

RON WYDEN
OREGON

RANKING MEMBER OF COMMITTEE ON
FINANCE

221 DIRKSEN SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-5244

United States Senate
WASHINGTON, DC 20510-3703

COMMITTEES:
COMMITTEE ON FINANCE
COMMITTEE ON BUDGET
COMMITTEE ON ENERGY & NATURAL RESOURCES
SELECT COMMITTEE ON INTELLIGENCE
JOINT COMMITTEE ON TAXATION

April 23, 2019

The Honorable Joseph J. Simons
Chairman
Federal Trade Commission

The Honorable Rohit Chopra
Commissioner
Federal Trade Commission

The Honorable Noah Joshua Phillips
Commissioner
Federal Trade Commission

The Honorable Rebecca Kelly Slaughter
Commissioner
Federal Trade Commission

The Honorable Christine S. Wilson
Commissioner
Federal Trade Commission

Dear Chairman Simons, Commissioner Chopra, Commissioner Phillips, Commissioner Slaughter, and Commissioner Wilson:

I write to urge the Federal Trade Commission (FTC) to ensure that any consent order negotiated with Facebook concerning his company's unfair and deceptive practices and its mishandling of users' data holds Mark Zuckerberg, the company's Chief Executive Officer (CEO), individually liable for the company's repeated violations of Americans' privacy.

In 2011, the FTC entered into a consent decree with Facebook after finding in an eight count complaint that the company deceived consumers and mishandled their data. The Commission has now publicly confirmed that—in the wake of the Cambridge Analytica scandal last year—it is investigating Facebook for potentially violating the terms of that same 2011 consent decree.

Mr. Zuckerberg launched Facebook in 2004, and has been the public face of the company ever since, including repeatedly making promises to Facebook users over privacy and data concerns. Mr. Zuckerberg is not merely the CEO of Facebook but he also controls a majority of the voting rights in the company. This control insulates him from accountability to Facebook's board and shareholders. Internal Facebook documents, released by the British Parliament in 2018, confirm that Mr. Zuckerberg was the ultimate decision-maker regarding Facebook's user data-sharing deals with its preferred corporate partners. In his own words, Mr. Zuckerberg said to the US House of Representatives Committee on Energy and Commerce in 2018: "I started Facebook. I run it, and I'm responsible for what happens here."

According to media reports, the FTC is now negotiating another consent order with Facebook. Any settlement with Facebook must hold Mr. Zuckerberg individually accountable or his flagrant, repeated violations of Americans' privacy will continue. The FTC has the authority to hold individuals responsible for the actions of a corporate entity where the individual

911 NE 11TH AVENUE
SUITE 500
PORTLAND, OR 97232
(503) 386-7735

405 EAST 8TH AVE
SUITE 3020
EUGENE, OR 97401
(541) 453-4029

SAC ANNEK BUILDING
205 E. 1ST
SUITE 201
LA GRANDE, OR 97630
(541) 962-7691

U.S. COURT HOUSE
700 WEST 6TH ST
ROOM 317
MEDFORD, OR 97501
(541) 658-8122

THE JAMISON BUILDING
131 W. HAWTHORNE AVE
SUITE 107
EUGENE, OR 97401
(541) 359-9142

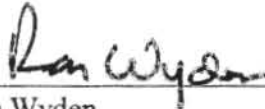
701 13TH ST, ET
SUITE 200
SALEM, OR 97301
(503) 581-4555

[HTTP://WYDEN.SENATE.GOV](http://WYDEN.SENATE.GOV)

participated directly in the deceptive practices or acts or had authority to control them. See e.g. *POM Wonderful v. FTC*, No. 13-1060 (D.C. Cir. 2015). Given Mr. Zuckerberg's deceptive statements, his personal control over Facebook, and his role in approving key decisions related to the sharing of user data, the FTC can and must hold Mr. Zuckerberg personally responsible for these continued violations. The FTC must also make clear the significant and material penalties that will apply to both Facebook the corporation and Mr. Zuckerberg the individual should any future violations occur.

