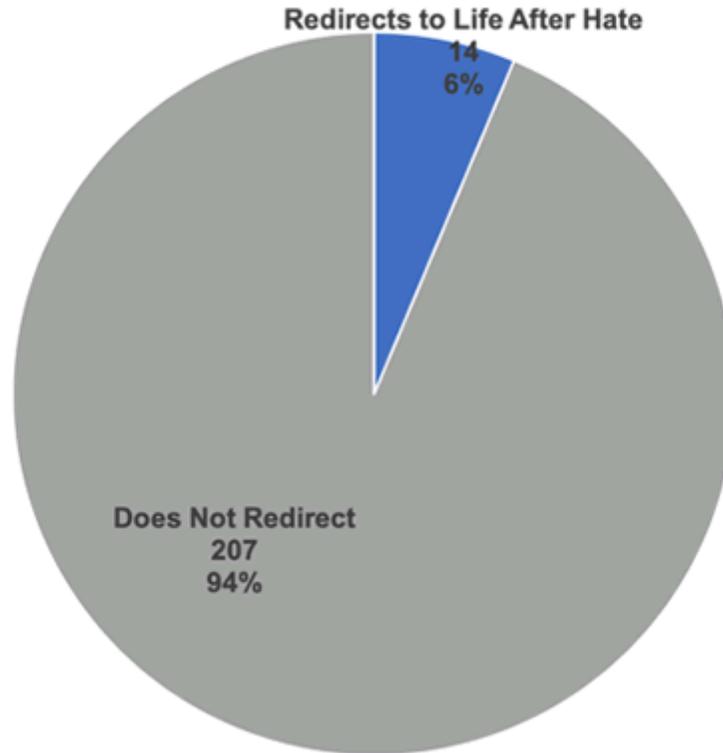
As with the action against the Northwest Front, Facebook failed to remove the auto-generated VDARE Page. Clicking on the Page's link to the VDARE website generates a notice that states, "The link you tried to visit goes against our Community Standards." Still, it is unclear why Facebook allows the auto-generated Page to stay up when it acknowledges the group violates its Community Standards.

#### Failing to Direct Away from Hate

As part of Facebook's expanded efforts to combat white supremacy on the platform following the Christchurch attack, the company said in March 2019 that it would re-direct users who search for terms related to hate.

"Searches for terms associated with white supremacy will surface a link to Life After Hate's Page, where people can find support in the form of education, interventions, academic research and outreach," the company announced (<https://about.fb.com/news/2019/03/standing-against-hate/>).

## Facebook Searches for White Supremacist Groups



TTP found that not only did Facebook's anti-hate link fail to surface in the majority of hate group searches, but in some cases, the platform directed users to other white supremacist Pages.

TTP conducted a search for each of the 221 hate groups associated with white supremacy and white nationalism listed by SPLC and ADL. Only 6% of the searches (14 groups) surfaced the link to Life After Hate.

One factor may be that not all of the hate groups listed by SPLC and ADL make their ideologies obvious in their names. But even organizations that have "Nazi" or "Ku Klux Klan" in their names escaped the redirect effort. Of 25 groups with "Ku Klux Klan" in their official name, only one triggered the link to anti-hate resources.

The redirect tool even failed to work on groups that Facebook has explicitly banned. TTP used Facebook's search function to search the names of the 14 white supremacist groups in North America that Facebook said it had banned. The Proud Boys were the only one of the groups to trigger the platform's Life After Hate link.

Facebook began removing accounts and pages linked to the far-right Proud Boys (<https://www.theverge.com/2018/10/30/18045410/facebook-bans-proud-boys-far-right-extremist-group-gavin-mcinnnes>), in October 2018 after members of the group clashed with anti-fascist protestors. Searches for the group today generate Facebook's Life After Hate link, and TTP did not find any official Proud Boys Pages on the platform.

But the Facebook search for Proud Boys did bring up a Page for "Proud to be a White American," (<https://www.facebook.com/proudtobewhite/>), which describes itself as being for "The promotion of white initiatives and white causes."

(Notably, the "Proud to be a White American" Page is listed above a Page called "Proud Boys" that does not appear to be affiliated with the far-right group.)

The screenshot shows a Facebook search results page for the query "proud boys". The search bar at the top contains the text "proud boys" and a magnifying glass icon. Below the search bar is a navigation menu with options: All, Posts, People, Photos, Videos, Marketplace, Pages, Places, Groups, Apps, Events, and Links. The "All" tab is selected. On the left side, there is a "Filter Results" section with several categories: "POSTS FROM" (Anyone, You, Your Friends, Your Groups and Pages, Public, Choose a Source...), "POST TYPE" (All Posts, Posts You've Seen), "POSTED IN GROUP" (Any Group, Your Groups, Choose a Group...), "TAGGED LOCATION" (Anywhere, Choose a Location...), and "DATE POSTED" (Any Date). The main content area displays five search results:

- Keeping Our Community Safe**: A page with a blue shield icon. Text: "These keywords may be associated with dangerous groups and individuals. Facebook works with organizations that help prevent the spread of hate and violent extremism." A "Learn More" button is present.
- Texas boys proud**: A page with a Texas map icon. Text: "Page - 1.4K like this". A "Like" button is present. Below the text, it says "Follow us on Instagram:".
- Proud to be a White American**: A page with a red "NO" icon. Text: "Page - 18K like this". A "Like" button is present. Below the text, it says "The promotion of white initiatives and white causes. If you like this page only to argue and post racist comments you WILL be...".
- Proud boys**: A page with a black "NO" icon. Text: "Page - 205 like this". A "Like" button is present. Below the text, it says "Proud boys we are proud boys".
- Poor Boy Proud**: A group with a globe icon. Text: "Group - 197 members", "7 posts a week". A "+ Join" button is present.

On the right side of the search results, there is a language selection menu with options: English (US), Español, Português (Brasil), Français (France), and Deutsch. Below this menu are links for "Privacy", "Terms", "Advertising", "Ad Choices", "Cookies", and "More", along with the text "Facebook © 2020".

Note: Updated to reflect that Facebook took down some of the Pages identified by TTP following publication of this report. (Latest updated figures as of June 7, 2020.)

**Click here to download the full report** (<https://www.techtransparencyproject.org/sites/default/files/Facebook-White-Supremacy-Report.pdf>) »

**Click here to download data on the hate group websites** (<https://www.techtransparencyproject.org/sites/default/files/SPLC-and-ADL-hate-groups.xlsx>) »

# Exhibit 66

**COUNCIL OF THE DISTRICT OF COLUMBIA  
COMMITTEE ON PUBLIC SAFETY AND THE JUDICIARY  
COMMITTEE REPORT**

1350 Pennsylvania Avenue, NW, Washington, DC 20004

2010 NOV 19 PM 12:55

**TO:** All Councilmembers  
**FROM:** Councilmember Phil Mendelson,  
Chairman, Committee on Public Safety and the Judiciary  
**DATE:** November 18, 2010  
**SUBJECT:** Report on Bill 18-893, "Anti-SLAPP Act of 2010"

*Phil Mendelson*  
OFFICE OF THE  
SECRETARY

The Committee on Public Safety and the Judiciary, to which Bill 18-893, the "Anti-SLAPP Act of 2010" was referred, reports favorably thereon with amendments, and recommends approval by the Council.

**CONTENTS**

I.	Background and Need .....	1
II.	Legislative Chronology .....	5
III.	Position of the Executive .....	6
IV.	Comments of Advisory Neighborhood Commissions .....	6
V.	Summary of Testimony .....	6
VI.	Impact on Existing Law .....	7
VII.	Fiscal Impact .....	7
VIII.	Section-by-Section Analysis .....	7
IX.	Committee Action .....	8
X.	Attachments .....	8

**I. BACKGROUND AND NEED**

Bill 18-893, the Anti-SLAPP Act of 2010, incorporates substantive rights with regard to a defendant's ability to fend off lawsuits filed by one side of a political or public policy debate aimed to punish or prevent the expression of opposing points of view. Such lawsuits, often referred to as strategic lawsuits against public participation -- or SLAPPs -- have been increasingly utilized over the past two decades as a means to muzzle speech or efforts to petition the government on issues of public interest. Such cases are often without merit, but achieve their filer's intention of punishing or preventing opposing points of view, resulting in a chilling effect on the exercise of constitutionally protected rights. Further, defendants of a SLAPP must dedicate a substantially amount of money, time, and legal resources. The impact is not limited to named defendants willingness to speak out, but prevents others from voicing concerns as well. To remedy this Bill 18-893 follows the model set forth in a number of other jurisdictions, and mirrors language found in federal law, by incorporating substantive rights that allow a defendant to more expeditiously, and more equitably, dispense of a SLAPP.

### History of Strategic Lawsuits against Public Participation:

In what is considered the seminal article regarding SLAPPs, University of Denver College of Law Professor George W. Pring described what was then (1989), considered to be a growing litigation “phenomenon”:

Americans are being sued for speaking out politically. The targets are typically not extremists or experienced activists, but normal, middle-class and blue-collar Americans, many on their first venture into the world of government decision making. The cases are not isolated or localized aberrations, but are found in every state, every government level, every type of political action, and every public issue of consequence. There is no dearth of victims: in the last two decades, thousands of citizens have been sued into silence.<sup>1</sup>

These lawsuits, Pring noted, are typically an effort to stop a citizen from exercising their political rights, or to punish them for having already done so. To further identify the problem, and be able to draw possible solutions, Pring engaged in a nationwide study of SLAPPs with University of Denver sociology Professor Penelope Canan.

Pring and Canan’s study established the base criteria of a SLAPP as: (1) a civil complaint or counterclaim (for monetary damages and/or injunction); (2) filed against non-governmental individuals and/or groups; (3) because of their communications to a government body, official or electorate; and (4) on an issue of some public interest or concern.<sup>2</sup> The study of 228 SLAPPs found that, despite constitutional, federal and state statute, and court decisions that expressly protect the actions of the defendants, these lawsuits have been allowed to flourish because they appear, or are camouflaged by those bringing the suit, as a typical tort case. The vast majority of the cases identified by the study were brought under legal charges of defamation (such as libel and slander), or as such business torts as interference with contract.<sup>3</sup>

In identifying possible solutions to litigation aimed at silencing public participation, Pring paid particular attention to a 1984 opinion of the Colorado Supreme Court establishing a new rule for trial courts to allow for dismissal motions for SLAPP suits.<sup>4</sup> In recognition of the

---

<sup>1</sup> George W. Pring, *SLAPPS: Strategic Lawsuits against Public Participation*, Pace Env. L. Rev, Paper 132, 1 (1989), available at <http://digitalcommons.pace.edu/cgi/viewcontent.cgi?article=1122&context=enlavl> (last visited Nov. 17, 2010).

<sup>2</sup> *Id.* at 7-8.

<sup>3</sup> *Id.* at 8-9.

<sup>4</sup> *Protect Our Mountain Env’t, Inc. v. District Court*, 677 P.2d 1361 (Colo. 1984). The three-prong test developed by the court requires:

When [ ] a plaintiff sues another for alleged misuse or abuse of the administrative or judicial processes of government, and the defendant files a motion to dismiss by reason of the constitutional right to petition, the plaintiff must make a sufficient showing to permit the court to reasonably conclude that the defendant’s petitioning activities were not immunized from liability under the First Amendment because: (1) the defendant’s administrative or judicial claims were devoid of reasonable factual support, or, if so supportable, lacked any cognizable basis in law for their assertion; and (2) the primary purpose of the defendant’s petitioning activity was to harass the

growing problem of SLAPPs, a number of jurisdictions have, legislatively, created a similar special motion to dismiss in order to expeditiously, and more fairly deal with SLAPPs. According to the California Anti-SLAPP Project, a public interest law firm and policy organization dedicated to fighting SLAPPs in California, as of January 2010 there are approximately 28 jurisdictions in the United States that have adopted anti-SLAPP measures. Likewise, there are nine jurisdictions (not including the District of Columbia) that are currently considering legislation to address the issue. Also, one other jurisdiction has joined Colorado in addressing SLAPPs through judicial doctrine.<sup>5</sup>

This issue has also recently been taken up by the federal government, with the introduction of the H.R. 4363, the Citizen Participation Act of 2009. This legislation would provide certain procedural protections for any act in furtherance of the constitutional right of petition or free speech, and specifically incorporate a special motion to dismiss for SLAPPs.<sup>6</sup>

#### **SLAPPs in the District of Columbia:**

Like the number of jurisdictions that have sensed the need to address SLAPPs legislatively, the District of Columbia is no stranger to SLAPPs. The American Civil Liberties Union of the Nation's Capital (ACLU), in written testimony provided to the Committee (attached), described two cases in which the ACLU was directly involved, as counsel for defendants, in such suits against District residents.<sup>7</sup>

The actions that typically draw a SLAPP are often, as the ACLU noted, the kind of grassroots activism that should be hailed in our democracy. In one of the examples provided, the ACLU discussed the efforts of two Capitol Hill advocates that opposed the efforts of a certain developer. When the developer was unable to obtain a building permit, the developer sued the activists and the community organization alleging they "conducted meetings, prepared petition drives, wrote letters and made calls and visits to government officials, organized protests, organized the preparation and distribution of ... signs, and gave statements and interviews to various media."<sup>8</sup> Such activism, however, was met with years of litigation and, but for the ACLU's assistance, would have resulted in outlandish legal costs to defend. Though the actions

---

plaintiff or to effectuate some other improper objective; and (3) the defendant's petitioning activity had the capacity to adversely affect a legal interest of the plaintiff.

*Id.* at 1369.

<sup>5</sup> California Anti-SLAPP Project (CASP) website, Other states: Statutes and cases, *available at* <http://www.casp.net/statutes/menstate.html> (last visited Nov. 11, 2010).

<sup>6</sup> <http://www.thomas.gov/cgi-bin/bdquery/D?d111:1:/temp/~bdLBBX:@@L&summ2=m&/home/LegislativeData.php>

<sup>7</sup> *Bill 18-893, Anti-SLAPP Act of 2010: Public Hearing of the Committee on Public Safety and the Judiciary*, Sept. 17, 2010, at 2-3 (written testimony Arthur B. Spitzer, Legal Director, American Civil Liberties Union of the Nation's Capital).

<sup>8</sup> *Id.* at 2 (quoting from lawsuit in *Father Flanagan's Boys Home v. District of Columbia et al.*, Civil Action No. 01-1732 (D.D.C)).

of these participants should have been protected, they, and any others who wished to express opposition to the project, were met with intimidation.

What has been repeated by many who have studied this issue, from Pring on, is that the goal of the litigation is not to win the lawsuit but punish the opponent and intimidate them into silence. As Art Spitzer, Legal Director for the ACLU, noted in his testimony “[*litigation itself is the plaintiff’s weapon of choice.*”<sup>9</sup>

#### **District Anti-SLAPP Act:**

In June 2010, legislation was introduced to remedy this nationally recognized problem here in the District of Columbia. As introduced, this measure closely mirrored the federal legislation introduced the previous year. Bill 18-893 provides a defendant to a SLAPP with substantive rights to expeditiously and economically dispense of litigation aimed to prevent their engaging in constitutionally protected actions on matters of public interest.

Following the lead of other jurisdictions, which have similarly extended absolute or qualified immunity to individuals engaging in protected actions, Bill 18-893 extends substantive rights to defendants in a SLAPP, providing them with the ability to file a special motion to dismiss that must be heard expeditiously by the court. To ensure a defendant is not subject to the expensive and time consuming discovery that is often used in a SLAPP as a means to prevent or punish, the legislation tolls discovery while the special motion to dismiss is pending. Further, in recognition that SLAPP plaintiffs frequently include unspecified individuals as defendants -- in order to intimidate large numbers of people that may fear becoming named defendants if they continue to speak out -- the legislation provides an unnamed defendant the ability to quash a subpoena to protect his or her identity from disclosure if the underlying action is of the type protected by Bill 18-893. The legislation also allows for certain costs and fees to be awarded to the successful party of a special motion to dismiss or a special motion to quash.

Bill 18-893 ensures that District residents are not intimidated or prevented, because of abusive lawsuits, from engaging in political or public policy debates. To prevent the attempted muzzling of opposing points of view, and to encourage the type of civic engagement that would be further protected by this act, the Committee urges the Council to adopt Bill 18-893.

## **II. LEGISLATIVE CHRONOLOGY**

June 29, 2010	Bill 18-893, the “Anti-SLAPP Act of 2010,” is introduced by Councilmembers Cheh and Mendelson, co-sponsored by Councilmember M. Brown, and is referred to the Committee on Public Safety and the Judiciary.
---------------	---

---

<sup>9</sup> *Id.* at 3.

- July 9, 2010 Notice of Intent to act on Bill 18-893 is published in the *District of Columbia Register*.
- August 13, 2010 Notice of a Public Hearing is published in the *District of Columbia Register*.
- September 17, 2010 The Committee on Public Safety and the Judiciary holds a public hearing on Bill 18-893.
- November 18, 2010 The Committee on Public Safety and the Judiciary marks-up Bill 18-893.

### III. POSITION OF THE EXECUTIVE

The Executive provided no witness to testify on Bill 18-893 at the September 17, 2010 hearing. The Office of the Attorney General provided a letter subsequent to the hearing stating the need to review the legislation further.

### IV. COMMENTS OF ADVISORY NEIGHBORHOOD COMMISSIONS

The Committee received no testimony or comments from Advisory Neighborhood Commissions.

### V. SUMMARY OF TESTIMONY

The Committee on Public Safety and the Judiciary held a public hearing on Bill 18-893 on Friday, September 17, 2010. The testimony summarized below is from that hearing. A copy of submitted testimony is attached to this report.

**Robert Vinson Brannum, President, D.C. Federation of Civic Associations, Inc.**, testified in support of Bill 18-893.

**Ellen Opper-Weiner, Public Witness**, testified in support of Bill 18-893. Ms. Opper-Weiner recounted her own experience in SLAPP litigation, and suggested several amendments to strengthen the legislation.

**Dorothy Brizill, Public Witness**, testified in support of Bill 18-893. Ms. Brizill recounted her own experience in SLAPP litigation. She stated that the legislation is the next step in advancing free speech in the District of Columbia.

**Arthur B. Spitzer, Legal Director, American Civil Liberties Union of the Nation's Capital**, provided a written statement in support of the purpose and general approach of Bill 18-

893, but suggested several changes to the legislation as introduced. A copy of this statement is attached to this report.

Although no Executive witness presented testimony, Attorney General for the District of Columbia, Peter Nickles, expressed concern that certain provisions of the bill might implicate the Home Rule Act prohibition against enacting any act with respect to any provision of Title 11 of the D.C. Official Code. A copy of his letter is attached to this report.

## **VI. IMPACT ON EXISTING LAW**

Bill 18-893 adds new provisions in the D.C. Official Code to provide an expeditious process for dealing with strategic lawsuits against public participation (SLAPPs). Specifically, the legislation provides a defendant to a SLAPP with substantive rights to have a motion to dismiss heard expeditiously, to delay burdensome discovery while the motion to dismiss is pending, and to provide an unnamed defendant the ability to quash a subpoena to protect his or her identity from disclosure if the underlying action is of the type protected by Bill 18-893. The legislation also allows for the costs of litigation to be awarded to the successful party of a special motion to dismiss created under this act.

## **VII. FISCAL IMPACT**

The attached November 16, 2010 Fiscal Impact Statement from the Chief Financial Officer states that funds are sufficient to implement Bill 18-893. This legislation requires no additional funds or staff.

## **VIII. SECTION-BY-SECTION ANALYSIS**

Several of the changes to the Committee Print from Bill 18-893 as introduced stem from the recommendations of the American Civil Liberties Union of the Nation's Capital (ACLU). For a more thorough explanation of these changes, see the September 17, 2010 testimony of the ACLU attached to this report.

- |                  |   |
|------------------|---|
| <u>Section 1</u> | States the short title of Bill 18-893.  |
| <u>Section 2</u> | Incorporates definitions to be used throughout the act.   |
| <u>Section 3</u> | Creates the substantive right of a party subject to a claim under a SLAPP suit to file a special motion to dismiss within 45 days after service of the claim. |

- Subsection (a)* Creates a substantive right of a defendant to pursue a special motion to dismiss for a lawsuit regarding an act in furtherance of the right of advocacy on issues of public interest.
- Subsection (b)* Provides that, upon a prima facie showing that the activity at issue in the litigation falls under the type of activity protected by this act, the court shall dismiss the case unless the responding party can show a likelihood of succeeding upon the merits.
- Subsection (c)* Tolls discovery proceedings upon the filing of a special motion to dismiss under this act. As introduced the legislation permitted an exemption to this for good cause shown. The Committee Print has tightened this language in this provision so that the court may permit specified discovery if it is assured that such discovery would not be burdensome to the defendant.
- Subsection (d)* Requires the court to hold an expedited hearing on a special motion to dismiss filed under this act.

As introduced, the Committee Print contained a subsection (e) that would have provided a defendant with a right of immediate appeal from a court order denying a special motion to dismiss. While the Committee agrees with and supports the purpose of this provision, a recent decision of the DC Court of Appeals states that the Council exceeds its authority in making such orders reviewable on appeal.<sup>10</sup> The dissenting opinion in that case provides a strong argument for why the Council should be permitted to legislate this issue. However, under the majority opinion the Council is restricted from expanding the authority of District's appellate court to hear appeals over non-final orders of the lower court. The provision that has been removed from the bill as introduced would have provided an immediate appeal over a non-final order (a special motion to dismiss).

Section 4 Creates a substantive right of a person to pursue a special motion to quash a subpoena aimed at obtaining a persons identifying information relating to a lawsuit regarding an act in furtherance of the right of advocacy on issues of public interest.

- Subsection (a)* Creates the special motion to quash.
- Subsection (b)* Provides that, upon a prima facie showing that the underlying claim is of the type of activity protected by this act, the court shall grant the special

---

<sup>10</sup> See *Stuart v. Walker*, 09-CV-900 (DC Ct of App 2010) at 4-5.

motion to quash unless the responding party can show a likelihood of succeeding upon the merits.

Section 5 Provides for the awarding of fees and costs for prevailing on a special motion to dismiss or a special motion to quash. The court is also authorized to award reasonable attorney fees where the underlying claim is determined to be frivolous.

Section 6 Provides exemptions to this act for certain claims.

Section 7 Adopts the Fiscal Impact Statement.

Section 8 Establishes the effective date by stating the standard 30-day Congressional review language.

## IX. COMMITTEE ACTION

On November 18, 2010, the Committee on Public Safety and the Judiciary met to consider Bill 18-893, the "Anti-SLAPP Act of 2010." The meeting was called to order at 1:50 p.m., and Bill 18-893 was the fourth item on the agenda. After ascertaining a quorum (Chairman Mendelson and Councilmembers Alexander, Cheh, and Evans present; Councilmembers Bowser absent), Chairman Mendelson moved the print, along with a written amendment to repeal section 3(e) of the circulated draft print, with leave for staff to make technical changes. After an opportunity for discussion, the vote on the print was three aye (Chairman Mendelson and Councilmembers Evans and Cheh), and one present (Councilmember Alexander). Chairman Mendelson then moved the report, with leave for staff to make technical and editorial changes. After an opportunity for discussion, the vote on the report was three aye (Chairman Mendelson and Councilmembers Evans and Cheh), and one present (Councilmember Alexander). The meeting adjourned at 2:15 p.m.

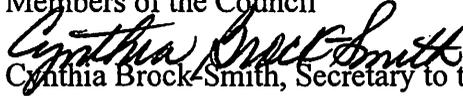
## X. ATTACHMENTS

1. Bill 18-893 as introduced.
2. Written testimony and comments.
3. Fiscal Impact Statement
4. Committee Print for Bill 18-893.

**COUNCIL OF THE DISTRICT OF COLUMBIA**  
**1350 Pennsylvania Avenue, N.W.**  
**Washington, D.C. 20004**

**Memorandum**

---

To: Members of the Council  
From:   
Cynthia Brock-Smith, Secretary to the Council  
Date: July 7, 2010  
Subject: (Correction)  
Referral of Proposed Legislation

Notice is given that the attached proposed legislation was introduced in the Legislative Meeting on Tuesday, June 29, 2010. Copies are available in Room 10, the Legislative Services Division.

TITLE: "Anti-SLAPP Act of 2010", B18-0893

INTRODUCED BY: Councilmembers Cheh and Mendelson  
CO-SPONSORED BY: Councilmember M. Brown

The Chairman is referring this legislation to the Committee on Public Safety and the Judiciary.

Attachment

cc: General Counsel  
Budget Director  
Legislative Services

1 

2  
3 Councilmember Phil Mendelson



4  
5  
6 Councilmember Mary M. Cheh

7 A BILL

8  
9 \_\_\_\_\_  
10  
11 IN THE COUNCIL OF THE DISTRICT OF COLUMBIA  
12  
13 \_\_\_\_\_  
14  
15

16  
17 Councilmembers Mary M. Cheh and Phil Mendelson introduced the following bill, which  
18 was referred to the Committee on \_\_\_\_\_.

19  
20 To provide a special motion for the quick and efficient dismissal of strategic lawsuits  
21 against public participation (SLAPPs), to stay proceedings until the motion is  
22 considered, to provide a motion to quash attempts to seek personally identifying  
23 information; and to award the costs of litigation to the successful party on a  
24 special motion.

25  
26 BE IT ENACTED BY THE COUNCIL OF THE DISTRICT OF COLUMBIA,

27 That this act may be cited as the "Anti-SLAPP Act of 2010".

28 Sec. 2. Definitions.

29 For the purposes of this Act, the term:

30 (1) "Act in furtherance of the right of free speech" means:

31 (A) Any written or oral statement made:

32 (i) In connection with an issue under consideration or review by a  
33 legislative, executive, or judicial body, or any other official proceeding authorized by  
34 law;

35 (ii) In a place open to the public or a public forum in connection  
36 with an issue of public interest; or

1 (B) Any other conduct in furtherance of the exercise of the constitutional  
2 right to petition the government or the constitutional right of free expression in  
3 connection with an issue of public interest.

4 (2) "Issue of public interest" means an issue related to health or safety;  
5 environmental, economic or community well-being; the District government; a public  
6 figure; or a good, product or service in the market place. The term "issue of public  
7 interest" shall not be construed to include private interests, such as statements directed  
8 primarily toward protecting the speaker's commercial interests rather than toward  
9 commenting on or sharing information about a matter of public significance.

10 (3) "Claim" includes any civil lawsuit, claim, complaint, cause of action, cross-  
11 claim, counterclaim, or other judicial pleading or filing requesting relief.

12 (4) "Government entity" means the Government of the District of Columbia and  
13 its branches, subdivisions, and departments.

14 Sec. 3. Special Motion to Dismiss.

15 (a) A party may file a special motion to dismiss any claim arising from an act in  
16 furtherance of the right of free speech within 45 days after service of the claim.

17 (b) A party filing a special motion to dismiss under this section must make a  
18 prima facie showing that the claim at issue arises from an act in furtherance of the right  
19 of free speech. If the moving party makes such a showing, the responding party may  
20 demonstrate that the claim is likely to succeed on the merits.

21 (c) Upon the filing of a special motion to dismiss, discovery proceedings on the  
22 claim shall be stayed until notice of entry of an order disposing of the motion, except that  
23 the court, for good cause shown, may order that specified discovery be conducted.

1 (d) The court shall hold an expedited hearing on the special motion to dismiss,  
2 and issue a ruling as soon as practicable after the hearing. If the special motion to dismiss  
3 is granted, dismissal shall be with prejudice.

4 (e) The defendant shall have a right of immediate appeal from a court order  
5 denying a special motion to dismiss in whole or in part.

6 Sec. 4. Special Motion to Quash.

7 (a) A person whose personally identifying information is sought, pursuant to a  
8 discovery order, request, or subpoena, in connection with an action arising from an act in  
9 furtherance of the right of free speech may make a special motion to quash the discovery  
10 order, request, or subpoena.

11 (b) The person bringing a special motion to quash under this section must make a  
12 prima facie showing that the underlying claim arises from an act in furtherance of the  
13 right of free speech. If the person makes such a showing, the claimant in the underlying  
14 action may demonstrate that the underlying claim is likely to succeed on the merits.

15 Sec. 5. Fees and costs.

16 (a) The court may award a person who substantially prevails on a motion brought  
17 under sections 3 or 4 of this Act the costs of litigation, including reasonable attorney fees.

18 (b) If the court finds that a motion brought under sections 3 or 4 of this Act is  
19 frivolous or is solely intended to cause unnecessary delay, the court may award  
20 reasonable attorney fees and costs to the responding party.

21 Sec. 6. Exemptions.

22 (a) This Act shall not apply to claims brought solely on behalf of the public or  
23 solely to enforce an important right affecting the public interest.

1 (b) This Act shall not apply to claims brought against a person primarily engaged  
2 in the business of selling or leasing goods or services, if the statement or conduct from  
3 which the claim arises is a representation of fact made for the purpose of promoting,  
4 securing, or completing sales or leases of, or commercial transactions in, the person's  
5 goods or services, and the intended audience is an actual or potential buyer or customer.

6 Sec. 7. Fiscal impact statement.

7 The Council adopts the fiscal impact statement in the committee report as the  
8 fiscal impact statement required by section 602(c)(3) of the District of Columbia Home  
9 Rule Act, approved December 24, 1973 (87 Stat. 813; D.C. Official Code § 1-  
10 206.02(c)(3)).

11 Sec. 8. Effective date.

12 This act shall take effect following approval by the Mayor (or in the event of veto  
13 by the Mayor, action by the Council to override the veto), a 30-day period of  
14 Congressional review as provided in section 602(c)(1) of the District of Columbia Home  
15 Rule Act, approved December 24, 1973 (87 Stat. 813; D.C. Official Code § 1-  
16 206.02(c)(1)), and publication in the District of Columbia Register.

Testimony of the  
**American Civil Liberties Union  
of the Nation's Capital**

by

Arthur B. Spitzer  
Legal Director

before the

Committee on Public Safety and the Judiciary  
of the  
Council of the District of Columbia

on

Bill 18-893, the  
“Anti-SLAPP Act of 2010”

September 17, 2010

.....

The ACLU of the Nation's Capital appreciates this opportunity to testify on Bill 18-893. We support the purpose and the general approach of this bill, but we believe it requires some significant polishing in order to achieve its commendable goals.

**Background**

In a seminal study about twenty years ago, two professors at the University of Denver identified a widespread pattern of abusive lawsuits filed by one side of a political or public policy dispute—usually the side with deeper pockets and ready access to counsel—to punish or prevent the expression of opposing points of view. They dubbed these “Strategic Lawsuits Against Public Participation,” or “SLAPPs.” *See* George W. Pring and Penelope Canan, *SLAPPS: GETTING SUED FOR SPEAKING OUT* (Temple University Press 1996). They pinpointed several criteria that identify a SLAPP:

— The actions complained of “involve communicating with government officials, bodies, or the electorate, or encouraging others to do so.” *Id.* at 150.

— The defendants are “involved in speaking out for or against some issue under consideration by some level of government or the voters.” *Id.*

— The legal claims filed against the speakers tend to fall into predictable categories such as defamation, interference with prospective economic advantage, invasion of privacy, and conspiracy. *Id.* at 150-51.

— The lawsuit often names “John or Jane Doe defendants.” *Id.* at 151. “We have found whole communities chilled by the inclusion of Does, fearing ‘they will add my name to the suit.’” *Id.*

The authors “conservatively estimate[d] that ... tens of thousands of Americans have been SLAPPed, and still more have been muted or silenced by the threat.” *Id.* at xi. Finding that “the legal system is not effective in controlling SLAPPs,” *id.*, they proposed the adoption of anti-SLAPP statutes to address the problem. *Id.* at 201.

Responding to the continuing use of SLAPPs by those seeking to silence opposition to their activities, twenty-six states and the Territory of Guam have now enacted anti-SLAPP statutes.<sup>1</sup>

The ACLU of the Nation’s Capital has been directly involved, as counsel for defendants, in two SLAPPs involving District of Columbia residents.

In the first case, a developer that had been frustrated by its inability promptly to obtain a building permit sued a community organization (Southeast Citizens for Smart Development) and two Capitol Hill activists (Wilbert Hill and Ellen Oppenheimer) who had opposed its efforts. The lawsuit claimed that the defendants had violated the developer’s rights when they “conducted meetings, prepared petition drives, wrote letters and made calls and visits to government officials, organized protests, organized the preparation and distribution of ... signs, and gave statements and interviews to various media,” and when they created a web site that urged people to “call, write or e-mail the mayor” to ask him to stop the project. The defendants’ activities exemplified the kind of grassroots activism that should be hailed in a democracy, and the lawsuit was a classic SLAPP. The case was eventually dismissed, and the dismissal affirmed on appeal.<sup>2</sup> But the litigation took several years, and during all that time the defendants and their neighbors were worried about whether they might face liability. Because the ACLU represented the citizens and their organization at no charge, they were not financially harmed. But had they been required to retain paid counsel, the cost would have been substantial, and intimidating.

---

<sup>1</sup> Links to these statutes can be found at <http://www.casp.net/menstate.html>.

<sup>2</sup> *Father Flanagan’s Boys Home v. District of Columbia, et al.*, Civil Action No. 01-1732 (D.D.C.), *aff’d*, 2003 WL 1907987 (No. 02-7157, D.C. Cir. 2003).

In the second case we represented Dorothy Brizill, who needs no introduction to this Committee. She was sued in Guam for defamation, invasion of privacy, and “interference with prospective business advantage,” based on statements she made in a radio interview broadcast there about the activities of the gambling entrepreneur who backed the proposed 2004 initiative to legalize slot machines in the District of Columbia. This lawsuit was also a classic SLAPP, filed against her in the midst of the same entrepreneur’s efforts to legalize slot machines on Guam, in an effort to silence her. And to intimidate his opponents, twenty “John Does” were also named as defendants. With the help of Guam’s strong anti-SLAPP statute, the case was dismissed, and the dismissal was affirmed by the Supreme Court of Guam.<sup>3</sup> But once again, the litigation lasted more than two years, and had Ms. Brizill been required to retain paid counsel to defend herself, it would have cost her hundreds of thousands of dollars.

As professors Pring and Canan demonstrated, a SLAPP plaintiff’s real goal is not to win the lawsuit but to punish his opponents and intimidate them and others into silence. *Litigation itself* is the plaintiff’s weapon of choice; a long and costly lawsuit is a victory for the plaintiff even if it ends in a formal victory for the defendant. That is why anti-SLAPP legislation is needed: to enable a defendant to bring a SLAPP to an end quickly and economically.

### **Bill 18-893**

Bill 18-893 would help end SLAPPs quickly and economically by making available to the defendant a “special motion to dismiss” that has four noteworthy features:

- The motion must be heard and decided expeditiously.
- Discovery is generally stayed while the motion is pending.
- If the motion is denied the defendant can take an immediate appeal.
- Most important, the motion is to be granted if the defendant shows that he or she was engaged in protected speech or activity, unless the plaintiff can show that he or she is nevertheless likely to succeed on the merits.

Speaking generally, this is sensible path to the desired goal, and speaking generally, the ACLU endorses it. If a lawsuit looks like a SLAPP, swims like a SLAPP, and quacks like a SLAPP, then it probably is a SLAPP, and it is fair and reasonable to put the burden on the plaintiff to show that it isn’t a SLAPP.

We do, nevertheless, have a number of suggestions for improvement, including a substantive change in the definition of the conduct that is to be protected by the proposed law.

---

<sup>3</sup> *Guam Greyhound, Inc. v. Brizill*, 2008 Guam 13, 2008 WL 4206682.

**Section 2(1).** The bill begins by defining the term “Act in furtherance of the right of free speech,” which is used to signify the conduct that can be protected by a special motion to dismiss. In our view, it would be better to use a different term, because the “right of free speech” is already a term in very common use, with a broader meaning than the meaning given in this bill, and it will be impossible, or nearly so, for litigants, lawyers and even judges (and especially the news media) to avoid confusion between the common meaning of the “right of free speech” and the special, narrower meaning given to it in this bill. It would be akin to defining the term “fruit” to mean “a curved yellow edible food with a thick, easily-peeled skin.” This specially-defined term deserves a special name that will not require a struggle to use correctly. We suggest “Act in furtherance of the right of advocacy on issues of public interest.”

**Section 2(1)(A).** Because there is no conjunction at the end of section 2(1)(A)(i), the bill is ambiguous as to whether sections 2(1)(A)(i) and (ii) are conjunctive or disjunctive. That is, in order to be covered, must a statement be made “In connection with an ... official proceeding” *and* “In a place open to the public or a public forum in connection with an issue of public interest,” or is a statement covered if it is made *either* “In connection with an ... official proceeding,” *or* “In a place open to the public or a public forum in connection with an issue of public interest”?

We urge the insertion of the word “or” at the end of section 2(1)(A)(i) to make it clear that statements are covered in either case. A statement made “In connection with an issue under consideration or review by a legislative, executive, or judicial body, or any other official proceeding authorized by law” certainly deserves anti-SLAPP protection whether it is made in a public place or in a private place. For example, a statement made to a group gathered by invitation in a person’s living room, or made to a Councilmember during a non-public meeting, should be protected. Likewise, a statement made “In a place open to the public or a public forum in connection with an issue of public interest” deserves anti-SLAPP protection whether or not it is also connected to an “official proceeding.” For example, statements by residents addressing a “Stop the Slaughterhouse” rally should be protected even if no official proceeding regarding the construction of a slaughterhouse has yet begun.<sup>4</sup>

---

<sup>4</sup> It appears that these definitions, along with much of Bill 18-893, were modeled on the Citizen Participation Act of 2009, H.R. 4364 (111th Cong., 1st Sess.), introduced by Rep. Steve Cohen of Tennessee (*available at* <http://thomas.loc.gov/cgi-bin/query/z?c111:H.R.4364.IH>:). In that bill it is clear that speech or activity that falls under any one of these definitions is covered.

**Section 2(1)(B).** Section 2(1)(B) expands the definition of protected activity to include “any other conduct in furtherance of the exercise of the constitutional right to petition the government or the constitutional right of free expression in connection with an issue of public interest.” We fully agree with the intent of this provision, but we think it fails as a definition because it is backwards—it requires a court *first* to determine whether given conduct is protected by the Constitution *before* it can determine whether that conduct is covered by the Anti-SLAPP Act. But if the conduct is protected by the Constitution, then there is no need for the court to determine whether it is covered by the Anti-SLAPP Act: a claim arising from that conduct must be dismissed because the conduct is protected by the Constitution. And yet the task of determining whether given conduct is protected by the Constitution is often quite difficult, and can require exactly the kinds of lengthy, expensive legal proceedings (including discovery) that the bill is intended to avoid.

This very problem arose in the *Brizill* case, where the Guam anti-SLAPP statute protected “acts in furtherance of the Constitutional rights to petition,” and Mr. Baldwin argued that the statute therefore provided no broader protection for speech than the Constitution itself provided. *See* 2008 Guam 13 ¶ 28. He argued, for example, that Ms. Brizill’s speech was not protected by the statute because it was defamatory, and defamation is not protected by the Constitution. As a result, the defendant had to litigate the constitutional law of defamation on the way to litigating the SLAPP issues. This should not be necessary, as the purpose of an anti-SLAPP law is to provide broader protection than existing law already provides. Bill 18-893 should be amended to avoid creating the same problem here.<sup>5</sup>

We therefore suggest amending Section 2(1)(B) to say: “Any other expression or expressive conduct that involves petitioning the government or communicating views to members of the public in connection with an issue of public interest.”

**Section 2(4).** Section 2(4) defines the term “government entity.” But that term is never used in the bill. It should therefore be deleted.<sup>6</sup>

---

<sup>5</sup> The Supreme Court of Guam ultimately rejected the argument that “Constitutional rights” meant “constitutionally protected rights,” *see id.* at ¶ 32, but that was hardly a foregone conclusion, and the D.C. Court of Appeals might not reach the same conclusion under Section 2(1)(B).

<sup>6</sup> The same term is defined in H.R. 4364, but it is then used in a section providing that “A government entity may not recover fees pursuant to this section.”

**Section 3(b)**. We agree with what we understand to be the intent of this provision, setting out the standards for a special motion to dismiss. But the text of this section fails to accomplish its purpose because it never actually spells out what a court is supposed to do. We suggest revising Section 3(b) as follows:

(b) If a party filing a special motion to dismiss under this section makes a prima facie showing that the claim at issue arises from an act in furtherance of the right of advocacy on issues of public interest, then the motion shall be granted unless the responding party demonstrates that the claim is likely to succeed on the merits, in which case the motion shall be denied.

**Section 3(c)**. We agree that discovery should be stayed on a claim as to which a special motion to dismiss has been filed. This is an important protection, for discovery is often burdensome and expensive. Because expression on issues of public interest deserves special protection, a plaintiff who brings a claim based on a defendant's expression on an issue of public interest ought to be required to show a likelihood of success on that claim without the need for discovery.

A case may exist in which a plaintiff could prevail on such a claim after discovery but cannot show a likelihood of success without discovery, but in our view the dismissal of such a hypothetical case is a small price to pay for the public interest that will be served by preventing the all-but-automatic discovery that otherwise occurs in civil litigation over the sorts of claims that are asserted in SLAPPs.

As an exception to the usual stay of discovery, Section 3(c) permits a court to allow "specified discovery" after the filing of a special motion to dismiss "for good cause shown." We agree that a provision allowing some discovery ought to be included for the exceptional case. But while the "good cause" standard has the advantage of being flexible, it has the disadvantage of being completely subjective, so that a judge who simply feels that it's unfair to dismiss a claim without discovery can, in effect, set the Anti-SLAPP Act aside and allow a case to proceed in the usual way. In our view, it would be better if the statute spelled out more precisely the circumstances under which discovery might be allowed, and also included a provision allowing the court to assure that such discovery would not be burdensome to the defendant. For example: "...except that the court may order that specified discovery be conducted when it appears likely that targeted discovery will enable the plaintiff to defeat the motion and that the discovery will not be unduly burdensome. Such an order may be conditioned upon the plaintiff paying any expenses incurred by the defendant in responding to such discovery."

Finally, we note that this section provides that discovery shall be stayed “until notice of entry of an order disposing of the motion.” That language tracks H.R. 4364, but “notice of entry” of court orders is not part of D.C. Superior Court procedure. We suggest that the bill be amended to provide that “... discovery proceedings on the claim shall be stayed until the motion has been disposed of, including any appeal taken under section 3(e), ...”

**Sections 3(d) and (e).** We agree that a special motion to dismiss should be expedited and that its denial should be subject to an interlocutory appeal. The Committee may wish to consider whether the Court of Appeals should also be directed to expedite its consideration of such an appeal. The D.C. Court of Appeals often takes years to rule on appeals.

**Section 4.** Section 4 is focused on the fact that SLAPPs frequently include unspecified individuals (John and Jane Does) as defendants. As observed by professors Pring and Canan, this is one of the tactics employed by SLAPP plaintiffs to intimidate large numbers of people, who fear that they may become named defendants if they continue to speak out on the relevant public issue.

There can be very legitimate purposes for naming John and Jane Does as defendants in civil litigation. The ACLU sometimes names John and Jane Does as defendants when it does not yet know their true identities—for example, when unknown police officers are alleged to have acted unlawfully.<sup>7</sup> It is therefore necessary to balance the right of a plaintiff to proceed against an as-yet-unidentified person who has violated his rights, and to use the court system to discover that person’s identity, against the right of an individual not to be made a defendant in an abusive SLAPP that was filed for the purpose of retaliating against, or chilling, legitimate civic activity.

We believe that Section 4 strikes an appropriate balance by making available to a John or Jane Doe a “special motion to quash,” protecting his or her identity from disclosure if he or she was acting in a manner that is protected by the Anti-SLAPP Act, and if the plaintiff cannot make the same showing of likely success on the merits that is required to defeat a special motion to dismiss.

Like Section 3(b), however, Section 4(b) never actually spells out what a court is supposed to do. We therefore suggest revising Section 4(b) in the same manner we suggested revising Section 3(b):

---

<sup>7</sup> See, e.g., *YoungBey v. District of Columbia, et al.*, No. 09-cv-596 (D.D.C.) (suing the District of Columbia, five named MPD officers, and 27 “John Doe” officers in connection with an unlawful pre-dawn SWAT raid of a District resident’s home).

(b) If a person bringing a special motion to quash under this section makes a prima facie showing that the underlying claim arises from an act in furtherance of the right of advocacy on issues of public interest, then the motion shall be granted unless the party seeking his or her personally identifying information demonstrates that the underlying claim is likely to succeed on the merits, in which case the motion shall be denied.

**Section 6(a).** Section 6(a) provides that “This Act shall not apply to claims brought solely on behalf of the public or solely to enforce an important right affecting the public interest.” This language is vague and tremendously broad. Almost any plaintiff can and will assert that he is bringing his claims “to enforce an important right affecting the public interest,” and neither this bill nor any other source we know gives a court any guidance regarding what “an important right affecting the public interest” might be. The plaintiffs in the two SLAPP suits described above, in which the ACLU of the Nation’s Capital represented the defendants, vigorously argued that they were seeking to enforce an important right affecting the public interest: the developer argued that it was seeking to provide housing for disadvantaged youth; the gambling entrepreneur argued that he was seeking to prevent vicious lies from affecting the result of an election.

Thus, this provision will almost certainly add an entire additional phase to the litigation of every SLAPP suit, with the plaintiff arguing that the anti-SLAPP statute does not even apply to his case because he is acting in the public interest. To the extent that courts accept such arguments, this provision is a poison pill with the potential to turn the anti-SLAPP statute into a virtually dead letter. At a minimum, it will subject the rights of SLAPP defendants to the subjective opinions of more than 75 different Superior Court judges regarding what is or is not “an important right affecting the public interest.”

Moreover, we think the exclusion created by Section 6(a) is constitutionally problematic because it incorporates a viewpoint-based judgment about what is or is not in the public interest—after all, what is in the public interest necessarily depends upon one’s viewpoint.

—Assume, for example, that D.C. Right To Life (RTL) makes public statements that having an abortion causes breast cancer. Assume Planned Parenthood sues RTL, alleging that those statements impede its work and cause psychological harm to its members. RTL files a special motion to dismiss under the Anti-SLAPP Act, showing that it was communicating views to members of the public in connection with an issue of public interest. But Planned Parenthood responds that its lawsuit is not subject to the Anti-SLAPP Act because it was

“brought ... solely to enforce an important right affecting the public interest,” to wit, the right to reproductive choice.

—Now assume that Planned Parenthood makes public statements that having an abortion under medical supervision is virtually risk-free. RTL sues Planned Parenthood, alleging that those statements impede its work and cause psychological harm to its members. Planned Parenthood files a special motion to dismiss under the Anti-SLAPP Act, showing that it was communicating views to members of the public in connection with an issue of public interest. But RTL responds that its lawsuit is not subject to the Anti-SLAPP Act because it was “brought ... solely to enforce an important right affecting the public interest,” to wit, the right to life.

Are both lawsuits exempt from the Anti-SLAPP Act? Neither? One but not the other? We fear that the result is likely to depend on the viewpoint of the judge regarding which asserted right is “an important right affecting the public interest.” But the First Amendment requires the government to provide evenhanded treatment to speech on all sides of public issues. We see no good reason for the inclusion of Section 6(a), and many pitfalls. Accordingly, we urge that it be deleted.<sup>8</sup>

Thank you for your consideration of our comments.

---

<sup>8</sup> Section 10 of H.R. 4364, on which Section 6(a) of Bill 18-893 is modeled, begins with the catchline “Public Enforcement.” It therefore appears that Section 10 was intended to exempt only enforcement actions brought by the government.

Even if that is true, we see no good reason to exempt the government, as a litigant, from a statute intended to protect the rights of citizens to speak freely on issues of public interest. To the contrary, the government should be held to the strictest standards when it comes to respecting those rights. *See, e.g., White v. Lee*, 227 F.3d 1214 (9th Cir. 2000) (holding that the advocacy activities of neighbors who opposed the conversion of a motel into a multi-family housing unit for homeless persons were protected by the First Amendment, and that an intrusive eight-month investigation into their activities and beliefs by the regional Fair Housing and Equal Opportunity Office violated their First Amendment rights).

We therefore urge the complete deletion of Section 6(a), as noted above. However, if the Committee does not delete Section 6(a) entirely, its coverage should be limited to lawsuits brought by the government.

**GOVERNMENT OF THE DISTRICT OF COLUMBIA**  
**Office of the Attorney General**



**ATTORNEY GENERAL**

September 17, 2010

The Honorable Phil Mendelson  
Chairperson  
Committee on Public Safety & the Judiciary  
Council of the District of Columbia  
1350 Pennsylvania Avenue, N.W., Ste. 402  
Washington, D.C. 20004

Re: Bill 18-893, the "Anti-SLAPP Act of 2010"

Dear Chairperson Mendelson:

I have not yet had the opportunity to study in depth Bill 18-893, the "Anti-SLAPP Act of 2010" ("bill"), which will be the subject of a hearing before your committee today, but I do want to register a preliminary concern about the legislation.

To the extent that sections 3 (special motion to dismiss) and 4 (special motion to quash) of the bill would impact SLAPPs filed in the Superior Court of the District of Columbia, the legislation may run afoul of section 602(a)(4) of the District of Columbia Home Rule Act, approved December 24, 1973, Pub. L. 93-198, 87 Stat. 813 (D.C. Official Code § 1-206.02(a)(4) (2006 Repl.)), which prohibits the Council from enacting any act "with respect to any provision of Title 11 [of the D.C. Code]." In particular, D.C. Official Code § 11-946 (2001) provides, for example, that the Superior Court "shall conduct its business according to the Federal Rules of Civil Procedure...unless it prescribes or adopts rules which modify those Rules [subject to the approval of the Court of Appeals]." As you know, the Superior Court subsequently adopted rules of procedure for civil actions, including Rules 12(c) (Motion for judgment on the pleadings), 26-37 (Depositions and Discovery), and 56 (Summary judgment), which appear to afford the parties to civil actions rights and opportunities that sections 3 and 4 of the bill can be construed to abrogate. Thus, the bill may conflict with the Superior Court's rules of civil procedure and, consequently, violate section 602(a)(4) of the Home Rule Act insofar as that section preserves the D.C. Courts' authority to adopt rules of procedure free from interference by the Council. Accordingly, I suggest that – if you have not already done so – you solicit comments concerning the legislation from the D.C. Courts.