Thank you for your attention to this pressing matter. I look forward to your prompt response.

Sincerely,

A handwritten signature in black ink, appearing to read "Ron Wyden", is written over a horizontal line.

Ron Wyden
United States Senator

United States Senate

WASHINGTON, DC 20510

May 6, 2019

The Honorable Joseph Simons
Chairman
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Dear Chairman Simons:

We write to urge the Commission to act swiftly to conclude its investigation of Facebook, and to move to compel sweeping changes to end the social network's pattern of misuse and abuse of personal data. This investigation has been long delayed in conclusion – raising the specter of a remedy that is too little too late. The Facebook consent decree violations have been blatant and brazen, an offensive defiance that adds insult to injury. The public is rightly asking whether Facebook is too big to be held accountable. The FTC must set a resounding precedent that is heard by Facebook and any other tech company that disregards the law in a rapacious quest for growth. The Commission should pursue deterrent monetary penalties and impose forceful accountability measures on Facebook, including limits on the use of consumer data, managerial responsibility for violations, and other structural remedies to stop further breaches of consumer trust.

According to its most recent financial earnings statement, Facebook has estimated that the FTC's investigation will cost the company between \$3 billion to \$5 billion.¹ While the reported penalty exceeds previous privacy cases, the scope and nature of the allegations are also unprecedented. The Cambridge Analytica incident that initially prompted the investigation affected the personal data of more than 70.6 million Americans, and Facebook still has not fully accounted for similar misuse by other third party applications.² This also does not consider further issues that the FTC may find in its investigation, such as recent reports that Facebook harvested address books from email accounts without user consent.³

In the same quarter it reported the FTC fine, Facebook recorded \$15 billion in revenue, beating market expectations. Considering the maximum civil penalty amount of \$42,530 per

¹ "Facebook Reports First Quarter 2019 Results", Facebook, accessed April 30, 2019, https://s21.q4cdn.com/399680738/files/doc_financials/2019/Q1/Q1-19-Press-Release.pdf.

² Schroepfer, Mike "An Update on Our Plans to Restrict Data Access on Facebook", Facebook, last modified April 4, 2018, <https://newsroom.fb.com/news/2018/04/restricting-data-access/>.

³ Goodin, Dan "In new gaffe, Facebook improperly collects email contacts for 1.5 million", Arstechnica, last modified April 8, 2019, <https://arstechnica.com/information-technology/2019/04/in-new-gaffe-facebook-improperly-collects-email-contacts-for-1-5-million/>.

Franceschi-Bicchiera, Lorenzo "Facebook's Phone Number Policy Could Push Users to Not Trust Two-Factor Authentication", Motherboard, last modified May 4, 2019, https://motherboard.vice.com/en_us/article/kzdxjx/facebook-phone-number-two-factor-authentication.

violation, the rumored number is a bargain for Facebook. Even a fine in the billions is simply a write-down for the company, and large penalties have done little to deter large tech firms.⁴ If the FTC is seen as traffic police handing out speeding tickets to companies profiting off breaking the law, then Facebook and others will continue to push the boundaries.

Fines alone are insufficient. Far-reaching reforms must finally hold Facebook accountable to consumers. We are deeply concerned that one-time penalties of any size every few years are woefully inadequate to effectively restrain Facebook. The FTC should impose long-term limits on Facebook's collection and use of personal information. It should consider setting rules of the road on what Facebook can do with consumers' private information, such as requiring the deletion of tracking data, restricting the collection of certain types of information, curbing advertising practices, and imposing a firewall on sharing private data between different products, including Facebook's ad platform.

As important as remedies on Facebook as a company are, the FTC should impose tough accountability measures and penalties for individual executives and management responsible for violations of the consent order and for privacy failures. Personal responsibility must be recognized from the top of the corporate board down to the product development teams. For decades, the FTC has understood that some violations require naming specific executives in its consent orders, particularly those that "formulates, directs, or controls the policies, acts, or practices" that break the law.⁵ According to the Washington Post, the FTC considered naming Mark Zuckerberg in its previous consent order but ultimately declined to do so.⁶ If the FTC finds that any Facebook executive knowingly broke the consent order or violated the law, it must name them in any further action.

It is also time for the FTC to learn from a history of broken and under-enforced consent orders. The FTC has an opportunity to establish a new set of requirements for consent orders that target data privacy cases and provide enduring safeguards for consumers. Such measures could include the direct appointment and oversight of auditors by the FTC, strict board or managerial liability for assessments and compliance, restriction on data practices or collection, and public disclosure of audits.

⁴ Bartunek, Robert-Jan, Blenkinsop, Philip, Mahlich, Greg "EU fines Facebook 110 million euros over WhatsApp deal", Reuters, last modified May 18, 2017 <https://www.reuters.com/article/us-eu-facebook-antitrust/eu-fines-facebook-110-million-euros-over-whatsapp-deal-idUSKCN18E0LA>.

⁵ "Google Forfeits \$500 Million Generated by Online Ads & Prescription Drug Sales by Canadian Online Pharmacies", Department of Justice, Office of Public Affairs, last modified August 24, 2011, <https://www.justice.gov/opa/pr/google-forfeits-500-million-generated-online-ads-prescription-drug-sales-canadian-online>.

Satariano, Adam "Google Fined \$1.7 Billion by E.U. for Unfair Advertising Rules", The New York Times, last modified March 20 2019, <https://www.nytimes.com/2019/03/20/business/google-fine-advertising.html>.

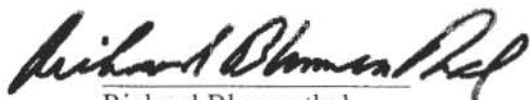
⁶ "Docket No. C-4161 Decision and Order", United States of America Federal Trade Commission, last modified June 20, 2006, <https://www.ftc.gov/sites/default/files/documents/cases/2006/06/0523117nationstitledecisionandorder.pdf>.

⁷ Romm, Tony "Facebook CEO Mark Zuckerberg said to be under close scrutiny in federal privacy probe", The Washington Post, last modified April 19, 2019, https://www.washingtonpost.com/technology/2019/04/19/federal-investigation-facebook-could-hold-mark-zuckerberg-accountable-privacy-sources-say/?utm_term=.d5816715b52c.

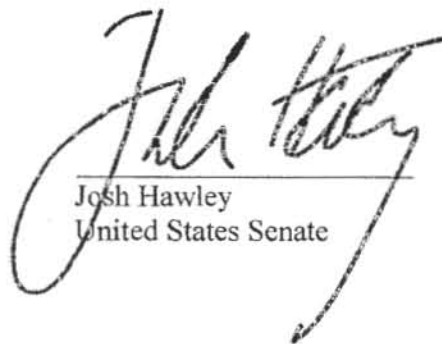
The Facebook investigation will be a defining moment for the Commission. It must be seen as a strong protector of consumer privacy and begin to set out a new era of enforcement, or it will not be taken as a credible enforcer. Action is overdue.

Thank you for your attention to this important matter.

Sincerely,



Richard Blumenthal
United States Senate



Josh Hawley
United States Senate

Congress of the United States

Washington, D.C. 20515

March 29, 2018

Maureen K. Ohlhausen
Acting Chairman
Federal Trade Commission
600 Pennsylvania Ave, N.W.
Washington, D.C. 20580

Terrell McSweeney
Commissioner
Federal Trade Commission
600 Pennsylvania Ave, N.W.
Washington, D.C. 20580

Dear Acting Chairman Ohlhausen and Commissioner McSweeney:

We were encouraged to learn that the Federal Trade Commission (FTC) has opened an investigation into whether Facebook failed to adequately protect the privacy of consumers.¹ Recent media accounts raise serious questions about whether Facebook violated a 2012 FTC consent order² or otherwise engaged in deceptive and unfair practices in violation of the FTC Act. Those reports make clear that Facebook failed to adequately protect the personal information of more than 50 million users from misuse by the political consulting firm Cambridge Analytica (CA) through an app developed by Aleksandr Kogan of Global Science Research (GSR).³ It is possible that other third parties also improperly accessed Facebook users' data in the same manner at CA.