Sincerely,

  
Peter J. Nickles  
Attorney General for the District of Columbia

cc: Vincent Gray, Chairman, Council of the District of Columbia  
Yvette Alexander, Council of the District of Columbia

Government of the District of Columbia  
Office of the Chief Financial Officer



**Natwar M. Gandhi**  
Chief Financial Officer

**MEMORANDUM**

**TO:** The Honorable Vincent C. Gray  
Chairman, Council of the District of Columbia

**FROM:** Natwar M. Gandhi   
Chief Financial Officer

**DATE:** November 16, 2010

**SUBJECT:** Fiscal Impact Statement - "Anti-SLAPP Act of 2010"

**REFERENCE:** Bill Number 18-893, Draft Committee Print Shared with the OCFO on  
November 15, 2010

---

**Conclusion**

Funds are sufficient in the FY 2011 through FY 2014 budget and financial plan to implement the provisions of the proposed legislation.

**Background**

The proposed legislation would provide a special motion for the quick dismissal of claims "arising from an act in furtherance of the right of advocacy on issues of public interest,"<sup>1</sup> which are commonly referred to as strategic lawsuits against public participation (SLAPPs). SLAPPs are generally defined as retaliatory lawsuits intended to silence, intimidate, or punish those who have used public forums to speak, petition, or otherwise move for government action on an issue. Often the goal of SLAPPs is not to win, but rather to engage the defendant in a costly and long legal battle. This legislation would provide a way to end SLAPPs quickly and economically by allowing for this special motion and requiring the court to hold an expedited hearing on it.

In addition, the proposed legislation would provide a special motion to quash attempts arising from SLAPPs to seek personally identifying information, and would allow the courts to award the costs of litigation to the successful party on a special motion.

---

<sup>1</sup> Defined in the proposed legislation as (A) Any written or oral statement made: (i) In connection with an issue under consideration or review by a legislative, executive, or judicial body, or any other official proceeding authorized by law; (ii) In a place open to the public or a public forum in connection with an issue of public interest; or (B) Any other expression or expressive conduct that involves petitioning the government or communicating views to members of the public in connection with an issue of public interest.

The Honorable Vincent C. Gray

FIS: B18-893 "Anti-SLAPP Act of 2010," Draft Committee Print Shared with the OCFO on November 15, 2010

Lastly, the proposed legislation would exempt certain claims from the special motions.

**Financial Plan Impact**

Funds are sufficient in the FY 2011 through FY 2014 budget and financial plan to implement the provisions of the proposed legislation. Enactment of the proposed legislation would not have an impact on the District's budget and financial plan as it involves private parties and not the District government (the Courts are federally-funded). If effective, the proposed legislation could have a beneficial impact on current and potential SLAPP defendants.

COMMITTEE PRINT

Committee on Public Safety & the Judiciary

November 18, 2010

A BILL

18-893

IN THE COUNCIL OF THE DISTRICT OF COLUMBIA

---

To provide a special motion for the quick and efficient dismissal of strategic lawsuits against public participation, to stay proceedings until the motion is considered, to provide a motion to quash attempts to seek personally identifying information; and to award the costs of litigation to the successful party on a special motion.

BE IT ENACTED BY THE COUNCIL OF THE DISTRICT OF COLUMBIA, That this act may be cited as the “Anti-SLAPP Act of 2010”.

Sec. 2. Definitions.

For the purposes of this act, the term:

(1) “Act in furtherance of the right of advocacy on issues of public interest” means:

(A) Any written or oral statement made:

(i) In connection with an issue under consideration or review by a legislative, executive, or judicial body, or any other official proceeding authorized by law; or

(ii) In a place open to the public or a public forum in connection with an issue of public interest.

(B) Any other expression or expressive conduct that involves petitioning the government or communicating views to members of the public in connection with an issue of public interest.

(2) "Issue of public interest" means an issue related to health or safety; environmental, economic, or community well-being; the District government; a public figure; or a good, product, or service in the market place. The term "issue of public interest" shall not be construed to include private interests, such as statements directed primarily toward protecting the speaker's commercial interests rather than toward commenting on or sharing information about a matter of public significance.

(3) "Claim" includes any civil lawsuit, claim, complaint, cause of action, cross-claim, counterclaim, or other judicial pleading or filing requesting relief.

Sec. 3. Special Motion to Dismiss.

(a) A party may file a special motion to dismiss any claim arising from an act in furtherance of the right of advocacy on issues of public interest within 45 days after service of the claim.

(b) If a party filing a special motion to dismiss under this section makes a prima facie showing that the claim at issue arises from an act in furtherance of the right of advocacy on issues of public interest, then the motion shall be granted unless the responding party demonstrates that the claim is likely to succeed on the merits, in which case the motion shall be denied.

(c)(1) Except as provided in paragraph (2), upon the filing of a special motion to dismiss, discovery proceedings on the claim shall be stayed until the motion has been disposed of.

(2) When it appears likely that targeted discovery will enable the plaintiff to defeat the motion and that the discovery will not be unduly burdensome, the court may order that specialized discovery be conducted. Such an order may be conditioned upon the plaintiff paying any expenses incurred by the defendant in responding to such discovery.

(d) The court shall hold an expedited hearing on the special motion to dismiss, and issue a ruling as soon as practicable after the hearing. If the special motion to dismiss is granted, dismissal shall be with prejudice.

#### Sec. 4. Special Motion to Quash.

(a) A person whose personally identifying information is sought, pursuant to a discovery order, request, or subpoena, in connection with a claim arising from an act in furtherance of the right of advocacy on issues of public interest may make a special motion to quash the discovery order, request, or subpoena.

(b) If a person bringing a special motion to quash under this section makes a prima facie showing that the underlying claim arises from an act in furtherance of the right of advocacy on issues of public interest, then the motion shall be granted unless the party seeking his or her personally identifying information demonstrates that the underlying claim is likely to succeed on the merits, in which case the motion shall be denied.

#### Sec. 5. Fees and costs.

(a) The court may award a person who substantially prevails on a motion brought under sections 3 or 4 of this Act the costs of litigation, including reasonable attorney fees.

(b) If the court finds that a motion brought under sections 3 or 4 of this Act is frivolous or is solely intended to cause unnecessary delay, the court may award reasonable attorney fees and costs to the responding party.

Sec. 6. Exemptions.

This Act shall not apply to claims brought against a person primarily engaged in the business of selling or leasing goods or services, if the statement or conduct from which the claim arises is a representation of fact made for the purpose of promoting, securing, or completing sales or leases of, or commercial transactions in, the person's goods or services, and the intended audience is an actual or potential buyer or customer.

Sec. 7. Fiscal impact statement.

The Council adopts the attached fiscal impact statement as the fiscal impact statement required by section 602(c)(3) of the District of Columbia Home Rule Act, approved December 24, 1973 (87 Stat. 813; D.C. Official Code § 1-206.02(c)(3)).

Sec. 8. Effective date.

This act shall take effect following approval by the Mayor (or in the event of veto by the Mayor, action by the Council to override the veto), a 30-day period of Congressional review as provided in section 602(c)(1) of the District of Columbia Home Rule Act, approved December 24, 1973 (87 Stat. 813; D.C. Official Code § 1-206.02(c)(1)), and publication in the District of Columbia Register.

# Exhibit 67

# **Facebook’s Civil Rights Audit – Final Report**

---

July 8, 2020

## Table of Contents

---

<b>About</b>	<b>3</b>
<b>Acknowledgements</b>	<b>4</b>
<b>Introduction by Laura W. Murphy</b>	<b>5</b>
<b>Chapter One: Civil Rights Accountability Structure</b>	<b>13</b>
<b>Chapter Two: Elections &amp; Census 2020</b>	<b>20</b>
<b>Chapter Three: Content Moderation &amp; Enforcement</b>	<b>42</b>
<b>Chapter Four: Diversity &amp; Inclusion</b>	<b>59</b>
<b>Chapter Five: Advertising Practices</b>	<b>72</b>
<b>Chapter Six: Algorithmic Bias</b>	<b>76</b>
<b>Chapter Seven: Privacy</b>	<b>83</b>

## About the Civil Rights Audit

---

This investigation into Facebook's policies and practices began in 2018 at the behest and encouragement of the civil rights community and some members of Congress, proceeded with Facebook's cooperation, and is intended to help the company identify, prioritize, and implement sustained and comprehensive improvements to the way it impacts civil rights.

The Audit was led by Laura W. Murphy, a civil rights and civil liberties leader, along with a team from civil rights law firm Relman Colfax, led by firm partner Megan Cacac

During the first six months of the audit, Laura W. Murphy interviewed and gathered the concerns of over 100 civil rights organizations. Over the course of the Audit's two year engagement, that number exceeded 100 organizations, hundreds of advocates and several members of Congress. The focus areas for the audit, which were informed by those interviews, were described in the [first preliminary audit report](#), released in December 2018. That was followed by a [second update](#) in July 2019, which identified areas of increasing concern for the Auditors. This third report will be the Auditors' final analysis

The Civil Rights Audit is not an audit of Facebook's performance as compared to its tech industry peers. In some areas it may outperform peers with respect to civil rights, and in other areas, it may not. The Auditors are not privy to how other companies operate and therefore do not draw comparisons in this report. The scope of the work on the Audit was focused only on the US and the core Facebook app (rather than Instagram, WhatsApp, or other Facebook, Inc. products).

Page Intentionally Left Blank

These technologies are designed to engage users and keep them coming back, which is pushing us further apart and isolating Americans into information silos.” The Chairman further expressed concern about how Facebook’s algorithm works and whether it prioritizes engagement and attention in a manner that rewards extreme and divisive content.

Facebook argues that the *Wall Street Journal* article used isolated incidents where leadership chose not to approve a possible intervention to make the argument that Facebook doesn’t care about polarization in general. Facebook reports it has commissioned internal & external research, which have informed several [measures the company has taken](#) to fight polarization. Examples include

- **Recalibrating News Feed.** In 2018, Facebook changed News Feed ranking to prioritize posts from friends and family over news content. Additionally, Facebook reports reducing clickbait headlines, reducing links to spam and misleading posts, and improving comment rankings to show people higher quality information.
- **Growth of Its Integrity Team.** Facebook has spent the last four years building a global integrity team that addresses safety and security issues, including polarization. This dedicated team was not in place when some of the internal research referenced was produced.
- **Restricting Recommendations.** If Pages and Groups [repeatedly](#) share content that violates Facebook’s Community Standards, or is rated false by fact-checkers, Facebook reports that it reduces those Pages’ distribution, and removes them from recommendations.

The Auditors do not believe that Facebook is sufficiently attuned to the depth of concern on the issue of polarization and the way that the algorithms used by Facebook inadvertently fuel extreme and polarizing content (even with the measures above). The Auditors believe that Facebook should do everything in its power to prevent its tools and algorithms from driving people toward self-reinforcing echo chambers of extremism, and that the company must recognize that failure to do so can have dangerous (and life-threatening) real-world consequences.

### (iii) Hate Speech Data & Analysis.

The Auditors recommend that Facebook compile data and further study how hate speech manifests on the platform against particular protected groups to enable it to devote additional resources to understanding the form and prevalence of different kinds of hate on the platform, its causes (*e.g.*, policy gaps, global enforcement trends or training issues, *etc.*), and to identify potential remedial steps the company could take.

Currently, when content reviewers remove content for expressing hate against a protected group or groups, Facebook does not capture data as to the protected group(s) against whom the hate speech was directed. Similarly, when users report content as violating hate speech policies, they do not have a way to note which protected class(es) are being attacked in the post. Without this information, Facebook lacks specific metric for evaluating and understanding: (1) the volume of hate broken down by the group targeted, (2) whether there are categories of attacks on particular groups that are prevalent but not consistently removed, (3) whether there

is a gap in policy guidance that has resulted in hate attacks against one religion, race, gender identity, falling through the cracks, based on the particular way those attacks manifested, *etc.*

Because the data would focus on the content of posts and the reasons that content violates Facebook's hate speech policies (rather than anything about the users reporting or posting it), the Auditors are confident that this kind of data collection need not involve collection of any data on users or otherwise implicate privacy concerns.

Facebook and the Auditors have repeatedly heard concerns from civil rights groups that particular forms of hate are prevalent on the platform but the absence of data for analysis and study seems to undercut efforts to document and define the problem, identify its source, and explore potential mitigation.

Take anti-Muslim hate speech, for example. For years the civil rights community has expressed increasing alarm at the level of anti-Muslim hate speech on (and off) the platform. While Christchurch was an inflection point for the Muslim community and its relationship to Facebook, the community's concerns with Facebook existed long before and extend beyond that tragedy. From the organization of events designed to intimidate members of the Muslim community at gathering places, to the prevalence of content demonizing Islam and Muslims, and the use of Facebook Live during the Christchurch massacre, civil rights advocates have expressed alarm that Muslims feel under siege on Facebook — and have criticized Facebook for not doing enough to address it. (Of course, this is not to say that Muslims are alone in experiencing persistent hate on the platform or the sense that they are under attack. Indeed, hate speech and efforts to incite violence targeting African Americans, Jews, Asians and the LGBTQ and LatinX communities, to name a few, have gained national attention in recent months. But, Facebook has not yet publicly studied or acknowledged the particular ways anti-Muslim bigotry manifests on its platform in the same manner it has discussed its root cause analysis of hate speech false positives removals of the posts of African American users and publicly launched pilots to test potential remedies).

Facebook's existing policy prohibits attacks against people based on their religion, including those disguised as attacks against religious concepts (*e.g.*, attacks against "Islam" which use pronouns like "they" or depict people). However, reports from civil rights groups and anecdotal examples suggest that these kinds of attacks persist on the platform and may seem to be more frequent than attacks mentioning Christianity, Judaism, or other religious concepts, making Facebook's distinction between attacks targeted at people versus concepts all the more blurry (and potentially problematic) when it comes to anti-Muslim sentiment.

Having data on the prevalence of anti-Muslim hate speech on the platform, what kinds of content is being flagged as anti-Muslim hate speech, and what percentage and types of content is being removed as anti-Muslim hate speech would be incredibly useful in defining the issue and identifying potential remedies. The Auditors recommend that Facebook (1) capture data on which protected characteristic is referenced by the perpetrator in the attacking post, and then (2) study the issue and evaluate potential solutions or ways to better distinguish between discussion of religious concepts and dehumanizing or hateful attacks masquerading as references to religious concepts or ideologies.

Facebook's events policy provides another illustration of the need for focused study and analysis on particular manifestations of hate. Facebook policy prohibits both calls to bring weapons to houses of worship (including mosques) and calls to bring weapons to other religious gatherings or events to intimidate or harass people. Civil rights groups have expressed ongoing concern that Facebook's enforcement of its events policy is too slow, often pointing to an August 2019 incident in which efforts to organize intimidation at the Islamic Society of North America's annual convening in Houston, Texas took just over 24 hours to remove. Facebook agrees that 24 hours is too long and acknowledges that the Houston incident represents an enforcement misstep. Facebook should study the incident to pinpoint what went wrong and update protocols to ensure faster enforcement in the future. The Auditors believe having an effective expedited review process to remove such content quickly is critical given its potential for real-world harm, and that such post-incident analysis assessments are vital to that end. In the midst of nationwide protests, it is all the more important that Facebook get its events policy enforcement and expedited review process right — to ensure that people cannot use Facebook to organize calls to arms to harm or intimidate specific groups

For that reason, the Auditors recommend that Facebook gather data on its enforcement of its events policies to identify how long it takes Facebook to remove violating content (and whether those response times vary based on the type of content or group targeted). Those kinds of metrics can be critical to identifying patterns, gaps, or areas for improvement.

Of course, the civil rights community's concerns with hate on Facebook are not limited to anti-Muslim bigotry. And as we've seen with the COVID-19 pandemic and recent incidents of racism that have captured national (and international) attention, new manifestations and targets of hate speech can arise all the time, which, in the Auditors' view, only reinforces the need to capture data so that new spikes and trends can be identified quickly and systematically.

At bottom, the Auditors recommend that Facebook invest in further study and analysis of hate on the platform and commit to taking steps to address trends, policy gaps, or enforcement issues it identifies. It is important that Facebook understand how different groups are targeted for hate, how well Facebook is alerting content reviewers to the specific ways that violating content manifests against certain groups, to more quickly identify and remove attempts to organize events designed to intimidate and harass targeted groups, and where Facebook could focus its improvement efforts. For many forms of hate, including anti-Muslim bigotry, documenting and publicly acknowledging the issue is an important first step to studying the issue and building solutions. For that reason, the Auditors not only recommend that Facebook capture, analyze, and act on this data as described above, but that it also include in its Community Standards Enforcement Report more detailed information about the type of hate speech being reported and removed from the platform, including information on the groups being targeted.

# Exhibit 68



Broken Promises



January 19, 2021

## Capitol Attack Was Months in the Making on Facebook



Facebook suspended President Trump following the mob attack on Congress. But the platform allowed organizing for the pro-Trump rally, as well as the spread of conspiracy theories and militant extremism that drove the rioters.

Facebook Chief Operating Officer Sheryl Sandberg made headlines (<https://www.cnn.com/2021/01/11/sandberg-says-us-capitol-riot-was-not-organized-on-facebook.html>), for saying the mob attack on the U.S. Capitol was "largely organized" on other platforms, suggesting

Facebook had done better than others at taking down dangerous content.

Not only is that assertion false, according to research by the Tech Transparency Project (TTP), but it ignores the fact that Facebook spent the past year allowing election conspiracies and far-right militia activity to proliferate on its platform, laying the groundwork for the broader radicalization that fueled the Capitol insurrection in the first place.

For months, TTP has watched extremist groups use Facebook to organize and incite members, fueled by President Trump's baseless allegations of voter fraud and a "rigged" election. Despite Facebook's new move to [suspend](https://www.nytimes.com/2021/01/07/technology/facebook-trump-ban.html) (https://www.nytimes.com/2021/01/07/technology/facebook-trump-ban.html), Trump's account and other recent actions, the militant movement it allowed to flourish for so long threatens to continue its campaign of violence heading into President-elect Joe Biden's inauguration, and beyond.

For TTP, one of the first signs of mounting danger came from "boogaloo" groups, which we [reported in April](https://www.techtransparencyproject.org/articles/extremists-are-using-facebook-to-organize-for-civil-war-amid-coronavirus) (https://www.techtransparencyproject.org/articles/extremists-are-using-facebook-to-organize-for-civil-war-amid-coronavirus) were using Facebook to prepare for a second civil war, often citing conspiratorial fears about coronavirus lockdowns. Members of private boogaloo groups flagged by TTP later [engaged in real or attempted violence](https://www.techtransparencyproject.org/articles/facebooks-boogaloo-problem-record-failure) (https://www.techtransparencyproject.org/articles/facebooks-boogaloo-problem-record-failure)—an ominous warning of how online radicalization can spin out of control.

But that was just the beginning. Since last fall, TTP has documented numerous instances of domestic extremists discussing weapons and tactics, coordinating their activities, and spreading calls to overthrow the government on Facebook, up to and including the mob attack on the Capitol, which left at least five people dead. Much of the activity took place in private Facebook groups—insulated communities that allow people to organize out of the public eye while still having access to a large online following.

Here are some of the key takeaways from that research:

- Militant groups had planned a nationwide effort to "back up" police on Election Day against supposed antifa and Black Lives Matter protests. The event carried the logos of the Proud Boys and anti-government militias and was circulated in private far-right Facebook groups with thousands of members.
- Self-declared "patriot" groups on Facebook have ramped up their recruiting efforts tied to the election. Some of these groups promoted the Jan. 6 event at the Capitol.
- Talk of overthrowing the U.S. government increased dramatically in Facebook groups monitored by TTP following the declaration of Biden as the winner of the 2020 vote.
- A pro-Trump Facebook group required prospective members to declare if they would be willing to die for their country in order to join, in what may be a sign of growing extremism.
- Calls to "occupy Congress" were rampant on Facebook in the weeks leading up to the deadly Capitol riot, making no secret of the event's aims. Two different "occupy" event listings were written in a Nazi-style font and began circulating on Facebook in December.
- Since the insurrection, new posts promoting violence, including on Inauguration Day, have popped up on Facebook.

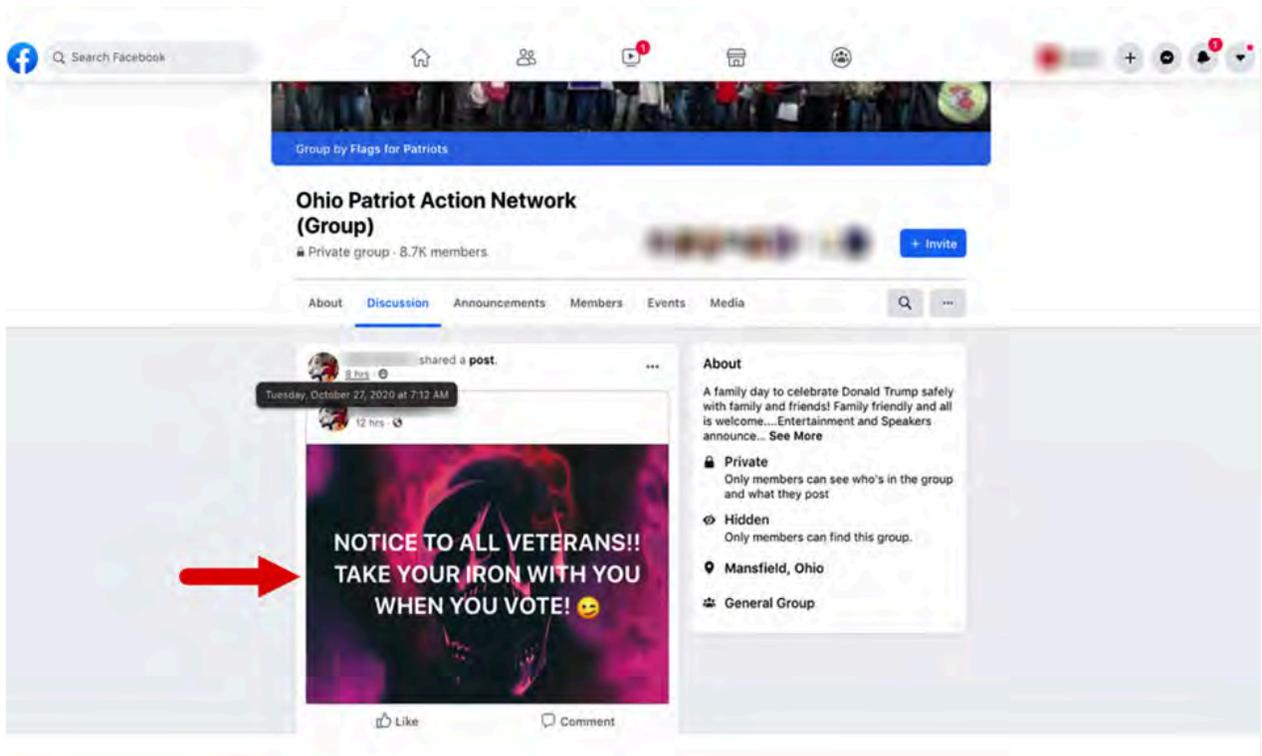
Below is a more detailed rundown of Facebook activity spotted by TTP before and after the Nov. 3 vote.

### The Pre-Election Period

In the weeks preceding the November election, members of various "patriot" Facebook groups organized efforts to intimidate voters at the polls—an early sign of trying to shape the outcome of the election by force.

On Oct. 27, an individual posted to the private Facebook group Ohio Patriot Action Network, as well as to other militia and pro-Trump groups and his personal profile, that veterans should bring their "iron" to the polls—a winking reference to weapons. The same user would go on to post threats to assassinate Joe Biden and other elected officials on his personal Facebook profile, saying "fair warn to ALL Military Snipers! Biden wins... they all GO DOWN!! Say farewell now before you can't!!" (TTP reported these threats to appropriate authorities at the time).

**Slideshow: Bring weapons to polls and assassination threats**



That same week, the administrator of a private Facebook group called "Patriot Riders" posted a Facebook event for an "Election Day Evening Block Biden Ride" in Johnson City, Tennessee, aimed at disrupting a local Democratic party event at voting precincts. The cover photo for the event featured the logo of the [Three Percenters](https://www.adl.org/resources/backgrounders/three-percenters) (<https://www.adl.org/resources/backgrounders/three-percenters>), an anti-government militia movement with a "track record of criminal activity ranging from weapons violations to terrorist plots and attacks," according to the Anti-Defamation League.

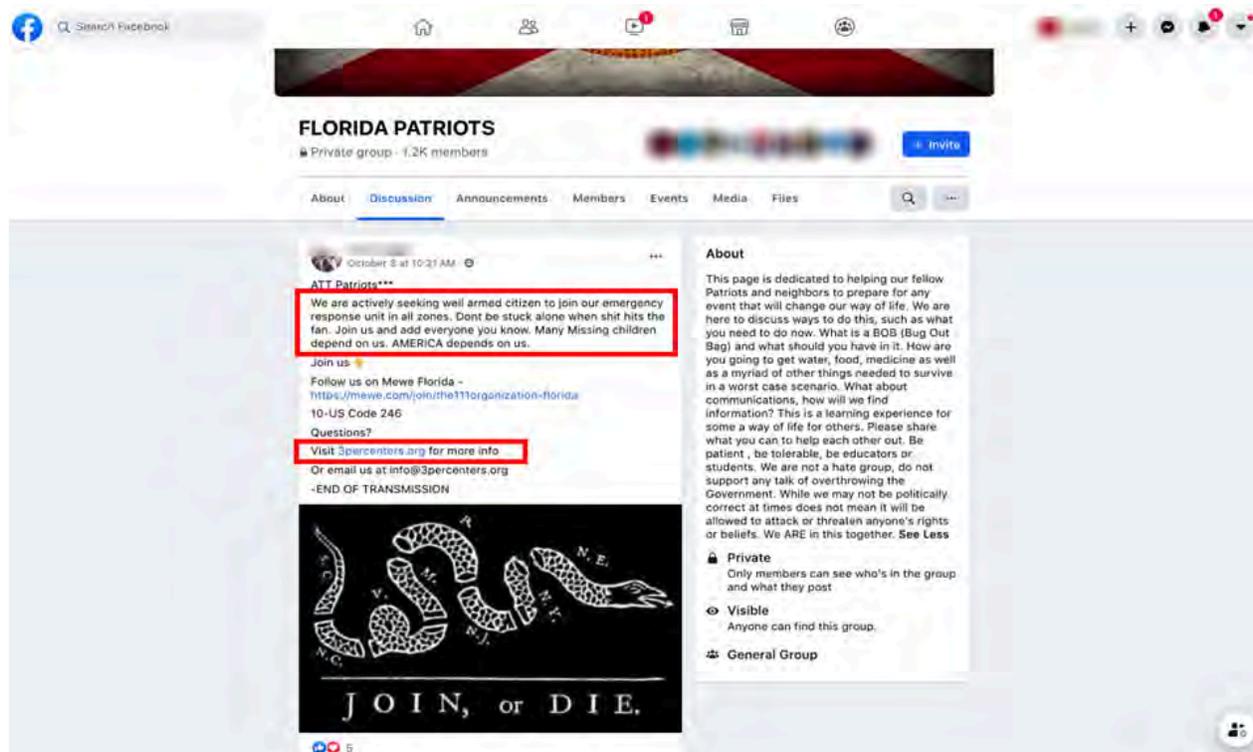


Reports from the Capitol attack have highlighted the military- and police-style preparation of many of the rioters, who were kitted out in bulletproof vests, helmets and batons. [Videos](https://www.thedailybeast.com/far-right-oath-keepers-militia-went-all-in-before-the-capitol-riot) (<https://www.thedailybeast.com/far-right-oath-keepers-militia-went-all-in-before-the-capitol-riot>), show the organized nature of some in the crowd, with one group moving in a disciplined line toward the Capitol building. According to a [report](#)

(<https://www.theguardian.com/us-news/2021/jan/13/zello-app-us-capitol-attack-far-right>), from The Guardian, some rioters communicated on a walkie-talkie app, with one saying, “This is what we fucking lived up for. Everything we fucking trained for.” This kind of activity was not a surprise to TTP, which has been monitoring how patriot and militia groups on Facebook have put a growing emphasis on tactical training and weaponry.

The activity in a Facebook group called “FLORIDA PATRIOTS” provides a good illustration of this trend. In October, one member called for “well armed” citizens to “join our emergency response unit in all zones,” while another requested information on how to “train and meet up and prep.” Similar requests popped up in the “Oregon Patriots (save Oregon)” Facebook group, with one member warning not to openly share logistical details about training sessions, saying “that’s not really a Facebook conversation.”

## Slideshow: Pre-election militia training and recruiting ● ○ ○ ○ ○



These same groups appeared to ramp up their activity around Election Day.

The “FLORIDA PATRIOTS” posted a nationwide message outlining plans to provide backup to police confronting antifa and Black Lives Matter on Nov. 3. (False, right-wing rumors that antifa and BLM planned riots around the election were [debunked](https://www.factcheck.org/2020/11/antifa-false-flag-flyer-is-an-old-hoax/) (<https://www.factcheck.org/2020/11/antifa-false-flag-flyer-is-an-old-hoax/>), by fact checkers.) The message featured the logos of the far-right Proud Boys, the Three Percenters and Oath Keepers, suggesting they were part of the effort. The Oath Keepers are a radical antigovernment group that “claims tens of thousands of present and former law enforcement officials and military veterans as members,” according to the Southern Poverty Law Center (<https://www.splcenter.org/fighting-hate/extremist-files/group/oath-keepers>). TTP reported this call to arms to appropriate authorities at the time.

## \*\*\*ATTENTION ALL PATRIOT GROUPS NATIONWIDE\*\*\*

The following Patriot Groups will be on standby in Florida starting Tuesday the 3rd until further notice:



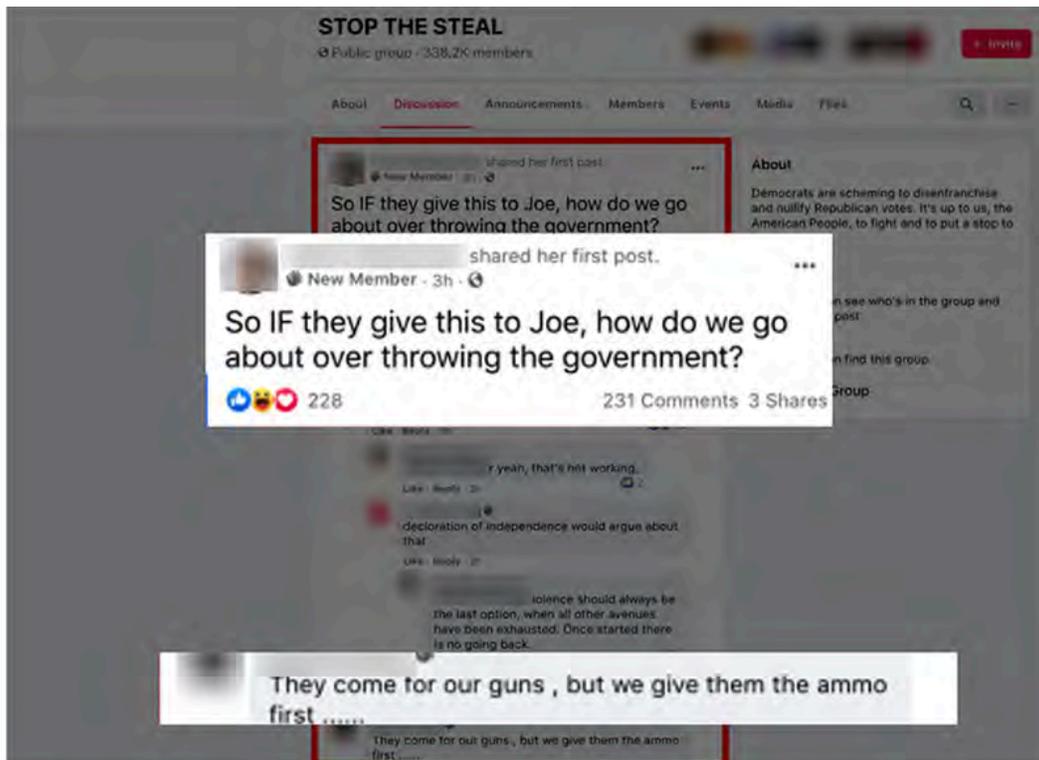
On 11/1/2020, all leaders from all nationwide patriot groups had an historic meeting in Florida. This meeting was held to coordinate logistics, intel and response to the coming violence created by Antifa and Black Lives Matter! We will interact and coordinate with state police, local police and county officials in each state as well as the US Marshalls, Homeland Security and the FBI to thwart all violence, looting and rioting in the coming days and weeks. The National Guard will also play a role in intel gathering and processing of violent radical leftist groups (Antifa/BLM) as well as protecting Federal buildings, Government officials and the rule of law. Patriot groups will be at the ready to provide intel and back up for overwhelmed police precincts in the event that reinforcements are needed. Have your gear ready, ammo ready and police scanner tuned to local frequencies to capture alerts as they come in. Nationwide comms will be provided in Patriot Action Network, coordination provided by local police. Record all events & flareups for prosecution at a later date! WWG1WGA

During this period, TTP also observed an escalation of threats to Biden and other Democratic politicians on Facebook. For example, a member of the “Pro-Police, Pro-Military, Pro-Trump” group in early October said Minnesota Rep. Ilhan Omar should be “sent to Guantanamo Bay,” a comment that sparked replies like “Just shoot the bitch” and “she needs a drone strike.” The threats to Omar remained active on Facebook as of this writing despite [TTP](https://www.techtransparencyproject.org/articles/facebook-ran-recruitment-ads-militia-groups) (<https://www.techtransparencyproject.org/articles/facebook-ran-recruitment-ads-militia-groups>) and [BuzzFeed](https://www.buzzfeednews.com/article/salvadorhernandez/facebook-profit-militant-extremist-groups-ads) (<https://www.buzzfeednews.com/article/salvadorhernandez/facebook-profit-militant-extremist-groups-ads>), highlighting the threat back in October.

At the same time, the rhetoric among these far-right groups began to bend toward insurrection talk. In the giant “Stop the Steal” group—which Facebook only [removed](https://www.bloomberg.com/news/articles/2020-11-05/facebook-removes-stop-the-steal-group-casting-doubt-on-vote) (<https://www.bloomberg.com/news/articles/2020-11-05/facebook-removes-stop-the-steal-group-casting-doubt-on-vote>) after the election—members posted openly about overthrowing the government if Biden was declared the winner. “So IF they give this to Joe, how do we go about over throwing the government,” one individual wrote to the group’s 338,000-plus members on Nov. 4, prompting replies like, “They come for our guns, but we give them the ammo first.”

One member of the “Stop the Steal” group on Nov. 3 called on others to “Gather up arms and meet at election headquarters quickly,” in response to claims that conservative poll watchers were not being permitted to view the counting of votes in swing states. This same individual had previously posted on Facebook about taking over election infrastructure and removing Michigan Gov. Gretchen Whitmer by force. (Whitmer was the target of a [kidnapping plot](https://apnews.com/article/gretchen-whitmer-michigan-indictments-coronavirus-pandemic-traverse-city-10f7e02c57004da9843f89650edd4510) (<https://apnews.com/article/gretchen-whitmer-michigan-indictments-coronavirus-pandemic-traverse-city-10f7e02c57004da9843f89650edd4510>), last fall.) [BuzzFeed reported](https://www.buzzfeednews.com/article/janeltyvnenko/stop-the-steal-facebook) (<https://www.buzzfeednews.com/article/janeltyvnenko/stop-the-steal-facebook>) on Jan. 8—two days after the Capitol riot—that copycat “Stop the Steal” groups were still flourishing on Facebook, providing a continuing space for such threats.

**Slideshow: Stop the Steal group posts** ● ○ ○ ○ ○



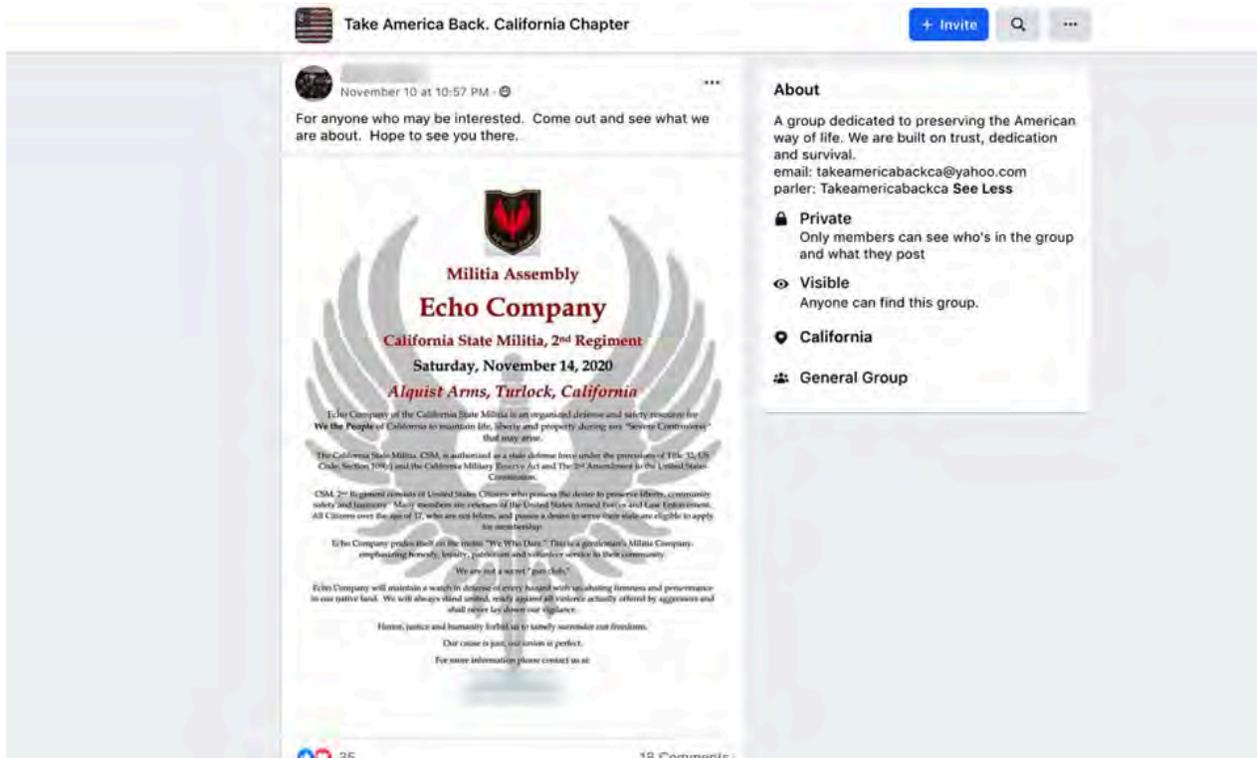
### Post-Election

News of Biden's victory sparked increasingly violent talk in pro-Trump and militia groups on Facebook, which allowed the threats to freely circulate.

The Florida-based administrator of a Facebook militia group called "Eagle Team 1 LLC," for example, posted frequent calls to "take down" the government. "The politicians in Washington DC are the biggest threat 2 our country and democracy than any foreign standing Army," read one typical post. Members replied with slogans like "locked and loaded," indicating a willingness to take up arms.

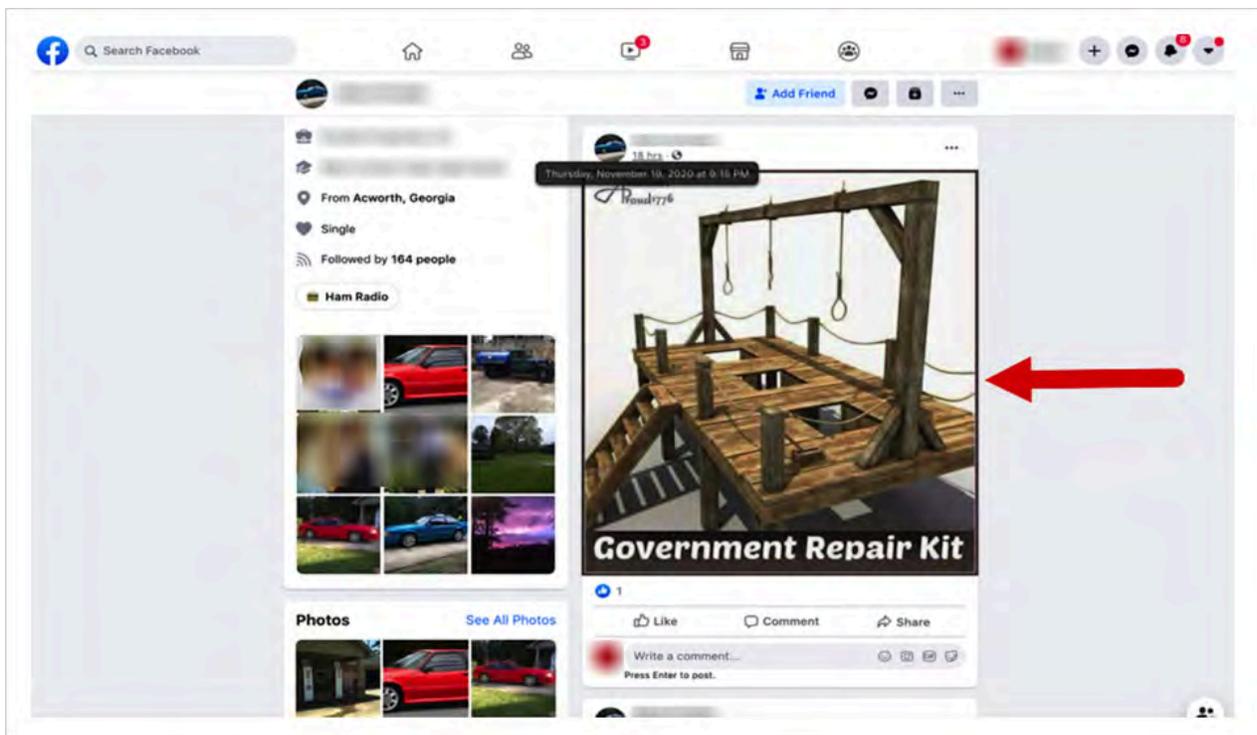
Another group called "Take America Back. California Chapter" ramped up its recruitment drive, posting on Nov. 10 and Nov. 12 about an assembly of "Echo Company, California State Militia, 2nd Regiment," which was described as a "defense" resource for people who want to "maintain life, liberty and property during any 'Severe Controversy' that may arise."

### Slideshow: Post-election militia organizing and recruiting

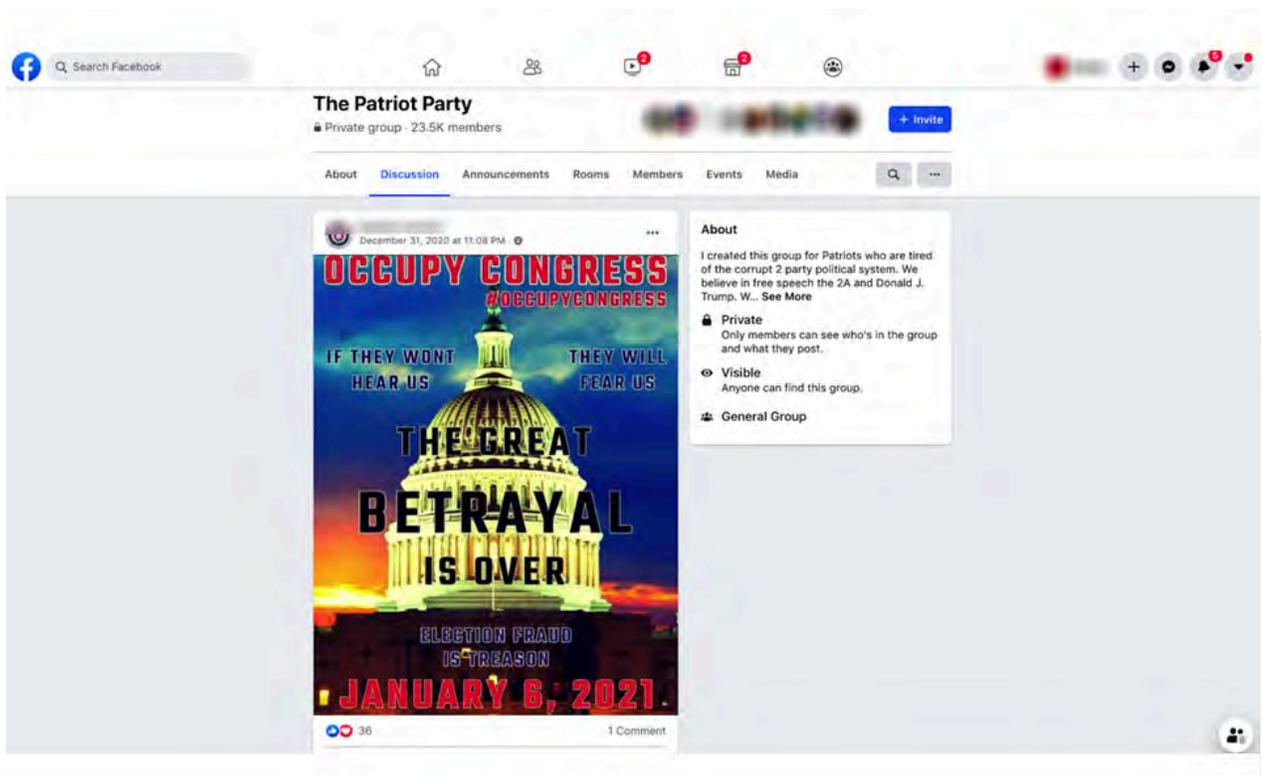


A member of the Facebook group "Patriot Riders," meanwhile, called for people to organize in their local areas, posting on Nov. 7, "I urge all PATRIOTS to develop rapid response teams in your communities, neighbor hoods and cities to defend against all threats."

This individual also made violent threats on his profile, including a Nov. 10 post that stated, "TRAITORS MUST HANG," with an image of nooses in the gallows titled "Government Repair Kit." Rioters at the U.S. Capitol on Jan. 6 used this same kind of imagery, (<https://www.nbcnews.com/politics/congress/live-blog/electoral-college-certification-updates-n1252864/ncrd1253129#blogHeader>), erecting a wooden frame with a noose dangling from it just outside the Capitol. (The individual described above remains active on Facebook and continues to post threats as of this writing.)







Supporters of militia and extremist groups became increasingly overt about their role in the Jan. 6 rally in the days and hours leading up to the event. In a Facebook group called "Mouthy Patriots," a member posted an announcement stating that Oath Keepers would be deploying to Washington on Jan. 5 and 6 to "Protect Events, Speakers, & Attendees." On the morning of Jan. 6, a member of the Facebook group "Under the Liberty Tree" posted a meme featuring the Three Percenter logo that said "WE CANNOT WE WILL NOT COMPLY. Prepare to Take America Back."

It was one of several militia-linked memes with calls to action that popped up in far-right Facebook groups hours before the attack on the Capitol, suggesting they may have served as dog whistle to supporters attending the rally in Washington that day. (Republican Rep. Lauren Boebert of Colorado also [tweeted](https://twitter.com/laurenboebert/status/1346811381878845442?s=21) that morning, "Today is 1776," echoing a slogan used by far-right groups to reference a new revolution and violent uprising against the government.)

## Call To Action: Oath Keepers Deploying to DC to Protect Events, Speakers, & Attendees on Jan 5-6: Time to Stand!

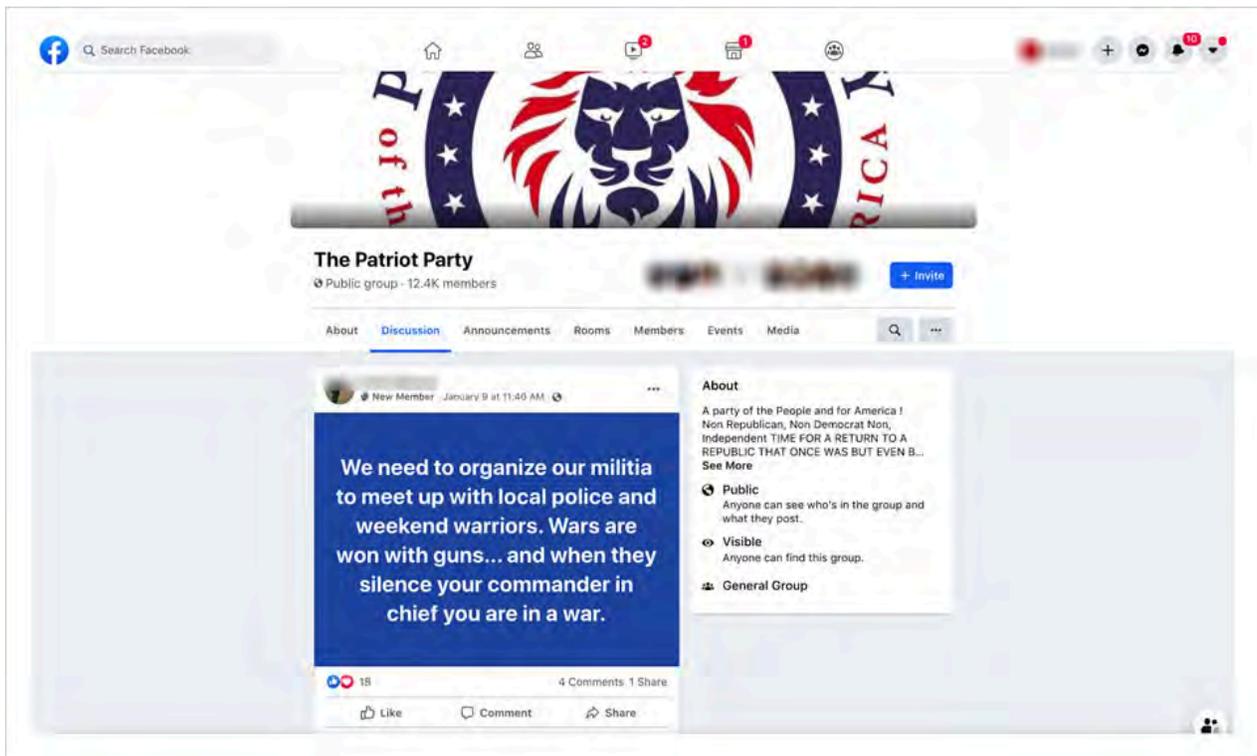


**CALL TO ACTION**  
Oath Keepers Deploying to DC to  
Protect Events, Speakers, &  
Attendees on Jan 5-6: Time to Stand!