Facebook has acknowledged that it anticipates receiving a letter from the FTC shortly.⁴ The scope of the breach and Facebook's failure to notify affected consumers or regulatory agencies for more than two years or to take any reasonable measures to ensure the disposal of the data calls for the strongest possible enforcement response. The Commission should also examine the role of all parties involved in this incident, including Kogan, GSR, and CA, which we understand to be a U.S. subsidiary of the British company SCL Group.

Based on Facebook's own statements about the matter and other widely reported details, the behavior that led to the misuse of millions of consumers' personal information appears strikingly reminiscent of conduct that was the focus of the FTC's 2012 complaint. As an example, the FTC charged Facebook in 2012 with misrepresenting that a "friends only" privacy setting would prevent collection of a user's information by apps that their friends downloaded.⁵ Despite being on notice that such a practice was deceptive, Facebook allowed the app launched

¹ FTC, *Statement by the Acting Director of FTC's Bureau of Consumer Protection Regarding Reported Concerns about Facebook Privacy Practices*, (Mar. 26, 2018) (press release).

² *In re Facebook, Inc.*, Decision and Order, No. C-4365 (2012).

³ *Facebook's Role in Data Misuse Sets Off Storms on Two Continents*, New York Times (Mar. 18, 2018)

⁴ *Id.*

⁵ *In re Facebook, Inc.*, Complaint, No. C-4365 (2012).

by Kogan/GSR in 2013 to override “friends only” privacy settings and harvest data not just from the 270,000 users who downloaded the app but also from tens of millions of those users’ friends.⁶

Facebook’s conduct prior to and in response to the CA breach raises more fundamental questions about whether the company has complied with FTC order provisions that require it to implement a “comprehensive privacy program.” Media accounts from past security officers and contractors suggest that Facebook’s approach to data collection by apps was largely hands off.⁷ The company opened its platform to app developers in 2007 and, until recently, continued to allow collection of user data with little or no oversight, relying on the developer’s word that it would not misuse the data.⁸ Facebook even reportedly ignored internal warnings about vulnerabilities in the platform that may have allowed foreign states and data brokers to access user data.⁹

Moreover, when Facebook learned of the CA breach in 2015, its response was both slow and passive. For example, Facebook did not send a formal letter to Kogan asking him to destroy data collected by GSR until August 2016.¹⁰ And the letter merely asked Kogan to self-certify that the data had been destroyed; Facebook did not take any steps to ensure the data was actually destroyed.¹¹ It now appears that hundreds of gigabytes of Facebook user information is still sitting on unencrypted files on CA servers.¹² For more than two years, Facebook did nothing to publicly acknowledge the breach or to notify affected users, and only now has Facebook committed to do a full forensic audit of the countless apps that have been collecting data from its site for years.¹³

If, after completing the investigation, the Commission determines that Facebook has violated the 2012 order, we hope that you will impose civil penalties commensurate with the scope and severity of the breach and sufficient to send a clear message to Facebook and other companies that they must take their consumer privacy responsibilities seriously. If the

⁶ See note 3.

⁷ *Facebook’s Rules for Accessing User Data Lured More than Just Cambridge Analytica*, Washington Post (Mar. 19, 2018).

⁸ *Id.*; *How Facebook’s Data Sharing Went from Feature to Bug*, New York Times (Mar. 19, 2018).

⁹ *Former Facebook Insider Says Company Cannot be Trusted to Regulate Itself*, NPR (Mar. 20, 2018).

¹⁰ *Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach*, The Guardian (Mar. 17, 2018).

¹¹ *Id.*

¹² *How Trump Consultants Exploited the Facebook Data of Millions*, New York Times (Mar. 17, 2018).