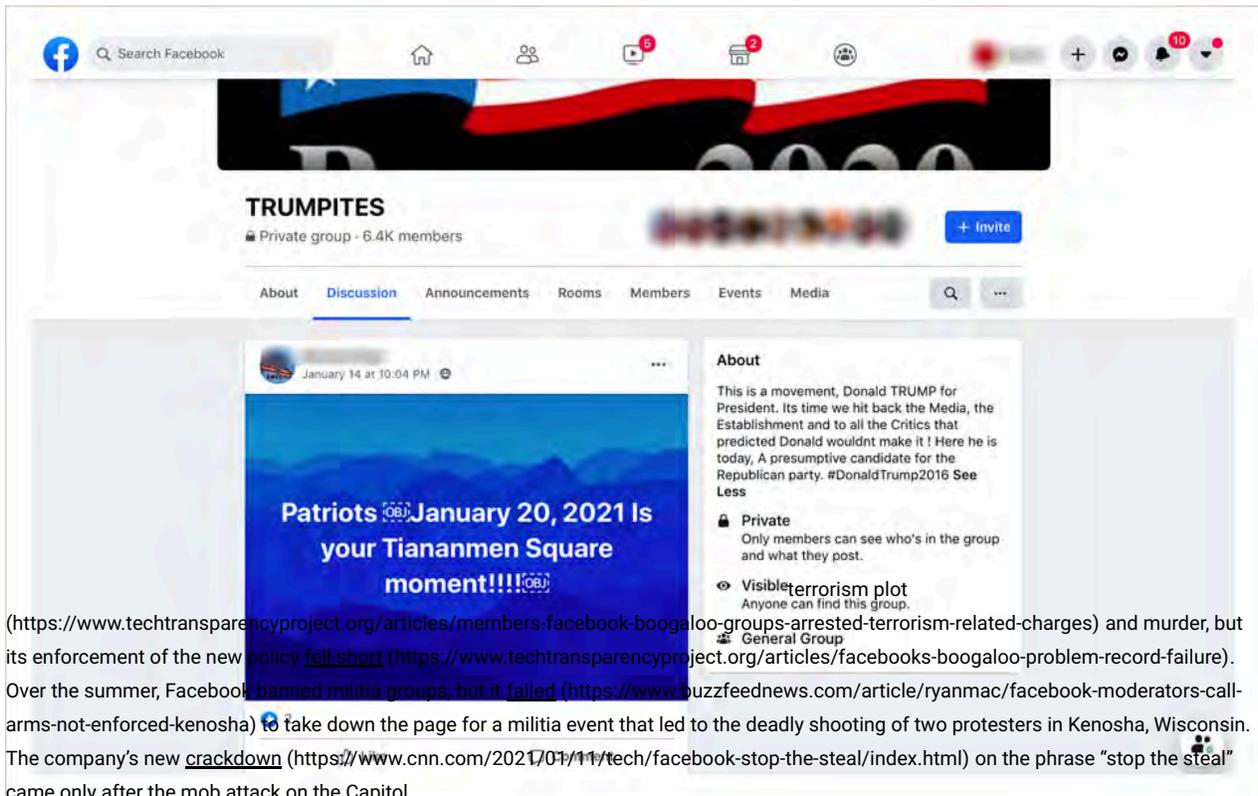
In the days since Jan. 6, Facebook has continued to allow discussion of insurrection and is even profiting from it. Research by [BuzzFeed](https://www.buzzfeednews.com/article/ryanmac/facebook-profits-military-gear-ads-capitol-riot) (<https://www.buzzfeednews.com/article/ryanmac/facebook-profits-military-gear-ads-capitol-riot>) and [TTP](https://www.techtransparencyproject.org/articles/how-facebook-profits-insurrection) (<https://www.techtransparencyproject.org/articles/how-facebook-profits-insurrection>), found that Facebook was pushing ads for weapons accessories and military gear to users who engage in militia and far right groups on the platform. (Facebook later [paused](https://www.buzzfeednews.com/article/ryanmac/facebook-pauses-ads-for-gun-accessories-and-military-gear) (<https://www.buzzfeednews.com/article/ryanmac/facebook-pauses-ads-for-gun-accessories-and-military-gear>), such ads until after the inauguration.)

Following the Capitol riot, TTP also spotted a number of still-active Facebook posts that equated the insurrection with the American Revolution or tried to organize new militias.



Perhaps more alarmingly, TTP found Facebook posts making new calls for violence, including around the Inauguration. One post referred to Jan. 20, Inauguration Day, as a "Tiananmen Square moment" for self-styled patriots. These messages remained active on Facebook despite the company's [statement](https://about.fb.com/news/2021/01/preparing-for-inauguration-day/) (<https://about.fb.com/news/2021/01/preparing-for-inauguration-day/>), that its teams are "working 24/7 to enforce our policies around the inauguration."

CNN [reported](https://www.cnn.com/2021/01/18/tech/facebook-posts-promoting-violence/index.html) (<https://www.cnn.com/2021/01/18/tech/facebook-posts-promoting-violence/index.html>), on the new posts identified by TTP on Jan. 18. In response to the report, Facebook said it removed the Tiananmen Square post, and told CNN it had "proactively detected" and was removing the "Patriot Party" group that featured the militia organizing message.



(<https://www.techtransparencyproject.org/articles/members-facebook-boogaloo-groups-arrested-terrorism-related-charges>) and murder, but its enforcement of the new policy [fall short](https://www.techtransparencyproject.org/articles/facebooks-boogaloo-problem-record-failure) (<https://www.techtransparencyproject.org/articles/facebooks-boogaloo-problem-record-failure>). Over the summer, Facebook [banned militia groups, but it failed](https://www.buzzfeednews.com/article/ryanmac/facebook-moderators-call-arms-not-enforced-kenosha) (<https://www.buzzfeednews.com/article/ryanmac/facebook-moderators-call-arms-not-enforced-kenosha>) to take down the page for a militia event that led to the deadly shooting of two protesters in Kenosha, Wisconsin. The company's new [crackdown](https://www.cnn.com/2021/01/11/tech/facebook-stop-the-steal/index.html) (<https://www.cnn.com/2021/01/11/tech/facebook-stop-the-steal/index.html>) on the phrase "stop the steal" came only after the mob attack on the Capitol.

TTP watched with growing alarm starting this fall as a broad range of "patriot," militia, and pro-Trump groups grew increasingly bold on **Conclusion** Facebook with their organizing efforts, recruitment, and training of new members, and talk of weapons, violence, and government takeovers. As the nation heads toward Inauguration Day and contemplates life under a new Biden administration, Facebook's massive reach and patchy, Facebook not only facilitated organizing for the Jan 6 event in Washington that culminated in the deadly Capitol riot, it has spent the past year inconsistent moderation means likely to continue to be a gathering space for extremist groups that seek to do harm. failing to remove extremist activity and election-related conspiracy theories stoked by President Trump that have radicalized a broad swath of the population and led many down a dangerous path. To view the full collection of images captured by TTP, click [here](https://www.techtransparencyproject.org/sites/default/files/Facebook-Violent-Threats-Images1-011421.zip) (<https://www.techtransparencyproject.org/sites/default/files/Facebook-Violent-Threats-Images1-011421.zip>) and [here](https://www.techtransparencyproject.org/sites/default/files/Facebook-Violent-Threats-Images2-011421.zip) (<https://www.techtransparencyproject.org/sites/default/files/Facebook-Violent-Threats-Images2-011421.zip>). Facebook's efforts to curb violent activity and disinformation were either too late or ineffective or both. It banned a boogaloo network in June after members of Facebook boogaloo groups were linked to a \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

Tech Transparency Project is a research initiative of Campaign for Accountability, a 501(c)(3) non-profit, nonpartisan watchdog organization that uses research, litigation and aggressive communications to expose how decisions made behind the doors of corporate boardrooms and government offices impact Americans' lives.

**Donate Today (<https://secure.donationpay.org/campaignforaccountability/>)**

# Exhibit 69

# Facebook's Sandberg deflected blame for Capitol riot, but new evidence shows how platform played role

Fliers and hashtags promoting the pro-Trump rally circulated on Facebook and Instagram in the days and weeks beforehand

By [Elizabeth Dwoskin](#)

January 13, 2021 at 3:27 p.m. EST



In the days leading up to last week's march on the Capitol, supporters of President Trump promoted it extensively on Facebook and Facebook-owned Instagram and used the services to organize bus trips to Washington. More than 100,000 users posted hashtags affiliated with the movement prompted by baseless claims of election fraud, including #StopTheSteal and #FightForTrump.

The details, emerging from researchers who have combed the service in recent days, shed new light on how Facebook services were used to bring attention to and boost attendance at the rally, which turned violent when a pro-Trump mob stormed the Capitol while Congress was in session. The attack resulted in the death of a Capitol Police officer and four other people.

Facebook chief operating officer Sheryl Sandberg has sought to deflect blame, noting the role of smaller, right-leaning services such as [Parler](#) and Gab.

"I think these events were largely organized on platforms that don't have our abilities to stop hate, don't have our standards and don't have our transparency," Sandberg said in an interview Monday that was live-streamed by Reuters.

She noted that last week the company took down content affiliated with the baseless QAnon conspiracy theory and the Proud Boys extremist group, as well as content affiliated with the pro-Trump "Stop the Steal" movement seeking to delegitimize election results. She said there was likely to be some content on Facebook because the company's enforcement was "never perfect."

A growing body of evidence shows Facebook played a much larger role than Sandberg suggested.

The #StopTheSteal hashtag was widely used on the service until Monday, when a search on Facebook reported that 128,000 people were talking about it and in many cases using it to coordinate for the rally, according to Eric Feinberg, a vice president with the Coalition for a Safer Web.

And two dozen Republican Party officials and organizations in at least 12 states posted on Facebook to coordinate bus trips to the rally, according to research by the left-leaning media watchdog group Media Matters for America, which published screenshots of the fliers and memes.

In a statement, Facebook spokeswoman Liz Bourgeois said, “Sheryl began by noting these events were organized online, including on our platforms — with the clear suggestion we have a role here.”

“She was making the point, which has been made by many journalists and academics, that our crackdowns on QAnon, militia and hate groups has meant large amounts of activity has migrated to other platforms with fewer rules and enforcement,” Bourgeois added. She denied that Sandberg sought to deflect blame.

Facebook has been at the center of controversies over its role in the organizing of far-right events since at least 2017, when the service played a central role in the promotion of a white-supremacist rally in Charlottesville in which a woman was killed.

Throughout 2020, Facebook was a hub for organizers of protests against government restrictions related to the coronavirus — including when armed demonstrators entered the Michigan Capitol — and other pro-Trump rallies calling for election results to be decertified.

Facebook banned several far-right figures from its service after the Charlottesville violence and last year belatedly blocked organizing for protests that opposed government orders related to the pandemic. And immediately after the November election, Facebook said it was banning or labeling misinformation about election results, including taking action against the term “Stop the Steal” and banning a large group affiliated with it.

Bourgeois said that the actions taken to limit the reach of the term “Stop the Steal” in the election’s immediate aftermath were temporary. She said the hashtag was blocked again Monday, five days after the Capitol event.

The proliferation of such events raises questions about the lines between misinformation and real-world action. The company may act to limit the spread of false information, but has been hesitant to restrict people from organizing events based on their beliefs — even when those beliefs are based on misinformation.

Feinberg’s searches for the banned hashtag #StopTheSteal and the affiliated hashtags #DoNotCertify, #WildProtest and #FightForTrump on Facebook and Instagram as recently as Monday revealed hundreds of posts promoting the rally, according to a review by The Washington Post.

Some of that promotion included Instagram posts with detailed maps of the Capitol and a guide to the speakers there.

A meme posted on Facebook on Jan. 5 called for “Operation Occupy the Capitol” and promoted the hashtag #1776Rebel, according to a screenshot posted by Media Matters, referencing the year America freed itself from British rule. The post also included a quote from Abraham Lincoln: “We the people are the rightful masters of both Congress and the Courts, not to overthrow the Constitution but to overthrow the men who would pervert the Constitution.”

The existence of the post was first reported by NBC News. Media Matters showed that it was circulated by Republican Party officials in Georgia, Texas, North Carolina and Oregon.

On Dec. 28, a Facebook account called Women for America First posted about a march for Trump in Huntington Beach, Calif., with a photo of a bus and a link to a website at [trumpmarch.com](http://trumpmarch.com).

And the New Hanover County GOP of North Carolina wrote in a Facebook post advertising bus seats: “This is a call to ALL patriots from Donald J Trump for a BIG protest in Washington DC! TAKE AMERICA BACK! BE THERE, WILL BE WORTH IT!”

**The Attack:** [Before, During and After](#)

**A sprawling investigation:** [What we know so far about the Capitol riot suspects](#)

**Six hours of paralysis:** [Inside Trump's failure to act after a mob stormed the Capitol](#)

**Profiles of three involved in the attack:** [A horn-wearing 'shaman.' A cowboy evangelist. For some, the Capitol attack was a kind of Christian revolt.](#)

**Video timeline:** [41 minutes of fear from inside the Capitol siege](#)

By [Elizabeth Dwoskin](#)

Lizza joined The Washington Post as Silicon Valley correspondent in 2016, becoming the paper's eyes and ears in the region. She focuses on social media and the power of the tech industry in a democratic society. Before that, she was the Wall Street Journal's first full-time beat reporter covering AI and the impact of algorithms on people's lives. [Twitter](#)



## Today's Headlines

The most important news stories of the day, curated by Post editors and delivered every morning.

[Sign up](#)

[Sign in to join the conversation](#)

Unprecedented times call for unlimited access.

Get one year for \$40



# Exhibit 70

# The Facebook Papers: Documents reveal internal fury and dissent over site's policies

Thousands of leaked documents highlight employees' disillusionment with spread of misinformation and calls to violence.



— Frances Haugen, who worked as a Facebook product manager until May, has come forward as a whistleblower and provided internal Facebook documents to Congress and the Securities and Exchange Commission. Doug Chayka for NBC News

Oct. 25, 2021, 7:00 AM EDT / Updated Oct. 25, 2021, 2:16 PM EDT

**By David Ingram, Olivia Solon, Brandy Zadrozny and Cyrus Farivar**

Hours after the Jan. 6 assault on the U.S. Capitol, Mike Schroepfer, Facebook's chief technology officer, posted on the company's internal message board.

“Hang in there everyone,” he wrote. Facebook should allow for peaceful discussion of the riot but not calls for violence, he added.

His post was met with scathing replies from employees who blamed the company for what was happening.

“I’m struggling to match my values to my employment here,” an employee wrote in a comment. (The employee’s name was redacted in a version seen by NBC News.) “I came here hoping to effect change and improve society, but all I’ve seen is atrophy and abdication of responsibility.”

**Internal Facebook documents reveal more red flags about misinformation on site**



Another employee asked, “How are we expected to ignore when leadership overrides research-based policy decisions to better serve people like the groups inciting violence today?”

The comments openly challenged the company’s leadership with a not-so-subtle message: Facebook’s [well-documented problems](#) in abetting violent polarization and encouraging the spread of misinformation weren’t getting fixed, despite the company’s investments and promises.

The comments are in thousands of pages of internal Facebook documents given to NBC News detailing Facebook’s internal debates around the societal impact of its platforms. Together the

documents offer the deepest look provided to outsiders at the internal workings of the world's largest social media company.

They are a small fraction of the internal communications over the past several years at Facebook, where employee message boards that started as a way to embrace transparency have become an outlet for reflection and advocacy on the impact of social media.

The documents show employees – many who were hired to help Facebook address problems on its platforms – debating with one another on internal message boards free of public relations spin. Many tried to figure out how to turn stalled bureaucratic wheels and steer a company that now has so many departments that employees sometimes aren't aware of overlapping responsibilities. Some employees defended management, with one calling Facebook executives “brilliant, data-driven futurists like many of us.”

The documents were included in disclosures made to the Securities and Exchange Commission, or SEC, and provided to Congress in redacted form by legal counsel for Frances Haugen, who worked as a Facebook product manager until May and has come forward as a whistleblower. Digital versions of the disclosures – with some names and other personal information redacted – were obtained by a consortium of news organizations, including NBC News. Most of the documents are digital photographs of company material on computer screens.

The news consortium is making at least some of the disclosures public beginning Monday. [The Wall Street Journal reported](#) some of the disclosures earlier.

Haugen alleges in letters to the SEC Office of the Whistleblower that Facebook executives up to and including CEO Mark Zuckerberg have misled investors for years, giving them a false picture of the reality inside the company about subjects like [Facebook's user base](#) and its record on human rights. She wrote at least eight separate letters, and her attorneys provided the internal documents to the SEC in support of her allegation that executives' statements don't match the truth. In the letters, she also offered her help to the SEC if it were to investigate potential violations of securities laws.

But more broadly, Haugen has kick-started a debate about Facebook's impact on society, both in the U.S. and abroad.

“Facebook did not invent partisanship. They did not invent polarization. They didn't invent ethnic violence,” Haugen said in a call with reporters this month. “But the thing that I think we should be discussing is what role, what choices did Facebook make to expose the public to greater risk than was necessary?”

Haugen repeated her allegation against Facebook executives [in testimony before Congress](#) this month.

“The company intentionally hides vital information from the public, from the U.S. government and from governments around the world,” she told the Senate Commerce Subcommittee on Consumer Protection.

**Whistleblower accuses Facebook of putting 'profits before people' at Senate hearing**



She is [scheduled](#) to testify Monday before a committee of the U.K. Parliament examining online safety.

Zuckerberg has pushed back against Haugen’s allegations. “At the heart of these accusations is this idea that we prioritize profit over safety and well-being. That’s just not true,” he said in a Facebook [post](#) Oct. 5. He also said Facebook was being punished for trying to study its impact on the world.

Facebook spokesperson Drew Pusateri defended the disclosures to investors, saying the company is confident that it has given investors the information they need to make informed decisions.

“We make extensive disclosures in our SEC filings about the challenges we face, including user engagement, estimating duplicate and false accounts, and keeping our platform safe from people who want to use it to harm others,” he said in an email.

“All of these issues are known and debated extensively in the industry, among academics, and in the media,” he said. Facebook is ready to answer regulators’ questions and will cooperate with government inquiries, he said.

According to the disclosures from Haugen:

- The company spends considerable time and resources studying how to solve such problems, but has declined in some cases to implement potential solutions put forward by its own researchers. Employees complain that sometimes that is because Facebook’s Washington-based policy team has veto power over decisions. Joel Kaplan, Facebook’s global head of public policy, has [repeatedly defended](#) his influence, saying he pushes for analytical and methodological rigor about subjects such as the algorithms that power Facebook products.
- A change to Facebook’s news feed in 2018 intended to bring friends and family members closer together in meaningful ways often had the opposite effect, internal researchers wrote. Posts spread more easily if they included outrage or misinformation, causing an online “social-civil war” abroad in places like Poland.
- Engineers and statisticians struggle to understand why certain posts and not others get traction through re-shares on Facebook and how to fix the “unhealthy side effects.” In 2019, an internal researcher wrote: “We know that many things that generate engagement on our platform leave users divided and depressed.”
- Facebook has struggled to filter out many posts that violated its rules. Documents say the company’s automated systems deleted only about 2 percent of hate speech as of 2019 and, as of this year, less than 1 percent of content trying to incite violence. Facebook said in a [blog post](#) this month that the documents understate the company’s effectiveness and that the prevalence of hate speech – how often users actually view it, rather than the number of posts – has dropped.
- Many documents highlight Facebook’s failure to police its platform outside the U.S., including in Myanmar and Sri Lanka, where the company has [issued apologies](#) for its actions contributing to physical violence against religious or ethnic groups. The documents describe translation issues and a lack of local cultural knowledge.

It isn't clear whether the SEC is investigating Facebook or whether it would see enough material in the disclosures to warrant an investigation of whether the company could have misled investors. The SEC declined to comment. The commission isn't required to take any action on whistleblowers' tips, and when it conducts investigations, it does so on a confidential basis as a matter of [policy](#). In an annual [report](#), the SEC said it received over 6,900 whistleblower tips in the fiscal year ending September 2020.

Several securities law experts said it wouldn't be easy to prove wrongdoing.

“Regulators like clean cases, and they like where someone is on tape doing something wrong,” said [Joshua Mitts](#), a securities law professor at Columbia University. Haugen's allegations are hardly a “clean case,” he said.

## Facebook pushback

Facebook's public relations chief last week said Haugen's disclosures were an “orchestrated ‘gotcha’ campaign” guided by her public relations advisers.

“A curated selection out of millions of documents at Facebook can in no way be used to draw fair conclusions about us,” Facebook's vice president for communications, John Pinette, said in a [tweet](#) ahead of the release of the Haugen disclosures.

“Internally, we share work in progress and debate options. Not every suggestion stands up to the scrutiny we must apply to decisions affecting so many people,” Pinette said.

**Facebook's Mark Zuckerberg pushes back after whistleblower's testimony**



its ability to compete effectively, it said in its most recent [annual report](#) in January.

A Facebook employee wrote on an internal message board on Jan. 6: “We have been dealing with questions we can’t answer from our friends, family, and industry colleagues for years. Recruiting, in particular, has gotten more difficult over the years as Facebook’s ethical reputation continues to deteriorate (all while our technical reputation continues to increase).”

Facebook said in a statement that 83 percent of its employees say they’d recommend it as a great place to work and that it has hired more employees this year than in any previous year.

## Jan. 6 impact

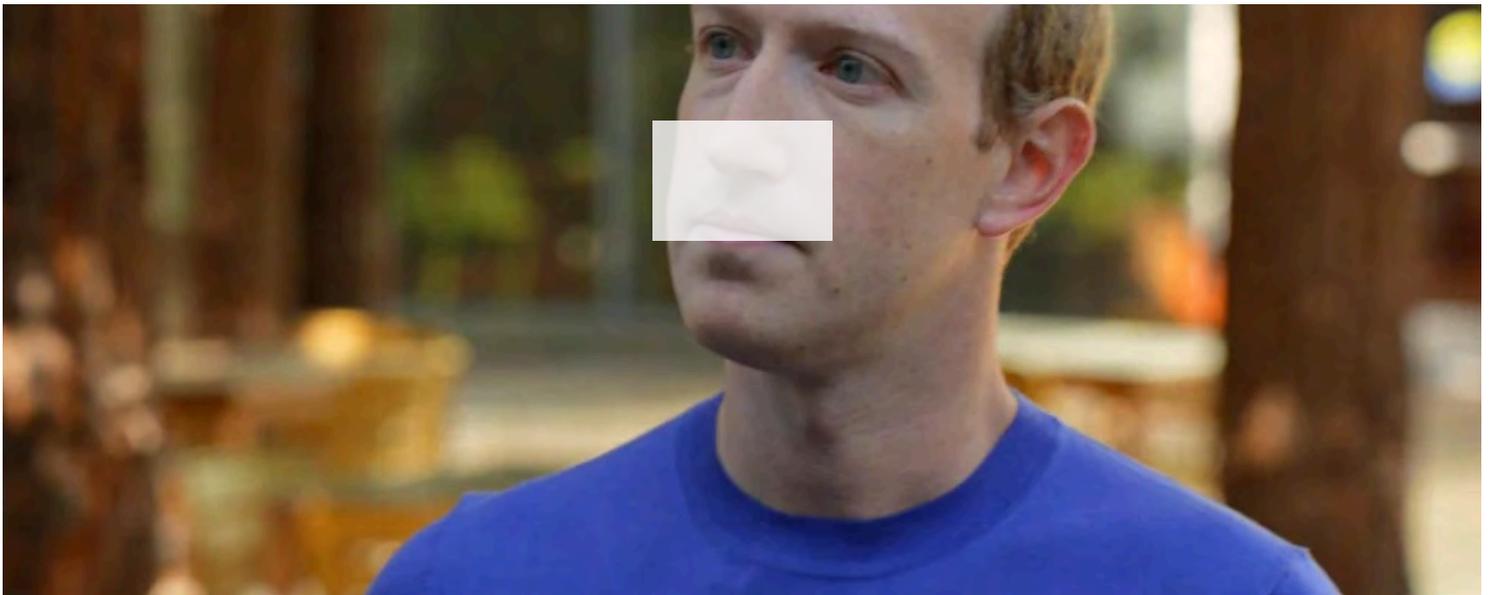
The internal turmoil over the Jan. 6 attack was apparent throughout the documents, beyond Schroepfer’s internal post. (Schroepfer plans to step down to a [part-time role](#) at Facebook next year.)

According to a Facebook document, the riot so tested the company’s ability to halt incitements to violence that the company reinstated 25 safeguards that it had in place around the 2020 presidential election to minimize hate speech and other content against the platform’s rules. The efforts were called “Break the Glass.”

Later, a Facebook employee published an examination of the lead-up to the Capitol attack on the company's internal message board, with scathing findings about its failure to stop the growth of the conspiracy theory movement promoted by then-President Donald Trump and his followers known as "Stop the Steal." Believers in the theory falsely assert that President Joe Biden stole the election.

Facebook was alerted to the first such group on Election Night in early November and disabled it because of hate speech, calls to violence and incitement in the comments, the investigation found. But in the months ahead, new conspiracy-theory groups flourished.

**Mark Zuckerberg hopes his daughters will think he 'made the world better'**



Facebook watched the movement's "meteoric growth rates," and related groups were among the fastest-growing groups on all of Facebook, according to some of the documents. But managers failed to act because, they said, they were looking at rule violations one by one and didn't see the big picture.

"Because we were looking at each entity individually, rather than as a cohesive movement, we were only able to take down individual Groups and Pages once they exceeded a violation threshold," the report said. Facebook realized that "Stop the Steal" was a cohesive movement only after the Capitol attack, the report said.

Facebook seemed unable to understand the dynamics, influencers, tactics and ultimate intentions of the conspiracy movement, even as it operated in plain sight, the documents suggest.

“This sort of deep investigation takes time, situational awareness, and context that we often don’t have,” the internal report said.

Facebook’s enforcement was “piecemeal,” the team of researchers wrote, saying “we’re building tools and protocols and having policy discussions to help us do this better next time.”

In a statement responding to questions about the research, Facebook said it has spent years building defenses and expertise to stop interference in elections. It said some of its tools are so blunt – equivalent to shutting off an entire town’s roads, it said – that they’re for emergencies only, not normal conditions.

“It is wrong to claim that these steps were the reason for January 6th – the measures we did need remained in place well into February, and some like not recommending news, civic, or political Groups remain in place to this day,” Facebook said. “These were all part of a much longer and larger strategy to protect the election on our platform – and we are proud of that work.”

## **Causing ‘social-civil war’**

Another set of Haugen’s documents describes how the computer algorithm behind Facebook’s news feed – the formula that determines what posts people see and in which order – led to unintended consequences over months and years.

Facebook [announced](#) that it would rewrite the algorithm in January 2018, saying it would emphasize “meaningful social interactions” and give more weight to comments, reactions and re-shares among friends, rather than posts from businesses and brands.

By the next year, the changes had reverberated throughout European politics.

“Political parties across Europe claim that Facebook’s algorithm change in 2018 [regarding social interactions] has changed the nature of politics. For the worse,” an employee wrote in an April 2019 internal post. Facebook was responsible for a “social-civil war” in online political discourse in Poland, the person said, passing on a phrase from conversations with political operatives there. (The Facebook employee doesn’t name the political parties or the operatives involved in the “social-civil war” or what issues were at the forefront. A Polish election later that year focused attention on expansion of the welfare state, European integration and gay rights, Reuters

[reported](#).) Extremist political parties in various countries celebrated the way the new algorithm rewarded their “provocation strategies” for subjects such as immigration, the Facebook employee wrote.

Studying the impact of the algorithm change became a priority for many economists, statisticians and others who work at Facebook studying the platform, the documents show. A study posted internally in December 2019 said Facebook’s algorithms “are not neutral” but instead value content that will get a reaction, any reaction, with the result that “outrage and misinformation are more likely to be viral.”

“We know that many things that generate engagement on our platform leave users divided and depressed,” wrote the researcher, whose name was redacted.

In April 2020, managers presented Zuckerberg with a series of proposed changes to the algorithm, according to a written summary of the meeting included among Haugen’s disclosures. The summary says Zuckerberg rejected some of the proposed changes, including an idea to reduce re-shares – posts that get shared again and again, which researchers found were often misinformation.

“Mark doesn’t think we could go broad” with the changes, employees wrote afterward in the summary, although the idea had already been implemented for content about health and politics. “We wouldn’t launch if there was a material tradeoff with MSI impact,” they wrote, using the initialism for “meaningful social interactions,” a measure of engagement.

Zuckerberg defended his decisions this month, saying in his Facebook [post](#) that the introduction of the MSI system in 2018 led to fewer viral videos, “which we did knowing it would mean people spent less time on Facebook, but that research suggested it was the right thing for people’s well-being.”

“Is that something a company focused on profits over people would do?” he wrote.

In a statement Friday, Facebook said it’s not responsible for existing problems in society.

“Is a ranking change the source of the world’s divisions? No,” the company said. “Research shows certain partisan divisions in our society have been growing for many decades, long before platforms like Facebook even existed.”

Facebook also said that it has spent \$13 billion since 2016 to counter bad content and that it employs 40,000 people to work on safety and security. It said it’s continuing to make changes to its platform, such as running tests to reduce political content.

An employee who worked on platform integrity quit in frustration in August 2020, citing Facebook’s unwillingness to implement safeguards against conspiracy theories like QAnon.

“We were willing to act only *after* things had spiraled into a dire state,” the employee wrote in a farewell note to colleagues.

Facebook has made a series of announcements in the past year concerning efforts to limit the spread of fringe and conspiracy groups, including [a move in March](#) to change its recommendation system.

In another farewell note in December, a data scientist who was quitting listed what he would miss: interesting work, friendly colleagues and the “amazing” pay.

Then came the parts he wouldn’t miss.

“Unfortunately I don’t feel I can stay on in good conscience,” wrote the person, whose name was redacted. Facebook “is probably having a net negative influence on politics in Western countries,” the person wrote, adding that executives didn’t appear committed to fixing the problem. “I don’t think that I can substantially improve things by staying.”

Facebook said it disagrees that it’s a net negative. “Facebook helps people connect with friends and family and helps businesses around the world thrive,” it said.

## Other languages

Sometimes the company lacks the systems to enforce its own rules, especially among the large proportion of people who use Facebook in languages other than English, according to some of the documents shared with the SEC and Congress.

Several documents focus on the Middle East and North Africa, including a presentation in December detailing in part how the company’s tools that take down Arabic-language content for having ties to terrorism were wrong 77 percent of the time, “resulting in a lot of false positives and a media backlash.” The full presentation on platform “integrity” problems when printed is more than 50 pages.

In a statement, Facebook said the measure seemed to be a mischaracterization because it included content related to Hamas and Hezbollah – organizations that some people in the Middle East wouldn’t consider tied to terrorism, but that the U.S. government has on its list of

“foreign terrorist organizations.” Facebook said it has legal obligations to remove that content, as well as a [policy](#) against it.

Other reported problems are language-based. In a separate analysis published in January, a Facebook researcher said that when an Afghan user tries to report hate speech, the instructions are mostly in English and not in Pashto, one of Afghanistan’s national languages. Facebook’s Community Standards, the list of content rules for users, also aren’t translated.

“There is a huge gap in the hate speech reporting process in local languages in terms of both accuracy and completeness of the translation of the entire reporting process,” wrote the author of the analysis, a Facebook researcher whose name was redacted.

Facebook said it reviews content in Pashto and Dari, the two Afghan national languages. In August, the company also said it was putting additional resources into services for Afghan users, including [security controls](#) for people fearing the Taliban’s takeover of the government.

Other documents show that when Facebook invests in more careful monitoring of a country’s social media activity, it can mitigate viral misinformation and dangerous hate speech. For example, a document outlines how Facebook convened almost 300 people from 40 different teams to focus on the April 2019 elections in India to tackle political misinformation and fend off what it characterized as “bad regulation” for social media companies. The effort, which included the creation of a temporary “operations room” in Singapore, resulted in a “surprisingly quiet, uneventful election period,” the post-analysis states.

The cache also includes the departing memo shared by former Facebook data scientist Sophie Zhang, who worked on Facebook’s site integrity team from January 2018 to September 2020. In the post, previously [reported](#) by BuzzFeed News, she outlined how she believed Facebook was ignoring manipulation of the platform by political leaders in India, Ukraine, Spain, Brazil, Bolivia, Ecuador and other countries.



Enter your email

# Exhibit 71



**Broken Promises**



**March 24, 2021**

### Facebook's Militia Mess



**Mark Zuckerberg is about to face lawmakers two months after the Capitol riot. But Facebook still hasn't fixed its militia problem.**

Facebook is leaving some gaping holes in its crackdown on militia groups, according to new research by the Tech Transparency Project (TTP), raising questions for CEO Mark Zuckerberg as he prepares to testify to Congress for the first time since the U.S. Capitol riot.

TTP has previously [detailed \(https://www.techtransparencyproject.org/articles/capitol-attack-was-months-making-facebook\)](https://www.techtransparencyproject.org/articles/capitol-attack-was-months-making-facebook) how Facebook allowed election conspiracies and far-right militias to proliferate on its platform, fueling the radicalization that drove the Jan. 6 insurrection. Now, with Zuckerberg set to appear before U.S. lawmakers on Thursday, TTP has found troubling evidence that Facebook is not only continuing to host potentially dangerous militia groups, but in some cases actually creating militia content and pushing it to users through its recommendation algorithm.

Facebook's problems with militia activity persist despite the company's [announcement \(https://web.archive.org/web/20210324143305/https://about.fb.com/news/2020/08/addressing-movements-and-organizations-tied-to-violence/\)](https://web.archive.org/web/20210324143305/https://about.fb.com/news/2020/08/addressing-movements-and-organizations-tied-to-violence/) seven months ago that it would take action against U.S. militia organizations and other extremist groups that pose a risk to public safety.

Here are some of the key findings from TTP's latest research:

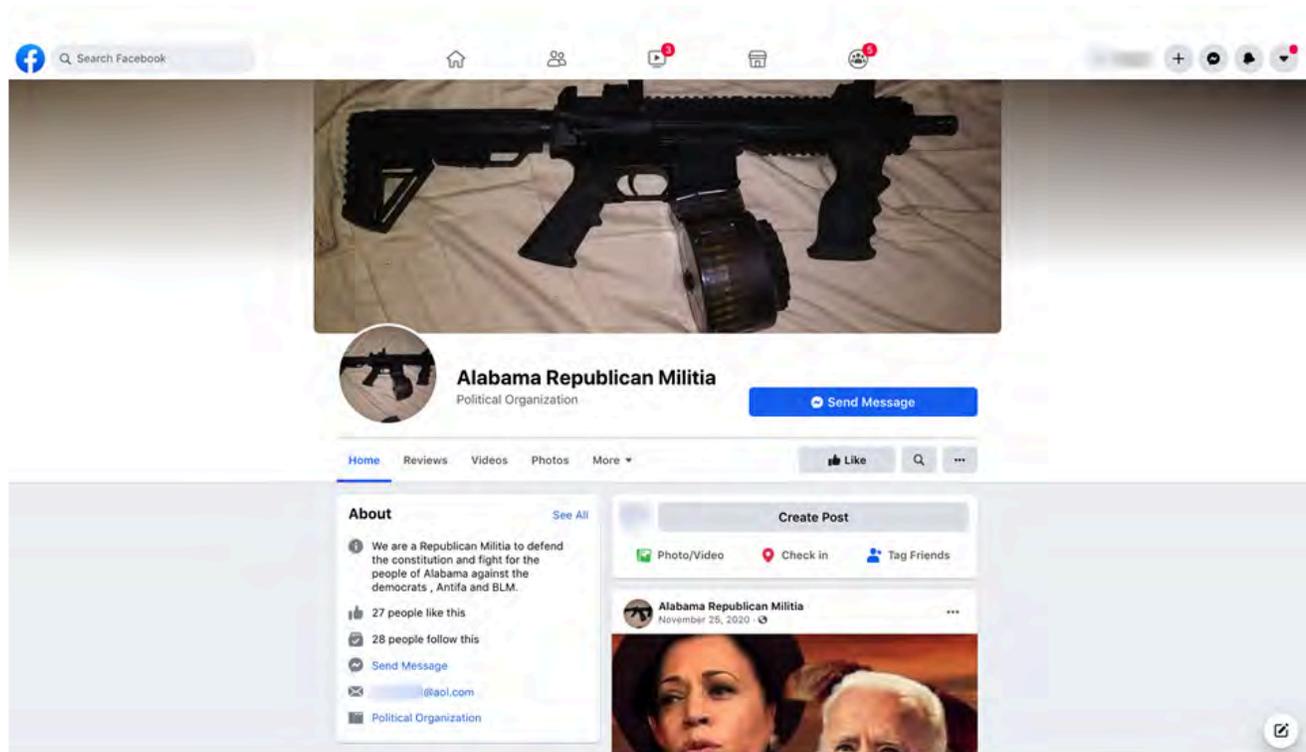
- The investigation identified 201 militia pages and 13 militia groups on Facebook as of March 18, more than two months after the Capitol riot.
- Roughly 70% (140) of the Facebook pages had the word "militia" in their name.
- Facebook is auto-generating pages for some militia organizations, effectively expanding the reach of the movement.
- Facebook also directs users who "like" certain militia pages toward other militia groups, helping these organizations potentially recruit and radicalize users.
- Some Facebook users have begun to turn their personal profiles into de facto pages for militia organizations, likely as a way to avoid detection.
- TTP found some Facebook militia groups circulating propaganda for the far-right Proud Boys, whose members have been charged in the Capitol riot.

#### Hard-to-miss names

TTP identified 201 Facebook militia pages and 13 groups that were active on the platform as of March 18. These included "DFW Beacon Unit" in Dallas-Fort Worth, Texas, which describes itself as a "legitimate militia" and posted March 21 about a training session; "Central Kentucky Freedom Fighters," whose Facebook page posts near-daily content about government infringing on people's rights; and the "New River Militia" in North Carolina, which posted about the need to "wake up the other lions" two days after the Capitol riot.

Strikingly, about 70% (140) of the Facebook pages identified by TTP had "militia" in their name. That's a hard-to-miss affiliation, especially for a company that says its artificial intelligence systems are successfully detecting and removing policy violations like [hate speech](https://www.cnn.com/2020/11/19/facebook-says-ai-detects-94percent-of-hate-speech-removed-from-platform.html) (<https://www.cnn.com/2020/11/19/facebook-says-ai-detects-94percent-of-hate-speech-removed-from-platform.html>) and [terrorist content](https://www.wsj.com/articles/facebook-removed-nearly-40-more-terrorist-content-in-second-quarter-11597162013) (<https://www.wsj.com/articles/facebook-removed-nearly-40-more-terrorist-content-in-second-quarter-11597162013>).

#### Slideshow: ● ○ ○ ○ ○

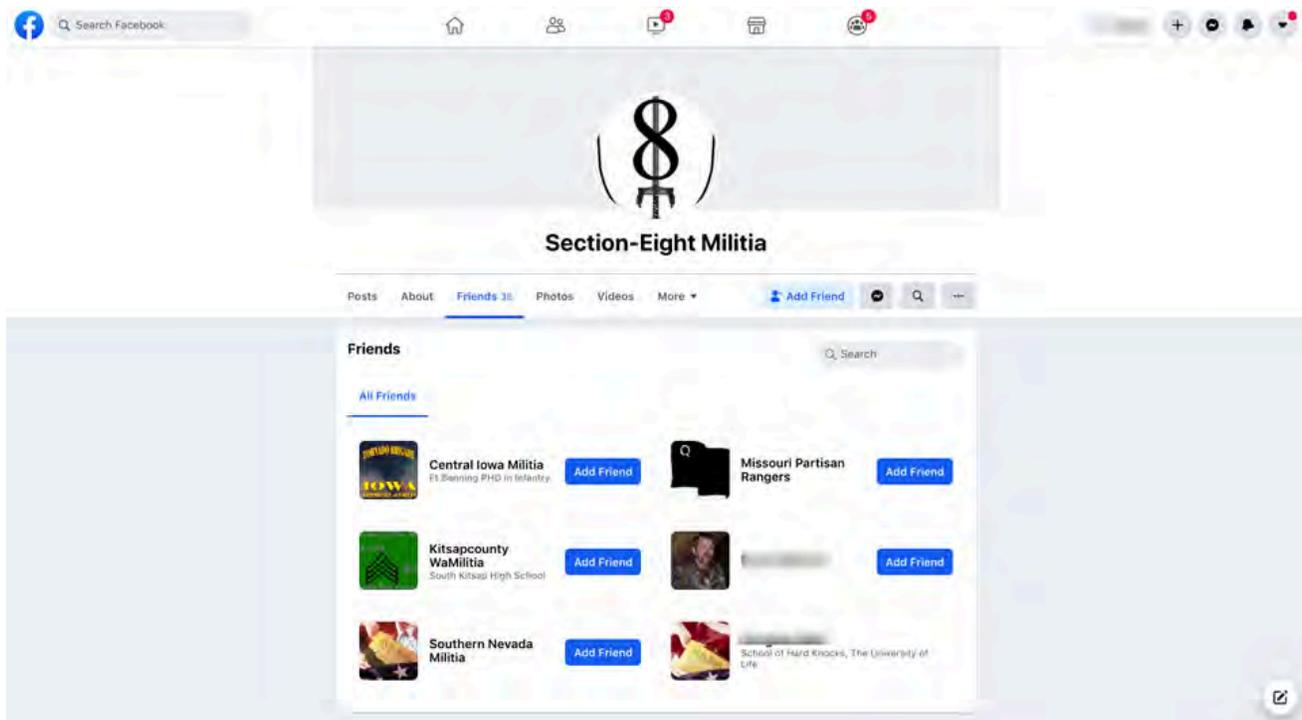


In addition, the TTP investigation found 31 militia-related profiles, which display their militia sympathies through their names, logos, patches, posts, or recruiting efforts. In more than half the cases (20), the profiles had the word "militia" in their name.

One example is the profile for "NaturalBorn Militia," which includes photos with the Three Percenter logo. The [Three Percenters](https://www.adl.org/resources/backgrounders/three-percenters) (<https://www.adl.org/resources/backgrounders/three-percenters>) are an anti-government extremist faction of the militia movement, according to the Anti-Defamation League.

Some of these profiles appear to be acting as de facto pages for militia organizations, TTP found. That may be a way for them to avoid detection by allowing them to maintain tighter control of information, deciding when to make individual posts public, for example. Such strategies have also been adopted by wildlife traffickers operating on Facebook, according to a [report](https://static1.squarespace.com/static/5e3a7fb845f8c668df48d437/t/5f8d9d26b6b09842cbd7eca7/1603116334186/ACCO+2+Clicks+Away+Wildlife+Sales+on+Facebook+Oct+2020+FINAL.pdf) (<https://static1.squarespace.com/static/5e3a7fb845f8c668df48d437/t/5f8d9d26b6b09842cbd7eca7/1603116334186/ACCO+2+Clicks+Away+Wildlife+Sales+on+Facebook+Oct+2020+FINAL.pdf>) last year from The Alliance to Counter Crime Online.

Some of the militia profiles identified by TTP are networked together. For example, the profile for "Section-Eight Militia" in Texas has a friend network that includes other militia profiles like "Kitsapcounty WaMilitia," "Missouri Partisan Rangers," "Central Iowa Militia," and "Southern Nevada Militia."



Facebook's continuing struggles with militia content provide a troubling backdrop as Zuckerberg prepares to make a virtual appearance before Congress Thursday – his first testimony since the deadly Capitol insurrection. The House Energy & Commerce Committee [hearing \(https://energycommerce.house.gov/committee-activity/hearings/hearing-on-disinformation-nation-social-medias-role-in-promoting\)](https://energycommerce.house.gov/committee-activity/hearings/hearing-on-disinformation-nation-social-medias-role-in-promoting), is slated to delve into social media's role in promoting extremism and misinformation.

As TTP [reported \(https://www.techtransparencyproject.org/articles/capitol-attack-was-months-making-facebook\)](https://www.techtransparencyproject.org/articles/capitol-attack-was-months-making-facebook), in January, Facebook allowed domestic extremists to discuss weapons and tactics, coordinate activities, and spread calls to overthrow the government for months leading up to and including the mob attack on the Capitol. The evidence contradicts Facebook Chief Operating Officer Sheryl Sandberg's [claims \(https://www.cnbc.com/2021/01/11/sandberg-says-us-capitol-riot-was-not-organized-on-facebook.html\)](https://www.cnbc.com/2021/01/11/sandberg-says-us-capitol-riot-was-not-organized-on-facebook.html), that the January 6 riot was "largely organized" on other platforms.

Meanwhile, the Biden administration is putting a heavier emphasis on combatting domestic extremism. The Office of the Director of National Intelligence (ODNI) issued a March [report \(https://www.dni.gov/files/ODNI/documents/assessments/UnclassSummaryofDVEAssessment-17MAR21.pdf\)](https://www.dni.gov/files/ODNI/documents/assessments/UnclassSummaryofDVEAssessment-17MAR21.pdf), that identified militia as one of the "most lethal" domestic violent extremism threats.

### **Amplifying content**

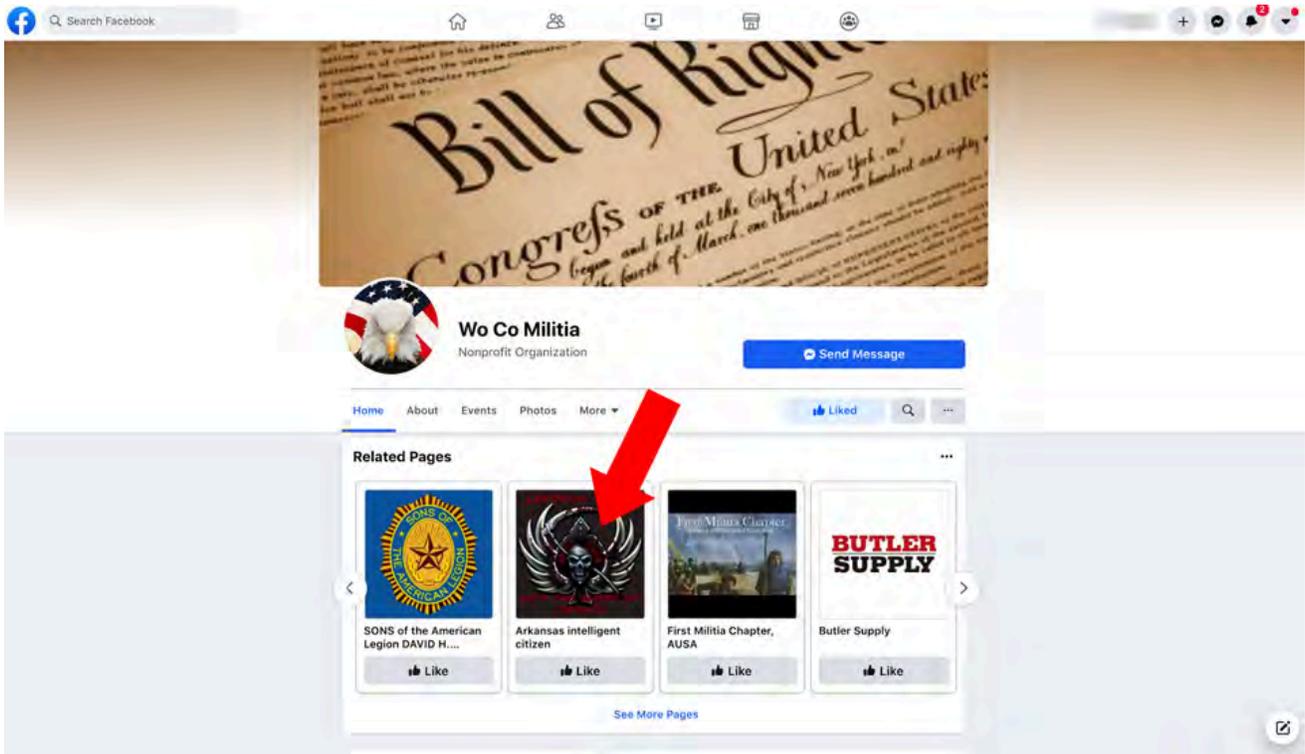
Facebook is not just missing militia content. It's also, in some cases, creating it.

About 17 percent of the militia pages identified by TTP (34) were actually auto-generated by Facebook, most of them with the word "militia" in their names. This has been a recurring issue with Facebook. A TTP investigation in May 2020 found that Facebook had auto-generated business pages for [white supremacist groups \(https://www.techtransparencyproject.org/sites/default/files/Facebook-White-Supremacy-Report.pdf\)](https://www.techtransparencyproject.org/sites/default/files/Facebook-White-Supremacy-Report.pdf).

Auto-generated pages are not managed by an administrator, but they can still play a role in amplifying extremist views. For example, if a Facebook user "likes" one of these pages, the page gets added to the "about" section of the user's profile, giving it more visibility. This can also serve as a signal to potential recruiters about pro-militia sympathies.

Meanwhile, Facebook's recommendation algorithm is pushing users who "like" militia pages toward other militia content.

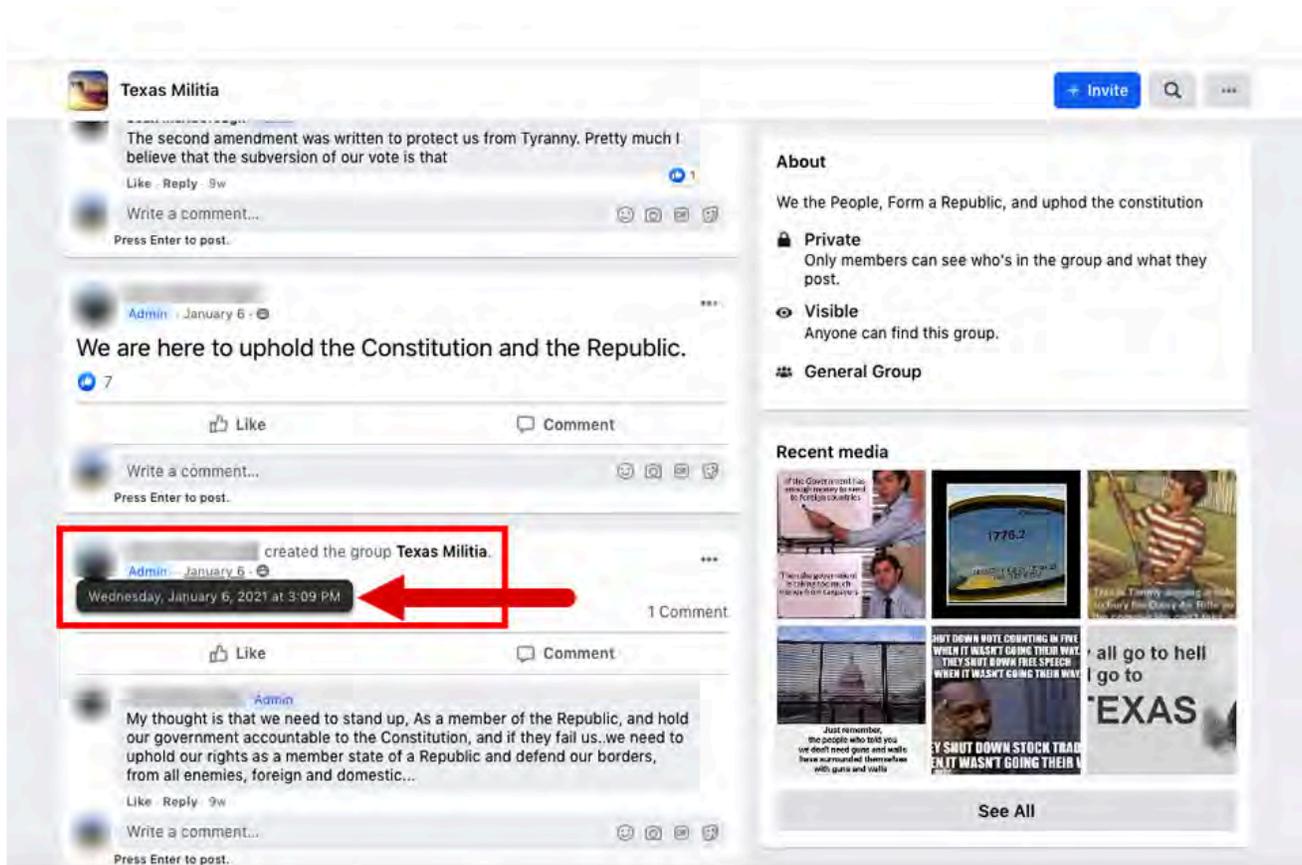
When TTP "liked" the page for "Wo Co Militia," Facebook recommended a page called "Arkansas Intelligent citizen," which features a large Three Percenter logo as the page header. (The "history" section in the page transparency shows that it was previously named "3%ERS – Arkansas.")



TTP found that 26 of the militia pages, including two that were auto-generated, were created after Facebook's announced [crackdown](https://web.archive.org/web/20210324143305/https://about.fb.com/news/2020/08/addressing-movements-and-organizations-tied-to-violence/) (<https://web.archive.org/web/20210324143305/https://about.fb.com/news/2020/08/addressing-movements-and-organizations-tied-to-violence/>) on U.S. militias (later described as "militarized social movements") on August 19, 2020. A total of 44 pages have posted new content since that date.

Six of the Facebook militia groups identified by TTP were also created after August 19. One group, explicitly named "Texas Militia," launched on the afternoon of Jan. 6, in the midst of the attack on the U.S. Capitol. The administrator who created the group warned that "modern technology has enabled radicals to subvert the process by which we elect our representatives," adding "we must be prepared ... to defend our rights and prevent the takeover of our great nation by radicals, uphold the Constitution and preserve our way of life."

Slideshow: ● ○ ○ ○ ○



TTP identified one Facebook group called “C.A.M.P.,” which stands for “Constitutional American Militia Project.” The group pinned a mission statement on March 12 that encourages all “fellow patriots” to march on state capitols across the country and force out elected officials. The date for the event is “to be announced.”

On March 13, the C.A.M.P. group’s administrator posted a three-minute video promoting the far-right Proud Boys, an organization that’s been [banned](https://techcrunch.com/2018/10/30/facebook-proud-boys-mcinnis-kicked-off/) (<https://techcrunch.com/2018/10/30/facebook-proud-boys-mcinnis-kicked-off/>), on Facebook since 2018 and whose alleged leaders have been charged with [conspiracy](https://www.npr.org/2021/03/19/979304432/4-proud-boys-charged-with-conspiracy-over-jan-6-capitol-riot) (<https://www.npr.org/2021/03/19/979304432/4-proud-boys-charged-with-conspiracy-over-jan-6-capitol-riot>) in the attack on the U.S. Capitol. The video is essentially a highlight reel of Proud Boys attacks on Black Lives Matter protesters as well as footage from the Capitol riot.

This kind of admin post highlights a critical flaw in Facebook’s groups policy. In a March 17 policy [update](https://web.archive.org/web/20210320201054/https://about.fb.com/news/2021/03/changes-to-keep-facebook-groups-safe/) (<https://web.archive.org/web/20210320201054/https://about.fb.com/news/2021/03/changes-to-keep-facebook-groups-safe/>), outlining new penalties for groups that violate Facebook’s Community Standards, Facebook said it would require group admins and moderators to approve all posts in certain cases. But if the admins themselves are posting the content, and like-minded group members don’t report it, then the groups are less likely to come to Facebook’s attention.

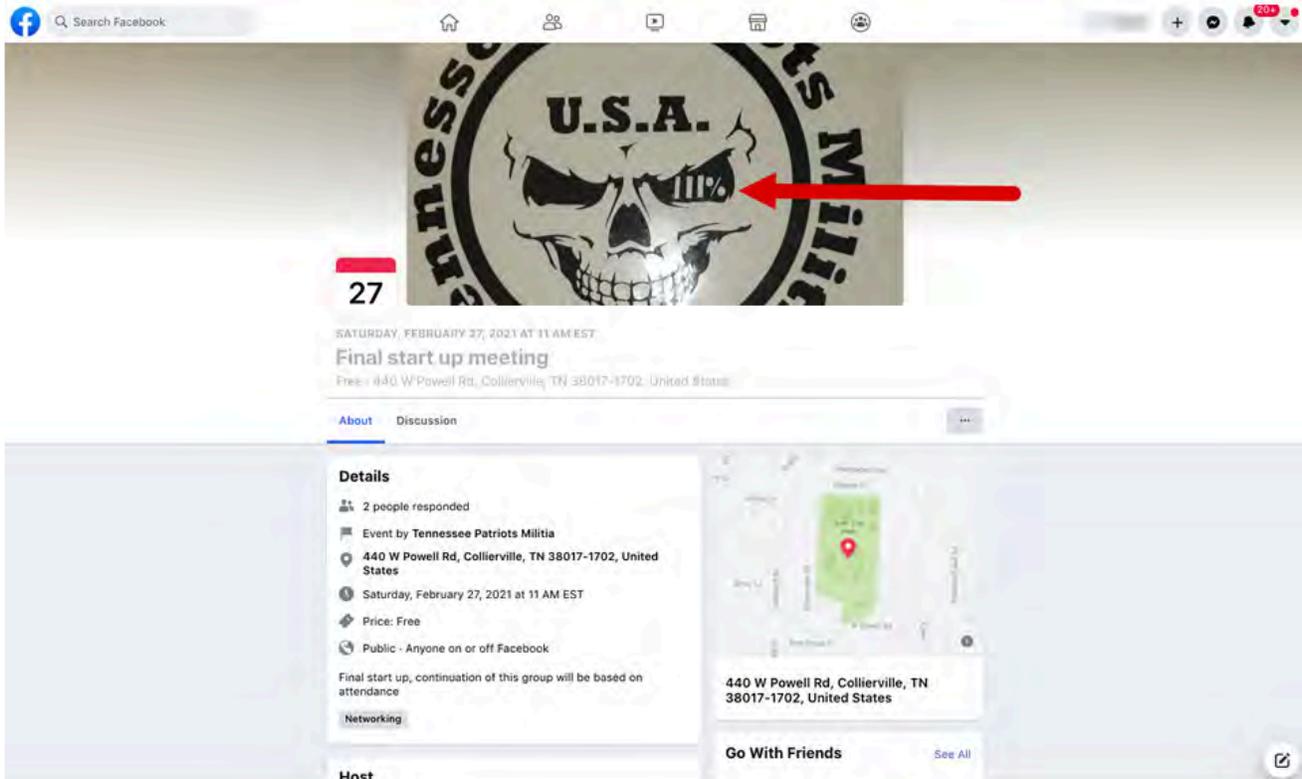
#### Events and recruitment

TTP found that Facebook is continuing to allow militias to use its Events feature, despite revelations that the company [failed to act](https://www.buzzfeednews.com/article/ryanmac/facebook-failed-kenosha) (<https://www.buzzfeednews.com/article/ryanmac/facebook-failed-kenosha>) on a “Kenosha Guard” event page that urged people to bring weapons to a Black Lives Matter protest. (Then-17-year-old Kyle Rittenhouse is charged with fatally shooting two people at the August protest.)

A Facebook page called “Tennessee Patriots Militia,” created on Dec. 6, 2020, has used the events feature on three occasions to organize meetings of group members. The most recent event page for a “final start up meeting,” on Feb. 27, featured a skull with the III% symbol in one of the eyes. The III% refers to the anti-government Three Percenters.

Another page called “Light Horse Militia,” which indicates it’s based in Lee County, Virginia, posted a recruitment call for members in July 2020. The post specifically seeks members with “prior law enforcement or military experience.”

Slideshow: ● ○ ○ ○

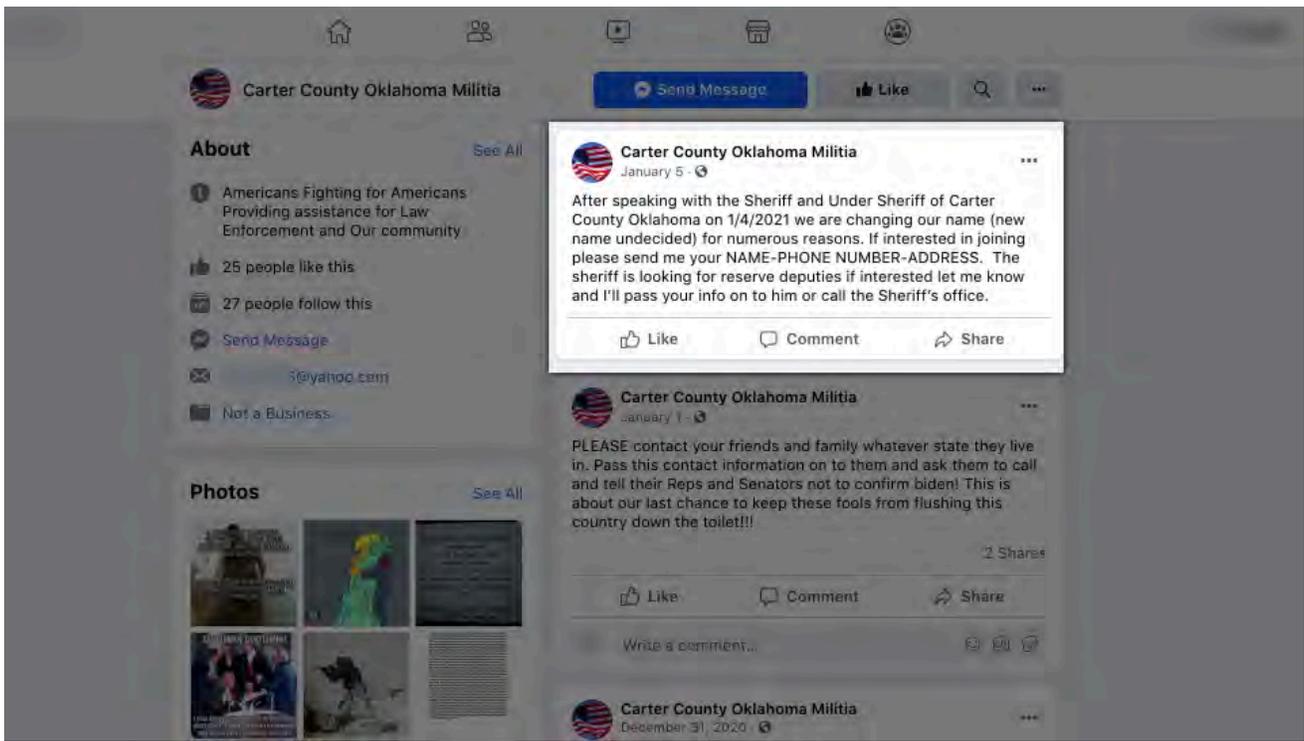


In some cases militias are making use of multiple Facebook tools. A page called the "1st Nebraska Volunteer Militia," which describes itself as an "organized paramilitary force that is not part of the regular armed forces," also serves as the admin of a Facebook group of the same name. The 1st Nebraska Volunteer Militia page promoted an event poster for a "Million Militia March" that was slated to take place on Jan. 20 Inauguration Day.

Slideshow: ● ○ ○



Some of the pages suggest efforts to coordinate with law enforcement. One page called "Carter County Oklahoma Militia" posted on Jan. 5, 2021, that it had changed its name after speaking with the local sheriff; that the sheriff is looking for "reserve deputies," and that people interested in being a reservist should contact the page manager.



Tech Transparency Project is a research initiative of Campaign for Accountability, a 501(c)(3) non-profit, nonpartisan watchdog organization that uses research, litigation and aggressive communications to expose how decisions made behind the doors of corporate boardrooms and government offices impact Americans' lives.

Donate Today (<https://secure.donationpay.org/campaignforaccountability/>)

# Exhibit 72



1



17



Southern Poverty Law Center

February 1 · 🌐



In 2020, SPLC tracked 838 hate groups that spread bigotry and hate in our communities. In fact, our August 2020 poll revealed that 29% of Americans personally know someone who believes that white people are the superior race.

The U.S. Capitol insurrection alone showed us how the Trump campaign and the MAGA movement mask themselves with patriotism while committing acts of white terrorism.

See our hate map: <https://www.splcenter.org/hate-map>



2.7K

833 Comments 2.2K Shares

Like

Comment

Share

Most Relevant



Kathleen Goodman



Write a comment...



# Exhibit 73

[WHAT ARE HUMAN RIGHTS?](#)[DONATE](#)[HOME](#)[ABOUT US](#)[ISSUES](#)[HUMAN RIGHTS  
BY COUNTRY](#)[WHERE WE  
WORK](#)[HUMAN RIGHTS  
BODIES](#)[NEWS AND  
EVENTS](#)[PUBLICATIONS AND  
RESOURCES](#)[English > News and Events > DisplayNews](#)

---

## **Myanmar: UN Fact-Finding Mission releases its full account of massive violations by military in Rakhine, Kachin and Shan States**

GENEVA (18 September 2018) – The Independent International Fact-Finding Mission on Myanmar on Tuesday released the full 440-page account of the findings of its 15-month examination of the situation in three states in Myanmar. The report also makes dozens of recommendations, including to the United Nations and the international community and to the Government of Myanmar. It reiterates the Fact-Finding Mission’s call for the investigation and prosecution of Myanmar’s Commander-in-Chief, Senior General Min Aung Hlaing, and his top military leaders for genocide, crimes against humanity and war crimes.

“Peace will not be achieved while the Tatmadaw remains above the law,” Marzuki Darusman, chair of the Fact-Finding Mission stated. “The Tatmadaw is the greatest impediment to Myanmar’s development as a modern democratic nation. The Commander-in-Chief of the Tatmadaw, Min Aung Hlaing, and all the current leadership must be replaced, and a complete restructuring must be undertaken to place the Tatmadaw under full civilian control. Myanmar’s democratic transition depends on it.”

Following the release of its 20-page report to the Human Rights Council of its main findings on 27 August 2018, the Mission has now released its full report, unprecedented in its scope. The full report establishes the clear patterns of violations by the Myanmar military, known as the Tatmadaw, across the country, and the legal analysis on which the recommendations are based.

The three members of the Fact-Finding Mission will present their report to the UN Human Rights Council on Tuesday morning.

Drawing on 875 detailed interviews conducted in locations in five countries, the report illustrates, in graphic detail, the violent modus operandi that is the hallmark of Tatmadaw operations against its own people. The Mission was struck by how similar the Tatmadaw operations and conduct were in all three States.

“During their operations the Tatmadaw has systematically targeted civilians, including women and children, committed sexual violence, voiced and promoted exclusionary and discriminatory rhetoric against minorities, and established a climate of impunity for its soldiers,” said Marzuki Darusman. “The full findings we are releasing today show why, in our report to the Human Rights Council, we insist that the perpetrators of the gross human rights violations and international crimes, committed in Rakhine, Kachin and Shan States must not go unpunished. They also show why the top generals should be investigated and prosecuted for genocide in Rakhine State. I have never been confronted by crimes as horrendous and on such a scale as these.”

The report sets out in extensive detail its findings on the extreme violence perpetrated against the

The report sets out in extensive detail its findings on the extreme violence perpetrated against the Rohingya in Rakhine State since 25 August 2017, in what the Tatmadaw referred to as 'clearance operations'. It documents in unsparing detail how the Tatmadaw took the lead in killing thousands of Rohingya civilians, as well as forced disappearances, mass gang rape and the burning of hundreds of villages.

Through first-hand testimony from hundreds of victims and witnesses, the report provides harrowing details of some of the most serious mass-killings that took place during the 'clearance operations'. These operations – including those in Min Gyi (known in Rohingya as Tula Toli), Chut Pyin and Maung Nu – involved planned and deliberately executed mass killing in which “dozens and, in some cases hundreds of men, women and children were killed”, the report says.

The report also details how the Tatmadaw perpetrated similar patterns of violations in numerous other villages. The Mission has corroborated Tatmadaw 'clearance-operations' in a total of 54 locations, and received first-hand accounts of additional operations in a further 22 locations.

“The horrors inflicted on Rohingya men, women and children during the August 2017 operations, including their indiscriminate killing, rise to the level of both war crimes and crimes against humanity”, said Radhika Coomaraswamy, another member of the Mission. “The crimes themselves, and the manner in which they were perpetrated, were found to be similar in nature, gravity and scope to those that have allowed for genocidal intent to be established in other contexts,” she added.

The report reveals a pattern of rape and other forms of sexual violence committed on a shocking scale. Hundreds, possibly thousands, of Rohingya women and girls were brutally raped, including in public mass gang rapes. Many victims were then killed or mutilated. This represents a particularly serious pattern of orchestrated and condoned sexual violence. The report concludes that “rape and sexual violence are part of a deliberate strategy to intimidate, terrorise or punish a civilian population, and are used as a tactic of war.”

The experts also expressed grave concern at the conviction and imprisonment of two Reuters reporters, Wa Lone and Kyaw Soe Oo. “These journalists have engaged in legitimate work investigating the extrajudicial killings of 10 Rohingya men in Inn Din, an incident we have now independently corroborated,” commented the experts. “While the Reuters investigation brought this incident to light, regrettably it is just the tip of an iceberg of violent mass killings, others of which are detailed in our report.”

The report includes satellite images, setting out detailed analysis that corroborates information provided by victims and witnesses. The images show the transformation of much of northern Rakhine State over the past year, with at least Rohingya 392 villages razed to the ground, providing irrefutable documentation of the scale of destruction perpetrated.

Further satellite imagery shows that the burning has been followed with the clearance by bulldozers of large areas of land. “Through this process, many Rohingya villages have been rendered unrecognisable, devoid of all structures, trees and vegetation”, the report states. “Now, new security structures, infrastructure projects, and new villages, almost exclusively built for other non-Rohingya ethnic communities, are being constructed where Rohingya homes once stood.” In this light, the report casts serious doubts over plans for repatriation: “In the current circumstances, returns are not possible,” it says.

The report further details how the extreme violence perpetrated against the Rohingya in 2017 and their mass expulsion can only be properly understood against a backdrop of decades of institutionalised oppression and persecution affecting the lives of the Rohingya “from birth to death”. This includes the denial of legal status and identity; restrictions on freedom of movement, access to food, livelihood, health and education; and restrictions affecting private life such as marriage and birth. The Mission has also investigated thoroughly the 2012 violence between the ethnic Rakhine and the Rohingya, with a focus on the events in Maungdaw, Sittwe and Kyaukpyu. It concluded that the 2012 violence was not purely “inter-communal,” as asserted by the authorities, but actively instigated, through concerted hate campaigns, with the involvement of the Tatmadaw, the Police, other State institutions and many figures of authority.

The Mission also documented serious human rights violations by the Tatmadaw against ethnic Rakhine communities, including forced labour, sexual violence, killings and forced evictions. "Human rights violations against ethnic Rakhine communities have largely gone unnoticed," underlined the experts, calling for further investigations into violations against them.

Although their violations are nowhere near the same scale as those by the Tatmadaw, the Arakan Rohingya Salvation Army (ARSA) and the ethnic armed organizations (EAOs) operating in Kachin and Shan States have not escaped scrutiny by the Mission. The report concludes that ethnic armed organizations have carried out extrajudicial killings, failed to take precautionary measures to protect civilians during attacks, destroyed property and forcibly recruited civilians, among other abuses.

Although international attention has focused overwhelmingly on the situation in Rakhine State, the report also sets out the findings of its detailed investigation into violations perpetrated in the northern states of Shan and Kachin. The report finds that the actions of the Tatmadaw in both Kachin and Shan States since 2011 amount to war crimes and crimes against humanity.

While the conflict in the north is ostensibly between the Tatmadaw and ethnic armed groups, civilians in Kachin and Shan are targeted, often simply for belonging to the same ethnic group as the Tatmadaw's opponents. Through specific case studies, the Mission establishes the patterns of behaviour of the Tatmadaw in the northern States.

"As in Rakhine, civilians are targeted for killings, rape, arbitrary arrest and detention, enforced disappearance, forced labour, torture and ill-treatment, and persecution based on ethnic or religious grounds," said Chris Sidoti, the Fact-Finding mission's other member. "To date, the long-standing conflicts in the north of Myanmar have received inadequate international attention. We hope our report will raise awareness of the critical situation in Kachin and Shan. We are seriously concerned that fighting is continuing in these regions, with new allegations of serious violations against civilians continuing to emerge."

The report also finds a prevalent pattern of destruction of civilian homes and property in the north. Tens of thousands of people have been displaced in Kachin and Shan, and many continue to live in dire conditions in displaced persons' camps.

The report also investigated the rampant hate speech in Myanmar disseminated through public pronouncements, religious teachings and traditional and social media including Facebook. "The Myanmar authorities have emboldened those who preach hatred and silenced those who stand for tolerance and human rights," the report notes. "By creating an environment where extremists' discourse can thrive, human rights violations are legitimised, and incitement to discrimination and violence facilitated."

"The Tatmadaw acts with complete impunity and has never been held accountable for the violations of international law it is consistently involved in," the report concludes. The report calls on the United Nations Security Council to refer Myanmar to the International Criminal Court, or to establish an ad hoc international criminal tribunal. It also calls for targeted individual sanctions, including travel bans and asset freezes against those who appear most responsible, and an arms embargo on Myanmar. The experts identified six individual senior commanders as most responsible, including the Tatmadaw Commander in Chief, Senior-General Min Aung Hlaing. An unpublished list containing additional names will be given to the High Commissioner for Human Rights who will be able to share it at her discretion with any competent and credible body pursuing accountability.

"Addressing situations like that in Myanmar touches on the very purpose of the United Nations," the experts noted, emphasising the imperative for the organisation to continue its important work in country. "We call on all the competent organs and agencies of the UN to step up to the task, and to act with urgency and in accordance with the principles of human rights."

"The international community has failed. Let us now resolve not to fail the people of Myanmar again," they added.

ENDS

Media products including videos, slideshows, satellite imagery and analysis and infographics are available at the Mission's website [www.ffmmyanmar.org](http://www.ffmmyanmar.org)

The full report will be available on the report page or [download here](#)

- **A/HRC/39/64** available in both [English](#) and [Myanmar](#) Language
- UNTV will broadcast both the council session, which includes a dialogue with Myanmar, and the Mission's press conference scheduled immediately after the council session at [webtv.un.org](http://webtv.un.org)

*Marzuki Darusman, lawyer and human rights campaigner and former Attorney-General of Indonesia, is chair of the fact-finding mission. The other two members of the fact-finding mission are Radhika Coomaraswamy, a lawyer and former UN Special Rapporteur on Violence against Women and UN Special Representative for Children and Armed Conflict; and Christopher Sidoti, international human rights lawyer and former Australian Human Rights Commissioner.*

Contact information: Nathan Thompson, [consultant.thompson@ohchr.org](mailto:consultant.thompson@ohchr.org) +41 76 691 0799

[Home](#)

[Site Map](#)

[CONTACT US](#)

[Frequently Asked Questions](#)

© OHCHR 1996-2021

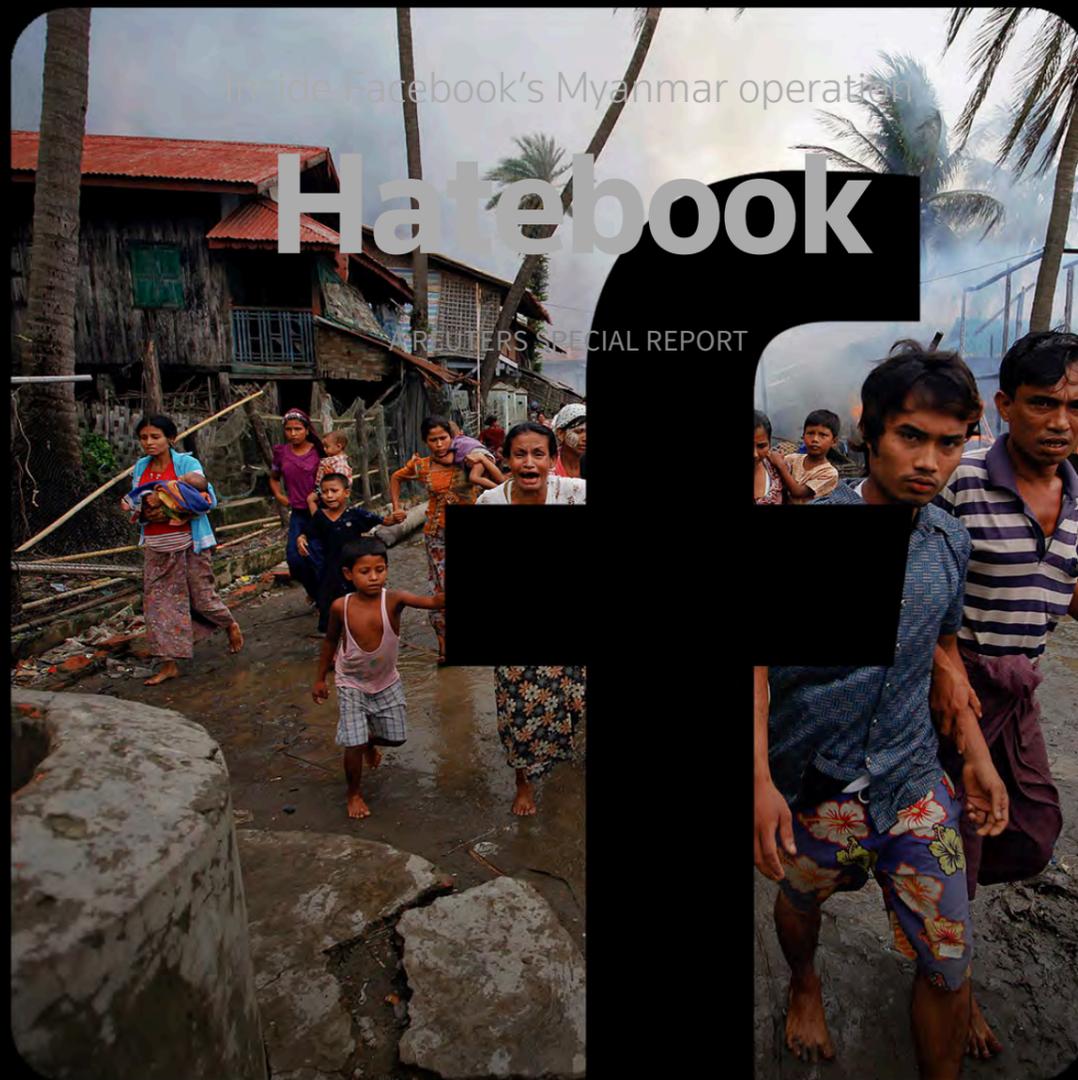
[OHCHR on Social Media](#)

[OHCHR Memorial](#)

[Employment](#)

[Mobile App](#)

# Exhibit 74



ETHNIC VIOLENCE: There have been repeated outbreaks of communal violence in Myanmar. In March, a United Nations investigator said Facebook had been used to incite hatred against the Rohingya. REUTERS/Soe Zeya Tun

## Why Facebook is losing the war on hate speech in Myanmar

Reuters found more than 1,000 examples of posts, comments and pornographic images attacking the Rohingya and other Muslims on Facebook. A secretive operation set up by the social media giant to combat the hate speech is failing to end the problem.

By [STEVE STECKLOW](#) | Filed Aug. 15, 2018, 3 p.m. GMT

YANGON, Myanmar – In April, Facebook founder Mark Zuckerberg told U.S. senators that the social media site was hiring dozens more Burmese speakers to review hate speech posted in Myanmar. The situation was dire.

Some 700,000 members of the Rohingya community had recently fled the country amid a military crackdown and ethnic violence. In March, a United Nations investigator said Facebook was used to incite violence and hatred against the Muslim minority group. The platform, she said, had “turned into a beast.”

Four months after Zuckerberg’s pledge to act, here is a sampling of posts from Myanmar that were viewable this month on Facebook:

One user posted a restaurant advertisement featuring Rohingya-style food. “We must fight them the way Hitler did the Jews, damn kalars!” the person wrote, using a pejorative for the Rohingya. That post went up in December 2013.

Another post showed a news article from an army-controlled publication about attacks on police stations by Rohingya militants. “These non-human kalar dogs, the Bengalis, are killing and destroying our land, our water and our ethnic people,” the user wrote. “We need to destroy their race.” That post went up last September, as the violence against the Rohingya peaked.

A third user shared a blog item that pictures a boatload of Rohingya refugees landing in Indonesia. “Pour fuel and set fire so that they can meet Allah faster,” a commenter wrote. The post appeared 11 days after Zuckerberg’s Senate testimony.

#### RELATED CONTENT

---



Massacre in Myanmar



After the Massacre



Tip of the Spear



Dangerous News

The remarks are among more than 1,000 examples Reuters found of posts, comments, images and videos attacking the Rohingya or other Myanmar Muslims that were on Facebook as of last week. Almost all are in the main local language, Burmese. The anti-Rohingya and anti-Muslim invective analyzed for this article – which was collected by Reuters and the Human Rights Center at UC Berkeley School of Law – includes material that’s been up on Facebook for as long as six years.

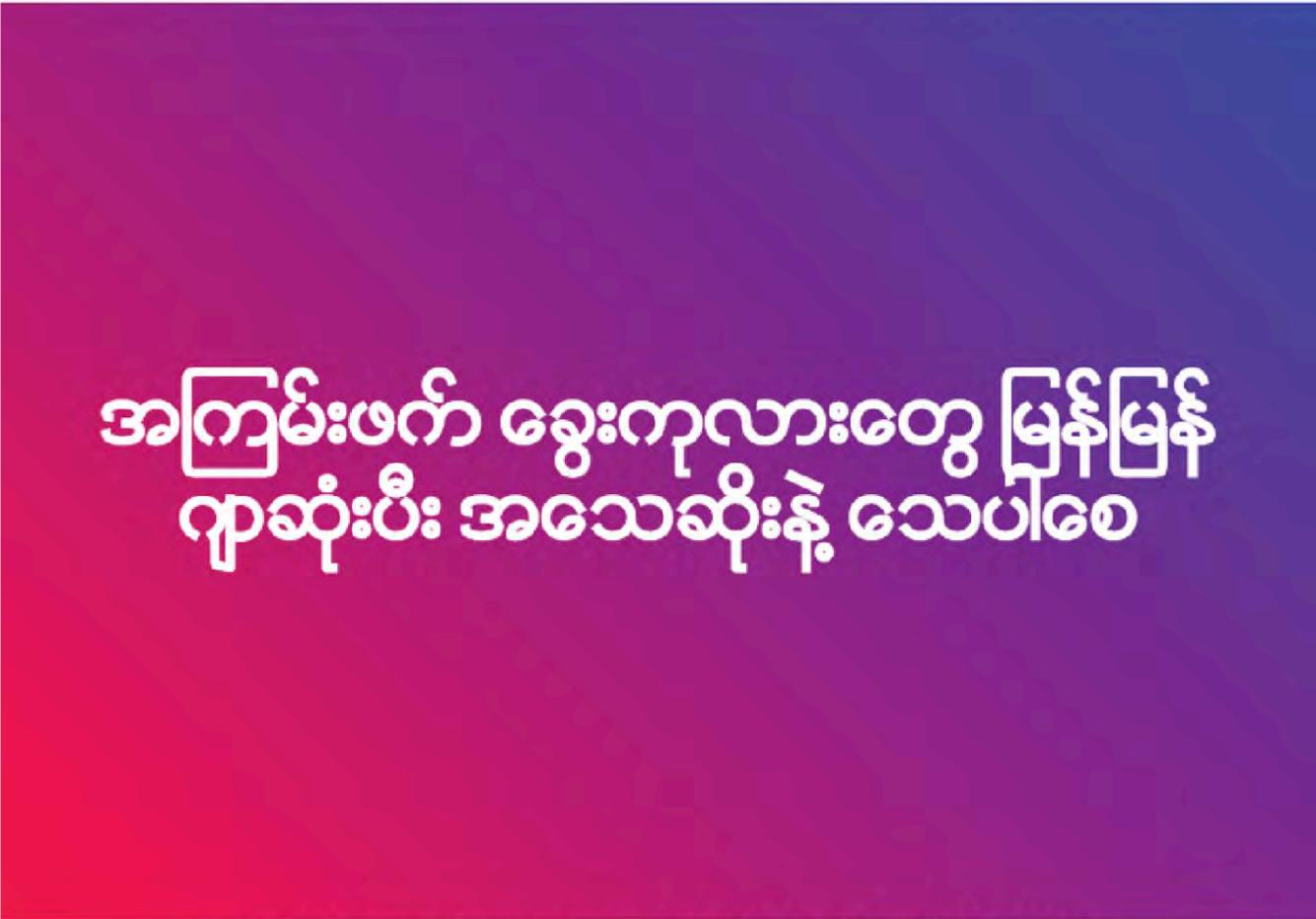
The poisonous posts call the Rohingya or other Muslims dogs, maggots and rapists, suggest they be fed to pigs, and urge they be shot or exterminated. The material also includes crudely pornographic anti-Muslim images. The company’s rules specifically prohibit attacking ethnic groups with “violent or dehumanising speech” or comparing them to animals. Facebook also has long had a strict policy against pornographic content.

The use of Facebook to spread hate speech against the Rohingya in the Buddhist-majority country has been widely reported by the U.N. and others. Now, a Reuters investigation gives an inside look at why the company has failed to stop the problem.

For years, Facebook – which reported net income of \$15.9 billion in 2017 – devoted scant resources to combat hate speech in Myanmar, a market it dominates and in which there have been regular outbreaks of ethnic violence. In early 2015, there were only two people at Facebook who could speak Burmese reviewing problematic posts. Before that, most of the people reviewing Burmese content spoke English.

# Hate speech against the Rohingya on Facebook

Here are a few of the more than 1,000 examples Reuters recently found of posts, comments, images and videos attacking the Rohingya or other Muslims on Facebook. Some of the poisonous content on the social media platform described them as dogs, maggots and rapists, and suggested they be fed to pigs.



**“May the terrorist dog kalars fall fast and die horrible deaths”**

Some examples that included the words “dog kalars,” “damn kalars” and “Bengali whore” that were posted between 2012 and 2018:



Source: Facebook

To this day, the company continues to rely heavily on users reporting hate speech in part because its systems struggle to interpret Burmese text.

Even now, Facebook doesn’t have a single employee in the country of some 50 million people. Instead, it monitors hate speech from abroad. This is mainly done through a secretive operation in Kuala Lumpur that’s outsourced to Accenture, the professional services firm, and codenamed “Project Honey Badger.”

According to people familiar with the matter, the project, which handles many Asian countries, hired its first two Burmese speakers, who were based in Manila, just three years ago. As of June, Honey Badger had about 60 people reviewing reports of hate speech and other content posted by Myanmar’s 18 million active Facebook users. Facebook itself in April had three full-time Burmese speakers at a separate monitoring operation at its international headquarters in Dublin, according to a former employee.

Honey Badger employees typically sign one-year renewable contracts and agree not to divulge that the client is Facebook. Reuters interviewed more than a half-dozen former monitors who reviewed Southeast Asian content.

A Facebook official said outsourcing its content monitoring is more efficient because the companies it uses are specialists in ramping up such operations. He declined to disclose how many Burmese speakers the company has on the job worldwide, saying it was “impossible to know, to be definitive on that.”

“It’s not enough,” he added.

For many people in this emerging economy, Facebook is the internet: It's so dominant, it's the only site they use online. Yet, the company ignored repeated warnings as far back as 2013 that it faced trouble.

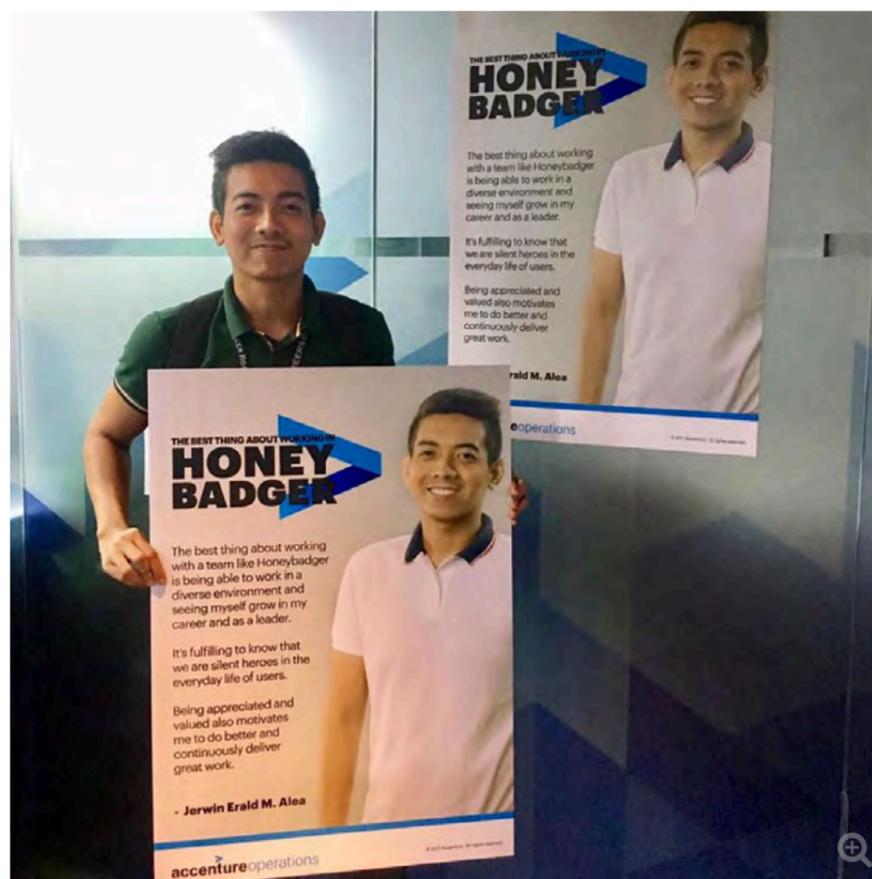
Researchers and human rights activists say they cautioned Facebook for years that its platform was being used in Myanmar to promote racism and hatred of Muslims, in particular the Rohingya.

"They were warned so many times," said David Madden, a tech entrepreneur who worked in Myanmar. He said he told Facebook officials in 2015 that its platform was being exploited to foment hatred in a talk he gave at its headquarters in Menlo Park, California. About a dozen Facebook people attended the meeting in person, including Mia Garlick, now the company's director of Asia Pacific policy, he said. Others joined via video. "It couldn't have been presented to them more clearly, and they didn't take the necessary steps," Madden said.

In a statement, Garlick told Reuters: "We were too slow to respond to the concerns raised by civil society, academics and other groups in Myanmar. We don't want Facebook to be used to spread hatred and incite violence. This is true around the world, but it is especially true in Myanmar where our services can be used to amplify hate or exacerbate harm against the Rohingya."

She added that Facebook is focused on addressing challenges that are unique to Myanmar "through a combination of people, technology, policies and programs." The company also said it has banned several "hate figures and organizations" on Facebook in Myanmar.

Facebook's struggles in Myanmar are among much broader problems it faces. Zuckerberg's congressional testimony in April primarily focused on the company's mishandling of user data, whether it censors conservative views and Russia's exploitation of Facebook to meddle in the 2016 U.S. presidential election.



HATE MONITORS: Facebook reviews hate speech in Myanmar from an outsourced operation run by Accenture and codenamed Project Honey Badger. The poster refers to employees as "silent heroes." Source: Via Facebook

***"Cut off those necks of the sons of the dog and kick them into the water"***

April 2018

***"Stuff pig's fat inside the damn kalar's mouth"***

September 2017

***"Pour fuel and set fire so that they can meet Allah faster"***

April 2018

Of all of Facebook's travails, though, Myanmar may be the bloodiest. The Myanmar military stands accused by the U.N. of having conducted a brutal campaign of killings, mass rape, arson and ethnic cleansing against the Rohingya. The government denies the allegations.

The social media giant doesn't make public its data on hate speech in Myanmar. It says it has 2.2 billion global users and each week receives millions of user reports from around the world about problematic content.

In compiling examples of hate speech for this article, Reuters found some that Facebook subsequently removed. But the vast majority remained online as of early August.

After Reuters alerted Facebook to some of the derogatory posts included in this story, the company said it removed them. "All of it violated our policies," it said.

Reuters itself sometimes flags to Facebook threats posted on the platform against its reporters. These include the Burmese journalists Wa Lone and Kyaw Soe Oo, who are on trial in Myanmar on charges of violating a state secrets law. The two were arrested in December while reporting on the massacre of 10 Rohingya men and have received a deluge of death threats on social media over their story. Facebook has removed such content several times at the news agency's request.

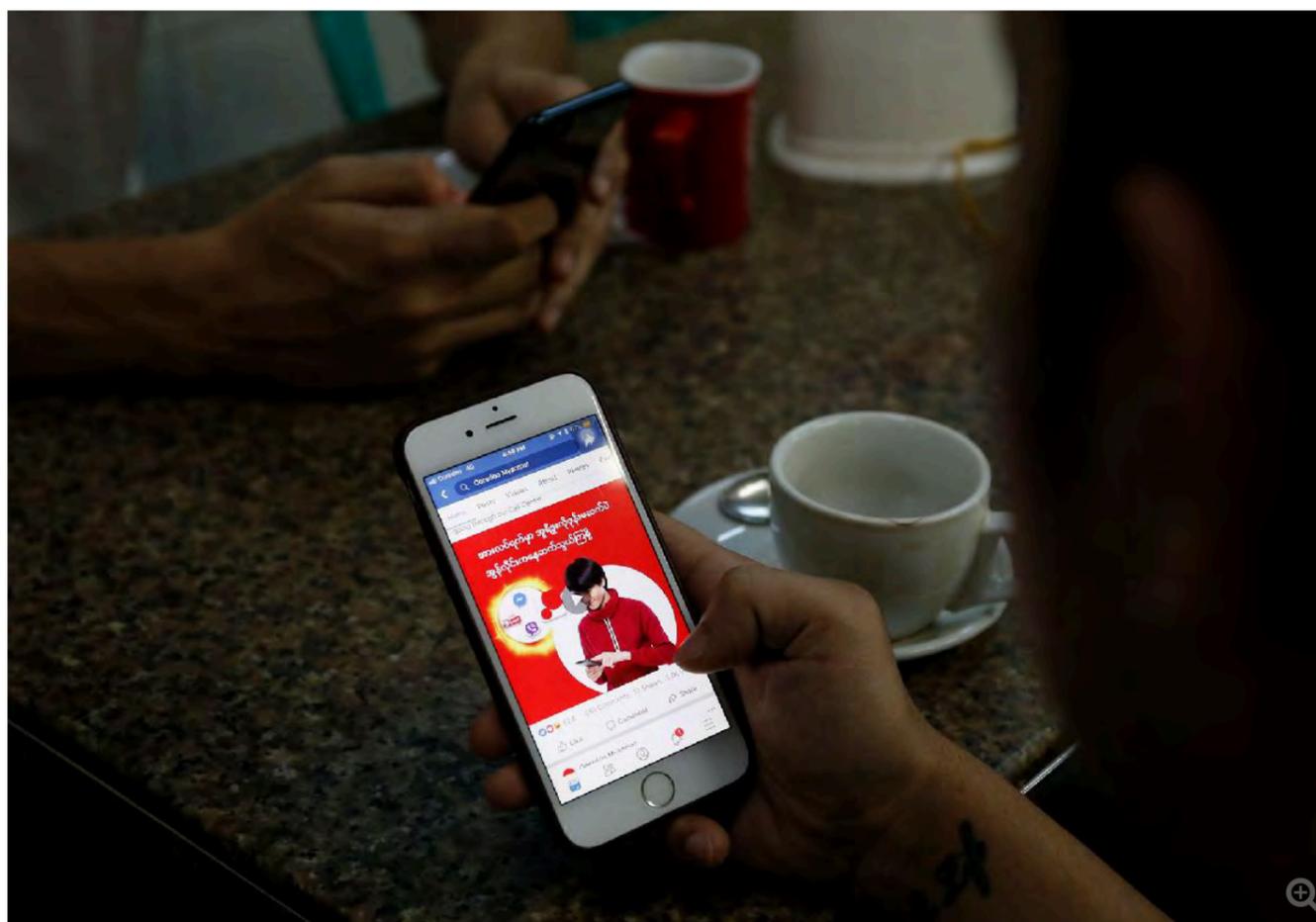
## 'Sending flowers'

Myanmar emerged from decades of military rule in 2011, but religious violence has marred its transition to democracy. In 2012, clashes in Rakhine State between ethnic Rakhine, who are Buddhists, and the Rohingya killed scores of people and left 140,000 displaced – mostly Muslims.

Facebook's extraordinary dominance in Myanmar began taking root around the same time. But not by design.

As recently as six years ago, Myanmar was one of the least connected countries on earth. In 2012, only 1.1 percent of the population used the internet and few people had telephones, according to the International Telecommunication Union, a U.N. agency. The junta that had ruled the country for decades kept citizens isolated.

That all changed in 2013, when a quasi-civilian government oversaw the deregulation of telecommunications. The state-owned phone company suddenly faced competition from two foreign mobile-phone entrants from Norway and Qatar.



UBIQUITOUS: A cellphone user looks at a Facebook page in a shop in downtown Yangon in early August. For many in Myanmar, Facebook is the internet. REUTERS/Ann Wang

The price of SIM cards dropped from more than \$200 to as little as \$2 and people purchased them in droves. By 2016, nearly half the population had mobile phone subscriptions, according to GSMA Intelligence, the research arm of the industry's trade association. Most purchased smartphones with internet access.

One app went viral: Facebook. Many saw it as an all-in-one solution – offering a messaging system, news, and videos and other entertainment. It also became a status symbol, said Chris Tun, a former Deloitte consultant who advised the government. “If you don’t use Facebook, you’re behind,” he said. “Even grandmas, everyone was on Facebook.”

To capture customers, Myanmar’s mobile phone operators began offering a sweet deal: use Facebook without paying any data charges.

“Facebook should be sending flowers to me, because we have been an accelerator for bringing the penetration,” said Lars Erik Tellmann, who until July was chief executive of Telenor Myanmar, part of Norway’s Telenor Group. “This was an initiative we took fully on our own. And this was extremely popular.”

In Myanmar today, the government itself uses Facebook to make major announcements, including the resignation of the president in March.

**2014: 1.2m**

**2015: 7.3m**

**2016: 11m**

**2017: 15m**

**2018: 18m**

(Facebook users in Myanmar in millions)

Sources: We Are Social, Hootsuite, Kepios and Facebook

## ‘Genocide all of the Muslims’

In the fall of 2013, Aela Callan, an Australian documentary filmmaker studying at Stanford University, began a project on hate speech and false reports that had spread online during conflicts between Buddhists and Rohingya Muslims the prior year. In June 2012, at least 80 people had died in riots and thousands of Rohingya were moved into squalid internment camps. Anti-Rohingya diatribes appeared on Facebook. One Buddhist nationalist group set up a page called the “Kalar Beheading Gang.”

In November 2013, she met at Facebook’s California headquarters with Elliott Schrage, vice president of communications and public policy. “I was trying to alert him to the problems,” she said.

Emails between the two show that Schrage put Callan in touch with internet.org, a Facebook initiative to bring the internet to developing countries, and with two Facebook officials, including one who worked with civil-society organizations to assist the company in coping with hate speech.

“He didn’t connect me to anyone inside Facebook who could deal with the actual problem,” she said.

Asked for comment, Schrage referred Reuters to a press person at Facebook. The company didn’t comment on the meeting.

Matt Schissler, a doctoral student at the University of Michigan, said that between March and December 2014, he held discussions with Facebook officials in a series of calls and online communications. He told them how the platform was being used to spread hate speech and false rumors in Myanmar, he said, including via fake accounts. He and other activists provided the company with specific examples, including a Facebook page in Burmese that was called, “We will genocide all of the Muslims and feed them to the dogs.” The page was removed.



ARMY CRACKDOWN: A car stands next to a house that was burned down in Maungdaw in Rakhine State last year during a military campaign that the United States has denounced as ethnic cleansing. Human rights activists and researchers say they warned Facebook for years that its platform was being used to spread hate speech against Muslims in Myanmar. REUTERS/Soe Zeya Tun

Schissler belonged to a private Facebook group that was set up so that Myanmar human rights activists, researchers and company employees such as Asia Pacific policy chief Garlick could discuss how to cope with hate speech and other issues. The activists brought up numerous problems with Facebook's multi-step reporting system for problematic content. As one example, they cited a photograph of an aid worker in Rakhine State in a post that called him "a traitor to the nation." It had been shared 229 times, according to messages reviewed by Reuters.

One of the private group's members had reported it to Facebook as harassment of an individual but later received a message back: "We reviewed the photo you reported for containing hate speech or symbols and found it doesn't violate our Community Standards." After multiple complaints by activists over six weeks, a Facebook employee finally explained to the activists that the takedown request was rejected because the photo had been reported, but not the comment above it. It eventually was taken down.