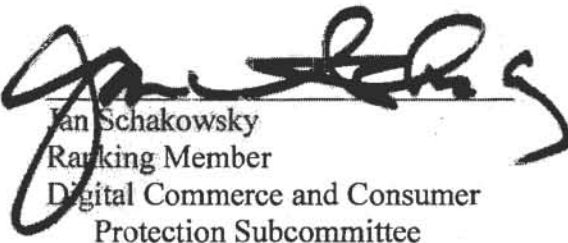
¹³ Facebook, *Hard Questions: Update on Cambridge Analytica*, (Mar. 21, 2018) (press release).

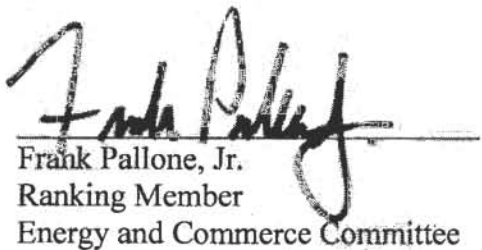
Commission determines that Facebook has engaged in deceptive or unfair practices outside the scope of the order, we request that you make appropriate modifications to ensure that future misconduct will be subject to civil penalties or respond to such other unfair and deceptive practices using the fullest extent of your law enforcement tools.

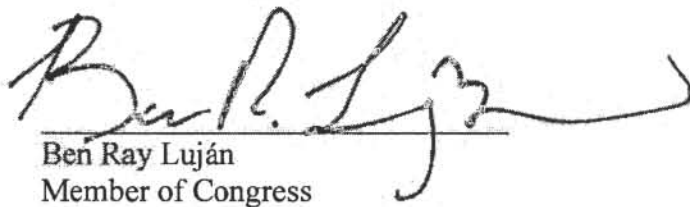
Finally, we are concerned that the consumer privacy vulnerabilities that have come to light are not isolated to Facebook and instead indicate broader problem across social media platforms. The FTC should assess more broadly whether other social media firms are vulnerable to similar exploitation of user data by unauthorized parties.

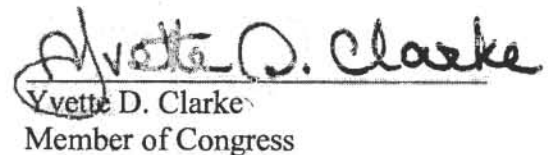
We appreciate that the FTC is at the beginning of its inquiry into this matter. We hope you will make it a priority of the agency and move expeditiously.

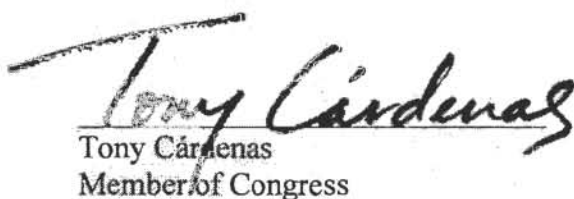
Sincerely,


Jan Schakowsky
Ranking Member
Digital Commerce and Consumer
Protection Subcommittee