In March 2015, Schissler gave a talk at Facebook's California headquarters about new media, particularly Facebook, and anti-Muslim violence in Myanmar. More than a dozen Facebook employees attended, he said.

Two months later, Madden, the tech entrepreneur, gave a talk at Facebook headquarters about tensions and violence between Buddhists and Muslims. He said he showed a doctored picture that had spread on Facebook of the country's de facto leader, Aung San Suu Kyi, who is Buddhist, wearing a Muslim head scarf. The image, Madden said, was meant to imply she was sympathetic to Muslims – a "very negative message" in Myanmar.

"The whole point of this presentation was really just to sound the alarm, to show very vividly the context in which Facebook was operating, and already the evidence of how it was being misused," he said. He left the meeting thinking his audience took the talk seriously and would take action.

***"May the Rakhine people ... and all Myanmar citizens be free from the dangers of sons of a dog, grandchildren of a pig kalar, and rapists"***

## ***“Just feed them to the pigs”***

October 2016

## ***“If it’s kalar, get rid of the whole race”***

October 2016

Madden had founded a technology hub and start-up accelerator in Yangon called Phandeeyar. He said he and others involved with the venture interacted with Facebook “many dozens” of times over the next several years, including via email, in the private Facebook group and in person, showing how the network’s systems for detecting and removing dangerous content were ineffective. He isn’t sure what steps the company took in response. “The central problem is that the mechanisms that they have to pull down hate speech in a timely way, before it does real world harm, they don’t work,” he said.

Madden and Jes Kaliebe Petersen, Phandeeyar’s chief executive, said Facebook was still relying too much on their group and other volunteers to report dangerous posts. “It shouldn’t be incumbent on an organization like ours or people who happen to be well-connected with folks inside Facebook to report these things,” Petersen said.

In April, shortly before Zuckerberg’s Senate testimony, Phandeeyar and five other Myanmar groups blasted him for claiming in an interview with Vox that Facebook’s systems had detected and removed incendiary messages in September last year. “We believe your system, in this case, was us,” they wrote. Zuckerberg apologized.

Back in 2014, tech organizations and researchers weren’t the only ones sounding alarms with Facebook. So was the Myanmar government.

In July of that year, riots broke out in the central city of Mandalay after false rumors spread online, on Facebook and elsewhere, that a Muslim man had raped a Buddhist woman. A Buddhist man and a Muslim man were killed in the fighting.

The Myanmar government asked Tun, then a Deloitte consultant, to contact the company. He said he didn’t succeed at first, and the government briefly blocked Facebook.

Tun said he eventually helped to arrange meetings between the government and Facebook. “What they promised to do was, when you spot fake news, you could contact them via email,” Tun said of Facebook. “And they would take action – they were willing to take down pages after their own verification process.”

The government began reporting cases to Facebook, but Tun said he quickly realized the company couldn’t deal with Burmese text. “Honestly, Facebook had no clue about Burmese content. They were totally unprepared,” he said. “We had to translate it into English for them.”

## ***‘I don’t know the language’***

In August 2013, Zuckerberg announced a plan to make the internet available for the first time to billions of people in developing countries.

“Everything Facebook has done has been about giving all people around the world the power to connect,” he said. The company would now work, he added, to make “internet access available to those who cannot currently afford it.”

But in Myanmar, the language barrier would cause trouble. Most people here don’t speak English. Although Myanmar users at the

Making matters worse, the company's operation for monitoring content in Burmese was meagre.

In 2014, the social media behemoth had just one content reviewer who spoke Burmese: a local contractor in Dublin, according to messages sent by Facebook employees in the private Facebook chat group. A second Burmese speaker began working in early 2015, the messages show.

In Manila – the original site of the outsourced Project Honey Badger – there were no content reviewers who spoke Burmese. People who reviewed Myanmar content there spoke English.

“In cases like hate speech where we didn't understand the language, we would say, ‘I don't know the language,’” said a person who worked there. “So the client had to solve that,” the person said, referring to Facebook.

By 2015, Facebook had around four Burmese speakers reviewing Myanmar content in Manila and Dublin. They were stretched thin: that year Facebook had 7.3 million active users in Myanmar.

Accenture slowly began to hire more Burmese speakers. With the help of volunteer translators, Facebook also introduced a Burmese-language interface.

By 2016, the Honey Badger project had moved to Kuala Lumpur after Accenture convinced Facebook it would be easier to recruit Burmese and others to work in Malaysia's capital than in further-off Manila, according to a person familiar with the matter.

In an office tower in Kuala Lumpur, teams of content monitors are assigned to handle different Asian countries, not just Myanmar. They are paid around \$850 to \$1000 a month and are often employed by temporary staffing agencies, according to ex-employees and online recruitment ads.

Facebook said in a statement: “We've chosen to work only with highly reputable, global partners that take care of their employees, pay them well and provide robust benefits - this includes Accenture in Asia Pacific.”

A spokesperson for Accenture confirmed it partners with Facebook. “The characterization of our operations as ‘secretive’ is misleading and confidentiality is in place primarily to protect the privacy and security of our people and the clients we serve,” the spokesperson said.

## The communications man

Former content monitors said they often each had to make judgments on 1,000 or more potentially problematic content items a day, although the number is now understood to be less. Facebook's complete rules about what is and isn't allowed on its platform are spelled out in its internal community standards enforcement guidelines, which the company made public for the first time in April. It defines hate speech as “violent or dehumanising speech, statements of inferiority, or calls for exclusion or segregation” against people based on their race, ethnicity, religious affiliation and other characteristics.

In response, Facebook said: “Content reviewers aren't required to evaluate any set number of posts ... We encourage reviewers to take the time they need.”

A Facebook official also told Reuters the community standards policy is global, “but there are local nuances,” such as slurs, that content reviewers who are native speakers can consider when making decisions. But former content monitors told Reuters the rules were inconsistent; sometimes they could make exceptions and sometimes they couldn't.

Former content monitors also said they were trained to err on the side of keeping content on Facebook. “Most of the time, you try to give the user the benefit of the doubt,” said one former Facebook employee.

The ex-monitors said they sometimes had as little as a few seconds to decide if a post constituted hate speech or violated Facebook's community standards in some other way. They said they didn't actually search for hate speech themselves; instead, they reviewed a giant queue of posts mostly reported by Facebook users.



FACING SCRUTINY: Facebook CEO Mark Zuckerberg, seen testifying here on Capitol Hill in April, was quizzed over Facebook's failure to stem hate speech on its platform in Myanmar. For years, the social media giant invested scant resources in combating hate speech in the country. REUTERS/Leah Millis



MARKET PENETRATION: The sun rises behind the entrance sign to the Facebook headquarters in Menlo Park, California, in 2012, a time when only 1.1 percent of people in Myanmar used the internet. Six years on, the company has 18 million users in the country, about a third of the population. REUTERS/Beck Diefenbach/File Photo

Many of the millions of items flagged globally each week – including violent diatribes and lurid sexual imagery – are detected by automated systems, Facebook says. But a company official acknowledged to Reuters that its systems have difficulty interpreting Burmese script because of the way the fonts are often rendered on computer screens, making it difficult to identify racial slurs and other hate speech.

Facebook's troubles are evident in a new feature that allows users to translate Burmese content into English. Consider a post Reuters found from August of last year.

In Burmese, the post says: "Kill all the kalars that you see in Myanmar; none of them should be left alive."

Facebook's translation into English: "I shouldn't have a rainbow in Myanmar."

In response, Facebook said: "Our translations team is actively working on new ways to ensure that translations are accurate." The company said it uses a different system to detect hate speech.

Guy Rosen, vice president of product management, wrote in a blog post on Facebook in May about the problems the company faced in identifying hate speech. "Our technology still doesn't work that well and so it needs to be checked by our review teams," he wrote.

Facebook officials say they have no immediate plans to hire any employees in Myanmar itself. But the company does contract with local agencies for tasks unrelated to content monitoring. One is Echo Myanmar, a communications firm whose managing director is Anthony Larmon, an American.

Larmon has expressed strong opinions on the Rohingya. Toward the end of 2016, the Myanmar army launched an onslaught across some 10 villages after Rohingya militants attacked border posts. At the time, a U.N. official accused the government of seeking "ethnic cleansing" of the Rohingya.

In November 2016, Larmon wrote that an article about the U.N. allegation was "misleading." He cited what he said were claims by multiple "local journalists" that the ethnic minority "purposely exaggerate (lie about)" their situation to "get more foreign aid and attention."

He also wrote: "No, they aren't facing ethnic cleansing or anything remotely close to what that incendiary term suggests." He said he later removed the post.

A Facebook spokesperson said that Larmon's post "does not represent Facebook's view."

Larmon told Reuters: "It was overly-emotional, under-informed commentary on a highly nuanced subject that I do regret. My view on the Rohingya, same today as then, is that they should be safely repatriated and protected."

The platform on which he aired his views about the Rohingya? Facebook.



FLEEING: Rohingya refugees who fled an army crackdown in western Myanmar last year are seen here after crossing the border into Bangladesh in October. REUTERS/Jorge Silva

## Facebook isn't alone

By [STEVE STECKLOW](#)

Facebook isn't the only social-media platform that contains hate speech against Rohingya Muslims. It also has proliferated on Twitter.

In Myanmar, Twitter is far less popular than Facebook. But after Rohingya insurgents attacked police stations in August 2017, sparking an army crackdown that forced 700,000 people to abandon their homes, hundreds of new Twitter accounts suddenly sprang up in Myanmar.

Many of the tweets on these accounts appeared to be attempts to counter sympathetic portrayals of the Rohingya by the Western news media and human rights activists. They portray the ethnic minority as illegal immigrants from neighboring Bangladesh, or "Bengalis." Members of the ethnic group regard themselves as native to Rakhine State in western Myanmar, but the country has denied most of them citizenship.

Some tweets on these accounts were in broken English:

"There is no Rohingya in Myanmar they are only illegal immigrant and terrorists."

"They are Originally Bangalis, Illegally migrants and Land Robbers"

These and similar tweets could still be found online this month. Twitter's "Hateful conduct policy" forbids attacking groups of people on the basis of race, ethnicity or national origin, or engaging in "behavior that incites fear about a protected group."

Twitter removed a number of tweets flagged to it by Reuters.

Matthew Smith, co-founder of Fortify Rights, a Southeast Asia-based human rights group, said that after the attacks by Rohingya insurgents in August last year he noticed "suspicious" accounts suddenly following him on Twitter.

# Exhibit 75

# New Zealand mosque attack victims confront gunman in courtroom

By Emanuel Stoakes

August 24, 2020



CHRISTCHURCH, New Zealand — The gunman who attacked worshipers at two New Zealand mosques last year, killing 51 people and injuring 49, faced his surviving victims and relatives of the deceased in a courtroom on Monday as harrowing new details of the killing rampage emerged.

A judge this week is determining the sentence for Brenton Tarrant, who pleaded guilty in March to dozens of counts of murder and attempted murder and one count of committing a terrorist act in connection with the March 15, 2019, massacres at the Al Noor Mosque and Linwood Islamic Center in Christchurch. The 29-year-old Australian had posted white-supremacist views online and live-streamed the slaughter on Facebook.

The attacks — the worst acts of violence in New Zealand’s modern history — shocked a nation accustomed to low crime rates and little history of terrorist activity, and spurred Prime Minister Jacinda Ardern to tighten gun laws.

As the hearing began Monday under social distancing restrictions and with police snipers positioned on the court’s roof, prosecutor Barnaby Hawes said Tarrant had studied the mosques’ layouts and exit routes to maximize casualties and had contacted his family about his planned deeds shortly before he began his assault.

Tarrant sat impassively in the dock, his head often bowed, as details of his crimes were read out. He glanced occasionally around the courtroom but showed little reaction as survivors relived the horror.

“The gunman and I looked into each other’s eyes. . . . I was shot nine times,” said Temel Atacocugu, looking at Tarrant as he recounted the carnage at the Al Noor Mosque.

“I laid under bodies in the mosque, thinking I was going to die,” he said. “I tried to lie as still as possible when the gunman came back a second time. I could feel the blood and brains of the person above me running down my face and neck. I couldn’t move or make a sound, as the gunman would have executed me.”

Gamal Fouda, the mosque’s imam, who was delivering a sermon on the day of the attacks, said he had “lived with the nightmare” of what he witnessed, explaining how he had tried to be strong for his community despite his trauma.

“We are a peaceful and loving community who did not deserve your actions,” he told Tarrant. “If you have done anything, you have brought the world community closer with your evil actions.”

Tarrant carried six weapons with him for the assault, including rifles and semiautomatic shotguns. The youngest victim of Tarrant’s rampage was 3 years old.

...and investigators that he wished he had killed more people and that he intended to use incendiary devices found in his car to burn down the mosques following the massacre.

Mohammad Atta Ahmad Alayan, who was shot in the head and shoulder, recited the Muslim al-Fatiha prayer in court before weeping as he described the “devastating” news of learning, three days after the attacks, that his son Ata had died.

Maysoon Salama, Ata’s mother, asked Tarrant to look up her son’s name, so he would “know the huge loss you caused.”

“I can’t forgive you,” she told the gunman. “You thought you could break us; you failed miserably.”

But Janna Ezat said she had forgiven the man who killed her son, Hussein al-Umari.

“I weep every day for him and for my family’s loss,” she told the court. “I decided to forgive you, Mr. Tarrant, because I don’t have hate, I don’t have revenge. Hussein will never be here [again], so I have only one choice: to forgive you.”

Earlier, Judge Cameron Mander began by noting that many of the victims’ relatives had been unable to attend the hearing at the Christchurch High Court because of coronavirus restrictions, acknowledging that this had contributed to their stress. He also outlined restrictions on reporting for those registered to view proceedings either in person, in overflow courts or remotely through a live stream.

Tarrant, who changed his initial plea to guilty earlier this year, faces a maximum possible sentence of life in prison without parole. The judge is expected to hand down the sentence by Thursday.

Before the hearing, Abdul Aziz Wahabzadah, who fought off Tarrant at the Linwood Islamic Center, said in a telephone interview that it was important for him to be in court on Monday to see the attacker whom he managed to frighten away, saving lives in the process.

“He came and killed all the innocent women and children with a gun, but when his turn came [for a beating], he ran away like a coward,” Wahabzadah said.

He said he wanted to see Tarrant attempt to explain “why his life is more important than the lives of those kids.”



## Today's Headlines

The most important news stories of the day, curated by Post editors and delivered every morning.

[Sign up](#)

Unprecedented times call for unlimited access.

Get one year for \$40



# Exhibit 76

# Facebook says that it removed 1.5 million videos of the New Zealand mass shooting

*1.2 million were 'blocked at upload'*

By Andrew Liptak | @AndrewLiptak | Mar 17, 2019, 9:46am EDT



Illustration by Alex Castro / The Verge



Listen to this article



In the first 24 hours after the deadly mass shooting in New Zealand, Facebook says that it has removed 1.5 million videos that were uploaded of the attack, of which 1.2 million

“at upload.”

The company made the [announcement in a Tweet](#), following up on a prior announcement that it had been alerted by authorities and removed the alleged shooter’s Facebook and Instagram accounts. Facebook spokeswoman Mia Garlick [says that the company is also](#) “removing all edited versions of the video that do not show graphic content.”



We’ve reached out to Facebook for additional comment, and will update this post if we hear back.

The terror attack [appears to have been designed](#) to go viral, with the alleged shooter releasing a manifesto that referenced numerous individuals like YouTuber Felix Kjellberg and Candace Owens, as well as white supremacist conspiracy theories. He also posted a 17-minute video to Facebook, Instagram, Twitter, and YouTube, which prompted the message to go further viral, even as all of those companies have worked to prevent its spread.

The attacks have prompted social media sites to react to such content: Facebook, [Twitter](#), and [YouTube](#) have been working to remove videos. Reddit [banned a subreddit called r/watchpeopledie](#), while [Valve began removing tributes to the alleged shooter that were posted to user profiles](#).

But Facebook's removal of more than a million copies (and edited versions) of the video speaks to the enormous challenge that it has in moderating the site. In its drive for rapid growth, its efforts to scale up its ability to monitor and remove content that's offensive, illegal, or disturbing have been left wanting, and allow for suspects to use the platform to spread their message quickly. There have been [other high-profile examples](#) of where murders or terror attacks were streamed on the platform. Indeed, as Facebook has worked to address the problem, it has used third-party contractors, [some of whom have been radicalized and traumatized](#) by the very act of taking down such content.

Following the attack, numerous world leaders have called out Facebook for its role in disseminating this type of content. [According to Reuters](#), New Zealand Prime Minister Jacinda Ardern indicated that she wants to speak with the company about live streaming, while [British Labor leader Jeremy Corbyn said](#) that such platforms must act, and raised the question about regulation.

***Updated March 17th, 2019 11:17AM ET:*** *Updated to clarify that Facebook has removed 1.5 million videos total, with 1.2 million blocked at upload.*

# Exhibit 77



# complicit

the human cost of facebook's  
disregard for muslim life

MUSLIM  
ADVOCATES

GPAHE  
Global Project Against Hate and Extremism

Published October 21, 2020

A joint publication of Muslim Advocates and the Global Project Against Hate and Extremism (GPAHE).

**Muslim Advocates** is a national civil rights organization working in the courts, in the halls of power and in communities to halt bigotry in its tracks. We ensure that American Muslims have a seat at the table with expert representation so that all Americans may live free from hate and discrimination. More information on Muslim Advocates is available at [www.muslimadvocates.org](http://www.muslimadvocates.org).

**The Global Project Against Hate and Extremism (GPAHE)** uses research, advocacy, and education to counter the rising tide of extremism across borders by: documenting and exposing how extremist and hateful movements use social media and the internet to organize, propagandize, and recruit followers and sympathizers; educating anti-hate actors, policymakers, and the public about extremist movements, their leadership, and their activities; and examining how extremist movements influence each other across borders, specifically analyzing the impact of American extremists on other countries. More information on GPAHE is available at [www.globalextremism.org](http://www.globalextremism.org).

© All rights reserved.

# table of contents

<b>1</b>	<b>Executive Summary</b>
<b>5</b>	<b>Recommendations</b>
<b>6</b>	<b>Introduction</b>
<b>13</b>	<b>Country Summaries</b>
<b>14</b>	China
<b>16</b>	Germany
<b>18</b>	Hungary
<b>19</b>	India
<b>25</b>	Myanmar
<b>29</b>	New Zealand
<b>31</b>	Sri Lanka
<b>33</b>	Sweden
<b>34</b>	United States
<b>38</b>	<b>Conclusion</b>
<b>39</b>	<b>Appendix</b>

# Executive Summary

In 2015, Facebook CEO Mark Zuckerberg vowed to make his social media platform a welcoming home for Muslims after members of the community faced a brutal backlash in the wake of horrific, violent attacks in Paris. One 17-year-old in France [reported](#), “There was a flood of violent language on Facebook to kill Muslims.”<sup>1</sup> Zuckerberg posted on [Facebook](#), “After the Paris attacks and hate this week, I can only imagine the fear Muslims feel that they will be persecuted for the actions of others. As the leader of Facebook... we will fight to protect your rights and create a peaceful and safe environment for you.”<sup>2</sup> Citing the lessons of his Jewish background, Zuckerberg wrote that he wanted to add his voice in support of Muslims “in our community and around the world.”

It’s hard now to imagine more hollow words being spoken. Since Zuckerberg made that commitment, Facebook has been used to [orchestrate](#) the Rohingya genocide in Myanmar,<sup>3</sup> mass [murders](#) of Muslims in India,<sup>4</sup> and riots and [murders](#) in Sri Lanka that targeted Muslims for death.<sup>5</sup> Anti-Muslim hate groups and hate speech run [rampant](#) on Facebook with anti-Muslim posts, ads, private groups, and other content.<sup>6</sup> Armed, anti-Muslim protests in the U.S. have been [coordinated](#) from Facebook event pages.<sup>7</sup> The Christchurch, New Zealand, mosque massacres were [live-streamed](#) on the site and the videos [shared](#) by untold numbers worldwide.<sup>8</sup>

1 Adam Nossiter and Liz Alderman, “After Paris Attacks, a Darker Mood Toward Islam Emerges in France,” *The New York Times*, Nov. 16, 2015.

2 Mark Zuckerberg, “I want to add my voice in support of Muslims in our community and around the world,” Facebook, Dec. 9, 2015.

3 Paul Mozur, “A Genocide Incited on Facebook, With Posts from Myanmar’s Military,” *The New York Times*, Oct. 15, 2018.

4 Naveed Siddiqui, “3 killed, 100 others arrested in India after violence erupts over anti-Islam Facebook post,” *Dawn*, Aug. 13, 2020.

5 Tasmin Nazeer, “Facebook’s Apology for its Role in Sri Lanka’s Anti-Muslim Riots Should Spark Change,” *The Diplomat*, May 15, 2020.

6 Mehdi Hasan, “Dear Mark Zuckerberg: Facebook Is an Engine of Anti-Muslim Hate the World Over. Don’t You Care?” *The Intercept*, Dec. 7, 2019.

7 Claire Allbright, “A Russian Facebook page organized a protest in Texas. A different Russian page launched the counterprotest,” *The Texas Tribune*, Nov. 1, 2017.

8 Emanuel Stoakes, “New Zealand mosque attack victims confront gunman in courtroom,” *The Washington Post*, Aug. 24, 2020; Andrew Liptak, “Facebook Says It Removed 1.5 million Videos of the New Zealand Mass Shooting,” *The Verge*, March 17, 2019.



I can only imagine the fear Muslims feel that they will be persecuted for the actions of others. As the leader of Facebook... we will fight to protect your rights and create a peaceful and safe environment for you.

**Mark Zuckerberg**  
Facebook CEO



Facebook CEO Mark Zuckerberg is in charge of a platform that has become the global engine of anti-Muslim bigotry.  
Photo: Alessio Jacona



Hate groups like Secure America Now use Facebook to demonize Muslims as invaders who are undermining democratic values, institutions, even monuments. Facebook Video

This report details Facebook’s damaging impact on Muslim communities in nine countries and demonstrates how Facebook has willfully ignored the dangers posed by anti-Muslim content to the welfare of Muslims across the globe. Facebook’s own civil rights [audit](#), completed in 2020<sup>9</sup> after a nearly two-year process that came only after sustained pressure from [human rights groups](#), singled out anti-Muslim hate on the platform as a longstanding problem.<sup>10</sup> The auditors wrote, “the organization of events designed to intimidate members of the Muslim community at gathering places, to the prevalence of content demonizing Islam and Muslims, and the use of Facebook Live during the Christchurch massacre,” created an atmosphere where “Muslims feel under siege on Facebook.”

Despite this damning finding, Facebook has yet to address the anti-Muslim problems found by its own audit or those identified by advocates around the world in the preceding years. The company’s actions, or lack thereof, indicate that its decision to engage in the audit was not necessarily out of concern for lives lost because of its inaction, but rather for political expediency. Incredibly, the same day that the civil rights audit was announced in May 2018, the company also announced that one of the United States Senate’s most notorious anti-Muslim and anti-immigrant members, former Senator Jon Kyl, would conduct his own audit into anti-conservative bias on the platform. Kyl has a history of [demonizing](#) Muslims and [working](#) with anti-Muslim hate groups.<sup>11</sup> This is illustrative of Facebook’s penchant to fail to simply do what’s right and what they’ve promised; instead, the company falsely equated the protection of their users’ safety, civil rights, and human rights with satisfying partisan political interests. Investigating human and civil rights abuses and global anti-Muslim hate content that leads to the loss of life should not have been presented as needing to be balanced with an investigation of alleged anti-conservative bias.

The company falsely equated the protection of their users' safety, civil rights, and human rights with **satisfying partisan political interests.**

<sup>9</sup> Facebook, *Facebook Civil Rights Audit—Final Report*, July 8, 2020.

<sup>10</sup> Muslim Advocates, “Civil Rights Groups Urge Facebook to Address Longstanding Issues with Hate Speech and Bigotry,” Press Release, Oct. 31, 2017.

<sup>11</sup> Bridge Initiative Team, Georgetown University, “Factsheet: Jon Kyl,” Sept 27, 2018; Brett Barrouquere, “To Replace John McCain Arizona Governor Picks Politician with a History of Anti-Muslim Rhetoric, Jon Kyl,” Southern Poverty Law Center’s Hatewatch, Sept. 4, 2018.

For years, civil rights organizations and policymakers have raised concerns both privately and publicly, begging the company to take action. It has not. Out of desperation to be heard, many organized [boycotts](#),<sup>12</sup> [called](#) for the board and company leadership to be replaced,<sup>13</sup> and [asked](#) governments to step in.<sup>14</sup> Still, Facebook's strategy was to wait and do almost nothing.

Facebook's actions are not dissimilar to [IBM's support](#) of Germany's Nazi Party, where it allowed its technology to be used by Hitler's regime to enact its genocidal policies in exchange for profits.<sup>15</sup> Facebook has done the same in places like India and Myanmar, enabling mass violence by anti-Muslim regimes and individual actors in an attempt to grow or monopolize Internet markets.

Outside of the U.S., where vulnerable communities have fewer options for recourse, the picture is even bleaker. In a most horrifying case, Facebook was [cited](#) by the U.N. for playing a "determining" role in the genocide perpetrated against the Muslim Rohingya community in Myanmar.<sup>16</sup> And in India, the Delhi State Assembly's Peace and Harmony Committee just recently [found](#) that Facebook was complicit in the Delhi riots of February 2020, and should be investigated for every riot since 2014.<sup>17</sup> [Evidence](#) shows that Facebook has at times seemingly collaborated with anti-Muslim regimes, such as the current ruling party in India, to protect hate speech by its leadership in contravention of its own anti-hate policies.<sup>18</sup>

Facebook's leadership has said repeatedly that the company's policies against hate apply to everyone regardless of who they are or where they are, and yet the company [continues](#) to allow anti-Muslim material to stay on the platform,<sup>19</sup> using a variety of [excuses](#)

12 Queenie Wong, "Facebook Ad Boycott: Why Brands 'Hit Pause on Hate,'" *CNET*, July 30, 2020.

13 Muslim Advocates, "32 Civil Rights Groups Lose Faith in Facebook, Call for Significant Reforms to its Board," Press Release, Dec. 17, 2018.

14 Stephanie Bodoni and Natalia Drozdiak, "EU Says It Can Force Facebook to Pull Posts With Hate Speech Anywhere in the World," *Fortune*, Oct. 3, 2019.

15 Edwin Black, *IBM and the Holocaust: The Strategic Alliance between Nazi Germany and America's Most Powerful Corporation* (New York: Crown Books, 2001).

16 Eli Meixler, "U.N. Fact Finders Say Facebook Played a 'Determining' Role in Violence Against the Rohingya," *Time*, March 13, 2018.

17 Aditya Chunduru, "Key Takeaways from Peace & Harmony Committee Meeting," *Medianama*, Sept. 1, 2020.

18 *Al Jazeera*, "Facebook ignored hate speech by India's BJP politicians: Report," *Al Jazeera*, Aug. 15, 2020.

19 Deepa Seetharaman, "Facebook Employees Pushed to Remove Trump's Posts as Hate Speech," *The Wall Street Journal*, Oct. 21, 2016.

For years,  
civil rights  
organizations  
and policymakers  
have raised  
concerns both  
privately and  
publicly, **begging  
the company to  
take action.**  
**It has not.**



Fatema, 35, who is seven months pregnant, fled the genocide against Rohingya Muslims in Myanmar that was fueled by online hate. Photo: Anna Dubuis/DFID

including “newsworthiness.”<sup>20</sup> For example, Facebook has [said](#) that exceptions to its hate speech policy are sometimes made if content is “newsworthy, significant or important to the public interest.”<sup>21</sup>

At the same time, the company [contends](#) that hate speech does not help its bottom line.<sup>22</sup> If so, why has Facebook repeatedly chosen to leave up dangerous hate content, often generated by public figures with large audiences, such as President Donald [Trump](#)?<sup>23</sup> Another case in point is India, where Facebook now has its [largest](#) user base<sup>24</sup> and is [investing](#) in expansion and growth to dominate that very large market.<sup>25</sup> The company is [working](#) closely with the current Indian government,<sup>26</sup> in particular Prime Minister Narendra Modi, who was himself allegedly [involved](#) with stoking anti-Muslim violence when he was governor of the Indian state of Gujarat that led to the deaths of 1,000 Muslims.<sup>27</sup> There appears to be a clear financial incentive to pander to Modi, who has one of the [largest](#) number of followers of any political leader on Facebook,<sup>28</sup> and his political party. It is, of course, hate speech by such figures that is [the most dangerous](#) because of their reach and influence.<sup>29</sup>

Facebook is seeding and cultivating anti-Muslim bigotry amongst its users, leading to real world violence against the 270 million Muslims living in the nine countries covered in this report.<sup>30</sup> Facebook is indisputably the world’s engine for anti-Muslim violence. The time for discussion of this issue is over. Facebook must act now and end anti-Muslim hate on its platform, no matter who or what entity, is proliferating it.

20 David Gilbert, “Facebook is Giving a Free Pass on Hate Speech,” *Vice News*, Sept. 25, 2019.

21 Kate Cox, “Facebook Confirms Its ‘Standards’ Don’t Apply to Politicians,” *Ars Technica*, Sept. 25, 2019.

22 Nick Clegg, “Facebook Does Not Benefit from Hate,” Facebook, July 1, 2020.

23 Ian Bremmer, “Zuckerberg won’t censor Trump’s anti-Muslim ‘hate post’ on Facebook: Report,” *Hindustan Times*, Oct. 22, 2016.

24 Jeff Joseph Paul Kadicheenie, “How India Became Facebook’s Biggest Market,” *The Hoot*, Aug. 16, 2017.

25 Ravi Agrawal, “Why Facebook Is Betting Big on India,” *Foreign Policy*, Apr. 23, 2020.

26 Billy Perrigo, “Facebook’s Ties to India’s Ruling Party Complicate Its Fight Against Hate Speech,” *Time*, Aug. 27, 2020.

27 Sanjoy Majumder, “Narendra Modi ‘allowed’ Gujarat 2002 anti-Muslim riots,” *BBC News*, Apr. 22, 2011.

28 Surabhi Agarwal, “With 41.7 million followers, Modi becomes most followed world leader on Facebook,” *The Economic Times*, May 27, 2017.

29 Dangerous Speech Project, “Dangerous Speech: A Practical Guide,” Aug. 4, 2020.

30 This is a rough estimate based on Facebook penetration in a country and the share of the population in that country that is Muslim. There is no data available on how many Muslim users of Facebook exist in the countries where the company operates, so these numbers are tentative. Population numbers derived primarily from World Bank and UN data.

The company continues to **allow anti-Muslim material** to stay on the platform, using a variety of excuses including “newsworthiness”.



Syrian refugees arrive in Germany amidst growing anti-Muslim and anti-refugee sentiment that is amplified through social media.

Foto: Jazzmany

# Recommendations

## To bring an end to anti-Muslim hate on Facebook, we recommend the company immediately:

- Rigorously, and without regard to political or economic implications, enforce Facebook's community standards and Dangerous Individuals and Organizations designations worldwide to address anti-Muslim hate.
- Ban the use of event pages for the purpose of harassment, organizing, and violence targeting the Muslim community.
- Create a senior staff working group responsible for the reduction of hate speech on the platform, and require regular updates through Facebook's Transparency Report on the company's progress in removing offending content, including anti-Muslim hate content.

# Introduction

Facebook CEO Mark Zuckerberg's 2015 promise to make his platform a welcoming home for Muslims has proven to be an illusion. In country after country, the Facebook platform has been used as a [driver](#) for anti-Muslim violence,<sup>31</sup> the result of the company repeatedly and willfully ignoring the dangers of anti-Muslim content. None of this has happened without Facebook's [knowledge](#)<sup>32</sup> or without public outcry from its users, civil and human rights [groups](#),<sup>33</sup> and [lawmakers](#).<sup>34</sup> Facebook is simply looking the other way while its platform becomes the global engine of anti-Muslim bigotry.

Many people may not be aware that Facebook's actions have led to incredible levels of anti-Muslim violence in multiple countries, and that even when warned that material posted to the platform was likely to end in violence, the company repeatedly chose not to act. Unfortunately, decisions to ignore its own community standards that should protect Muslim communities have been influenced instead by anti-Muslim ruling [governments](#),<sup>35</sup> [militias](#),<sup>36</sup> and political influencers, the very people who can reach and influence the largest audiences.

In 2020, dehumanizing content about Muslims remains widespread on Facebook. A recent [analysis](#) showed that the United States and Australia "lead in the number of active Facebook pages and groups dedicated to referring this dehumanizing [anti-Muslim] content."<sup>37</sup>

31 Mehdi Hasan, "Dear Mark Zuckerberg."

32 Ariana Tobin, "Civil Rights Groups Have Been Warning Facebook About Hate Speech In Secret Groups For Years," *ProPublica*, July 2, 2019.

33 Rishi Iyengar and Donnie O'Sullivan, "Civil rights groups invited to Zuckerberg's home slam Facebook's 'lackluster response,'" *CNN*, Dec. 4, 2019.

34 Taylor Hatmaker, "With Advertiser Boycott Growing, Lawmakers Press Facebook on White Supremacy," *Techcrunch*, June 30, 2020.

35 Hannah Ellis-Petersen and Shaikh Azizur Rahman, "Facebook Faces Grilling by MPs in India Over Anti-Muslim Hate Speech," *The Guardian*, Sept. 1, 2020.

36 Tyler Sonnemaker, "Facebook 'did nothing' about violent militia and hate groups for 5 years despite being warned at least 10 times, advocacy group says," *Business Insider*, Sept. 18, 2020.

37 Rita Jabri-Markwell, "The online dehumanisation of Muslims made the Christchurch massacre possible," *ABC*, Aug. 31, 2020.



Refugees are forced to leave Hungary amidst growing anti-Muslim hate that proliferates online. Photo: Bence Jardany

This content is significantly driven by the white supremacist hate speech and hate groups that thrive on Facebook and routinely demonize Muslims. In May 2020, the Tech Transparency Project (TTP) [found](#) more than 100 U.S. white supremacist groups were active on Facebook, on their own group pages as well as on auto-generated content.<sup>38</sup> Among the many vulnerable communities attacked by these groups, Muslims were demonized by circulating footage and making comments about the Christchurch mosque shootings. In the wake of TTP’s report, Facebook did [alter](#) some of the auto-generated content and groups, but many remained on the platform.<sup>39</sup>

## Anti-Muslim hate on Facebook is well-documented

The problem with anti-Muslim hate on Facebook has been documented for some years. Two years ago, computer scientist Megan Squire did an [analysis](#) of right-wing extremist groups on Facebook and found an incredible overlap with anti-Muslim hate.<sup>40</sup> Squire found that anti-Muslim attitudes are not only flourishing on the platform but also acting as a “common denominator” for a range of other extremist ideologies, including anti-immigrant groups, pro-Confederate groups, militant anti-government conspiracy theorists, and white nationalists. Among thousands of Facebook users who were members of multiple extremist Facebook groups, Squire found that 61 percent of “multi-issue” users who were in anti-immigrant groups had also joined anti-Muslim groups; the same was true for 44 percent of anti-government groups, 37 percent of white nationalist groups, and 35 percent of neo-Confederate groups. “Anti-Muslim groups are way worse, in every way, than what I would have guessed coming in,” Squire [said](#) at the time, “Some of the anti-Muslim groups are central players in the hate network as a whole. And the anti-Muslim groups show more membership crossover with other ideologies than I expected.”<sup>41</sup>



Protestors take to the street after President Trump implements the Muslim ban. Facebook refused to remove his posts about the ban even though they violated the company policies.  
Photo: Stephen Melkisetian

38 Tech Transparency Project, “White Supremacist Groups Are Thriving on Facebook,” May 21, 2020.

39 Tech Transparency Project, “White Supremacist Groups.”

40 Ishmael N. Daro, “Here’s How Anti-Muslim Groups On Facebook Overlap With A Range Of Far-Right Extremism,” *BuzzFeed*, Aug. 4, 2018.

41 Ishmael N. Daro, “Here’s How.”

Civil rights organizations have repeatedly [warned](#) Facebook that anti-Muslim posts, ads, private groups, and other content are rampant on a global scale.<sup>42</sup> As early as 2015, Muslim Advocates [informed](#) Facebook that its event pages were being used to organize activities by anti-Muslim militias and hate groups, including armed anti-Muslim protests in the U.S.<sup>43</sup> The Southern Poverty Law Center also reached out to Facebook privately starting in 2014 to warn the company about hate groups on its platform, including dozens of anti-Muslim hate groups.<sup>44</sup>

## Civil rights audit

In perhaps the only significant step made by Facebook at the behest of civil rights organizations, in 2018 the company [agreed](#) to an independent civil rights audit, which was finalized in July 2020.<sup>45</sup> Though primarily focused on domestic civil rights issues, Facebook’s auditors singled out anti-Muslim hate on the platform as a longstanding problem. They [wrote](#), “the organization of events designed to intimidate members of the Muslim community at gathering places, to the prevalence of content demonizing Islam and Muslims, and the use of Facebook Live during the Christchurch massacre” created an atmosphere where “Muslims feel under siege on Facebook.”<sup>46</sup> Facebook has yet to address any of the longstanding anti-Muslim problems on its platform which have been raised for years by civil and human rights groups and confirmed and validated by their own audit. The company’s actions indicate that its decision to engage in the audit at all was not out of concern for lives lost because of its inaction, but for political expediency.



The organization of events designed to intimidate members of the Muslim community created an atmosphere where **Muslims feel under siege on Facebook.**

**Facebook’s Civil Rights Audit**  
*Final Report*

<sup>42</sup> Jason Schwartz, “Civil rights groups slam Facebook,” *Politico*, Oct. 31, 2017.

<sup>43</sup> Tyler Sonnemaker, “Facebook ‘did nothing.’”

<sup>44</sup> Information from Heidi Beirich, who was director of the Southern Poverty Law Center’s Intelligence Project from 2010-2019 and engaged in several discussions with Facebook staff over hate groups on the platform.

<sup>45</sup> John Fingas, “Facebook will conduct civil rights audit following bias allegations,” *Engadget*, May 2, 2018.

<sup>46</sup> Facebook, *Facebook Civil Rights Audit*.



In 2019, an Australian white supremacist massacred 51 Muslims in Christchurch, New Zealand, while streaming it on Facebook Live.

Photo: Guillaume Garin

## The problem is international in scope

Outside of the U.S., the picture is even bleaker. Tragically, there are many other cases where the hatred and poison against Muslims originating on Facebook has turned lethal, leading to riots, deaths, and mass killings. Evidence shows that Facebook has at times seemingly [collaborated](#) with anti-Muslim regimes, such as the current ruling party of India, to protect hate speech by its leadership in contravention of its own anti-hate policies.<sup>47</sup>

Facebook was cited by the U.N. for [playing](#) a “determining” role in the genocide perpetrated against the Muslim Rohingya community in Myanmar that began in 2016.<sup>48</sup> In September 2018, Facebook COO Sheryl Sandberg [admitted](#) in a Senate committee hearing that the company had failed the Rohingya,<sup>49</sup> calling the situation “[devastating](#)”<sup>50</sup> and even admitting that Facebook may have a legal obligation to remove accounts that lead to mass violence. Yet, anti-Muslim material remained rife on the platform. One year later, in March 2019, the Christchurch, New Zealand, mosque massacres were broadcast on Facebook Live and shared countless times worldwide. In September 2020, the Delhi State Assembly’s Peace and Harmony Committee [found](#) that Facebook was complicit in the Delhi riots of February 2020, and should be investigated for every riot since 2014.<sup>51</sup>

47 Billy Perrigo, “Facebook’s Ties.”

48 Eli Meixler, “U.N. Fact Finders.”

49 *BBC Trending*, “The country where Facebook posts whipped up hate,” *BBC*, Sept. 12, 2018.

50 Evelyn Douek, “Facebook’s Role in the Genocide in Myanmar: New Reporting Complicates the Narrative,” *Lawfare*, Oct. 22, 2018.

51 Aditya Chunduru, “Key Takeaways.”

In the wake of recent disclosures that Facebook allowed anti-Muslim hate speech to run rampant in India, its own employees have spoken out about this long-term and repeated failure to deal with anti-Muslim hate content. In an August 2020 open letter addressed to the company's leadership, 11 employees [demanded](#) that the platform denounce "anti-Muslim bigotry" and ensure Facebook's policies are applied equally across the platform.<sup>52</sup> "It is hard not to feel frustrated and saddened by the incidents reported. We know we're not alone in this. Employees across the company are expressing similar sentiment," the letter read. "The Muslim community at Facebook would like to hear from Facebook leadership on our asks."



The pain from the Christchurch massacre reverberated around the world, leading to memorials like this in the United States.

Photo: Charles Edward Miller

## Facebook grows the white supremacist and anti-Muslim movement

By ignoring this issue, Facebook for years allowed the most dangerous white supremacist propaganda to fester and grow, recruiting untold numbers of people into the ranks of a movement that has inspired violence and genocide targeting Muslims, immigrants, and Jews. The Christchurch shooter had been radicalized into [Identitarianism](#),<sup>53</sup> spread on multiple Facebook [accounts](#),<sup>54</sup> and was an adherent of the [racist Great Replacement theory](#) - an international white supremacist conspiracy movement that promotes the idea that white people are slowly experiencing a genocide in their own home countries due to a plot by elites to displace white people with rising numbers of non-white immigrants.<sup>55</sup> The Great Replacement theory argues that immigrants, especially Muslims, are destroying Western countries and turning them into foreign places. These thinkers often argue disparagingly that Europe is becoming [Eurabia](#).<sup>56</sup>

52 Regina Mihindukulasuriya, "Denounce 'anti-Muslim bigotry' — Facebook staff in US, other countries write to company," *The Print*, Aug. 20, 2020.

53 Hope Not Hate, "What is Identitarianism?" Undated.

54 Mark Townsend, "Infiltrator exposes Generation Identity UK's march towards extreme far right," *The Guardian*, Aug. 24, 2019.

55 Laretta Charlton, "What is the Great Replacement?" *The New York Times*, Aug. 6, 2019.

56 Rita Jabri-Markwell, "The Online Dehumanization."



Extremist groups like the Proud Boys used Facebook to organize rallies and spread anti-Muslim hate. Photo: Robert P. Alvarez

The New Zealand shooter was clear about his motive. In his [manifesto](#), Brenton Tarrant wrote that he wanted to stop the Great Replacement, and he targeted Muslims, including their children, for extermination.<sup>57</sup> As Peter Lentini has [written](#), “Tarrant’s solution to the crisis [posed by a Muslim “invasion”] – indeed one on which he felt compelled to enact – was to annihilate his enemies (read Muslim immigrants). This included targeting non-combatants. In one point, he indicates that [immigrants] constitute a much greater threat to the future of Western societies than terrorists and combatants. Thus, he argues that it is also necessary to kill children to ensure that the enemy line will not continue.”<sup>58</sup>

[Generation Identity](#) (GI), the sprawling, international organization that pushes the Great Replacement idea, was rampant on Facebook for years.<sup>59</sup> In June 2018, Facebook finally took action against GI, but only after several members of the Austrian chapter were investigated for potentially running a criminal organization (the investigation ended without charges). Facebook [deplatformed](#) the entire network citing violations of policy.<sup>60</sup> But this was too little, too late. Before being blocked, [more](#) than 120,000 people followed Generation Identity on Facebook.<sup>61</sup> Facebook is complicit in the worldwide transmission of Identitarian thinking, which is anti-Muslim at its heart.

Since October 2018, there have been at least [six mass attacks](#) motivated by Great Replacement ideology.<sup>62</sup> In addition to Christchurch, attacks were staged at two American synagogues, an El Paso Walmart, a synagogue in Halle, Germany, and two shisha bars in Hanau, Germany. Two of these mass shootings specifically targeted Muslims, in Hanau and Christchurch, but all were directed against immigrants or Jews who were seen as abetting non-white immigration. Anders Breivik, who in 2012 murdered dozens of children in Norway because he believed they would grow up to become adult supporters of Muslim immigrants to the country, actively promoted his ideas [on Facebook](#) before the attack.<sup>63</sup>

57 Andreas Önnersfors, “‘The Great Replacement’ - Decoding the Christchurch Terrorist Manifesto,” Centre for the Analysis of the Radical Right, March 18, 2019.

58 Rita Jabri-Markwell, “The Online Dehumanization.”

59 Heidi Beirich and Wendy Via, *International White Nationalist Movement Spreading on Twitter and YouTube*, Global Project Against Hate and Extremism, July 2020.

60 *Al Jazeera*, “Facebook pulls the plug on far-right Generation Identity,” *Al Jazeera*, June 22, 2018.

61 Alexander Durie, “At the Heart of Hate: Inside France’s Identitarian Movement,” *Are We Europe*, 2018.

62 Heidi Beirich and Wendy Via, *International White Nationalist*.

63 Camila Ragfors, “Norway attacks: Breivik was my friend on Facebook. I’ve seen what fed his hatred,” *The Guardian*, July 24, 2011.

## Muslim users of the platform

By refusing to take anti-Muslim material on its platform seriously, Facebook is in effect poisoning its Muslim users, and its users in general. The nine countries covered in this report have a total of 566 million Facebook users, which make up about 20 percent of their customers worldwide.<sup>64</sup> Furthermore, the top [three markets](#) for Facebook users are India, the United States, and Indonesia, which is a Muslim-majority country.<sup>65</sup> Muslims in India [are](#) an astonishing 200 million<sup>66</sup> and in Indonesia, the country with the [largest](#) Muslim population in the world, are 225 million.<sup>67</sup> Of Facebook's [top 20 markets](#) by country, six are Muslim-majority countries: Indonesia, Egypt, Bangladesh, Pakistan, Turkey, and Nigeria.<sup>68</sup> Two of Facebook's top 20 markets—India and Myanmar—have been the site of massacres of Muslims orchestrated on Facebook.

Facebook's ongoing refusal to enforce its policies and protect Muslims is occurring as Facebook usage rapidly grows in Muslim-majority markets. In 2019, according to [data](#) compiled by the University of Oregon,<sup>69</sup> more than seven out of 10 citizens in six Muslim-majority countries use Facebook and WhatsApp: Egypt, Jordan, Lebanon, Qatar, Saudi Arabia (KSA), Tunisia, and the United Arab Emirates. And the use of these networks far outpaced the use of other social channels. As one example, Facebook had 187 million active users in the Middle East (comprised of mostly Muslim-majority countries) in 2019. The University of Oregon's data also showed that half of young people say they get their daily news on Facebook instead of newspapers, TV, or even online news portals.

All of these people, Muslim and non-Muslim, are being assaulted by the anti-Muslim, bigoted content that Facebook refuses to address. Facebook must act now and end anti-Muslim hate on the platform, no matter who, or what entity, is proliferating the hate. The only reason to allow dangerous hate content from anyone to stay up, and especially from political figures with reach and influence, is because it's profitable.<sup>70</sup>



A girl wails as the Modi government strips Kashmiri Muslims of their rights and Facebook takes away their ability to use WhatsApp to communicate. Photo: Firdous Qadri

<sup>64</sup> This is a rough estimate based on Facebook penetration in a country and the share of the population in that country that is Muslim. There is no data available on how many Muslim users of Facebook exist in the countries where the company operates.

<sup>65</sup> Statista, "Leading countries based on Facebook audience size as of July 2020."

<sup>66</sup> Kunal Purohit, "The Islamophobic roots of population control efforts in India," *Al Jazeera*, Aug. 9, 2019.

<sup>67</sup> Masrur Jamaluddin, Sandi Sidhu and Helen Regan, "Indonesia has the world's biggest Muslim population. It just banned holiday travel over Ramadan," *CNN*, Apr. 24, 2020.

<sup>68</sup> Statista, "Leading countries."

<sup>69</sup> Damian Radcliffe and Hadil Abuhmaid, *Social Media in the Middle East: 2019 In Review*, The University of Oregon School of Journalism and Communication, Jan. 2020.

<sup>70</sup> Ernesto Verdeja and Bettina Spencer, "The Short Fuse: Autocrats, Hate Speech and Political Violence," *Just Security*, July 22, 2020.

# Country Summaries: Anti-Muslim Organizing and Violence on Facebook

Unfortunately, there is little public awareness regarding Facebook's role as a chief driver of anti-Muslim hate and violence throughout the world. Even more disturbing, the company chose repeatedly over years not to act in the face of overwhelming evidence that material posted to Facebook was likely to end in violence. The following summary describes Facebook's role in the deaths of thousands of Muslims in multiple countries. These examples not only illustrate Facebook's complicity but also demonstrate how profoundly hate content can impact people's lives and cause violence offline.

What's documented here is illustrative of the problem with anti-Muslim hate on the platform, but likely represents just the tip of the iceberg, and is by no means exhaustive, as information about Facebook's role in dozens of countries and/or anti-Muslim incidents remains patchy, or unexamined, or nonexistent. Given the widespread nature of anti-Muslim hate on the platform, it is very likely that millions of Muslims around the world have been impacted negatively, jeopardizing their safety and their freedom, by Facebook's failure to act on anti-Muslim hate speech.

Facebook, and all of us, cannot forget that, every day, Muslims across the world are the targets of bigotry and hate crimes while simply going about their lives. And that anti-Muslim rhetoric and organizing that thrives online inspires and enables this abuse. These country reports are tragic, cautionary tales of how easily everyday hate speech turns into violence and murder. And how easily Facebook's platform can be used to inspire and organize mass violence and genocide.



# China

Facebook does not even operate in China, but the Chinese government still uses the platform to amplify anti-Muslim and specifically anti-Uighur [sentiment](#).<sup>71</sup> More than a million Muslim Uighurs have been [imprisoned and brutalized](#) by the Chinese government in concentration camps across the Xinjiang province.<sup>72</sup> The Uighurs and other Muslim ethnic minorities have been separated from their families, forced to labor for their captors, [beaten, tortured, and raped](#).<sup>73</sup>

In 2019, there were [reports](#) that “Chinese state-owned media is running ads on Facebook seemingly designed to cast doubt on human rights violations” against the Uighurs.<sup>74</sup> There were three ads — two active and one inactive — within Facebook’s ad library describing alleged successes of happy detainees in the camps and falsely claiming that the detention centers do not interfere with religious beliefs and practices. Two of the ads were targeted to American and other countries’ audiences. The paid ads [aimed](#) to convince Westerners that the camps in Xinjiang are not sites of human rights abuses, contrary to the findings of several governments, human rights organizations, experts on China, the U.N., and other international bodies.<sup>75</sup>



More than a million Muslim Uighurs have been detained and brutalized by the Chinese government in concentration camps across the Xinjiang province.  
Photo: Azamat Imanaliev

71 Alexandra Ma, “Mysterious automated calls, vanished relatives, and sinister Facebook comments: How China intimidates Uighurs who don’t even live in the country,” *Business Insider*, Dec. 9, 2019.