Frank Pallone, Jr.
Ranking Member
Energy and Commerce Committee

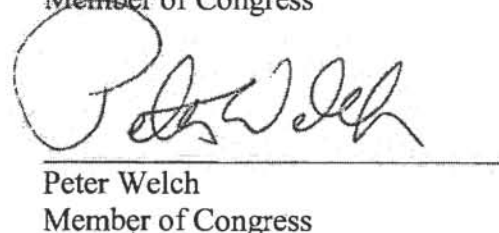

Ben Ray Luján
Member of Congress


Yvette D. Clarke
Member of Congress

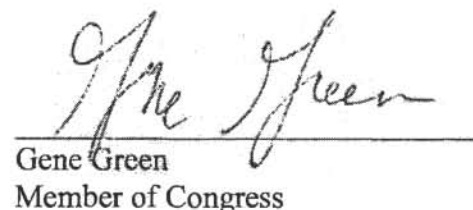

Tony Cárdenas
Member of Congress


Debbie Dingell
Member of Congress


Doris Matsui
Member of Congress


Peter Welch
Member of Congress


Joseph P. Kennedy III
Member of Congress


Gene Green
Member of Congress

DAVID N. CICILLINE
1ST DISTRICT, RHODE ISLAND

2244 RAYBURN BUILDING
WASHINGTON, D.C. 20515
(202) 225-4911
(202) 225-3290 (FAX)

1070 MAIN STREET, SUITE 300
PAWTUCKET, RI 02860
(401) 729-6000
(401) 729-6608 (FAX)



Congress of the United States
House of Representatives
Washington, DC 20515

March 19, 2019

CO-CHAIR, DEMOCRATIC POLICY AND
COMMUNICATIONS COMMITTEE

COMMITTEE ON THE JUDICIARY

RANKING MEMBER, SUBCOMMITTEE ON
REGULATORY REFORM, COMMERCE
AND ANTITRUST LAW

SUBCOMMITTEE ON
COURTS, INTELLECTUAL PROPERTY,
AND THE INTERNET

COMMITTEE ON FOREIGN AFFAIRS

SUBCOMMITTEE ON
EUROPE, EURASIA, AND EMERGING THREATS

SUBCOMMITTEE ON MIDDLE EAST
AND NORTH AFRICA

The Honorable Joseph J. Simons
Chairman
Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, DC 20580

The Honorable Rohit Chopra
Commissioner
Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, DC 20580

The Honorable Noah Joshua Phillips
Commissioner
Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, DC 20580

The Honorable Rebecca Kelly Slaughter
Commissioner
Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, DC 20580

The Honorable Christine S. Wilson
Commissioner
Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, DC 20580

Dear Chairman Simons, Commissioner Chopra, Commissioner Phillips, Commissioner
Slaughter, and Commissioner Wilson:

I write to urge the Commission to open an immediate investigation into whether Facebook has
violated the antitrust laws.

It has been a year since news broke that Facebook exposed user data to Cambridge Analytica, a
political consulting firm that sought to manipulate voter behavior.¹ Since then, a torrent of
reports has revealed that the Cambridge Analytica scandal was part of a much broader pattern of

¹ Carole Cadwalladr & Emma Graham-Harrison, *Revealed: 50 million Facebook Profiles harvested for Cambridge
Analytica in major data breach*, THE GUARDIAN (Mar. 17, 2018),
<https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>.

misconduct by Facebook.² This includes mounting evidence of anticompetitive behavior.³ Facebook's predatory acquisition strategy, foreclosure of rivals from its platform, and declining product quality strongly suggest that it has abused its position as a monopoly to undermine competition and the competitive process.

An antitrust investigation responding to these revelations should focus on at least three aspects of Facebook's conduct.

First, the Commission should examine whether any of Facebook's acquisitions substantially lessened competition in violation of Section 7 of the Clayton Act.⁴ Since its founding, Facebook has acquired over 75 companies.⁵ Two of the most significant purchases were Instagram, which Facebook bought in 2012 for \$1 billion, and WhatsApp, which Facebook purchased in 2014 for \$19 billion. Through these acquisitions, Facebook now owns three of the top four, and four of the top eight, social media apps.⁶

When Facebook acquired Instagram, the photo-based app posed a competitive threat.⁷ It was growing faster than even Facebook had at its peak and proved especially attractive to teenagers and young adults, a demographic Facebook was losing. Moreover, buying up Instagram enabled Facebook to make the switch to mobile, a market where Facebook was struggling to adapt. In