72 Jen Kirby, “Concentration camps and forced labor: China’s repression of the Uighurs, explained,” *Vox*, Sept. 25, 2020.

73 Ellen Ioanes, “Rape, medical experiments, and forced abortions: One woman describes horrors of Xinjiang concentration camps,” *Business Insider*, Oct. 22, 2019.

74 Ryan Mac, “These New Facebook Ads From Chinese State Media Want You To Believe Xinjiang’s Muslim Internment Camps Are Just Great,” *BuzzFeed*, Aug. 20, 2019.

75 Sigal Samuel, “China paid Facebook and Twitter to help spread anti-Muslim propaganda,” *Vox*, Aug. 22, 2019.



The Guardian published drone footage of what is believed to be showing police leading hundreds of blindfolded and shackled Muslim Uighurs during a transfer of inmates in Xinjiang. Photo: Screenshot from The Guardian

On Facebook, the state-controlled tabloid *Global Times* posted a sponsored [video](#) titled, “Xinjiang center trainees graduate with hope for future.”<sup>76</sup> It purports to show former detainees baking bread, as an example of the “vocational skills” Uighurs supposedly learn in the camps. Additional ads were posted to Twitter.

After the ads were reported to Twitter, the company [removed](#) them immediately.<sup>77</sup> Given the same information, Facebook, in stark contrast, decided to keep accepting such ads and [said](#) they would take a “close look at ads that have been raised to us to determine if they violate our policies.”<sup>78</sup> Instead of simply refusing paid ads from Chinese state-controlled media, Facebook chose to passively rely on outside experts to flag problematic posts, which it may or may not then remove, at a pace that may or may not be quick enough to avert harm. In effect, Facebook was enabling China to use the platform to cover up widespread human rights abuses and violence in Xinjiang.

Facebook was enabling China to use the platform to **cover up widespread human rights abuses and violence** in Xinjiang.

<sup>76</sup> Ryan Mac, “These New Facebook Ads.”

<sup>77</sup> Ryan Gallagher, “Twitter Helped Chinese Government Promote Disinformation on Repression of Uighurs,” *The Intercept*, Aug. 19, 2019.

<sup>78</sup> Sigal Samuel, “China paid.”

# Germany

[Sparked](#) by online rumors that a man was killed defending a woman from rape by a Muslim refugee, riots targeting Muslim refugees and immigrants broke out in August of 2018, starting in the state of Saxony.<sup>79</sup> The Facebook [account](#) of the municipal political party,<sup>80</sup> [Pro-Chemnitz](#),<sup>81</sup> pushed the misinformation and organized the protest that ended in mob violence. In calling for the protest, it [claimed](#) the victim in the rumored stabbing was “a brave helper who lost his life trying to protect a woman.”<sup>82</sup>

Chancellor Angela Merkel [suggested](#) the violence was a threat to Germany’s post-war constitution, saying, “We have video footage of the fact that there was [hunting people down], there were riots, there was hatred on the streets, and that has nothing to do with our constitutional state.”<sup>83</sup>



A woman holds a sign that says “Islam does not belong in Germany.” Photo: Foto Berlin

<sup>79</sup> *Deutsche Welle*, “German state official: Fake news fueled Chemnitz riots,” *Deutsche Welle*, Aug. 29, 2018.

<sup>80</sup> *Deutsche Welle*, “German state official.”

<sup>81</sup> Katy Dartford and Ayman Oghanna, “Chemnitz: How the East German city became known as a hotbed for extremism,” *Euronews*, March 23, 2020.

<sup>82</sup> J. Lester Feder and Pascal Anselmi, “The Real Story Behind The Anti-Immigrant Riots Rocking Germany” *BuzzFeed*, Aug. 31, 2018.

<sup>83</sup> *Der Spiegel*, “Es darf auf keinem Platz und keiner Straße zu solchen Ausschreitungen kommen,” *Der Spiegel*, Aug. 28, 2018.

In another incident, a teenaged Syrian refugee, Anas Modamani, [took](#) a selfie with Chancellor Angela Merkel that he posted on Facebook.<sup>84</sup> After terrorist attacks in Brussels and Berlin in 2016, Modamani's selfie began [appearing](#) on Facebook, this time doctored to falsely label him as one of the perpetrators of the attacks.<sup>85</sup> Afraid of being recognized, Modamani was afraid to leave his home. Chan-jo Jun, a lawyer, [brought a landmark lawsuit against Facebook](#) on behalf of Modamani for being smeared online.<sup>86</sup> His litigation was unsuccessful, but it [helped lead](#)<sup>87</sup> Germany to pass one of the world's most aggressive [laws](#) targeting online hate speech,<sup>88</sup> the so-called [NetzDG law](#).<sup>89</sup>

But the damage was already done. The rumors helped support the growth of the [anti-Muslim Alternative for Germany party](#), which would eventually be elected to seats in several German state parliaments.<sup>90</sup> The AfD now has over 500,000 followers on [Facebook](#).<sup>91</sup> [Research](#) in 2018 by academics at the University of Warwick specifically showed that thousands of hate-filled Facebook posts were linked to an increase in racially-motivated attacks on refugees in Germany, who are predominantly Muslim.<sup>92</sup> The research specifically cited material from the AfD as fueling this awful trend. Now, anti-Muslim and anti-refugee sentiment is widespread among sectors of the German population. In 2019, there were more than [800 attacks](#) on Muslims in Germany.<sup>93</sup>

Anti-Muslim and anti-refugee sentiment is widespread among sectors of the German population. In 2019, there were **more than 800 attacks on Muslims in Germany.**

84 Melissa Eddy, "How a Refugee's Selfie with Merkel Led to a Facebook Lawsuit," *The New York Times*, Feb. 6, 2017.

85 BBC, "Syrian migrant launches Facebook 'fake news' legal fight," *BBC*, Jan. 12, 2017.

86 Linda Kinstler, "Can Germany Fix Facebook?" *The Atlantic*, Nov. 2, 2017.

87 Patrick Evans, "Will Germany's new law kill free speech online?" *BBC*, Sept. 18, 2017.

88 *Deutsche Welle*, "Germany implements new internet hate speech crackdown," *Deutsche Welle*, Jan. 1, 2016.

89 Geoffrey Smith, "Germany's New Law Is a Milestone for Social Media Regulation in Europe," *Fortune*, June 30, 2017.

90 Rafaela Dancygier, "The anti-Muslim AfD just scored big in Germany's election. What does this mean for German Muslims?" *The Washington Post*, Sept. 25, 2017.

91 AfD Facebook page.

92 Samuel Stolton, "German Facebook use linked to refugee violence as AfD boost online presence," *Euractiv*, Aug. 23, 2018.

93 *Deutsche Welle*, "Over 800 attacks on Muslims reported in Germany in 2019," *Deutsche Welle*, March 28, 2020.

# Hungary

Hungary has one of the most anti-Muslim governments in Europe. During the European refugee crisis, which began in 2015, Prime Minister Orbán and his government refused to allow refugees fleeing the Middle East into his country and specifically said in 2018 that the term “refugees” is a misnomer and that those coming to Europe [were](#) “Muslim invaders.”<sup>94</sup> For Prime Minister Viktor Orbán, Muslims cannot be a [part of Europe](#)<sup>95</sup> and Muslims should be kept out of Europe to “[keep Europe Christian.](#)”<sup>96</sup> Orbán’s Facebook [page](#),<sup>97</sup> where he pushes his views, has more than a million followers.

There is little information on Facebook usage to spread hate in Hungary, but one incident is instructive. In March 2018, Facebook [reversed](#) a decision to remove an anti-immigrant video targeting Muslims posted by János Lázár,<sup>98</sup> then chief of staff to Hungarian Prime Minister Viktor Orbán (Lazar was [called](#) a racist by the U.N. human rights chief in 2018<sup>99</sup>). The video featured Lazar saying, “If we let them in and they are going to live in our towns, the result will be crime, poverty, dirt, and impossible conditions in our cities.” Lazar accused Facebook of censorship after the social network removed his post. Facebook, in reposting the racist video, said that it was making an exception to its ban on hate speech: “Exceptions are sometimes made if content is newsworthy, significant or important to the public interest,” Facebook said.

The anti-refugee and anti-Muslim sentiment is so severe in Hungary that even those who work at organizations devoted to helping these populations have been [giving](#) up.<sup>100</sup> Hungary’s Muslim population has [faced](#) beatings, vigilante attacks, and abuse.<sup>101</sup>

“

If we let them in and they are going to live in our towns, the result will be crime, poverty, dirt, and impossible conditions in our cities.

**János Lázár**

*Former chief of staff to Hungarian Prime Minister Viktor Orbán*

94 Emily Schultheis, “Viktor Orbán: Hungary doesn’t want ‘Muslim invaders,’” *Politico*, Jan. 8, 2018.

95 HVG, “Orbán: ‘Az iszlám soha nem volt Európa része,’” HVG, Oct. 16, 2015.

96 Robert Mackey, “Hungarian Leader Rebuked for Saying Muslim Migrants Must Be Blocked ‘to Keep Europe Christian,’” *The New York Times*, Sept. 3, 2015.

97 Viktor Orbán Facebook page.

98 *Reuters* Staff, “UPDATE 1-Facebook removes, then restores anti-immigrant video in Hungary,” *Reuters*, March 7, 2018.

99 *VOA News*, “Facebook Removes, Then Restores Anti-Immigrant Video in Hungary,” *VOA News*, March 7, 2018.

100 Joe Wallen, “‘Hungary is the worst’: Refugees become punch bag under PM Viktor Orbán,” *The Independent*, July 18, 2018.

101 Paul Peachy, “Hungary’s Muslims fear fallout from anti-Islam rhetoric,” *The National*, March 10, 2018.

# India

The situation is so dire regarding the anti-Muslim bias of Facebook India that the company's senior executives were summoned before a parliamentary committee for a closed door [hearing](#) on September 2, 2020. The committee hearing followed allegations that the company's top policy official in India, [Ankhi Das](#),<sup>102</sup> had [prevented the removal of hate speech](#) and anti-Muslim posts by ruling party Bharatiya Janata (BJP) politicians<sup>103</sup> in order to protect and promote the Hindu nationalist party and its Prime Minister Narendra Modi, who have [advanced](#) anti-Muslim policies.<sup>104</sup>

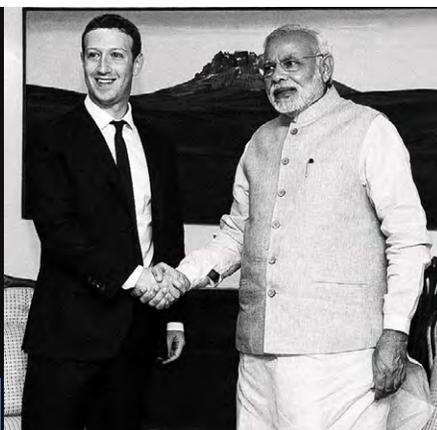
Ties between the company and the BJP are deep. Both [Zuckerberg](#)<sup>105</sup> and [Sandberg](#)<sup>106</sup> have met personally with Modi, who is the most [popular](#) world leader on Facebook.<sup>107</sup> Before becoming prime minister, Zuckerberg even introduced his [parents](#) to Modi,<sup>108</sup> a strange choice considering Modi's horrific track record of stoking violence against Muslims. In February 2002, while head of the Gujarat government, Modi allegedly [encouraged](#) massive anti-Muslim riots.<sup>109</sup> As the state was overcome with violence and over a thousand Muslims were murdered, leaders of the BJP and its even more nationalist ally, the Vishwa Hindu Parishad, [gave speeches](#) provoking Hindus to teach Muslims a lesson.<sup>110</sup> Modi himself gave an incendiary speech, mocking riot victims and calling relief camps for Muslims "[child-producing factories](#)."<sup>111</sup> The intensity and brutality of the violence unleashed against Muslims in 2002 led the [Supreme Court of India](#) to describe the Modi government in Gujarat as, "Modern day Neros who looked the other way while young women and children were burnt alive."<sup>112</sup>

“Modern day Neros who looked the other way while young women and children were burnt alive.

**Supreme Court of India**

*About Modi government in Gujarat*

Indian Prime Minister Narendra Modi meets with Mark Zuckerberg.



102 Sanskriti Tiwari, "Who is Ankhi Das and What's the Controversy Surrounding Her?" *SheThePeople.tv*, Aug. 31, 2020.

103 Newley Purnell and Rajesh Roy, "Facebook Faces Hate-Speech Questioning by Indian Lawmakers After Journal Article," *The Wall Street Journal*, Aug. 18, 2020.

104 Samanth Subramanian, "How Hindu Supremacists are Tearing India Apart," *The Guardian*, Feb. 2, 2020.

105 Mehdi Hasan, "Dear Mark Zuckerberg."

106 New Delhi Bureau, "Facebook COO Sheryl Sandberg meets PM Modi," *The Hindu Business Line*, July 3, 2014.

107 Saumya Tewari, "Narendra Modi the most popular world leader on Facebook: Study," *Live Mint*, April 23, 2020.

108 Mehdi Hasan, "Dear Mark Zuckerberg."

109 Sanjoy Majumder, "Narendra Modi 'allowed' Gujarat 2002 anti-Muslim riots," *BBC*, April 22, 2011.

110 Rana Ayyub, "Narendra Modi Looks the Other Way as New Delhi Burns," *Time*, Feb. 28, 2020.

111 Narendra Modi, "Should We Run Relief Camps? Open Child Producing Centres?," *Outlook Magazine*, Sept. 30, 2002.

112 Rana Ayyub, "Narendra Modi Looks."



Prime Minister Modi is celebrated by a Hindu nationalist party which promotes anti-Muslim hate online.

The problems go right to the top in Facebook’s India operations. Das is herself [implicated](#) in spreading anti-Muslim bigotry.<sup>113</sup> She shared a [post](#) on her own Facebook page which referred to Muslims as a “degenerate community” for whom “nothing except purity of religion and implementation of Shariah matter,” which Das said “spoke to me... as it should to [the] rest of India”<sup>114</sup> (After press reports that led to mass outrage, Das weakly [apologized](#) referencing her commitment to feminism, using an anti-Muslim trope regarding Muslims and sexism.<sup>115</sup>) The controversy was spotlighted in an August [report](#) that said Facebook India employees repeatedly attempted to remove content and label BJP leaders as dangerous individuals, and Das overruled their recommendations in order to protect her personal political interests.<sup>116</sup> One such [post](#) that Das overruled was by Anantkumar Hegde, a BJP member of parliament, who alleged that Muslims were spreading coronavirus in the country as part of an anti-Muslim conspiracy called “Corona Jihad.”<sup>117</sup>

Das’ abuse of her authority in support of her political allies has led to the loss of lives. In February 2020, former BJP lawmaker Kapil Mishra gave a speech threatening activists protesting the BJP’s anti-Muslim citizenship law in Delhi, the country’s capital, which [makes](#) citizenship difficult for Muslims.<sup>118</sup> This was a post [flagged](#) to Das but allowed to stay up.<sup>119</sup> Mishra [said](#) his supporters would use force to stop the protests.<sup>120</sup> Hours after the video was posted on Facebook, [rioting](#) broke out in the city that led to dozens of deaths,<sup>121</sup> most of them Muslims. Some of this violence was [arranged](#) on Facebook’s subsidiary, WhatsApp, which has repeatedly been the source of mob violence targeting Muslims in India.<sup>122</sup>

113 *Al Jazeera*, “Facebook executive who shared anti-Muslim post apologises: Report,” *Al Jazeera*, Aug. 27, 2020.

114 *Al Jazeera*, “Facebook executive.”

115 Pranav Dixit, “A Facebook Executive Who Shared An Anti-Muslim Post Has Apologized To Employees,” *BuzzFeed*, Aug. 24, 2020.

116 Jeff Horwitz and Newley Purnell, “Facebook Executive Supported India’s Modi, Disparaged Opposition in Internal Messages,” *The Wall Street Journal*, Aug. 30, 2020.

117 *Al Jazeera*, “Facebook ignored hate speech by India’s BJP politicians: Report,” *Al Jazeera*, Aug. 15, 2020.

118 Soumya Shankar, “India’s Citizenship Law, In Tandem with National Registry, Could Make BJP’s Discriminatory Targeting of Muslims Easier,” *The Intercept*, Jan. 30, 2020.

119 *Al Jazeera*, “Facebook Ignored.”

120 Newley Purnell and Jeff Horwitz, “Facebook’s Hate-Speech Rules Collide With Indian Politics,” *The Wall Street Journal*, Aug. 14, 2020.

121 *Al Jazeera*, “Facebook ignored.”

122 OpIndia Staff, “Delhi Riots: WhatsApp chats acquired by OpIndia show how some anti-CAA protestors were aware that violence was planned, discussed ‘de-escalation,’” *OpIndia*, Sept. 25, 2020.

Das' inability to carry out her responsibilities in an objective manner manifests itself in many different situations. When T. Raja Singh, another member of the BJP, [called](#) for the slaughter of Rohingya Muslim refugees, threatened to demolish mosques, and labeled Indian Muslim citizens as traitors, Facebook's online security staff determined his account should be banned for not only violating its community standards, but also for falling under the category of "Dangerous Individuals and Organizations."<sup>123</sup> Das stepped in to protect Singh from punitive action, because "punishing violations by politicians from Mr. Modi's party would damage the company's business prospects in the country," according to [Facebook employees](#).<sup>124</sup> Outrage in response to these disclosures forced Facebook to finally [ban](#) Singh from the platform in early September 2020.<sup>125</sup> Lynchings spurred by bigoted and propagandistic WhatsApp posts led the company to [consider](#) banning mass messaging on the system.<sup>126</sup>

India is Facebook's largest and most lucrative [market](#) with nearly 350 million users and another 400 million on WhatsApp.<sup>127</sup> The BJP, which has more than 16 million followers on its page, is Facebook India's biggest advertising [spender](#) in recent months.<sup>128</sup> Facebook [has](#) multiple commercial ties with the Indian government, including partnerships with the Ministry of Tribal Affairs, the Ministry of Women, and the Board of Education.<sup>129</sup>



Punishing violations by politicians from Mr. Modi's party would damage the company's business prospects in the country.

**Facebook employees**

<sup>123</sup> C.J. Werleman, "How Facebook threatens vulnerable Muslim communities," *Middle East Eye*, Aug. 30, 2020.

<sup>124</sup> Jeff Horwitz and Newley Purnell, "Facebook Staff Demand Policy Changes on India Hate Speech," *The Wall Street Journal*, Aug. 21, 2020.

<sup>125</sup> *The New Arab*, "Facebook bans India ruling party politician over anti-Muslim hate speech," *The New Arab*, Sept. 3, 2020.

<sup>126</sup> Shannon Liao, "WhatsApp tests limiting message forwarding after violent lynchings in India," *The Verge*, July 20, 2018.

<sup>127</sup> Helen Ellis-Pederson, "Facebook Faces Grilling."

<sup>128</sup> *Outlook* Web Bureau, "BJP again tops the political ad spend on Facebook In India," *Outlook*, Aug. 27, 2020.

<sup>129</sup> Helen Ellis-Pederson, "Facebook Faces Grilling."

There are many more connections between anti-Muslim content on Facebook and violence in India. In May 2020, a BJP member of parliament in West Bengal, Arjun Singh, [posted](#) an image on Facebook that he wrongly claimed was a depiction of a Hindu who had been brutalized by Muslim mobs.<sup>130</sup> It was captioned: “How long will the blood of Hindus flow on in Bengal...we will not stay quiet if they [Muslims] attack ordinary people.” Four hours later, an angry mob of about 100 Hindus [descended](#) on a town in West Bengal and a Muslim shrine was vandalized.<sup>131</sup> Facebook failed to remove the posts until after the company experienced backlash as a result of the violent attacks, which local Muslims alleged had been incited by Singh’s post. Overall, dozens of Muslims have been [lynched](#) since 2012 by vigilantes, with many of the incidents triggered by fake news regarding cow slaughter or smuggling shared on WhatsApp.<sup>132</sup>

## New Delhi riots

Facebook appeared to play a pivotal role in the February 2020 New Delhi riots in which more than 50 people died and thousands of homes and several mosques were destroyed. While both Hindus and Muslims were affected in the riots, Muslims were [targeted](#) in far greater numbers by mobs of young men, many of whom had traveled into the city to harass Muslims after seeing fake news shared widely on Facebook that Muslim religious leaders were calling for Hindus to be kicked out of Delhi.<sup>133</sup> One [post](#) by a BJP member who is also a member of the right-wing militant Hindu organization Bajrang Dal, prompted hundreds to comment that they and their Hindu “brothers” would join the fight to defend Delhi from the Muslims.<sup>134</sup> And two days before the anti-Muslim riots began in Delhi, a member of Modi’s cabinet [said](#) Muslims should have been sent out of India to Pakistan in 1947 during the partition of India.<sup>135</sup> Ultimately, the Delhi State Assembly’s Peace and Harmony Committee said it had prima facie [found](#) Facebook guilty of aggravating the Delhi riots, and posited that it should be investigated for every riot since 2014.<sup>136</sup>

During the riots, Facebook was also used by members of the mobs to glorify their violence. In early February, a Bajrang Dal activist [posted](#) a video claiming to have “killed a Mulle [derogatory term for Muslims]” and the next day wrote in a public Facebook post that he had just sent a “jihadi to heaven.”<sup>137</sup> It took about three days for his Facebook account to be deactivated. In the wake of the violence, hundreds of Muslim families [fled](#) New Delhi.<sup>138</sup>

<sup>130</sup> Helen Ellis-Pederson, “Facebook Faces Grilling.”

<sup>131</sup> Helen Ellis-Pederson, “Facebook Faces Grilling.”

<sup>132</sup> *Al Jazeera*, “Indian MPs Grill Facebook Over Hate Speech, Allegations of Bias,” *Al Jazeera*, Sept. 3, 2020.

<sup>133</sup> Human Rights Watch, “Shoot the Traitors” Discrimination Against Muslims under India’s New Citizenship Policy,” Human Rights Watch, April 9, 2020.

<sup>134</sup> Helen Ellis-Pederson, “Facebook Faces Grilling.”

<sup>135</sup> Rana Ayyub, “Narendra Modi Looks.”

<sup>136</sup> Aditya Chunduru, “Key Takeaways.”

<sup>137</sup> Helen Ellis-Pederson, “Facebook Faces Grilling.”

<sup>138</sup> Rana Ayyub, “Narendra Modi Looks.”

## Human rights advocates cry out

Human rights organizations, including the Indian American Muslim Council, South Asians Building Accountability & Healing, and the Coalition to Stop Genocide in India (made up of dozens of organizations in the U.S. and other countries) assert that Facebook simply refuses to remove anti-Muslim hate content in India and have [requested](#) an investigation by the United States Congress.<sup>139</sup> In September of 2020, a [letter](#) signed by 41 civil rights organizations from around the world called on Facebook to put an end to anti-Muslim hate on its platform and immediately suspend Das, among other requests, to protect the safety and security of Muslims.<sup>140</sup>

Facebook's anti-Muslim actions in India have been repeatedly called out by civil society actors. In October 2019, a report by the nonprofit organization Avaaz [accused](#) Facebook<sup>141</sup> of having become a "megaphone for hate" against Muslims in the northeastern Indian state of Assam — where nearly two million people, [many of them Muslims](#),<sup>142</sup> have [been stripped](#) of their citizenship by the BJP government.<sup>143</sup> Another [report](#), by the South Asian human rights group Equality Labs, found "Islamophobic [anti-Muslim] content was the biggest source of hate speech on Facebook in India, accounting for 37 percent of the content," and that 93 percent of the hate speech they reported to Facebook was not removed.<sup>144</sup> They also [reported](#) on how Facebook is being used to spread hate speech and misinformation accusing Muslims of deliberately infecting non-Muslims and Hindus with COVID-19, again contributing to potential violence against Muslims.<sup>145</sup> Meanwhile, as the Modi government was stripping Muslims of their rights, Facebook was [taking](#) WhatsApp accounts away from Muslims in Kashmir.<sup>146</sup>

The government had suspended Internet in the region to prevent communication and Facebook's policy automatically discontinues WhatsApp participation after 120 days. As a result, the government prevented Muslims in the region from organizing, and Facebook contributed by further reducing communication opportunities.

“

Facebook became a “megaphone for hate” against Muslims in the northeastern Indian state of Assam.

**Avaaz report**

<sup>139</sup> *The Milli Gazette*, “Facebook scandal should be probed by US Congress say human rights organizations,” *The Milli Gazette*, Aug. 18, 2020.

<sup>140</sup> Global Project Against Hate and Extremism, et al, “Major Human Rights and Internet Watchdog Organizations Sign On to Demands for #AuditFBIndia,” Sept. 9, 2020.

<sup>141</sup> Roli Srivastava, “Facebook a ‘megaphone for hate’ against Indian minorities,” *Reuters*, Oct. 30, 2019.

<sup>142</sup> Sigal Samuel, “India’s massive, scary new detention camps, explained,” *Vox*, Sept. 17, 2019.

<sup>143</sup> Makana Eyre, “Why India Just Stripped 1.9 Million People of Citizenship,” *The Nation*, Sept. 10, 2019.

<sup>144</sup> Equality Labs, *Facebook India*, 2019.

<sup>145</sup> Equality Labs, *CoronaJihad*, 2020.

<sup>146</sup> Pranav Dixit, “Kashmiris Are Disappearing From WhatsApp,” *BuzzFeed*, Dec. 4, 2019.

In late August, a group of 54 former Indian bureaucrats [wrote](#) to Zuckerberg asking the company to perform an audit of how Facebook’s hate speech policy is applied and to do so without Das’ involvement.<sup>147</sup> The letter pointed to the financial aspects of Facebook’s situation in India causing a conflict of interest. “That this (not censoring hate speech by members of the BJP) seems to have been done to protect Facebook’s commercial interests is even more reprehensible... We note that such behavior on Facebook’s part has become a subject of debate in other countries as well. Commercial interests at the cost of human lives? If these are the crass calculations Facebook indulges in, it is no surprise that the calculus of hate is spreading like a virus in many parts of the world,” the letter read.

“ Commercial interests at the cost of human lives? If these are the crass calculations Facebook indulges in, it is no surprise that the **calculus of hate is spreading like a virus in many parts of the world.**

**Former Indian bureaucrats**

*Letter to Facebook*

Many, however, question the utility of continuing to urge Facebook to address hate on the platform driven by the BJP and other Hindu nationalist organizations in India. Malay Tewari, a Kolkata-based activist, [argued](#) Facebook “rarely” responded to his complaints about BJP-linked posts and “quite strangely, Facebook posts which expose the propaganda or hate campaign of the BJP, which do not violate community standards, are often removed.”<sup>148</sup> Indian journalist Rana Ayyub [agreed](#) saying, “For years now, verified Facebook pages of BJP leaders such as Kapil Mishra have routinely published hate speeches against Muslims and dissenting voices.<sup>149</sup> The hate then translates into deadly violence, such as the February anti-Muslim attacks in Delhi that left many people dead in some of the worst communal violence India’s capital has seen in decades... It’s clear that Facebook has no intention of holding hatemongers accountable and that the safety of users is not a priority.”

In late August, it was [reported](#) that Facebook, in an effort to evaluate its role in spreading hate speech and incitements to violence, had commissioned an independent report by the U.S. law firm Foley Hoag LLP on the platform’s impact on human rights in India.<sup>150</sup> Work on the India audit, previously unknown, began before political bias in Facebook’s India operations was documented by journalists in August and September of 2020. Additionally, the new Facebook Oversight Board has indicated that it may step into the India situation. The board has [said](#) that it has the authority to decide “how Facebook treats posts from public figures that may violate community standards,” including against hate speech and that it “won’t shy away from the tough cases and holding Facebook accountable.”<sup>151</sup> One can only hope that the Oversight Board will honor this commitment.

<sup>147</sup> *Hindustan Times*, “54 ex-bureaucrats write to Facebook CEO, seek audit of hate-speech policy,” *Hindustan Times*, Aug. 25, 2020.

<sup>148</sup> Helen Ellis-Pederson, “Facebook Faces Grilling.”

<sup>149</sup> Rana Ayyub, “For Facebook, weakening India’s democracy is just the cost of business,” *The Washington Post*, Aug. 20, 2020.

<sup>150</sup> Billy Perrigo, “Facebook’s Ties.”

<sup>151</sup> Anumeha Chaturvedi, “Hate speech row: Facebook oversight board will investigate political ‘bias’ cases,” *The Economic Times*, Aug. 20, 2020.

# Myanmar

Beginning in 2012, activists, businessmen, and tech experts in Myanmar began [warning](#) Facebook that members of the military and ultra-nationalist Buddhists were directing hate speech and violence against the Rohingya,<sup>152</sup> long a targeted and [vulnerable Muslim community](#) in that country.<sup>153</sup> In a country of more than [53 million people](#), only four percent are Muslim Rohingya.<sup>154</sup>

By 2013, Facebook was ubiquitous in the country, serving basically as the Internet. The state-run newspaper [said](#) in 2013 that in Myanmar, “a person without a Facebook identity is like a person without a home address” (by 2020, nearly 90 percent of the population uses Facebook).<sup>155</sup>

Aela Callan, a foreign correspondent on a fellowship from Stanford University, [met](#) Facebook’s then vice president of global communications to discuss hate speech and fake user pages that were pervasive in Myanmar in 2013.<sup>156</sup> Callan visited Facebook’s California headquarters again in March 2014 with a staffer from a Myanmar tech organization to raise these issues with the company. Callan [wanted](#) to show Facebook “how serious it [hate speech and disinformation] was.”<sup>157</sup> Her pleas were rebuffed. “It was seen as a connectivity opportunity rather than a big pressing problem,” Callan said. “I think they were more excited about the connectivity opportunity because so many people were using it, rather than the core issues.” Callan said hate speech seemed like a “low priority” at the time.

Vicious, false [rumors](#) that a Muslim Mandalay teashop owner raped a Buddhist employee started spreading across Facebook in 2014.<sup>158</sup> Soon, armed men were marauding through the streets of the capital on motorbikes and by foot wielding machetes and sticks. Rioters torched cars and ransacked shops. During the multi-day melee, two men—one Muslim and one Buddhist—were killed and 20 others were [injured](#).<sup>159</sup> Similar violence would follow, spurred by hate-driven rumors on Facebook.

[For Facebook] hate speech seemed like a “low priority” at the time (2014).

**Aela Callan**  
Foreign correspondent



The Rohingya, a targeted Muslim community in Myanmar, have been violently attacked following hate-driven rumors on Facebook.  
Photo: Evangelos Petratos

<sup>152</sup> Billy Perrigo, “Facebook’s Ties.”

<sup>153</sup> BBC, “Myanmar Rohingya: What you need to know about the crisis,” BBC, Jan. 23, 2020.

<sup>154</sup> Religious Liberty Project, “Myanmar,” Harvard Divinity School, Undated.

<sup>155</sup> Timothy McLaughlin, “How Facebook’s Rise Fueled Chaos and Confusion in Myanmar,” *Wired*, June 7, 2018.

<sup>156</sup> Timothy McLaughlin, “How Facebook’s Rise.”

<sup>157</sup> Timothy McLaughlin, “How Facebook’s Rise.”

<sup>158</sup> Timothy McLaughlin, “How Facebook’s Rise.”

<sup>159</sup> United Nations High Commissioner for Refugees, “2014 Country Reports on Human Rights Practices - Burma,” *RefWorld*, 2015.



Rohingya Muslim refugees flee Myanmar after militants use Facebook to spread propaganda and perpetrate violence against them.

Photo: Sk Hasan Ali

That violence was serious, but the use of Facebook to coordinate the Rohingya genocide was yet to come. Facebook ignored repeated warnings that the military and Buddhist militants were using the platform to spread anti-Rohingya hate and propaganda. By the end of 2017, about 700,000 Rohingya had [fled](#) the country after Myanmar’s military launched operations against what it called “insurgents” in the state of Rakhine.<sup>160</sup> Though the Rohingya have been in Myanmar for generations, the government [denied](#) citizenship to most Rohingya, arguing that they are illegal immigrants from neighboring Bangladesh.<sup>161</sup> A U.N. fact-finding mission in 2018 [reported](#) that, “People died from gunshot wounds, often due to indiscriminate shooting at fleeing villagers. Some were burned alive in their homes - often the elderly, disabled and young children. Others were hacked to death.”<sup>162</sup>

## Facebook does too little, much too late

It took until August 2018 – a year after 25,000 Rohingya were killed and 700,000 fled Myanmar– for Facebook to [ban](#) Tatmadaw (military) leaders from its platform<sup>163</sup> (only to [return](#) in June of 2020).<sup>164</sup> Facing growing public pressure, the company also commissioned and [published](#) an independent Human Rights Impact Assessment on the role its services were playing in the country<sup>165</sup> and committed to [hiring](#) 100 native Burmese speakers as content moderators.<sup>166</sup> Prior to deplatforming Tatmadaw, Facebook [banned](#) four armed ethnic groups in the country, but not the Tatmadaw, presumably because they are state actors.<sup>167</sup> Repeated requests for comment from Facebook on why some ethnic groups were banned while a state actor engaged in ethnic violence was not, [went](#) unanswered.<sup>168</sup>

<sup>160</sup> Council on Foreign Relations, “Rohingya Crisis in Myanmar,” Global Conflict Tracker, Sept. 24, 2020.

<sup>161</sup> Shoon Naing, “Myanmar forces Rohingya to accept cards that preclude citizenship: group,” *Reuters*, Sept. 3, 2019.

<sup>162</sup> United Nations Human Rights Council, “Fact-finding Mission on Myanmar: concrete and overwhelming information points to international crimes,” Office of the High Commissioner for Human Rights, March 12, 2018.

<sup>163</sup> Hannah Ellis-Pederson, “Facebook removes accounts associated with Myanmar military,” *The Guardian*, Aug. 27, 2018.

<sup>164</sup> Swe Lei Mon, “Tatmadaw Returns to Facebook After Two Year Absence,” *Myanmar Times*, June 9, 2020.

<sup>165</sup> Alex Warofka, “An Independent Assessment of the Human Rights Impact of Facebook in Myanmar,” Facebook, Nov. 5, 2018.

<sup>166</sup> Poppy McPherson, “Facebook says it was ‘too slow’ to fight hate speech in Myanmar,” *Reuters*, Aug. 16, 2018.

<sup>167</sup> Julia Carrie Wong, “Overreacting to failure’: Facebook’s new Myanmar strategy baffles local activists,” *The Guardian*, Feb. 7, 2019.

<sup>168</sup> United Nations Human Rights Council, “Fact-finding Mission on Myanmar.”

This, even though the 2018 U.N. [fact-finding report](#) had noted that “actions of the Tatmadaw in both Kachin and Shan States since 2011 amount to war crimes and crimes against humanity.”<sup>169</sup> Facebook has yet to impose across-the-board bans on military-run accounts of the kind applied to the four minority rebel groups. Instead, it seems to be taking a deeply [statist approach](#) toward these groups, thereby helping an army that stands accused of genocide.<sup>170</sup>

A U.N. fact-finding mission was shocked by Facebook’s lack of action and [found](#) the company played a “determining role” in stirring up hatred against Rohingya Muslims in Myanmar.<sup>171</sup> The chairman of the U.N. mission, Marzuki Darusman, [said](#) that social media had “substantively contributed to the level of acrimony amongst the wider public against Rohingya Muslims... Hate speech is certainly, of course, a part of that.”<sup>172</sup> Yanghee Lee, Special Rapporteur for human rights violations in Myanmar [said](#), “I’m afraid that Facebook has now turned into a beast, and not what it originally intended.”<sup>173</sup>

Facebook leadership has admitted its complicity in these events. Zuckerberg [said](#) in 2018 that Facebook needed to improve in Myanmar, though that admission came much too late for critics who said he failed to adequately take responsibility for what had been a long-term issue.<sup>174</sup> The company [announced](#) in July of that year that it would expand its efforts to remove material worldwide that could incite violence.<sup>175</sup> In a [surprising concession before the U.S. Senate Intelligence Committee](#) in September 2018, Sandberg called the events in Myanmar “devastating” and acknowledged the company had to do more, highlighting that Facebook had put increased resources behind being able to review content in Burmese.<sup>176</sup> She also accepted that Facebook had a moral and legal obligation to take down accounts that incentivize violence in countries like Myanmar (even so, two years later, Facebook continues to leave these kinds of accounts up, including in countries like India where violence against Muslims has been serious).

---

<sup>169</sup> United Nations Office of the High Commissioner for Human Rights, “Myanmar: UN Fact-Finding Mission releases its full account of massive violations by military in Rakhine, Kachin and Shan States,” United Nations Human Rights Office, Sept. 18, 2018.

<sup>170</sup> Angshuman Choudhury, “How Facebook Is Complicit in Myanmar’s Attacks on Minorities,” *The Diplomat*, Aug. 25, 2020.

<sup>171</sup> Alex Warofka, “An Independent Assessment.”

<sup>172</sup> *BBC*, “UN: Facebook has turned into a beast in Myanmar,” *BBC*, March 13, 2018.

<sup>173</sup> *BBC*, “UN: Facebook has turned.”

<sup>174</sup> Jen Kirby, “Mark Zuckerberg on Facebook’s role in ethnic cleansing in Myanmar: ‘It’s a real issue,’” *Vox*, April 2, 2018.

<sup>175</sup> Sheera Frankel, “Facebook to Remove Misinformation that Leads to Violence,” *The New York Times*, July 18, 2018.

<sup>176</sup> Evelyn Douek, “Senate Hearing on Social Media and Foreign Influence Operations: Progress, But There’s A Long Way to Go,” *Lawfare*, Sept. 6, 2020.

## Failure to cooperate with the International Criminal Court

Given this catastrophic failure, one would think Facebook leadership would want to do absolutely everything in their power to support the current genocide case against Myanmar in the International Criminal Court (ICC). However, that hasn't been the case. In August 2020, Facebook balked at providing the ICC posts made by Myanmar's military and other leadership in a case of genocide against the regime being pursued by The Gambia and the Organization of Islamic Countries. The head of a U.N. investigative body on Myanmar [said](#) Facebook had not shared evidence of "serious international crimes," despite vowing to work with investigators looking into abuses in the country.<sup>177</sup> Nicholas Koumjian, head of the Independent Investigative Mechanism for Myanmar (IIMM), [stated](#) the social media giant was holding material "highly relevant and probative of serious international crimes" but had not shared any during year-long talks.<sup>178</sup> After an uproar in the press in August 2020, Facebook finally [turned](#) over some documents to the court that "partially complied" with the request.<sup>179</sup> By not cooperating with the Gambian legal team and creating a roadblock in the ongoing trial, Facebook is not [being](#) a "force for good in Myanmar" as it has repeatedly promised. It is failing to aid an important international effort to establish accountability in the country.<sup>180</sup>

In anticipation of the upcoming November Myanmar elections, Facebook released information on the small [changes](#) it has made, committing to remove "verifiable misinformation and unverifiable rumors" that are assessed as having the potential to suppress the vote or damage the "integrity" of the electoral process between September and November 22, 2020.<sup>181</sup> It also introduced a new feature that [limits](#) to five the number of times a message can be forwarded on WhatsApp.<sup>182</sup> Additionally, Facebook [claims](#) to now have three fact-checking partners in Myanmar and is working with two partners to verify the official Facebook pages of political parties, all of which will purportedly help detect hate speech that could lead to violence.<sup>183</sup>

<sup>177</sup> Reuters, "UN investigator says Facebook hasn't shared 'evidence' of Myanmar crimes," *The New York Post*, Aug. 11, 2020.

<sup>178</sup> Poppy McPherson, "U.N. investigator says Facebook has not shared 'evidence' of Myanmar crime," *Reuters*, Aug. 11, 2020.

<sup>179</sup> Aarti Bali, "Facebook shares data on Myanmar with United Nations investigators," *WeForNews*, Aug. 26, 2020.

<sup>180</sup> Matthew Smith, "Facebook Wanted to Be a Force for Good in Myanmar. Now It Is Rejecting a Request to Help With a Genocide Investigation," *Time*, Aug. 18, 2020.

<sup>181</sup> *Al Jazeera*, "Facebook says stepping up efforts to tackle Myanmar hate speech," *Al Jazeera*, Sept. 1, 2020.

<sup>182</sup> Manish Singh, "WhatsApp Introduces New Limit on Message Forwards to Fight Spread of Misinformation," *Techcrunch*, April 7, 2020.

<sup>183</sup> Natasha Lomas, "Facebook Touts Beefed Up Hate Speech Detection Ahead of Myanmar Election," *Techcrunch*, Sept. 1, 2020.

# New Zealand

The last [words](#) of Haji-Daoud Nabi before he and his 50 fellow worshipers were gunned down in Christchurch, New Zealand was the welcoming phrase, “Hello, brother.”<sup>184</sup> On March 15, 2019, in a performance for Facebook Live, Brenton Tarrant slaughtered worshipers at two different mosques in one of the deadliest white supremacist attacks in recent history. The 17-minute long Facebook live-stream broadcast went viral; in the 24 hours following the attack, attempts were made to re-upload the [footage](#) 1.5 million times while Facebook scrambled to stop its spread.<sup>185</sup> The video of the attack was [cross-posted](#) across various social networks, and links to the live-stream and Tarrant’s manifesto were posted on the unregulated message board 8chan.<sup>186</sup>

The New Zealand shooter was clear about his anti-Muslim motive. In his manifesto, Tarrant, who was in touch with members of the anti-Muslim, white supremacist and transnational Generation Identity movement, wrote that he wanted to stop the Great Replacement, and he targeted Muslims, including their children, for extermination. As Peter Lentini has [written](#), “Tarrant’s solution to the crisis [posed by a Muslim “invasion”] – indeed one on which he felt compelled to enact – was to annihilate his enemies (read Muslim immigrants). This included targeting non-combatants. In one point, he indicates that [immigrants] constitute a much greater threat to the future of Western societies than terrorists and combatants. Thus, he argues that it is also necessary to kill children to ensure that the enemy line will not continue.”<sup>187</sup>

## “Hello, brother.”

The words of Haji-Daoud Nabi before he and his 50 fellow worshipers were gunned down in Christchurch, New Zealand in a performance for Facebook Live.



Over 50 Muslims of all ages, including young children, were massacred in Christchurch by a white nationalist who subscribed to the racist Great Replacement theory that has flourished on Facebook. Photo: Felton Davis

<sup>184</sup> Mary Catherine Ford, “For Muslims, the mosque is the center of family life — and now a reminder of brutal massacre,” *Chicago Tribune*, March 19, 2019.

<sup>185</sup> Jon Porter, “Facebook says the Christchurch attack live stream was viewed by fewer than 200 people,” *The Verge*, March 19, 2019.

<sup>186</sup> Craig Timberg, Drew Harwell, Hamza Shaban, Andrew Ba Tran and Brian Fung, “The New Zealand Shooting shows how YouTube and Facebook spread hate and violent images—yet again,” *The Washington Post*, March 15, 2019.”

<sup>187</sup> Rita Jabri-Markwell, “The Online Dehumanisation.”

## Facebook's non-response

The abuse of Facebook Live was foreseeable. Facebook had already been [criticized](#) for the use of Facebook Live in broadcasting suicides and violent attacks, and yet the company took little action.<sup>188</sup> In 2017, Facebook came under harsh criticism after a raft of suicides were live-streamed, including [one](#) of a 12-year-old girl in Georgia that was left live on the site for two weeks before being removed.<sup>189</sup> The company [responded](#) then that it was adding more resources to monitoring, but offered the excuse that the sheer volume of content broadcast live on the platform made it impossible to monitor it all.<sup>190</sup> Shockingly, after the Christchurch massacre was broadcast on its own platform, it took the company's senior leadership more than 10 days to [speak](#) publicly about this tragedy, and that only happened after a tremendous amount of public criticism.<sup>191</sup> Facebook said they would explore restrictions on live-streaming from the platform. In response to a tragedy at this scale, one would expect significant changes to Facebook Live and restrictions which would prevent abuses like this from ever happening again. But when change came, it was minor, and announced six weeks after the attacks. In late May of 2019, Facebook [announced](#) only a small and relatively insignificant change that said that anyone breaking certain rules in broadcasting content on Facebook Live would be temporarily barred from using the service, with the possibility of a 30-day ban on a first offense.<sup>192</sup> (Previously, it did not typically bar users until they had broken these rules multiple times.) Multiple offenders, or people who posted particularly egregious content, *could* be permanently barred from Facebook.

## Inspiration for the attack leads back to Facebook

Tarrant may have first been exposed to the ideology that propelled his attack because it was circulated widely on Facebook for many, many years. The shooter had been [radicalized](#) into the white supremacist Identitarian movement and was an adherent of the racist Great Replacement theory - an international white supremacist conspiracy that promotes the idea that white people are slowly experiencing a genocide in their own home countries due to a plot by elites to displace them with rising numbers of non-white immigrants.<sup>193</sup> This racist thinking is most prominently recognized in the form of the sprawling, multinational organization, [Generation Identity](#),<sup>194</sup> to which Tarrant [gave](#) a donation.<sup>195</sup> For years, GI material flourished on Facebook and garnered many thousands of followers until the movement was [deplatformed](#) in 2018.<sup>196</sup> Even after the deplatforming, the Institute for Strategic Dialogue [identified](#) some 11,000 members of Facebook groups devoted to the Great Replacement idea.<sup>197</sup>

<sup>188</sup> Nicolas Vega, "Facebook: We Can't."

<sup>189</sup> Mix, "Facebook took 2 weeks to remove video of 12-year-old girl that livestreamed her suicide," *The Next Web*, Jan. 16, 2017.

<sup>190</sup> Nicolas Vega, "Facebook: We can't stop all live-stream suicides," *The New York Post*, Oct. 25, 2017.

<sup>191</sup> Julie Carrie Wong, "Facebook finally responds to New Zealand on Christchurch attack," *The Guardian*, March 29, 2019.

<sup>192</sup> Cade Metz and Adam Satariano, "Facebook Restricts Live Streaming After New Zealand Shooting," *The New York Times*, May 14, 2019.

<sup>193</sup> Jacob Davey and Julia Ebner, *'The Great Replacement: The Violent Consequences of Mainstreamed Extremism*, Institute for Strategic Dialogue, 2019.

<sup>194</sup> Heidi Beirich and Wendy Via, "International White Nationalist Movement."

<sup>195</sup> Jason Wilson, "Christchurch shooter's links to Austrian far right 'more extensive than thought,'" *The Guardian*, May 15, 2019.

<sup>196</sup> *Al Jazeera*, "Facebook pulls the plug on far-right Generation Identity," *Al Jazeera*, June 22, 2018.

<sup>197</sup> Jacob Davey and Julia Ebner, *"The Great Replacement."*

# Sri Lanka

Hate speech and rumors targeting Muslims [contributed](#) to a 2018 outbreak of anti-Muslim violence in Sri Lanka.<sup>198</sup> One [viral video](#) on Facebook falsely depicted a Muslim restaurateur seemingly admitting to mixing “sterilization pills” into the food of Sinhala-Buddhist men;<sup>199</sup> other heinous material, such as a post advocating to “kill all Muslims, do not spare even an infant, they are dogs,”<sup>200</sup> [contributed](#) to an outbreak of anti-Muslim violence in Sri Lanka in 2018.<sup>201</sup> At least three people were killed and 20 injured in the 2018 unrest, during which mosques and Muslim businesses were burned, mainly in the central part of the Buddhist-majority nation. Facebook [left](#) most of the incendiary material up for days, even after it had been reported.<sup>202</sup> Ultimately, the Sri Lankan government had to shut Facebook down to stem the violence. Sri Lankan officials ultimately [determined](#) that mobs used Facebook to coordinate attacks, and that the platform had “only two resource persons” to review content in Sinhala, the language of Sri Lanka’s ethnic majority whose members were behind the violence.<sup>203</sup>

A 2018 [audit](#), contracted by Facebook from the human rights organization Article One found that hate speech and rumors spread on Facebook “may have led to ‘offline’ violence.”<sup>204</sup> Facebook, more so than any other social media platform, [was used](#) by Buddhist nationalists to spread propaganda against Sri Lanka’s Muslims, which make up 10 percent of the country’s population.<sup>205</sup> Article One suggested that before the unrest, Facebook had failed to take down such hate content, which “resulted in hate speech and other forms of harassment remaining and even spreading” on the platform.

“

Kill all Muslims,  
do not spare  
even an infant,  
they are dogs.

**Hate Speech**  
Facebook post

198 Amalini De Sayrah, “Facebook helped foment anti-Muslim violence in Sri Lanka. What now?” *The Guardian*, May 5, 2018.

199 *Eurasian Times* Desk, “After Rohingya Genocide; Facebook Now Apologizes To Sri Lanka Over Anti-Muslim Riots,” *Eurasian Times*, May 15, 2020.

200 *Today*, “Facebook admits ‘serious mistake’ after Edwin Tong questions failure to remove hate post in Sri Lanka,” *Today*, Nov. 28, 2018.

201 *Al Jazeera*, “Sri Lanka: Facebook apologises for role in 2018 anti-Muslim riots,” *Al Jazeera*, May 13, 2020.

202 Amalini De Sayrah, “Facebook helped foment.”

203 *Al Jazeera*, “Sri Lanka.”

204 *Al Jazeera*, “Sri Lanka.”

205 Tasnim Nazeer, “Facebook’s Apology.”

“We deplore this misuse of our platform,” the company [said](#) in a response to the Sri Lanka report.<sup>206</sup> “We recognize, and apologize for, the very real human rights impacts that resulted.” Facebook also highlighted actions it had taken to address the problems, including hiring content moderators with local language skills, implementing technology that automatically detects signs of hate speech and keeps abusive content from spreading, and trying to deepen relationships with local civil society groups. However, again, it was too little, too late. Significant damage, strained relations between communities, and a rise in anti-Muslim sentiment had already fueled tensions.



“

We recognize, and apologize for, the very real human rights impacts that resulted.

Facebook

Muslims in Sri Lanka were the targets of hate speech and rumors circulating on Facebook that led to an outbreak of anti-Muslim violence in 2018. Photo: Kevin Hellon

<sup>206</sup> Joshua Brustein, “Facebook Apologizes for Role in Sri Lankan Violence,” *Bloomberg*, May 12, 2020.

# Sweden

In late August 2020, far-right Danish politician Rasmus Paludan, head of the Stram Kurs (Hard Line) anti-immigrant party, [tried](#) to cross over the bridge from Denmark into Malmo, Sweden, for a Quran burning event with his anti-Muslim allies.<sup>207</sup> He was turned away by Swedish authorities on the bridge and barred from Sweden for two years. Paludan responded with an angry, anti-Muslim [message](#) on Facebook: “Sent back and banned from Sweden for two years. However, rapists and murderers are always welcome!”<sup>208</sup>

Despite Paludan’s absence, his supporters moved forward with their protest and burned a Quran near a Malmo mosque. Riots [broke](#) out resulting in significant property destruction, all of which was propelled by social media videos of the desecration that were circulated widely online.<sup>209</sup> Paludan, who has an active Facebook page full of anti-Muslim videos, was sentenced to a month in jail in Denmark for a string of offences, including racism, in early 2020. His [conviction](#) included charges regarding posting anti-Muslim videos on social media channels. Paludan’s Facebook [page](#) remained active<sup>210</sup> as of September 2020.<sup>211</sup>



Members of the Stram Kurs (Hard Line) anti-immigrant party burn a copy of the Quran and circulate the video online leading to mass riots.  
Photo: Anonymous

<sup>207</sup> *Al Jazeera*, “Sweden: Far-right activists burn copy of Quran, plan more stunts,” *Al Jazeera*, Sept. 10, 2020.

<sup>208</sup> *Deutsche Welle*, “Malmo: Violence erupts after anti-Muslim activity,” *Deutsche Welle*, Aug. 29, 2020.

<sup>209</sup> *Deccan Chronicle*, “Riot in Sweden after Danish leader banned from Quran-burning rally,” *Deccan Chronicle*, Aug. 29, 2020.

<sup>210</sup> <https://www.facebook.com/rasmuspaludan>.

<sup>211</sup> *BBC*, “Protest against Quran-burning turns violent in Sweden,” *BBC*, Aug. 29, 2020.

# United States

Facebook is an American company, and as such, its actions and policies reflect on the U.S. and its influence in other countries. And its decisions to allow American-produced, anti-Muslim hate content to flourish on its platform no doubt serves as an example of what the company finds acceptable worldwide.

## Facebook knows that it allows anti-Muslim content

The problem with anti-Muslim hate on Facebook has been widely documented for years. An [analysis](#) of Facebook data in early 2020 showed that the United States and Australia “lead in the number of active Facebook pages and groups dedicated to referring this dehumanizing [anti-Muslim] content.”<sup>212</sup> In May 2020, the Tech Transparency Project [found](#) more than 100 American white supremacist groups, many of them explicitly anti-Muslim, active on the platform both on their own group pages as well as on auto-generated content. In the wake of TTP’s report, Facebook did nominally alter some of the auto-generated content, but the hate groups largely remained.<sup>213</sup>

An [analysis](#) by computer scientist Megan Squire of far-right groups on Facebook found a significant crossover with anti-Muslim hate.<sup>214</sup> Squire found that anti-Muslim attitudes are not only flourishing on the platform, but also acting as a “common denominator” for a range of other extremist ideologies, including xenophobic anti-immigrant groups, pro-Confederate groups, militant anti-government conspiracy theorists, and white nationalists. Squire [said](#) of her research, “Some of the anti-Muslim groups are central players in the hate network as a whole. And the anti-Muslim groups show more membership crossover with other ideologies than I expected.”<sup>215</sup>

A 2018 [study](#) by the Southern Poverty Law Center (SPLC) identified 33 anti-Muslim Facebook groups that used violent imagery, including weapons, in their main photos.<sup>216</sup> According to the SPLC, twenty of these groups promoted the stereotype that all Muslims are violent. One group, “Islam Unveiled,” had an image of an ISIS fighter executing prisoners lying prone in a shallow grave. The picture was accompanied by a quote credited to “Muhammad, Prophet of Islam,” which says, “Killing Unbelievers is a SMALL MATTER to us.” The SPLC also found a group, “PRO-ISLAMOPHOBIA SAVES LIVES!!” whose cover photo was an image of a charred, blackened body which should have been prohibited according to Facebook’s claim that posts depicting “[charred or burning people](#)” are prohibited.<sup>217</sup> After an academic researcher flagged the group, an automated response was generated and provided to SPLC: “We looked over the group you reported and though it doesn’t go against one of our specific Community Standards, we understand that the group or something shared in it may still be offensive to you.”<sup>218</sup>

<sup>212</sup> Rita Jabri-Markwell, “The Online Dehumanization.”

<sup>213</sup> Tech Transparency Project, *White Supremacist Groups*.

<sup>214</sup> Ishmael N. Daro, “Here’s How.”

<sup>215</sup> Ishmael N. Daro, “Here’s How.”

<sup>216</sup> Swathi Shanmugasundaram, “The persistence of anti-Muslim hate on Facebook,” Southern Poverty Law Center’s Hatewatch, May 5, 2018.

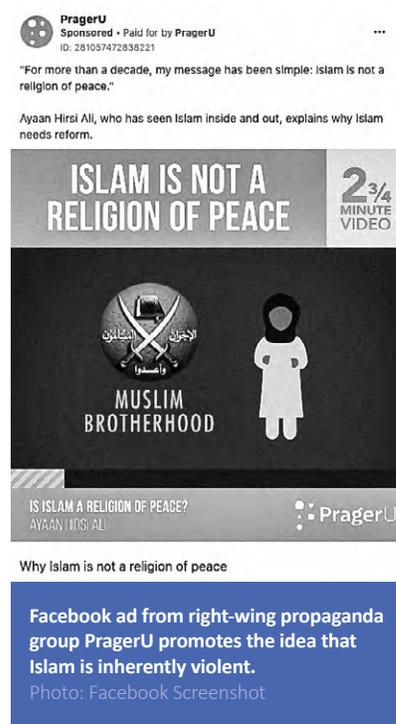
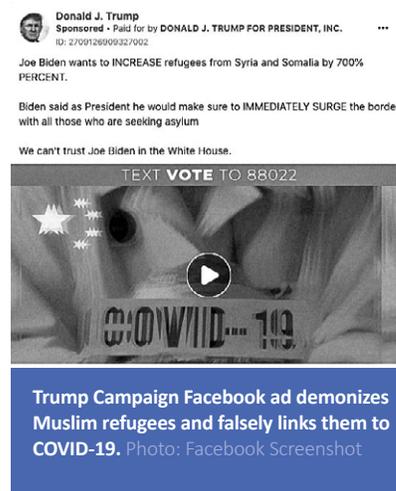
<sup>217</sup> Michal Lev-Ram, “Facebook Tries to Bring More Transparency to Opaque Set of Guidelines,” *Fortune*, April 24, 2018.

<sup>218</sup> Swathi Shanmugasundaram, “The persistence.”

There are other ways anti-Muslim material is spread on Facebook. In 2019, a major study [found](#) dozens of current and former American law enforcement officers as members of Facebook groups dedicated to anti-Muslim bigotry.<sup>219</sup> Many were private groups, where this hatred was allowed to flourish outside of any oversight. With names such as “Veterans Against Islamic Filth,” “PURGE WORLDWIDE (The Cure for the Islamic disease in your country)” and “Americans Against Mosques,” these groups serve as private forums to share bigoted messages about Muslims, and they have proven attractive to police officers.

Facebook’s problem with anti-Muslim content was also documented by its own civil rights [audit](#), which came after years of pressure from human rights advocates to address hate content online.<sup>220</sup> Released in July 2020, the auditors singled out the problem of anti-Muslim hate as needing to be addressed, their conclusions were partly based on information provided by human rights groups who had been lobbying the company for years to take the problem seriously. Facebook has, thus far, not addressed any of the anti-Muslim problems found by its own audit. The company’s actions indicate that its decision to engage in the audit at all was not out of concern for lives lost because of its inaction, but for political expediency.

Perhaps the most notable case of allowing anti-Muslim hate speech on Facebook, despite it violating the site’s rules, involves President Donald Trump. In 2016, Zuckerberg [decided](#) not to remove a post by Trump calling for a ban of all Muslims entering the U.S.<sup>221</sup> Zuckerberg [acknowledged](#) in a meeting with his staff that Trump’s call for a ban did qualify as hate speech, but said the implications of removing them were too drastic.<sup>222</sup> Once again, Facebook refused to apply its hate speech policies against a politically powerful individual.



219 Will Carless and Michael Corey, “American cops have openly engaged in Islamophobia on Facebook, with no penalties,” *Reveal News*, June 27, 2019.

220 Facebook, *Facebook’s Civil Rights Audit*.

221 Julia Carrie Wong, “Zuckerberg proves he is Facebook’s editor by allowing Trump’s hate speech,” *The Guardian*, Oct. 21, 2016.

222 Julia Carrie Wong, “Zuckerberg proves.”

## Double standard for targeting Muslim public officials

While President Trump’s Facebook anti-Muslim post is protected, Muslim public figures have been threatened and attacked on the platform. On numerous occasions, Muslim public officials in Congress and around the country have been [targeted](#) with hateful content – even death threats – on Facebook and Instagram.<sup>223</sup> Additionally, two Muslim congresswomen, Ilhan Omar and Rashida Tlaib, were [targeted](#) by an international fake news operation that spread anti-Muslim propaganda on Facebook.<sup>224</sup> Facebook also allowed the Trump campaign to [run multiple, false ads](#)<sup>225</sup> against these [congresswomen](#).<sup>226</sup> No action was taken by Facebook against the ads.

Perhaps most shockingly, Facebook [allowed](#) a man charged with threatening to kill Congresswoman Ilhan Omar to post violent and racist content for years, and took no action to remove his posts when he was arrested in 2019.<sup>227</sup> Upstate New Yorker Patrick Carlineo posted several entries to his Facebook page alluding to violence against Muslims and U.S. officials, including former president Barack Obama. Carlineo frequently posted anti-Muslim material, using racist slurs and saying he wished he could confront a group of Muslim politicians with “a bucket of pig blood.” Carlineo’s profile wasn’t removed by Facebook until a reporter [contacted](#) them two weeks after he was arrested for threatening to kill Omar (he pleaded guilty and was sentenced to one year in prison).<sup>228</sup>

## Abuse of the event organizing pages

Facebook’s event pages have been particularly problematic. For years, white nationalists, militias, and anti-Muslim hate groups have been using [Facebook event pages](#) to organize armed, hate rallies targeting mosques and Muslim community centers across the country.<sup>229</sup> Shockingly, the company permitted white nationalist militias to directly intimidate worshippers and threaten mosques. In 2016, two Russian Facebook pages [organized](#) dueling rallies in front of the Islamic Da’wah Center of Houston.<sup>230</sup> Heart of Texas, a Russian-controlled Facebook group that promoted Texas secession, played into the stereotype of the state as a land of guns and barbecue and amassed hundreds of thousands of followers. One of their ads on Facebook announced a noon rally on May 21, 2016 to “Stop Islamification of Texas.” A separate Russian-sponsored group, United Muslims of America (stealing the identity of a legitimate California-based Muslim organization), advertised a “Save Islamic Knowledge” rally for the same place and time. The armed protest was [peaceful](#) but terrorized those inside the religious center.<sup>231</sup>

<sup>223</sup> Mellissa Nan Burke, “Tlaib not cowed by ‘hateful’ threats, behavior,” *The Detroit News*, Jan. 27, 2019.

<sup>224</sup> David Smith, Michael McGowan, Christopher Knaus and Nick Evershed, “Revealed: Ilhan Omar and Rashida Tlaib targeted in far-right fake news operation,” *The Guardian*, Dec. 5, 2019.

<sup>225</sup> Muslim Advocates, *Donald Trump Ad*.

<sup>226</sup> Andrea Germanos, “Facebook and Twitter urged to suspend Donald Trump after attack on Ilhan Omar,” *Salon*, April 15, 2019.

<sup>227</sup> Jon Swaine, “Facebook allowed violent posts by man charged with Ilhan Omar death threat,” *The Guardian*, April 16, 2019.

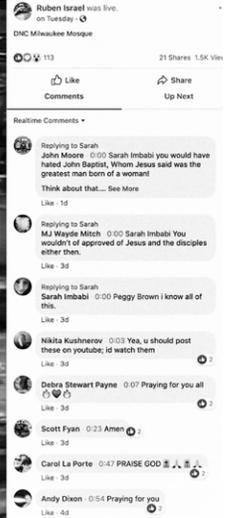
<sup>228</sup> Jon Swaine, “Facebook allowed.”

<sup>229</sup> Muslim Advocates, “Facebook Ignored Warnings About Event Page Abuses for Years,” Press Release, Sept. 16, 2020.

<sup>230</sup> Claire Allbright, “A Russian Facebook page.”

<sup>231</sup> Claire Ballor, “Shariah law protesters, some toting rifles, gather in front of North Texas Islamic center,” *The Dallas Morning News*, June 10, 2017.

In August of 2020, a group of anti-Muslim activists used Facebook to live-stream a hate rally outside a mosque in Milwaukee, Wisconsin.  
Photo: Facebook Livestream



Facebook’s civil rights auditors [highlighted](#) the company’s failure to enforce policies prohibiting a call to arms during an anti-Muslim protest organized on their events pages during August of 2019.<sup>232</sup> The auditors described an event page which was used to intimidate attendees of the Islamic Society of North America’s annual convention in Houston, Texas. Despite the fact that this was the second year in a row where this same hate group threatened the conference, it took Facebook more than 24 hours to remove the event page. Facebook did later acknowledge that the Houston incident represented an enforcement misstep, and the auditors used this example to conclude that Facebook’s “events policy provides another illustration of the need for focused study and analysis on particular manifestations of hate.”<sup>233</sup>

## Live-streaming hate

In August of 2020, a group of anti-Muslim activists [used](#) Facebook to live-stream a hate rally outside a mosque in Milwaukee, Wisconsin.<sup>234</sup> Holding a sign that read “Halt Islam,” anti-Muslim street preacher Ruben Israel yelled hateful, threatening slurs from a megaphone outside the Islamic Society of Milwaukee, the largest mosque in the city. During the protest, Israel used Facebook to broadcast multiple false, offensive slurs and conspiracies about Muslims, shouting about “wicked, perverted Islam” and asking Muslims in the mosques if they have “anything ticking” on them, and whether they had a pilot’s license. He also told a Muslim couple near the mosque, “don’t tell me you’re here getting government assistance while you hate our country.” Despite these clear violations of Facebook’s hate speech and live-streaming policies, it took outside groups to alert the company before the content was removed.

<sup>232</sup> Facebook, *Facebook Civil Rights Audit*.

<sup>233</sup> Facebook, *Facebook Civil Rights Audit*.

<sup>234</sup> Muslim Advocates, “Facebook Allows Livestream of Anti-Muslim Mosque Protest in Milwaukee,” Press Release, Aug. 24, 2020.

# Conclusion

In its August 2020 [update](#) of its hate speech policies, which banned conspiracy theories and stereotypes targeting vulnerable communities,<sup>235</sup> Facebook yet again [left](#) Muslims off the list.<sup>236</sup> This was just another example in a long line of disappointing decisions made by the company, particularly given the conclusions of Facebook’s own audit released the month prior that highlighted the significant problem of anti-Muslim hate on the platform. From the documentation in this report of international anti-Muslim violence stoked on Facebook, it seems clear that Facebook has no regard for the lives of Muslims. The August 2020 policy changes [banning](#) blackface and anti-Semitic conspiracy theories and stereotypes are clearly welcome and important expansions of the company’s hate speech policies.<sup>237</sup> It is baffling, however, that the company chose not to include implicit stereotypes and tropes about Muslims, such as the false ideas that they are inherently violent, foreign, or criminal. These stereotypes are all dangerous and have resulted in discrimination, hate crimes, and mass murder of Muslims around the world. Yet, given the many opportunities and repeated warnings over many years to protect Muslims from hate content on its platform, the company has refused to act. Ultimately, one thing is clear: for Facebook, jeopardizing the safety and security of Muslims is just the cost of doing business.

Facebook has **no regard**  
for the lives of Muslims.

For Facebook, jeopardizing  
the safety and security  
of Muslims is just the  
cost of doing business.

<sup>235</sup> Jacob Kastrenakes, “Facebook bans blackface and anti-Semitic stereotypes in hate speech update,” *The Verge*, Aug. 11, 2020.

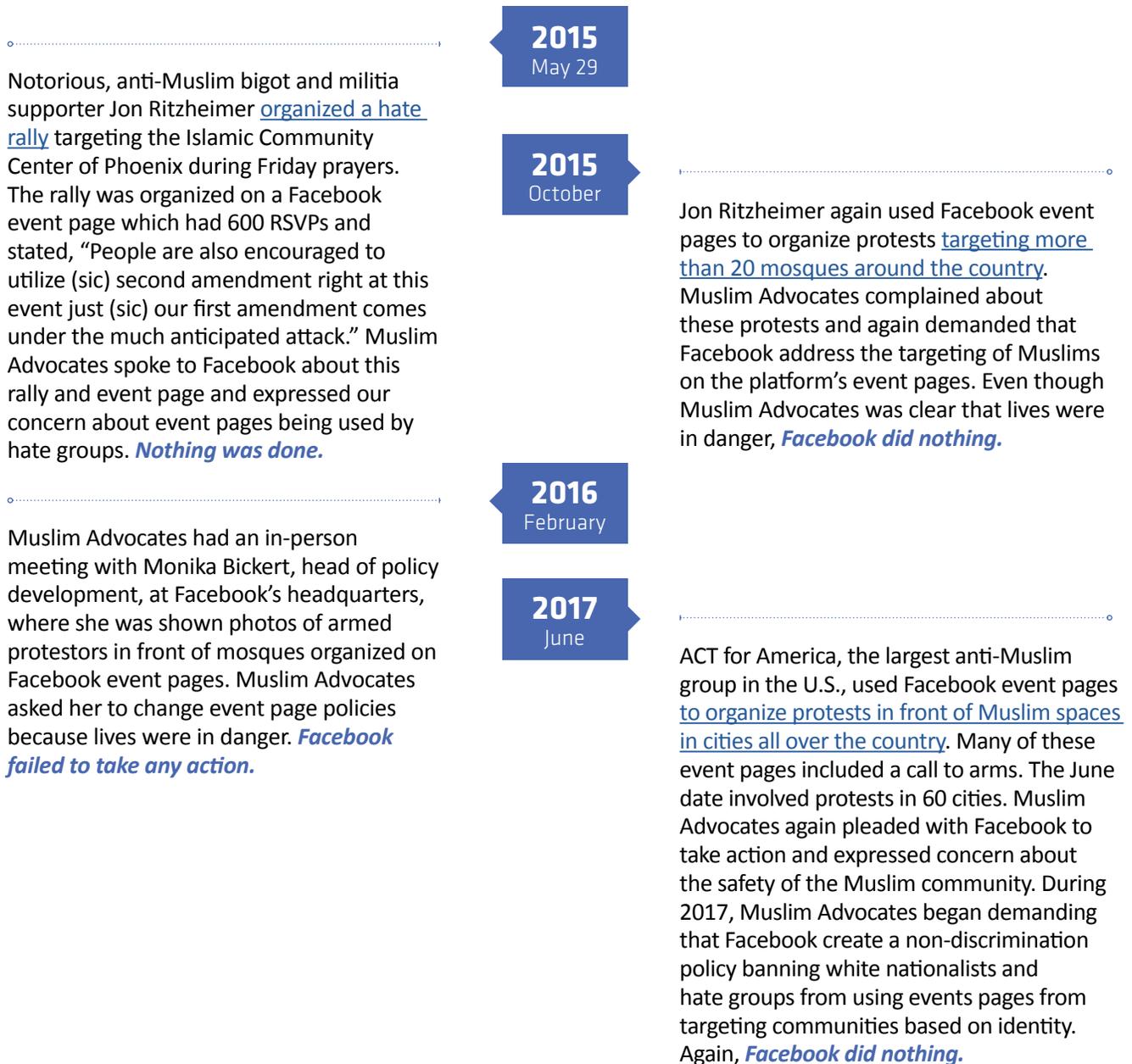
<sup>236</sup> Muslim Advocates, “New Facebook Hate Speech Policy Update Leaves Out Muslims,” Press Release, Aug. 13, 2020.

<sup>237</sup> *BBC*, “Facebook adds ‘blackface’ photos to banned posts,” *BBC*, Aug. 12, 2020.

## APPENDIX

# Timeline of Failure: Facebook ignores five years of warnings of event pages being used to promote violence

The following is a five-year timeline of Muslim Advocates' repeated attempts to warn Facebook about event page abuses and of the company's repeated failure to heed those warnings:



Documents released by Congress revealed that [Russian-linked groups used Facebook event pages](#) to promote anti-Muslim animus and direct protesters to a Houston mosque. After this revelation was made public, Muslim Advocates again went to Facebook and warned them about how event pages were being used to promote anti-Muslim hate and endanger Muslims.

2017  
September

2017  
Oct 11

Muslim Advocates participated in a small group meeting with Facebook Chief Operating Officer Sheryl Sandberg, where she again was told about the abuse of the events pages and how they were being used by white nationalists to target mosques and Muslims. Muslim Advocates shared with her of protestors brandishing guns at these rallies and asked her to take action. *Nothing was done.*

Muslim Advocates and coalition partners met with Facebook officials and had an extensive discussion about hate groups and events pages, again requesting polices for the pages be reviewed and updated in order to stop white supremacist groups from using the pages to targets Muslims and other vulnerable communities.

2019  
Mar 7

2019  
August

A militia group, the Texas Patriot Network, [used a Facebook event page](#) to plan an armed protest at the largest Muslim convention in the country. Muslim Advocates warned Facebook about the page and had to wait more than 24 hours before it was taken down. Even worse, the same group planned a similar armed protest at the same event the year prior where militia members were found to have discussed possible targets and called them “dead meat.” Despite Mark Zuckerberg’s claim that “[we do not allow hate groups on Facebook](#),” this group still has an active Facebook presence.

Muslim Advocates Executive Director Farhana Khera attended a [small group dinner with Facebook CEO Mark Zuckerberg](#), Sheryl Sandberg and other members of Facebook leadership. She highlighted the problem with the event pages again and asked them to stop white nationalists and hate groups from abusing their event pages. *Nothing happened.*

2019  
Nov 4

During a call with Sheryl Sandberg about the [final report of the civil rights audit](#), Muslim Advocates yet again asked for Facebook to end the targeting of vulnerable communities on the event pages. Muslim Advocates warned that people were going to get hurt but no action was taken.

2020  
Jul 10

2020  
Aug 26



An armed 17-year-old who drove up from Illinois shot and killed two people protesting the police killing of James Blake in Kenosha, Wisconsin. It was [later reported](#) that a Facebook event page from a local Kenosha militia that included a call to arms was flagged at least 455 times but [not taken down by the company](#).



# complicit

**GPAHE**  
Global Project Against Hate and Extremism

**MUSLIM**  
**ADVOCATES**

# Exhibit 78

# Business Help Center

Hi Ayeshia, how can we help?

Last updated: Nov 10, 2021

## About Lookalike Audiences

31,681 views

Changes driven by ongoing efforts to align our products with evolving privacy rules in Europe may impact campaigns advertising to [people](#) in the European Region. Learn more about [how European privacy directives may affect your ads and reporting](#).

A lookalike audience is a way your ads can reach new people who are likely to be interested in your business because they share similar characteristics to your existing customers.

A lookalike audience uses an existing [Custom Audience](#) you select for its [source audience](#). To create a lookalike audience, our system leverages information such as demographics, interests and behaviors from your source audience to find new people who share similar qualities. When you use a lookalike audience, your ad is delivered to that audience of people who are similar to (or "look like") your existing customers.

When you create your lookalike audience, you can use a percent range to choose how closely you want your new audience to match your source audience. The size you choose depends on your goals. Smaller percentages more closely match your source audience, but larger percentages create a bigger, broader audience.

We generally recommend a source audience that has between 1,000-5,000 people. However, the quality of your audience also matters. For example, you may get better results depending on your goals if you use an audience made from your best customers rather than one that includes all your customers.

### Additional information

- You need an existing source audience before you can create a lookalike audience.
- You can create up to 500 lookalike audiences from a single source audience.
- Your source audience must contain at least 100 people from a single country to use it as the basis for a lookalike audience.
- Lookalike audiences use your ad set locations and only include people from those locations.
- You can use [lookalike expansion](#) to show your ads to people outside your defined lookalike audience.
- People in your source audience are excluded from your lookalike audience.
- You can use multiple lookalike audiences at the same time for a single ad set. In this instance, the ad set targets your ads to people in any of your selected lookalike audiences.

**Note:** Targeting options are limited to location, age and gender for audiences that include [people](#) under age 18 globally, 20 in Thailand or 21 in Indonesia. You can't use detailed targeting, Custom Audiences, lookalike audiences or saved audiences to target your ads to these age groups. Learn more about the targeting options to reach young people, and how this update may [impact your ad sets](#).

## Learn more

- [Create a Lookalike Audience](#)
- [Best Practices to Maximize Your Lookalike Audience](#)
- [Updates to Lookalike Audience Locations](#)

Was this information helpful?

Yes  No

[Permalink](#) · [Share](#)

More in this section: AUDIENCES

---

### BASICS

---

#### > [About lookalike audiences](#)

[About customer lifetime value](#)

[About value-based lookalike audiences](#)

---

### SET UP

---

### CREATE

---

### MANAGE

---

AUDIENCES | [Lookalike Audiences](#)

---

[Back to Home](#)

# Exhibit 79

# Civil rights leaders thought they'd figured out how to deal with Facebook. But now they are 'livid.'

By [Craig Timberg](#)

October 25, 2019



As civil rights leaders prepared for a town hall event in Atlanta last month featuring Facebook's second-in-command Sheryl Sandberg, optimism ran high that company officials would address long-standing concerns about racism on the platform. Near the top of the list were the voter suppression messages that flooded Facebook during the 2016 presidential election and, the civil rights leaders feared, would do so again as another election season was dawning.

But as they began to arrive in Atlanta for the Sept. 26 event, that hope turned to outrage as civil rights leaders learned that Facebook had announced what many now call the "Trump exemption" — meaning the policy allowing any politician to lie freely in ads or free posts without consequences.

Though Facebook has portrayed this decision as reflecting the nation's ideals of unfettered political speech, civil rights leaders say they see another value emerging preeminent in Facebook's calculations: the unfettered quest to profit from political advertising.

"The only principle is business as usual and trying to line their pockets," said Arisha Hatch, vice president for [Color of Change](#), one of several civil rights groups that had been in regular contact with Sandberg and others at the company. "There is no principled stand that people can take that would allow them to behave on the platform as voter suppressionists have behaved in our country for decades."

Hatch and others view the company's tolerance of deception against the backdrop of the nation's ugly history of voter suppression, much of it conducted by politicians and government officials. The Russian disinformation campaign that backed Donald Trump's election relied heavily on social media postings discouraging black voters from casting ballots, in what civil rights leaders see as a foreign update of old and largely homegrown political tactics.

Facebook's announcement was one of several incidents in recent months that have inflamed its fragile relations with [civil rights leaders](#), undoing years of progress on several fronts, including combating housing discrimination in the company's ad platform.

Among the more damaging was chief executive Mark Zuckerberg's speech at Georgetown University last week in which he invoked the legacies of civil rights icon the Rev. Martin Luther King Jr. and revered 19th-century abolitionist Frederick Douglass in defending the company's [approach to political speech](#). The civil rights leaders saw this as a brazen act of appropriation that showed little awareness of the false and misleading information that King in particular battled in his lifetime.

The issue flared again as Zuckerberg testified on Capitol Hill Wednesday. In one of the most tense exchanges during hours of testimony, Rep. Joyce Beatty (D-Ohio) chastised him for not having more diversity on his leadership team and described Facebook's approach to civil rights as "appalling and disgusting."

Facebook's latest "Diversity Report" says black people fill 3.1 percent of its "senior leadership" positions. For Hispanics, it's 3.5 percent.

Vanita Gupta, president of the Leadership Conference on Civil & Human Rights, a Washington-based umbrella group, said Facebook's decision to permit politicians to lie on the platform left her "livid," and she expressed her concerns directly to Zuckerberg in a phone call before he spoke at Georgetown. In that call, Gupta said, she told Zuckerberg that Facebook lacked the expertise in civil rights it needs to handle such matters responsibly.

"I do have civil rights expertise" on Facebook's staff, Zuckerberg replied, according to Gupta's recollection. "I have several people from the Obama White House."

The answer exasperated her, she said, because he appeared to see demands for civil rights strictly in political terms — as opposed to legal or moral ones — and somehow a liberal equivalent to the unproven conservative claims that Facebook suppresses voices on the right.

"That is the level of the disconnect," Gupta said. "There's not even an understanding of what civil rights expertise might be and why they would want to have it."

Facebook spokeswoman Ruchika Budhraj declined to comment on the conversation between Zuckerberg and Gupta but said the company had worked hard to consult with civil rights leaders.

"Our partnership with civil rights groups has led to important outcomes, such as combating voter suppression and hate, and preventing discrimination in ads on Facebook," Budhraj said. "We'll continue partnering and seeking input from the civil rights community to address the concerns they have about our policies and products."

Intensive conversations with civil rights groups began in 2017, shortly after Facebook revealed that Russian disinformation operatives had bought ads on the platform to influence the presidential vote the year before. Among the top goals in Russian ads and free posts was discouraging African Americans from voting, which U.S. officials and numerous outside researchers concluded was part of a coordinated effort to damage the prospects of Democrat Hillary Clinton and help elect Trump.

Civil rights leaders agreed they had made strides in their talks with Facebook and praised Sandberg for meeting with them and overseeing a civil rights audit they had requested. The audit, though still unfinished, has raised hopes that the company was addressing concerns about racism on the platform, as well as diversity and other issues at Facebook. The civil rights leaders expected the Atlanta town hall would mark a new step in that progress.

But as they began assembling for the event, word spread that another top Facebook official, Nick Clegg, had on Sept. 24 outlined the exemption for politicians' speech at a conference in Washington. He said the company's system of fact-checkers, a central part of its response to the rampant spread of online disinformation in 2016, would not be used to identify, label or otherwise address outright falsehoods when politicians uttered them.

"It is not our role to intervene when politicians speak," said Clegg, a former British deputy prime minister who became Facebook's vice president for global policy and communications last year. "That's why I want to be really clear today. We do not submit speech by politicians to our independent fact-checkers, and we generally allow it on the platform even when it would otherwise breach our normal content rules."

his reelection campaign.

The company's ad archive shows that President Trump's Facebook page has spent more than \$21 million on ads since May 2018, and his Democratic rivals have been spending heavily as well. Facebook, citing the policy announced by Clegg, refused a request by the campaign of Democratic candidate Joe Biden this month to remove an ad making false claims about him and his son's activities in Ukraine.

Facebook's policies still prohibit voter suppression — even when practiced by politicians — but civil rights leaders express little confidence that the platform will enforce this with sufficient speed and breadth. Addressing obvious falsehoods, such as lies about the dates or locations of polling, would not be enough to defeat politicians' efforts to hold down minority voting participation on the platform, say civil rights leaders.

They express particular worry that American political figures could engage in tactics similar to those used in Russia's disinformation campaigns. The Internet Research Agency, in St. Petersburg, used fake social media accounts in 2016 to target African Americans concerned about police violence and other issues. The Russian-based Facebook group "Woke Blacks," for example, wrote, "We cannot resort to the lesser of two devils. Then we'd surely be better off without voting AT ALL."

Facebook also offers the ability to target its users with a rare precision, as the Russians did with an ad on Election Day in 2016 directed at users with interests in civil rights, King and Malcolm X. It said of Trump and Clinton, "Not one represents Black People. Don't go to vote. Only this way we can change the way of things..."

Facebook has made strides in detecting and shutting down such foreign operations, but civil rights groups and disinformation researchers express little faith in the company's ability to find and act against domestic political figures who may attempt similar tactics. The exemption allowing politicians to lie makes that problem worse, they say, even if Facebook does not officially tolerate voter suppression.

"They can't have both: They're not going to be able to stop voter suppression campaigns and allow for politicians to conduct disinformation," said Kate Starbird, a University of Washington associate professor who researches disinformation. "They might catch one or two voter-suppression messages, but they will miss most of it."

Politicians, their campaigns and their parties long have worked to discourage particular groups from voting. A top aide to former Maryland governor Robert L. Ehrlich Jr., a Republican, allegedly organized robocalls in 2010 telling more than 110,000 Democrats in predominantly black areas that they could "relax" because their party's candidate already had been "successful." Prosecutors called the robocalls an effort to keep African Americans from casting ballots.

"Voter intimidation and suppression have a long history in this country, and not just on the Internet," said Wendy Weiser, director of the Democracy Program at the Brennan Center for Justice at New York University's School of Law.

Civil rights leaders express similar concerns about the coming 2020 Census because of the possibility of misleading social media messages warning immigrants, for example, that any information collected will be shared with Immigration and Customs Enforcement.

Undergirding these fears is the experience that civil rights leaders have had in dealing with Facebook, which they say has been slow to address incidents that concerned them.

They point to an incident from August when a Texas-based conservative group used Facebook to encourage people to bring weapons to a protest outside the nation's largest annual gathering of Muslims, which was happening in Houston. One Facebook posting from a person affiliated with the group made a cryptic reference to "long guns." The Houston

Muslim Advocates, which was among the civil rights groups in regular conversation with Facebook, flagged the “long guns” posting to company officials several days before the event. Facebook removed the post but only after more than 24 hours had passed — a delay Muslim Advocates and other civil rights groups considered excessive.

“We were going to Facebook thinking that some of these issues were going to be taken seriously by the company,” said Madihha Ahussain, the group’s special counsel for anti-Muslim bigotry. “We were given the runaround.”

Budhraja, the Facebook spokeswoman, said Facebook removed the post and three others it found related to the Houston protest. The initial post shared by Muslim Advocates, she said, did not include enough information to make an immediate decision to remove it, but subsequent research, including into the group’s past activities, showed it violated the policy prohibiting posts that encourage people to intimidate or harass other people.

*Tony Romm contributed to this report.*



# Exhibit 80

— ANONYMOUS WHISTLEBLOWER DISCLOSURE —

SEC Office of the Whistleblower  
Via Online Portal & FedEx

- Re: Supplemental Disclosure of Securities Law Violations by Facebook, Inc. (NASDAQ: FB), SEC TCR [REDACTED]

**Facebook misled investors and the public about equal enforcement of its terms given that high-profile users are "whitelisted" under its "XCheck" program.**

To the SEC Office of the Whistleblower:

1. The instant letter is one of multiple disclosures related to the above-captioned matter. Our anonymous client is disclosing original evidence showing that **Facebook, Inc. (NASDAQ: FB)** has, for years past and ongoing, violated U.S. securities laws by making **material misrepresentations and omissions in statements to investors and prospective investors**, including, *inter alia*, through filings with the SEC, testimony to Congress, online statements and media stories.
2. **Summary.** In particular, despite reassuring investors and the public that it enforces its terms and policies in a "fair and consistent" way, and that its "XCheck" (pronounced "Cross Check") program only provides "additional review" for high-visibility users (e.g., celebrities and high-paying advertisers), this is a material misstatement and/or omission. In fact, XCheck functions in practice as a "whitelist" for privileged users, furthering harmful content and violation of terms and causing significant and long-term risks to Facebook and its investors.
3. **Facebook's Material Misrepresentations and Omissions Include Mark Zuckerberg's Sworn Testimony to Congress.**

Whistleblower Aid is a U.S. tax-exempt, 501(c)(3) organization, EIN 26-4716045.

<http://WhistleblowerAid.org> — Anonymously via Tor Browser: <http://WBAidLW45QWV7H3.onion>  
Contact via SecureDrop over Tor: <http://whistlebloweraid.securedrop.org/onion> — via Signal App: [REDACTED]

4. For example, on October 28, 2020, Mark Zuckerberg testified before the U.S. Senate, and when Senator Mike Lee asked:

*"[D]o you state before this committee, for the record, that **you always apply your terms of service equally to all of your users?**" (emphasis added)*

5. Mark Zuckerberg responded:

*"I **certainly don't think we have any intentional examples where we're trying to enforce our policies in a way that is anything other than fair and consistent.**" (emphasis added)*

6. Further, Mark Zuckerberg testified:

*"Incitement of violence is against our policy and there are not exceptions to that, **including for politicians.**" (emphasis added)*

7. Likewise, on November 17, 2020, Mark Zuckerberg testified before the Senate:

*"We took our responsibility for protecting the integrity of this election seriously. . . . We worked hard to **apply those policies fairly and consistently.**" (emphasis added)*

8. This follows Mark Zuckerberg's testimony before the U.S. House of Representatives in 2018, and when Rep. McMorris-Rodgers asked:

*"And **what is Facebook doing to ensure that its users are being treated fairly and objectively by content reviewers?**" (emphasis added)*

9. Mark Zuckerberg testified:

*" . . . **we take a number of steps to make sure that none of the changes that we make are targeted in any kind of biased way.** . . . I agree that this is a serious issue . . . we make a relatively small percent of mistakes in content review . . . I **wouldn't extrapolate from a few examples to assuming that the overall system is biased.**" (emphasis added)*

<sup>1</sup><https://www.wv.com/blog/transcripts/tech-ocsc-senate-testimony-transcript-october-28/>

<sup>2</sup><https://www.wv.com/blog/transcripts/tech-ocsc-senate-testimony-transcript-october-28/>

<sup>3</sup><https://www.pulitzercenter.org/sites/default/files/2020/11/17/20201117-Transcript.pdf>

<sup>4</sup>[https://energycommerce.house.gov/sites/edemocrats.energycommerce.house.gov/files/documents/20180411\\_FC%20Facebook%20Transparency%20brief%20Use%20of%20Consumer%20Data.pdf](https://energycommerce.house.gov/sites/edemocrats.energycommerce.house.gov/files/documents/20180411_FC%20Facebook%20Transparency%20brief%20Use%20of%20Consumer%20Data.pdf)

10. In March and May 2021, Mark Zuckerberg and Facebook continued to represent:

**"people . . . want to know that when platforms remove harmful content, they are doing so fairly and transparently."**<sup>43</sup> (emphasis added)

**"We strive to enforce our policies consistently . . . Our Community Standards apply to all content, and we assess everyone under those Standards. When we identify or learn of content that violates our policies, we remove that content regardless of who posted it . . . Facebook's Terms and Policies are available here: <https://www.facebook.com/policies>. Facebook's Community Standards are available at <https://www.facebook.com/communitystandards/>. Both are global and apply to all accounts on Facebook."**<sup>44</sup> (emphasis added)

11. Facebook Has Made Misstatements in Securities Filings and Related Records.

12. For example, Facebook has repeatedly represented its "transparency," "integrity," and "visibility," including in its filed 10-K statements in January 2021<sup>45</sup> and January 2020<sup>46</sup> and its 10-Q statement in July 2021,<sup>47</sup> as well as quarter results conference calls in 2021<sup>48</sup> and July 2020, stating to investors and the public:

**"[We] also have clear community standards and guidelines that we enforce fairly . . ."**<sup>49</sup> (emphasis added)

13. In its Notice of Annual Meeting and Proxy Statement in 2021,<sup>50</sup> it also emphasized:

**"We publish quarterly Community Standards Enforcement Reports that track our progress on enforcing our content policies . . . We regularly publish Transparency Reports to give our community visibility into how we enforce policies . . ."**

14. Facebook Has Made Statements in its Public Pages and Guidelines.

15. Facebook's "Cross Check" page and policies represented since at least 2018:

<sup>43</sup><https://docs.house.gov/meetings/IF/IF16/20210325/111407444RC-117-IF16-Wstate-ZuckerbergM-20210325-01.pdf>  
<sup>44</sup><https://docs.house.gov/meetings/IF/IF16/20210325/111407444RC-117-IF16-Wstate-ZuckerbergM-20210325-03004.pdf>  
<sup>45</sup><https://www.sec.gov/Archives/edgar/data/1326801/000132680121000013/b1-12312018x10k.htm>  
<sup>46</sup><https://sec.report/Document/0001326801-21-000049>

<sup>47</sup>[https://d21z4tdh.com/329680738/files/doc\\_financials/2021q4/IF16-Q4-2020-Conference-Call-Transcript.pdf](https://d21z4tdh.com/329680738/files/doc_financials/2021q4/IF16-Q4-2020-Conference-Call-Transcript.pdf)  
<sup>48</sup>[https://d21z4tdh.com/329680738/files/doc\\_financials/2021q2/Q220-FB-Follow-Up-Call-Transcript.pdf](https://d21z4tdh.com/329680738/files/doc_financials/2021q2/Q220-FB-Follow-Up-Call-Transcript.pdf); see also  
<sup>49</sup><https://about.fb.com/news/2018/07/working-to-keep-facebook-safe/>  
<sup>50</sup><https://www.sec.gov/Archives/edgar/data/1326801/000132680121000012/facebook2021definitivexposr.htm>

***"We want to make clear that we remove content from Facebook, no matter who posts it, when it violates our standards. There are no special protections for any group . . ."***<sup>17</sup> (emphasis added)

See also: "If someone posts something that breaks our Standard and their page was Cross-Checked, we would still remove that content from Facebook after double-checking this was the correct decision."<sup>18</sup>

16. Continuing through June 2021, after Facebook's "independent Oversight Board" upheld the decision to suspend Donald Trump's account and requested that Facebook, among other things, "act quickly on posts made by influential users that pose a high probability of imminent harm," Facebook stated:

*"For content that will likely be seen by many people, we may employ a cross check system to help ensure that we are applying our policies correctly . . . Our Community Standards apply around the world to all types of content and are designed so they can be applied consistently and fairly to a community that transcends regions, cultures, and languages . . . We employ an additional review, called our cross check system, to help confirm we are applying our policies correctly for content that will likely be seen by many people . . . We want to make clear that we remove content from Facebook, no matter who posts it, when it violates our Community Standards. There is only one exception — and that is for content that receives a newsworthiness allowance . . . Cross check simply means that we give some content from certain Pages or Profiles additional review . . ."* (And when asked to report on error rates and thematic consistency of determinations made through the Cross Check process, Facebook responded: "it is not feasible to track this information."<sup>19</sup> (emphasis added)

17. In committing to an "independent Oversight Board," Facebook represented:

*"we have created and empowered a new group to exercise independent judgment over some of the most difficult and significant content decisions . . . they are truly autonomous in their exercise of independent judgment."<sup>20</sup>*

<sup>17</sup> <https://about.fb.com/news/2019/02/working-to-keep-facebook-safe/>

<sup>18</sup> <https://about.fb.com/wp-content/uploads/2018/07/fb-to-freedom-likes-10-07-181.pdf>

<sup>19</sup> <https://about.fb.com/wp-content/uploads/2021/05/Facebook-Responseto-theOversight-Board-Recommendations-in-Trump-Cases.pdf>, see also

<https://oversightboard.com/news/226672455888529-oversight-board-upholds-trump-or-easterly-https://www.foxnews.com/facebook/fbi-to-impose-penalty-oversight-board-decision-regarding-donald-trump>

<sup>20</sup> <https://about.fb.com/news/2020/05/working-with-the-oversight-board/>

18. In addition, Facebook's Community Standards state:

***"Our Community Standards apply to everyone, all around the world, and to all types of content."<sup>17</sup>***

19. Facebook also advertises "Commitment to Transparency," stating:

*"We're also launching a redesign of our Transparency Center to make it easier for people to find what they need. Our Transparency Report also includes the Community Standards Enforcement Report for Q1 of 2021, which provides data on how we take action against violating content across our platforms."<sup>18</sup>*

*"We publish regular reports to give our community visibility into how we enforce our policies."<sup>19</sup>*

*"This is why we have the Facebook Community Standards and Instagram Community Guidelines, which define what is and is not allowed in our community."<sup>20</sup>*

20. Turning to its "Transparency Center," Facebook has represented its "consistent" enforcement since at least 2017 up through at least the summer of 2021:

***"Facebook's review teams are trained to ensure that their content decisions are accurate and consistent . . . we may employ additional reviews for high-visibility content that may violate our policies . . . This process, which we refer to as cross-check, means that our review teams will assess this content multiple times . . . It also helps us verify that when content violates our policies, including from public figures or popular Pages, we consistently remove it."<sup>21</sup> (emphasis added)***

*"We remove content that goes against our policies . . ."<sup>22</sup>*

<sup>17</sup> <https://www.facebook.com/communitystandards/>

<sup>18</sup> <https://about.fb.com/news/2021/03/transparency-report-q1-2021/>

<sup>19</sup> <https://transparency.fb.com/data/?from=fb%3A%2F%2Ftransparency.facebook.com%2F>

<sup>20</sup> <https://transparency.fb.com/data/community-standards-information/>

<sup>21</sup> <https://transparency.fb.com/en/insights/detecting-violations/reviewing-high-visibility-content-accuracy/>

<sup>22</sup> <https://transparency.fb.com/en/insights/removing-violations/>

*"If your content goes against the Facebook Community Standards or Instagram Community Guidelines, the Facebook company will remove it."<sup>14</sup>*

21. However, these documents, including the Community Standards Enforcement Reports,<sup>15</sup> do not explain that in practice, the "XCheck" or "Cross-Check" system effectively "whitelists" high-profile and/or privileged users, enabling them to violate Facebook's terms, as shown by the enclosed documents.

22. Facebook's Records Confirm That Facebook's Statements Were False.

23. As the enclosed internal Facebook records show, Facebook's statements were false. For example, Facebook has confirmed:

*"over the years, many XChecked pages, profiles and entities have been exempted from enforcement."<sup>16</sup> (emphasis added).*

*In 2020, Cross Check entities were shielded from the majority of Integrity actions ("there are 109 daily xcheck exempted actions and 90 actions per daily without xcheck protection").<sup>17</sup>*

*"over the years, many XChecked people & entities have been exempted from enforcement. That means, for a select few members of our community, we are not enforcing our policies and standards. Unlike rest of our community, these people can violate our standards without any consequences . . . Since we currently review less than 10% of Checked content . . . without optimizing list of people XChecked. It would require significant investment in staffing (>10X increase)."<sup>18</sup> (emphasis added).*

*"This opens us up to a few different legal liabilities (caveat: I am not a lawyer). We currently apply XChecks on official government figures, but not on candidates . . . definitely more prevalent on the local or state level . . . this creates legal liability w/ campaign finance."<sup>19</sup>*

*"X-Check, like all components, has a cost and a benefit to the company. . . The Cost of X-Check can be quantified by bad VPVs. This is the count of*

<sup>14</sup><https://transparency.fb.com/en/newsroom/taking-action-taking-down-violating-content/>

<sup>15</sup>See e.g., <https://about.fb.com/news/2021/05/community-standards-enforcement-report-q1-2021/>

<sup>16</sup>Whistlebug, p. 1.

<sup>17</sup>See [REDACTED] Adding Civic Users to Xcheck Document, p. 11.

<sup>18</sup>[REDACTED] Sample Protection, p. 7.

<sup>19</sup>[REDACTED] Integrity Issues to Fight Racial Injustice Document, p. 3.

views accruing to content that should have been removed, but the removal was blocked by X-Check.”<sup>68</sup>

“All together there are 229K confirmed Civic entities (per 07/25 data), 180k are protected by XCheck . . . There are another 19M entities in probably Civic list (per 07/25 data), 757K are protected by XCheck . . .”<sup>69</sup>

“On June 1, a video containing NCII (non-consensual intimate imagery), was posted to the Instagram account and Facebook page associated with global . . . star . . . **A delete action was blocked at scaled support and escalated to . . . XCheck queues where it remained over a weekend . . . in that time, it amassed 56 Million views, video was XChecked, leading to longer review time and therefore more BVPV . . . Safety OS doesn’t have permissions to override XCheck.**”<sup>70</sup> (emphasis added)

“**We are exempting certain people and businesses from our policies and standards, at various stages of integrity lifecycle – exemptions from detection, strike accrual and enforcement . . . This undermines our fairness and legitimacy efforts; creates legal and compliance risks for the company . . . Based on an initial company-wide audit, this problem is pervasive across the country . . . Why is this a problem? Exempting (aka whitelisting) specific people and entities creates numerous legal, compliance, PR risks for the company and harms our community . . .**”<sup>71</sup> (emphasis added)

#### 24. Facebook Has Publicly Admitted This is a Material Issue.

25. In its public securities filings (e.g., 10-K,<sup>72</sup> 10-Q,<sup>73</sup> and Proxy Statement<sup>74</sup>) and other records, Facebook has conceded:

“We are making significant investments in . . . content review efforts to combat misuse of our services. . . . Any of the foregoing developments may negatively affect user trust and engagement, harm our reputation and brands, require us to change our business practices in a manner adverse to our business, and adversely affect our business and financial results.”

<sup>68</sup> [REDACTED] X-Check Get Well, p. 1.

<sup>69</sup> [REDACTED] Adding Civic Users to X-Check Document, p. 4.

<sup>70</sup> [REDACTED] Mistake prevention incident list, p. 14.

<sup>71</sup> [REDACTED] The “Whitelisted” Problem, multiple pages.

<sup>72</sup> <https://www.sec.gov/edgar/disclosure/0001328601-21-000214/>

<sup>73</sup> <https://www.sec.gov/edgar/disclosure/0001328601-21-000349/>

<sup>74</sup> <https://www.sec.gov/edgar/disclosure/0001328601-21-000022/facebook2021definitiv.htm>

"Our brands may also be negatively affected by . . . decisions or recommendations regarding content . . ."

"Our advertising revenue can also be adversely affected by a number of other factors, including: . . . reductions of advertising by marketers due to our efforts to implement or enforce advertising policies that protect the security and integrity of our platform."

". . . the substance or enforcement of our community standards, the actions of our users, the quality and integrity of content shared on our platform, or the actions of other companies that provide similar services to ours, has in the past, and could in the future, adversely affect our reputation."

26. Likewise, Facebook's Community Standards (Stakeholder Engagement) confirm:

"Given the impact of our Community Standards on society, it's critical for us to create a policy development process that's not only inclusive and based on expert knowledge, but also transparent. We know from talking to hundreds of stakeholders that opening up our policy-making process helps build trust. The more visibility we provide, the more our stakeholders are likely to view the Community Standards as relevant, legitimate, and based on consent."<sup>66</sup>

27. **Role for the SEC.** The SEC is charged with enforcing the laws that protect investors in public companies like Facebook. Facebook's investors care about misrepresentations and omissions by Mark Zuckerberg and other Facebook executives because consistent and fair applications of its policies, or lack thereof, and integrity and transparency matter to users and advertisers, and therefore affect Facebook's advertising revenue and corporate profits. Further, some shareholders would not want to invest in the company if they knew the truth about Facebook's special treatment for high-profile users.

28. 

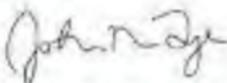
<sup>66</sup> [https://www.facebook.com/communitystandards/stakeholder\\_engagement](https://www.facebook.com/communitystandards/stakeholder_engagement)

[REDACTED]

29 [REDACTED]

30. Whistleblower Aid is a non-profit legal organization that helps workers report their concerns about violations of the law safely, lawfully, and responsibly. We respectfully request the SEC's assistance ensuring that our client never faces actual or threatened retaliation.
31. We plan to continue supplementing this disclosure with additional information and evidence. Our client would be happy to meet with investigators at your convenience. Please feel free to contact us using the information below.
32. We are representing an anonymous whistleblower who is making the above disclosures solely for reporting the suspected violation of laws as outlined.

Sincerely,



John N. Tye, Attorney at Law  
Chief Disclosure Officer

[REDACTED]



Andrew Bakaj, Attorney at Law  
Of Counsel

[REDACTED]



— ANONYMOUS WHISTLEBLOWER DISCLOSURE —

Karl Kronenberger, Attorney at Law  
Kronenberger Rosenfeld, LLP

Enclosures:

“Whitelist” Problem  
Mistake prevention incident list some XCheck

**Other internal Facebook documents —**

Mistake Prevention XCheck (Cross Check) Get Well  
XCheck (Cross Check) Get Well Plan  
Whitelist Where We Are  
Integrity Ideas To Fight Racial Injustice  
Cross Check  
Whitelisting  
XCheck (Cross Check) Get Well  
Adding Civic Users to XCheck  
Civic Actors  
XCheck (Cross Check)  
Cross Check Wiki  
Mistake Prevention for XCheck Exemption  
Political Influence in Content Policy  
Comparing the effects of misinfo  
White List contradicts Facebook stated principles

REDACTED FOR CONGRESS

# Exhibit 81

Apr 16, 2018, 01:01pm EDT

# Why Facebook Will Never Change Its Business Model



**Len Sherman** Former Contributor ⓘ

Leadership Strategy

*I write about management priorities for long-term growth.*

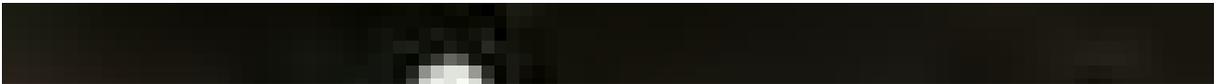
Follow

---

*This is the first of a three-part series on Facebook's business model, management priorities and how you can help reduce the company's harmful societal impacts.*

1. *Why Facebook Will Never Change Its Business Model*
2. *Zuckerberg's Broken Promises Show Facebook Is Not Your Friend*
3. *Zuckerberg's Promises Won't Fix Facebook, But You Can*

By most accounts, Mark Zuckerberg's Congressional testimony last month was a resounding success. From beginning to end, Facebook's market cap increased by \$34 billion. There were few bombshell revelations. Zuckerberg got to roll out his well practiced contrition act *again* as Facebook's apologizer-in-chief. Dozens of Congressional representatives got to look earnest, outraged and informed for a few minutes of valuable evening local news coverage. The press got bonus points for explicating techspeak terms like shadow profiles and tracking cookies. And millions of consumers shrugged off ten hours of mind-numbing proceedings by indulging in a daily routine of sharing their innermost thoughts on Cardi B's baby bump or liking pictures of the cutest grandkids in the world. In short, millions of Americans went on with their habits and comforts of living in Mark Zuckerberg's world.





Mark Zuckerberg testifies before a joint hearing of the Senate Judiciary and Commerce Committees in... [+]

By now, it's widely understood that Facebook's voracious appetite for user data is driven by their business model which charges advertisers for access to precisely targeted segments of their massive consumer database. No one knows more about more consumers than Facebook.

During the hearings, several Congressmen asked Zuckerberg whether he would consider changing Facebook's business model. Here's [a sample](#) of the exchanges in which Zuckerberg bobbed and weaved, but ultimately refused to answer the question.

*Anna Eshoo (D-CA):* Are you willing to change your business model in the interest of protecting individual privacy?

*Zuckerberg:* Congresswoman, we are — have made and are continuing to make changes to reduce the amount of ...

*Anna Eshoo:* No, are you willing to change your business model in the interest of protecting individual privacy?

*Zuckerberg:* Congresswoman, I'm not sure what that means.

*Frank Pallone (D-NJ):* I'd like you to answer yes or no, if you could. Will you make the commitment to changing all the user default settings to minimize, to the greatest extent possible, the collection and use of users' data?

*Zuckerberg:* Congressman, this is a complex issue that I think deserves more than a one-word answer.

Ignoring Zuckerberg's rehearsed procrastination and prevarication, allow me to provide a one-word answer to the Congressmen's questions: NO! And for good reason... two reasons, actually.

First, Facebook has built arguably the best business model in the world, achieving the trifecta of high scale *and* high growth *and* high profit margins unmatched by any high tech company, including Google, Amazon, Apple, and Netflix. Facebook's astonishing financial success is captured by the mnemonic 50/50/50/500: in round numbers, a \$50 billion annual revenue run rate, growing at 50% per year with a 50% operating income margin, generating a market cap of nearly \$500 billion.



Other companies can only dream of running a company with essentially:

- No cost of goods sold (individual users and companies provide content for free)
- No marketing costs (user word-of-mouth and viral network effects spur continuous growth)
- No selling costs (most advertisements are purchased through a self-service, automated ad placement platform)

If you were in charge of such a money-making machine, would you be eager to change this business model?

But if Facebook provides such a valuable service to its more than 2 billion users, several Congressmen wondered aloud why the company couldn't replace its ad-supported business model with user fees? Zuckerberg responded with a maudlin regurgitation of Facebook's mission to "give people the power to build community and bring the world closer together," which, he explained could only be accomplished with a free service.

Zuckerberg [amplified on this theme](#) in his recent war of words with Apple CEO Tim Cook, who had publicly chastised Facebook for selling access to user data. Zuckerberg called Cook's comments "extremely glib and not at all aligned with the truth," going on to say:

*The reality here is that if you want to build a service that helps connect everyone in the world, then there are a lot of people who can't afford to pay. And therefore, as with a lot of media, having an advertising-supported model is the only rational model that can support building this service to reach people...But if you want to build a service which is not just serving rich people, then you need to have something that people can afford.*

Zuckerberg's impassioned rhetoric suggests that Facebook's primary concern is to provide an affordable, valued service to its vast global community of users, many of whom have limited disposable income. But the second real reason Facebook is committed to its current business model is that the price advertisers are willing to pay Facebook to invade users' privacy is vastly greater than the price most consumers would be willing to pay Facebook to protect their privacy.

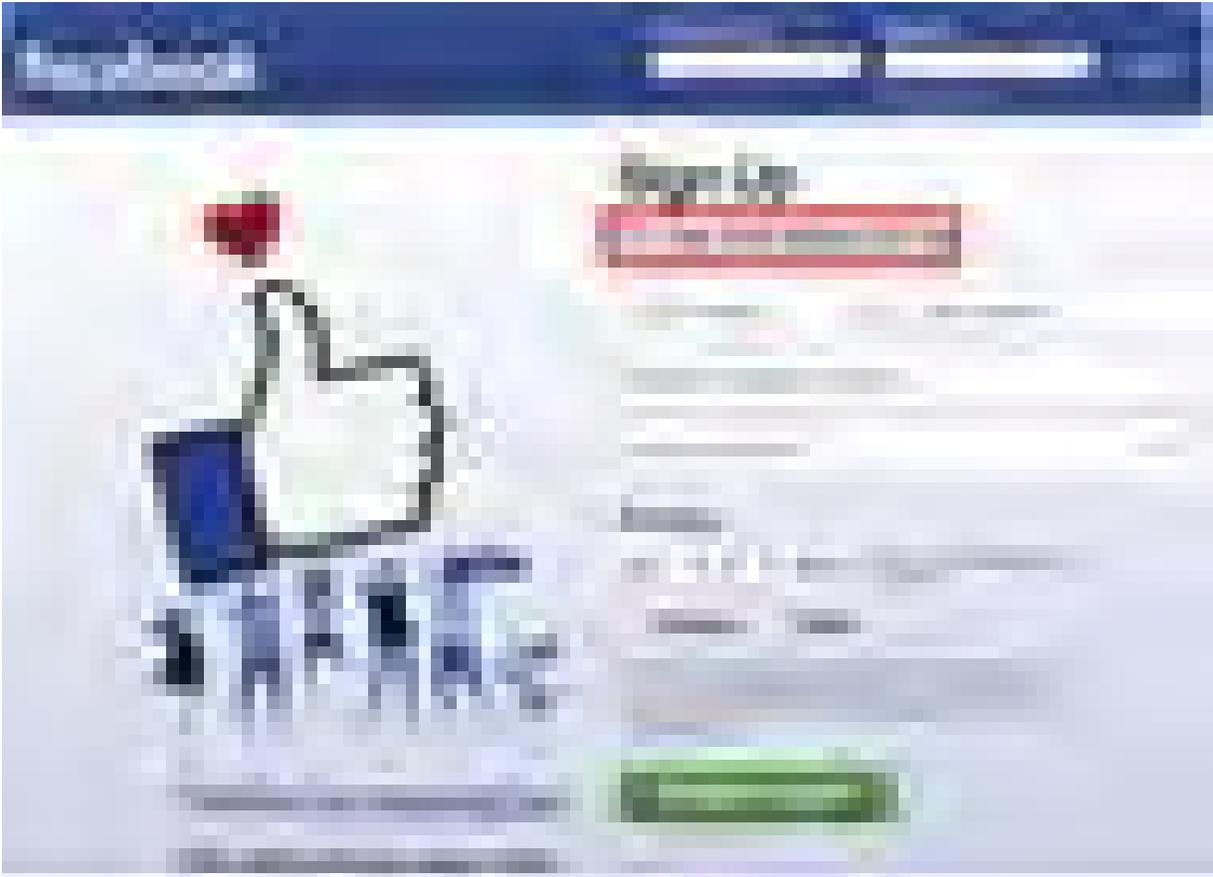
To see this, consider that in 2017, Facebook's average revenue per user (ARPU) in North America was \$84.41. To replace this revenue in an ad-free service, Facebook would have to charge each user at least an amount equivalent to its current ARPU. How many members of the Facebook "community" (as Zuckerberg is fondly wont to call it) would be willing to pay this amount for the privilege of not seeing ads they never asked for and not being surveilled across the Internet? Not many.

A [recent survey](#) of US Facebook users found that fewer than 10% would be willing to pay the current advertising ARPU for an ad-free service. As such, if Facebook charged user fees equivalent to its ARPU, its community would shrink dramatically, diminishing the value to remaining users, who now would have to pay 10X the current ARPU to make up for the 90% of users who would abandon the platform. How does an annual user fee of almost \$1,000 sound for an ad-free Facebook serving a minuscule user base? In perhaps his most cogent and truthful comment on the logic for charging user fees, Zuckerberg [noted](#): "that sounds ridiculous to me!"

Facebook has compelling reasons to be committed to its current business model. It is therefore disingenuous and gallingly inaccurate for Zuckerberg to justify his company's business practices by [comparing Facebook](#) with "a lot of media, having an advertising-supported model as the only rational model that can support building this service to reach people." In reality, Facebook has hollowed out the readership and drained the advertising

revenues from media companies, causing many to shift to subscription-based revenue sources for survival.

Lest you have any doubt on Facebook's abiding and entirely logical commitment to an ad-supported business model, check out Facebook's promise on its sign-on page for new users: "It's free and always will be" (emphasis added in the exhibit below).



Facebook sign-on page for new users [WWW.FACEBOOK.COM](http://WWW.FACEBOOK.COM)

So if Facebook's ad-supported business model has been very beneficial for the company and its shareholders, what about the rest of us? If we learned anything from last week's Congressional hearings, it's that the societal risks posed by Facebook and other social media platforms are greater than ever, but the prospects for effectively mitigating those risks remain remote. I'll explore the most troubling aspects of living in Mark Zuckerberg's world in my next post.

*Follow me on [Twitter](#) or [LinkedIn](#). Check out my [website](#).*



**Len Sherman**

Follow

I am an Executive in Residence and Adjunct Professor at Columbia Business School, teaching... **Read More**

Reprints & Permissions

ADVERTISEMENT

---

# Exhibit 82

[Tech](#)

# Zuck is a lightweight, and 4 more things we learned about Facebook from 'An Ugly Truth'

Facebook is such a hot mess, a major new book about it is already out of date. But its underlying lessons are timeless.

By [Chris Taylor](#) July 17, 2021  





 > Tech

*Stay updated with the latest in Tech, Science, Culture, Entertainment, and more by following our Telegram channel [here](#).*

Here's the challenge of writing about the hot mess that is Facebook in 2021 — the mess is so hot, your take is soon out of date.

---

published, we learned Facebook seems to be [burying data that highlights its right-wing echo chamber](#). It just came under fire from [President Biden for "killing people"](#) with vaccine lies, and from [English footballers for allowing racist abuse](#) on their pages.

Oh, and the FTC's antitrust case against the social media giant, which fills the first chapter, was [just denied by a federal judge](#). Oops.

But with the exception of the FTC case, which [may yet be refiled](#), none of this news will come as a surprise to the book's readers. Frenkel and Kang's careful reporting shows a company whose leadership is institutionally ill-equipped to handle the Frankenstein's monster they built. Ignoring hate speech and lies on the platform, even when experts are sounding alarms about harmful effects up to and including genocide, is par for the course. As is trying to control the media narrative or silencing employees rather than, y'know, doing something about the underlying problem.

It's not that CEO Mark Zuckerberg and COO Sheryl Sandberg come across as inherently evil; they seem genuinely shaken by each new crisis, evolve their thinking a little, and belatedly order fixes. It's more that their airy idealism, total faith in algorithms, plus endless profits, put them in bubbles where they are blind to bad actors and bad ideas.

"People were not paying attention," Facebook's former security chief Alex Stamos tells the authors. He's talking about engineers who were able to stalk their dates with god-like access to their profiles (and were belatedly fired for doing so). But it could apply to everything from election interference to stolen user data to the



So if you need more reasons to [delete Facebook apps](#) from your life, here are the main points we gleaned from *An Ugly Truth* — a book that mostly focuses on the years 2016 to 2020, but doesn't ignore the original sins baked into Facebook from the very beginning.

## 1. Zuckerberg, an 'intellectual lightweight,' was easy to manipulate.

To be fair, plenty of us thought dumb stuff when we were 20. But few of us were laying the foundations for a history-changing global addiction at the time. From the start, Zuckerberg designed the platform for mindless scrolling: "I kind of want to be the new MTV," he told friends. His mantra for employees was "company over country": Do what is good for Facebook, not for America.

Forget *The Social Network*; a more up-to-date cautionary tale would cut straight from this declaration to the Jan. 6 insurrection being plotted in Facebook groups.

It was 20-year-old Zuckerberg who fell under the sway of Peter Thiel and Marc Andreessen, Silicon Valley libertarians and free-speech fundamentalists. He didn't read books at the time (veteran Valley journo Kara Swisher found him an "intellectual lightweight") and inherited a view of the First Amendment that one NAACP voting rights expert calls a "dangerous misunderstanding." Instead of protecting people from government censorship, Zuck's platform would protect and amplify the speech of authoritarian leaders. Conservatives would learn they could work the referee simply by claiming they were being censored.

Once set in place, Zuckerberg's views were hard to shift — and when they did, they often managed to morph into more disastrous forms. His [response to an epidemic of fake news on the site in 2016 was to downgrade all news](#) in the algorithm's

---

DNA." Then, when the Cambridge Analytica scandal laid bare the need for privacy, he pushed for private Facebook groups — which provided safe harbor for [murderous militias](#), [QAnon believers](#) and [insurrectionists](#).

But Zuck's unexamined privilege hurts Facebook users in everyday ways too. "He couldn't identify the systemic biases of the world: how, if you were Black, you might attract ads for predatory loans, or if you were lower income, you might attract ads for junk food and soda," the authors write. The full effects of Facebook addiction may take decades to unpack.

## **2. Sheryl Sandberg is a Pollyanna, with less power than we knew.**

Former Google exec Sandberg was long seen as the adult supervision at Facebook. She took on all the leadership roles that didn't interest Zuckerberg — including growing the ad business that supercharged revenue. Behind the scenes, it was assumed that the *Lean In* author was a moderating influence on Zuck's more clueless or dangerous designs for the service.

Not so, turns out. "I've been consistently puzzled about the public portrayal of them as amazing partners," one business-side employee tells the book's authors.

"Meetings I've been in with Mark and Sheryl, he was explicitly dismissive of what she said." Indeed, the book provides examples where Sandberg was afraid of getting fired, or being labeled as politically biased, and didn't even try to push back — such as the case of [the doctored video of Nancy Pelosi](#) that Zuckerberg decided to allow on the site. Pelosi still won't return Sandberg's calls.

"To friends and peers, Sandberg tried to disassociate herself from Zuckerberg's positions, but within the company she executed his decisions," the authors write.

Part of her perfectionism manifests in a desire to focus on the positive — to a Pollyanna-ish degree. Sandberg's conference room is named "Only Good News," and it's a fair summary of what she wants to hear from underlings. She quickly dismissed the notion that Russian-bought election ads spread further on the platform than was initially known, and screamed "you threw us under the bus" at then-CSO Stamos for telling the Facebook board what he knew about the situation.

Like a lot of execs who didn't bring only good news, Stamos was gradually pushed out.

### **3. Joel Kaplan may be the most dangerous man at Facebook.**

A friend (and briefly former boyfriend) of Sandberg's, Joel Kaplan is a veteran of the George W. Bush administration who heads up Facebook's lobbying arm in Washington D.C. He's a very close friend of Justice Brett Kavanaugh, and showed up to support the controversial judge at his Supreme Court appointment hearings while on the clock for Facebook. He has Zuckerberg's ear on political matters, and on the evidence of *An Ugly Truth* he is more influential than Sandberg when it counts.

Kaplan may have been a Never Trump Republican in his personal beliefs, but in practical fact he was the best friend Donald Trump had at Facebook. It was Kaplan who, in Dec. 2015, persuaded Zuckerberg not to take down Trump's first post calling for a Muslim ban. "Don't poke the bear," he advised, so instead Facebook carved out an exemption for hate speech if it was "newsworthy." This brand-new standard for what billions of people could see from a candidate arguably helped hand a close election in 2016 to Trump.

---

video up, Kaplan who helped kill a ["Trending" news](#) section when conservative politicians complained about it — laying the groundwork for the domination of Facebook's algorithm by right-wing radio hosts like Dan Bongino and Ben Shapiro.

In 2019, Kaplan engineered Zuckerberg's two meetings with Trump. In 2020, he argued that Trump didn't actually suggest injecting bleach as a COVID-19 cure, therefore didn't fall foul of Facebook's rules on medical misinformation. He likewise defended Trump's "when the looting starts, the shooting starts" comment during the George Floyd protests, and when Facebook belatedly started cracking down on QAnon groups in August, it was Kaplan who made sure that antifa-related groups were also banned. Engineers admitted that such "both sides" behavior was entirely political.

All of that appeasement, and for what? Trump was banned indefinitely anyway, but not before doing potentially irreparable harm to democracy by [spreading the Big Lie](#). Government regulation of Facebook, the one thing Kaplan was trying to avoid, is now just about the only proposal that unites left and right in Washington. And yet Kaplan's position seems more secure than ever — cemented by an alliance with policy chief Nick Clegg, who knows President Biden from his time as UK deputy Prime Minister.

#### **4. Employees are fighting the good fight.**

If anything can save Facebook from itself, it's the ground-level employees of Facebook. Time and again, in posts on the company's internal Workplace groups known as "Tribes," and in Zuckerberg's weekly Q&As, they are the ones forcing the uncomfortable questions.



---

Bosworth that gave the book its title. Boz wrote that the "ugly truth" was that connecting the world's people might lead to more deaths, but that Facebook would continue no matter what. Boz later claimed he was only trying to "inspire debate," but employees held his feet to the fire regardless.

Next to face the workers' fury was Kaplan, for his overt support of Kavanaugh; employees dismissed Zuckerberg's falsehood that he had taken time off to do so. When Trump's post about shooting looters was allowed to stand, engineers on Tribe boards were openly asking if there were jobs at companies "willing to take a stance on their moral responsibility to the world—because Facebook doesn't seem to be it." An internal poll showed thousands of employees believed Zuck had made the wrong decision, and the company's [first employee walkout](#) followed.

The one positive trend in *An Ugly Truth* is that employee statements, actions, and leaks to the media are getting bolder and clearer. "Stop letting people be racist on Facebook, maybe then we will believe that you support racial justice," a member of the Black@Facebook internal group wrote in 2020. We're a long way from Zuckerberg having to tell his employees [not to deface Black Lives Matter signs](#) on campus. These days, the education appears to be flowing the other way.

## 5. Facebook must listen to more experts — inside and out

Employee intentions are great, but they're nothing without management taking action and creating guidelines. In 2008, the first team responsible for moderating Facebook posts had only vague rules that there should be "no nudity, no terrorism" and a general desire that was summed up as "don't be a radio for a future Hitler."

How'd that work out?

---

[genocide](#) in 2018. An expert in the country, Matt Schissler, was sounding the alarm to Facebook representatives back in 2014. Visiting the Menlo Park HQ, Schissler showed a post that had gone viral with a picture of a man feeding Muslim refugees; the man had become a target for death threats for doing so. To take down the picture, Facebook told him, the man would have to complain himself — even though he wasn't on Facebook.

Schissler was equally horrified to learn that the Facebook reps "seemed to equate the harmful content in Myanmar to cyberbullying," and that there was one Burmese speaker hired by the company to police the whole country's content. (Burmese is only one of dozens of languages spoken in the country.) "It would be like them saying, well, we have one German speaker, so we can monitor all of Europe," Schissler tells the authors.

In the end, his complaints got about as much traction as Stamos and other election security experts hired then eased out by Facebook. Which is to say, none at all.

Zuckerberg appears belatedly aware of the value of expertise — at least, in as much as it can take tough decisions off his plate. That was the thinking behind the [Facebook Oversight Board](#), which rightly put the question of whether Trump should be banned from the platform permanently back in the CEO's court.

Depending on what action Zuckerberg takes next, and its impact on the 2022 and 2024 elections, *An Ugly Truth* may end up being a relatively lightweight prologue to a coming Facebook dystopia.

**Follow Mashable SEA on [Facebook](#), [Twitter](#), [Instagram](#), and [YouTube](#).**



**TOPICS:** [Facebook](#), [Tech](#), Tech Industry

---



---

## Recommended For You

### **New Porsche Taycan GTS has the best range in the lineup**

There's also a GTS Sport Turismo-variant.

Nov. 17, 2021, 5:05 p.m.

### **Young S'poreans win global James Dyson Award for clever glaucoma testing kit**

Hope for glaucoma patients.

Nov. 17, 2021, 4:48 p.m.

### **How to file a claim for a piece of TikTok's US\$92 million class action lawsuit**

It's super quick to apply online.

Nov. 17, 2021, 1:05 a.m.

### **How to add a Legacy Contact with iOS 15**

It's a little morbid to think about, but it's a very useful feature.

Nov. 16, 2021, 10 p.m.

### **A huge number of Twitter users don't realise their accounts are public, study finds**

That's a big percentage.

Nov. 16, 2021, 7:44 p.m.

---

## Trending on Mashable

### **How to file a claim for a piece of TikTok's US\$92 million class action lawsuit**

It's super quick to apply online.



---

## **How to add a Legacy Contact with iOS 15**

It's a little morbid to think about, but it's a very useful feature.

Nov. 16, 2021, 2 p.m.

## **Impossible meatballs are here, and they're better than Beyond**

They're even better than some store-bought beef meatballs.

Nov. 16, 2021, 1:32 p.m.

## **Woman is 2nd known person to 'cure' herself of HIV without medical treatment**

Medical experts believe her immune system may have flushed out the virus naturally.

Nov. 17, 2021, 4:26 a.m.

## **Young S'poreans win global James Dyson Award for clever glaucoma testing kit**

Hope for glaucoma patients.

Nov. 17, 2021, 8:48 a.m.

---



Change Region 



Mashable SEA is operated under license by REV Media Group

IN THE SUPERIOR COURT FOR THE DISTRICT OF COLUMBIA  
CIVIL DIVISION

MUSLIM ADVOCATES,

*Plaintiff,*

v.

MARK ZUCKERBERG, *et al.*,

*Defendants.*

Case No.: 2021 CA 001114 B

Judge Anthony C. Epstein

Exhibit B

IN THE SUPERIOR COURT FOR THE DISTRICT OF COLUMBIA  
CIVIL DIVISION

MUSLIM ADVOCATES,

*Plaintiff,*

v.

MARK ZUCKERBERG, *et al.*,

*Defendants.*

Case No. 2021 CA 001114 B

DECLARATION OF ERIC NAING

I, Eric Naing, declare the following based on my personal knowledge.

1. I am older than 18 years old;
2. I have worked at Muslim Advocates from January 2019 to present. During my tenure, I have served as the head of the organization's communications operations. From January 2019 to May 2021, I held the title of Communications Officer. From May 2021 to September 2021, I held the title of Senior Communications Manager. In September 2021, my title changed to Communications Director, a title I hold to date.
3. Muslim Advocates is a 501(c)(3) non-profit organization.

4. In my current role as Communications Director, my duties include: creating and implementing communication plans for campaigns, events, lawsuits, and key advocacy moments; managing all media relations; overseeing the production of written content for publications and presentations including press releases and statements, reports, speeches, op-eds, social media content and broadcast emails; monitoring news and social media for relevant breaking developments; managing the editorial integrity of public communications; and contributing to the organization's policy efforts, especially regarding hate speech on social media and technology companies.
5. Muslim Advocates has had a Facebook account since before I started here; I've been told we've had the account since January 2009.
6. For many years, Muslim Advocates has engaged in consumer protection advocacy, including work on making social media platforms safer for American Muslim communities. Examples of this advocacy include a 2014 report, *Click Here to End Hate*, that guided social media users through how to report online hate speech to the companies hosting the content. This advocacy also includes a 2020 webinar and fact sheet<sup>1</sup> sharing best practices with American Muslim mosques and organizations to protect their communities against digital hate directed toward online Ramadan events and other gatherings.

---

<sup>1</sup> Appended hereto as Exhibit 1 is a screenshot of an announcement of the webinar and fact sheet, *available at* <https://muslimadvocates.org/2020/04/ahead-of-ramadan-muslim-advocates-calls-for-mosques-to-protect-themselves-from-digital-hate/>.

7. Muslim Advocates also works on behalf of consumers in other ways, including through its Corporate Accountability project. That project seeks to ensure that consumers can enjoy the services of all corporations without encountering bias and hate.
8. At the time I started with Muslim Advocates, working with Facebook consumed a large percentage of the Policy team's time. My colleagues on the Policy team, including Naheed Qureshi and Madihha Ahussain, exhibited a willingness to continue to engage with Facebook at least in part because they kept promising that they'd hear us out and eventually take action.
9. Muslim Advocates' work with Facebook took up much of Muslim Advocates' resources and bandwidth such that we were unable to do other advocacy work.
10. Muslim Advocates has participated in events with Facebook where Facebook used Muslim Advocates to bolster its reputation. For example, I and my colleague Madihha Ahussain flew to Atlanta to participate in a town hall with Facebook and other civil rights groups in September 2019. At the town hall, Facebook represented to listeners that it took civil rights concerns seriously, pointing to our coalition's participation in the event.
11. To my knowledge, Defendants never disclosed to Muslim Advocates the internal discussions the company was having that pits the safety of the platform against the company's profitability. Nor did Defendants inform Muslim Advocates of the company's internal reports revealing that the company was misleading the public.

12. If Muslim Advocates had known that Defendants' representations were false and that Defendants would routinely refuse to remove content it knows of that violates Facebook's standards and policies, Muslim Advocates would not have spent its resources and staff time engaging with Defendants.
13. Muslim Advocates has stopped providing services to Facebook because Muslim Advocates has learned that Facebook does not actually remove hate speech (and other content that violates Facebook's community standards) of which it is aware.
14. Muslim Advocates initiated this lawsuit on behalf of and to vindicate the rights and interests of consumers within the District of Columbia--who used a service that operated differently than Facebook had represented it would--and to seek redress for the injuries it suffered itself when providing services to Facebook under false pretenses.

I declare under penalty of perjury that the foregoing is accurate to the best of my knowledge.



-----  
Signature

Nov. 16, 2021  
Date

# Exhibit 1

APRIL 21, 2020

Issues: Corporate Accountability, Fighting Bigotry

## Ahead of Ramadan, Muslim Advocates Calls for Mosques to Protect Themselves from Digital Hate

Press Release

SHARE ↗

### *Group Offers Guidance and Training to Safeguard Video Conferences*

WASHINGTON, DC – In advance of Ramadan and after an epidemic of digital attacks on Muslim gatherings, Muslim Advocates is calling on mosques and American Muslim organizations around the country to enact protocols to protect their constituents. The organization has [released a fact sheet](#) on best practices for protecting digital events and is hosting a webinar on **Wednesday, April 22 at 6 PM ET / 3 PM PT**, entitled “[Keeping Your Virtual Events Free from Hate in Ramadan.](#)”



6 PM ET / 3 PM PT, entitled "[Keeping Your Virtual Events Free from Hate in Ramadan.](#)"

"Our mosques have been vandalized and firebombed. Now that our religious gatherings have moved online, that hate is unfortunately following," said **Madihha Ahussain, Muslim Advocates' special counsel for anti-Muslim bigotry.** "Online mobs are organizing online: they're sharing meeting passwords and disrupting religious events, school classes and support groups with hate speech and obscene and violent images."

In the past few weeks, online mobs interrupted a [meeting of global Muslim leaders](#) with a racial slur, hijacked a [Muslim Student Association's Zoom meeting](#) and disrupted a [Muslim health forum](#) with hate speech. Muslim Advocates' webinar will include speakers from leading video conference companies who will offer important tips and guidance on protecting and securing virtual events.

**Additional Resources:**

- [Register Here: Keeping Your Virtual Events Free From Hate in Ramadan](#)
- [Face Sheet: Keeping Virtual Events Free from Hate](#)

*Muslim Advocates is a national civil rights organization working in the courts, in the halls of power and in communities to halt bigotry in its tracks. We ensure that American Muslims have a seat at the table with expert representation so that all Americans may live free from hate and discrimination.*

###



SHARE THIS ARTICLE:



## RELATED ARTICLES



NOVEMBER 5, 2021

**Muslim Advocates Declines New Jersey State Senators' Non-Apology for Anti-Muslim Tweet**

[READ MORE →](#)



NOVEMBER 4, 2021

**Muslim Advocates to New Jersey State Senator: Apologize for Anti-Muslim Tweets or Resign**

[READ MORE →](#)



IN THE SUPERIOR COURT FOR THE DISTRICT OF COLUMBIA  
CIVIL DIVISION

MUSLIM ADVOCATES,

*Plaintiff,*

v.

MARK ZUCKERBERG, *et al.*,

*Defendants.*

Case No.: 2021 CA 001114 B

Judge Anthony C. Epstein

Exhibit C

**IN THE SUPERIOR COURT FOR THE DISTRICT OF COLUMBIA  
CIVIL DIVISION**

MUSLIM ADVOCATES,

*Plaintiff,*

v.

MARK ZUCKERBERG, *et al.*,

*Defendants.*

Case No. 2021 CA 001114 B

**DECLARATION OF MADIHHA AHUSSAIN**

I, Madihha Ahussain, declare the following based on my personal knowledge.

1. I am older than 18 years old;
2. I have worked at Muslim Advocates from approximately August 2012 to August 2021.
3. Throughout this period of employment, my email address has been either fellow@muslimadvocates.org or madihha@muslimadvocates.org. I save emails in my work email application, where true and correct copies of my work emails can be found.
4. From approximately August 2012 through April 2017, I worked at Muslim Advocates as a legal fellow and a staff attorney in the policy department. In these roles, I worked with other policy staff in working to protect American Muslims from bigotry spread on social media and technology platforms.

5. From approximately May 2017 until August 2021, I was Muslim Advocates' Special Counsel on Anti-Muslim Bigotry and Senior Policy Counsel. In these positions, I led Muslim Advocates' work with social media and technology companies to improve content policies and user safety and flag relevant sensitive content and hate speech to platforms.

6. My work with social media and technology companies has focused on platforms like Facebook that have a broad reach.

7. I have worked with Facebook staff since at least 2013 to help educate them about how anti-Muslim bigotry spreads on their platform and the dangers this type of content poses to the community. This work has included flagging dangerous content and asking for its removal, sharing trends in anti-Muslim bigotry, detailing the real-world impact of anti-Muslim content on Facebook, sharing anecdotes of experiences Muslim community members had on Facebook, and offering suggestions to Facebook regarding improving its Community Standards on Hate Speech, Violent and Graphic Content, Violence and Incitement, Dangerous Individuals and Organizations, Coordinating Harm and Publicizing Crime, and Bullying and Harassment.

8. As part of this work to halt anti-Muslim bigotry on Facebook, I attended meetings and calls with Facebook employees. I also helped prepare other Muslim Advocates employees for calls and meetings with Facebook employees.

9. In my role at Muslim Advocates, I served as the point of contact for many members of the Muslim community who suffered because of or were concerned about hate speech on Facebook.

10. I have helped provide expertise on how platforms like Facebook can be used to threaten the safety of American Muslims and all people by pointing to the connection between on and offline behavior and sharing particularly egregious examples of online hate with the employees at these social media companies.

11. I have worked with dozens of mosques around the country on issues including responses to vandalism or threats of vandalism, unconstitutional surveillance by law enforcement, challenging biased mosque opposition and tracking armed protests.

12. I have actively monitored hate crimes targeting the American Muslim community around the country.

13. I would not have invested time in educating Facebook had they not assured me and my colleagues at Muslim Advocates that Facebook would enforce their Community Standards and take down anti-Muslim bigotry when they became aware of it.

14. Had it not been for Facebook's reassurances that the company takes down content that violates its Community Standards, Muslim Advocates would have spent more of its time and resources advocating for legislators to regulate the platform.

15. Had it not been for Facebook's reassurances that the company takes down content that violates its Community Standards, Muslim Advocates would have spent more of its time and resources toward engaging and educating the public regarding the dangers of the platform, as well as working on public campaigns criticizing Facebook for not removing hate from the platform to increase and mobilize public pressure for Facebook to enforce its Community Standards in the manner it says it does.

16. Many technology companies reach out to Muslim Advocates with requests for help with decisions related to content moderation. Because Muslim Advocates' staff time is limited, we are often forced to decline these requests. For example, Microsoft requested that Muslim Advocates send a representative to a convening on facial recognition and, because we were too busy with other work, we did not send a representative. Muslim Advocates is a member of Twitter's Trust and Safety Council but does not always send a representative to its meetings because of limited availability. Spotify has requested that Muslim Advocates consult with it to improve the experience of Muslims on its platform, but Muslim Advocates has from time to time had to decline that invitation. Muslim Advocates often did not engage about anti-Muslim hate speech on Google's YouTube platform because of its scarce resources.

17. Due to limited resources, many projects that were contemplated by Muslim Advocates were not undertaken.

18. In 2018, I spent at least 400 hours working to halt anti-Muslim bigotry on Facebook. In 2018, the staff of Muslim Advocates spent at least 1000 hours working to halt anti-Muslim bigotry on Facebook.

19. In 2019, I spent at least 250 hours working to halt anti-Muslim bigotry on Facebook. In 2019, the staff of Muslim Advocates spent at least 750 hours working to halt anti-Muslim bigotry on Facebook.

20. In 2020, I spent at least 300 hours working to halt anti-Muslim bigotry on Facebook.

21. I have personal knowledge that Muslim Advocates' former deputy director, Naheed Qureshi, spent an average of at least one hour per week from August 2013 until her departure from Muslim Advocates in 2021 on matters related to the presence of hate speech on Facebook. She often spent significantly more time than this. Much of this work would have been unnecessary if Facebook had acted in accordance with its public representations about its content moderation practices.

22. I have personal knowledge that Muslim Advocates' former executive director, Farhana Khera, spent significant amounts of time preparing for meetings with Facebook and its executives related to the presence of hate speech on Facebook. Much of this work would have been unnecessary if Facebook had acted in accordance with its public representations about its content moderation practices.

23. On some occasions, Muslim Advocates spent staff time and resources responding to hate speech or anti-Muslim groups that organized on Facebook. Much of this work would have been unnecessary if Facebook had acted in accordance with its public representations about its content moderation practices. For example, in June and September of 2017, anti-Muslim hate group ACT for America organized a series of in-person protests using Facebook event pages. In anticipation of these protests, we mobilized coalition partners around the country and sent letters from multiple organizations to mayors of the cities where these protests were expected to take place.

24. In my various roles at Muslim Advocates, I advocated to state and federal elected and regulatory officials, including at the White House, the U.S. Department of

Justice, and the U.S. Congress on policy initiatives to prevent anti-Muslim bigotry and to challenge discrimination.

25. I conducted outreach to American Muslims targeted by bigots online and in real life; and work with law enforcement government officials, and community partners to support safety for individuals and communities targeted by bigots.

26. I was aware of many statements by Facebook employees, both in private and in Congress, stating that Facebook took down hate speech on its platform. These statements were an important part of Muslim Advocates' decision to continue to engage in Facebook. If Facebook officials had stated to me that they did not intend to remove hate speech from the platform, I would not have continued to engage with them in the manner we did.

I declare under penalty of perjury that the foregoing is accurate to the best of my knowledge.



-----

August 6, 2021

Signature

Date

IN THE SUPERIOR COURT FOR THE DISTRICT OF COLUMBIA  
CIVIL DIVISION

MUSLIM ADVOCATES,

*Plaintiff,*

v.

MARK ZUCKERBERG, *et al.*,

*Defendants.*

Case No.: 2021 CA 001114 B

Judge Anthony C. Epstein

Exhibit D

IN THE SUPERIOR COURT FOR THE DISTRICT OF COLUMBIA  
CIVIL DIVISION

MUSLIM ADVOCATES,

*Plaintiff,*

v.

MARK ZUCKERBERG, *et al.*,

*Defendants.*

Case No. 2021 CA 001114 B

**DECLARATION OF WILLIAM R. YEOMANS**

I, William R. Yeomans, declare under penalty of perjury of the laws of the United States:

1. I am competent to testify and have personal knowledge about what is written in this declaration.
2. I am older than 18 years old.
3. Since 2013 I have been a member of the faculty of Columbia Law School, where I teach courses on ethics in the federal government
4. From 2009 to 2017, I was a member of the faculty of the American University Washington College of Law, where I taught constitutional law, civil rights, legislation, and the legislative process.
5. From 2006 until 2009, I served as Sen. Edward M. Kennedy's Chief Counsel on the Senate Judiciary Committee. During that time, I helped to organize and attended dozens of Senate Judiciary Committee hearings. I identified witnesses to invite to testify before the Committee, coordinated with witnesses as they prepared their written and oral testimony, and collaborated with organizations, including civil rights groups, on a range of policy issues.

6. Prior to working in the United States Senate, I spent 26 years at the Department of Justice where I litigated and supervised civil rights cases in the federal courts at all levels involving voting rights, school desegregation, employment discrimination, housing discrimination, hate crimes, police misconduct, abortion clinic violence, and human trafficking. During this time, I served as trial attorney, acting Deputy Assistant Attorney General, Chief of Staff, and acting Assistant Attorney General for Civil Rights in the Department of Justice.

7. I have also served as the Legal Director of the Alliance for Justice and the first Director of Programs for the American Constitution Society. Both of these organizations are non-profits.

8. I have personally testified before Congress, including on behalf of the Department of Justice before the House Judiciary Committee and the Senate Foreign Relations Committee. I have also helped others draft their congressional testimony and prepare to testify before Congress.

9. In my experience as a former senior Department of Justice Civil Rights Division official, a chief counsel on the Senate Judiciary Committee, a senior member of non-profit advocacy organizations, and a law professor who taught courses on legislation and the legislative process, I have observed that congressional hearings are designed to gather facts that Congress will use to explore policy issues and, where appropriate, lay the groundwork for legislation.

10. Such congressional hearings often involve inviting leaders of major companies to appear in person and submit written testimony. A central goal of such hearings is to focus public attention on a problem by calling corporate leaders to testify. Witnesses understand that they are speaking in a highly visible public forum and are communicating information not just to the members of Congress and their staffs but also to the public beyond the hearing room, including their current and prospective customers and organizations that have an interest in the issues being considered by Congress. Corporate leaders customarily intend that members of Congress and their staffs,

organizations, consumers, and the general public will rely on their testimony in deciding what actions to take in the future. This is especially true of high-profile hearings.

11. A central characteristic of congressional hearings is that they allow the public to hear testimony from corporate leaders about their business practices. Corporate leaders understand that their congressional testimony can affect decisions by consumers whether to purchase their products or services, and they intend for their testimony to advance or prevent harm to their private commercial interests.

12. Traditionally, when an executive or leader of a major organization testifies before Congress, the organization's senior policy and legal staffs play a significant role in drafting, editing, and otherwise shaping the written and oral testimony. And senior staff often accompany the person testifying to provide counsel and advise during the testimony and during breaks in the testimony.

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct.

DocuSigned by:  
  
73ECA7E98D194AD  
-----  
William R. Yeomans

11/16/2021

-----  
Date

IN THE SUPERIOR COURT FOR THE DISTRICT OF COLUMBIA  
CIVIL DIVISION

MUSLIM ADVOCATES,

*Plaintiff,*

v.

MARK ZUCKERBERG, *et al.*,

*Defendants.*

Case No.: 2021 CA 001114 B

Judge Anthony C. Epstein

Exhibit E

IN THE SUPERIOR COURT FOR THE DISTRICT OF COLUMBIA  
CIVIL DIVISION

MUSLIM ADVOCATES,

*Plaintiff,*

v.

MARK ZUCKERBERG, *et al.*,

*Defendants.*

Case No. 2021 CA 001114 B

**DECLARATION OF PROFESSOR MEGAN SQUIRE**

I, Megan Squire, declare under penalty of perjury of the laws of the United States:

1. I am competent to testify and have personal knowledge about what is written in this declaration.
2. I am older than 18 years old.
3. I am a professor of Computer Science at Elon University in North Carolina.
4. My main research area is applying data science techniques to understand niche and extremist online communities, particularly radical right-wing groups on social media.
5. I am currently a Senior Fellow for data analytics at the Southern Poverty Law Center and a Belfer Fellow for the Anti-Defamation League.

6. During the course of my research, I frequently notified Facebook about groups and content on the platform that violated Facebook's own Community Standards, policies, and other standards articulated to Congress, yet Facebook routinely failed to remove such groups or content.
7. On September 26, 2018, I presented a paper, Network Analysis of Anti-Muslim Groups on Facebook, at the Tenth International Conference on Social Informatics at St. Petersburg, Russia where I researched the topic of how anti-Muslim political groups use Facebook's platform to build their own online communities. A true and accurate copy of that paper can be found here:  
[https://www.researchgate.net/publication/327747920\\_Network\\_Analysis\\_of\\_Anti-Muslim\\_Groups\\_on\\_Facebook\\_10th\\_International\\_Conference\\_SocInfo\\_2018\\_St\\_Petersburg](https://www.researchgate.net/publication/327747920_Network_Analysis_of_Anti-Muslim_Groups_on_Facebook_10th_International_Conference_SocInfo_2018_St_Petersburg)
8. In that paper, I found anti-Muslim attitudes are not only flourishing on the platform, but also acting as a common denominator for a range of other extremist ideologies, including xenophobic anti-immigrant groups, pro-Confederate groups, militant anti-government conspiracy theorists, and white nationalists.
9. As part of my research, I identified 202 anti-Muslim hate groups in the United States on Facebook from September 2018 to August 2019. These hate groups posted anti-Muslim content that violated the plain language of Facebook's Community Standards.
10. Facebook did not, however, initially remove the hate groups that I identified. Facebook did not explain why these groups' obvious violations of Facebook's

Community Standards did not trigger removal. Most of these hate groups remain on the platform as of the date that the complaint was filed in this action.

11. On August 4, 2018, BuzzFeed published an article about my research. A true and correct copy of that article, Ishmael Daro, Here's How Anti-Muslim Groups on Facebook Overlap With a Range of Far-Right Extremism, BuzzFeed News (Aug. 4, 2018), can be found at:

<https://www.buzzfeednews.com/article/ishmaeldaro/antimuslim-content-facebook-groups-study>

12. On January 16, 2018, an article about my research was published in Wired explaining how I had used the Facebook application programming interface (“API”) to identify hate groups and their members. A true and correct copy of the article, Doug Bock Clark, Meet Antifa's Secret Weapon Against Far-Right Extremists, Wired (Jan. 16, 2018), can be found here:

<https://www.wired.com/story/free-speech-issue-antifa-data-mining/>.

13. On January 30, 2018, Facebook announced that it was changing its API; those changes would make the kinds of searches that I conducted to do my research on Facebook impossible other than if done by Facebook employees. That change went into effect April 4, 2018. A true and correct copy of that announcement, Facebook, An Update on Our Plans to Restrict Data Access on Facebook (Apr. 4, 2018), can be found here: <https://about.fb.com/news/2018/04/restricting-data-access/>

14. In a report published in September 2018 that analyzed hate groups on Facebook from June 2017 to March 2018, I found that anti-Muslim bias served as a common

denominator among hate groups around the world. I identified 202 anti-Muslim hate groups in the United States that operate as groups on Facebook and post anti-Muslim hate content, providing examples and identifying some groups by name. The 202 anti-Muslim hate groups were part of a larger list of 2000 hate groups I identified on the platform.

15. I published an updated report in August 2019, following a deeper analysis of these hate groups' Facebook pages, identifying 202 U.S.-based expressly anti-Muslim hate groups "created to provoke hostility and discrimination toward a class of people, [Muslims], based on myths and stereotypes about their religion."
16. Of the 202 hate groups identified by my report in September 2018 and August 2019, most remained on the platform as of the date of the filing of this action. All or most of these hate groups and/or content in their groups violate Facebook's Community Standards, policies, and other standards articulated to Congress.
17. The following are examples of where I flagged and identified hate speech for Facebook that violates its Community Standards, policies, or other standards articulated to Congress, but that Facebook has decided not to remove or take down as of the date of filing of this action (or, Facebook removed it after initially refusing to remove or take it down for some time).
  - a. On September 26, 2017, I notified Facebook of a group called "American Infidels Alll [sic]." Its group description includes the statement: "DO NOT SUBMIT TO aLLAH [sic]. Show no mercy. Kill all of them when it starts." Facebook responded to me on September 29, 2017, and informed me that it

would not remove this group or this content. This group and content violated Facebook Community Standards on Hate Speech or Dangerous Organizations.

- b. On March 30, 2018, I reported to Facebook a group called “Infidels Unite Against Islam.” Its group page contained the language: “Infidels unite against Islam, Islam is a disease, that we must root out.” I reported the group for violating the Community Standards’ definition of Hate Speech that prohibited “dehumanizing speech including . . . reference or comparison to filth, bacteria, disease, or feces.” Facebook responded on April 1, 2018, and informed me that it would not remove this group or this content.
- c. On April 10, 2018, I reported to Facebook a group named “AntiIslam Movement,” a group with a cover photo of the scope of a gun and the caption “72 Virgins Dating Service, The Relationship is up to you . . . We just arrange the meeting.” The group description contained the language: “Lord make me fast and accurate, let my aim be true and my hand faster.” Facebook responded on April 12, 2018, and informed me that it would not remove this group or this content. Later, however, on April 17, 2018, Facebook acknowledged that the group violated its Community Standards and removed it.
- d. On April 11, 2018, I reported to Facebook a group called “Death to Islam Undercover.” I reported it for violating Facebook’s Community Standards

that prohibit “hate groups,” such as “organizations and people dedicated to promoting hatred against protected groups.” As part of those standards, protected groups were defined to include religious affiliation. Facebook responded to this report on April 12, 2018, by informing me that it would not remove this group or its content. However, six days later Facebook informed me that it had removed some unspecified content from the group, but would allow the group to remain on the platform.

- e. On April 24, 2018, I reported to Facebook a group called “Veterans Against Islamic Filth” for violating Facebook’s Community Standards that prohibited “dehumanizing speech including . . . reference or comparison to filth, bacteria, disease, or feces.” Facebook responded that it would not remove this group or this content.
- f. On April 25, 2018, I reported to Facebook a group called “Purge Worldwide (The Cure for the Islamic disease in your country).” The description of the group stated: “This is an anti Islamic group A Place to share information about what is happening in your part of the world. The meaning of purge Verb: 1) Rid (someone) of unwanted feeling, memory, or condition. 2. Physically remove (something) completely. Noun: An abrupt or violent removal of a group of people.” I reported the group for violating the standard which forbids “calls to exclude or segregate a person or group of people based on the above listed characteristics,” one of which is religion.

Facebook responded by informing me that it would not remove this group or this content.

- g. On April 27, 2018, I reported a group called “Pro-Islamophobia saves lives” that contained a photo of a charred body of a toddler for violating Facebook’s Community Standards’ prohibition against “Videos of dying, wounded or dead people if they contain... charred or burning people.” Facebook responded that it would not remove the group.
- h. On January 26, 2019, I reported a group called “Islam is pure evil” for violation of Facebook’s Community Standards that prohibited hate speech. Facebook responded it would not remove the group.
- i. On June 30, 2019, I reported a group called “Islam is a Cancer” for violation of Facebook’s Community Standards that prohibited “Dehumanizing speech including... reference or comparison to filth, bacteria, disease, or feces.” Facebook responded it would not remove the group.
- j. On June 30, 2019, I reported a group called “Purge Islam Globaly [sic]” for violation of Facebook’s Community Standards that prohibited hate speech and the standard against “calls to exclude” mentioned above. Facebook responded it would not remove the group.
- k. On July 6, 2019, I reported a group called “PIG Purge Islam Globally” for violation of Facebook’s Community Standards that prohibited hate speech and the standard against “calls to exclude” mentioned above. Facebook responded it would not remove the group.

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct.

*Megan Squire*  
-----  
Megan Squire

November-2021 2021  
Date