² See, e.g., Ryan Mac et al., *Growth At Any Cost: Top Facebook Executive Defended Data Collection In 2016 Memo – And Warned That Facebook Could Get People Killed*, BUZZFEED (Mar. 29, 2018), <https://www.buzzfeednews.com/article/ryanmac/growth-at-any-cost-top-facebook-executive-defended-data#.at6JrEZrk>; Hallie Detrick, *Facebook Is Sorry for Keeping the Videos You Thought You Deleted*, FORTUNE MAG. (Apr. 3, 2018), <http://fortune.com/2018/04/03/facebook-videos-delete-personal-data>; Matt Binder, *Facebook and Google accused of using 'dark patterns' to mislead users into sharing personal data*, MASHABLE (June 28, 2018), <https://mashable.com/2018/06/28/facebook-google-privacy-gdpr-deceived-by-design/#uVQFBHa0gmqg>; Sheera Frenkel et al., *Delay, Deny and Deflect: How Facebook's Leaders Fought Through Crisis*, N.Y. TIMES (Nov. 14, 2018), <https://www.nytimes.com/2018/11/14/technology/facebook-data-russia-election-racism.html>; Josh Constine, *Facebook pays teens to install VPN that spies on them*, TECHCRUNCH (Jan. 29, 2019), <https://techcrunch.com/2019/01/29/facebook-project-atlas/>. For an ongoing list, see FREEDOM FROM FACEBOOK, *Scandals*, <http://freedomfromfb.com/scandals> (last visited Mar. 18, 2019). This reporting has spurred investigations by a bipartisan group of 37 state attorneys general, the Justice Department, the Securities and Exchange Commission, and the FBI, as well as a host of foreign governments.

³ See, e.g., Note by Damian Collins, Member of Parliament, Chair, Digital, Culture, Media and Sport Committee, U.K. Parliament, and Selected Documents Ordered from Six4Three (Dec. 5, 2018), <https://www.parliament.uk/documents/commons-committees/culture-media-and-sport/Note-by-Chair-and-selected-documents-ordered-from-Six4Three.pdf> [hereinafter "Six4Three"]; Dina Srinivasan, *The Antitrust Case Against Facebook*, 16 BERKELEY L. & TECH. J. 39, 90-98 (2019).

⁴ 15 U.S.C. § 18 (2019).

⁵ *List of Facebook's 77 acquisitions*, CRUNCHBASE, https://www.crunchbase.com/search/acquisitions/field/organizations/num_acquisitions/facebook (last visited Mar. 18, 2019).

⁶ *Most Popular Mobile Social Networking Apps in the United States as of October 2018, by Monthly Users (in millions)*, STATISTA, <https://www.statista.com/statistics/248074/most-popular-us-social-networking-apps-ranked-by-audience/> (last visited Mar. 18, 2019).

⁷ Tim Wu, *The case for breaking up Facebook and Instagram*, WASH. POST (Sept. 28, 2018), <https://www.washingtonpost.com/outlook/2018/09/28/case-breaking-up-facebook-instagram>.

hindsight, it is clear that by approving this purchase, the Commission enabled Facebook to swallow up its most significant rival in the social network market.

WhatsApp, meanwhile, threatened to outdo Facebook Messenger. As documents released by the UK Parliament reveal, Facebook had been using its surveillance tool Onavo to obsessively track WhatsApp.⁸ By doing so it learned that WhatsApp's market reach was expanding steadily, outdoing then-popular apps like Foursquare and Tumblr while also beating out Facebook Messenger in certain markets.⁹ In other words, WhatsApp "was quickly demonstrating that it could compete with Facebook on its most important battleground."¹⁰ Instead of protecting this competition—as the antitrust laws require—the Commission permitted Facebook to neuter it. And while Facebook promised at the time of the acquisition that "nothing" will change for WhatsApp users' privacy,¹¹ it has since gone on to use WhatsApp users' data for marketing purposes—a breach of its commitment.¹²

Since the Commission generally does not share with the public its analysis justifying inaction, we do not know what led the agency to approve these acquisitions. But it is clear that allowing Facebook to purchase Instagram and WhatsApp has deprived users of critical competition. As Facebook's serial disregard for users' privacy has prompted some users to delete their Facebook accounts, they find themselves unable to escape Facebook's ecosystem.¹³ Given that Facebook used spyware to systematically track and target actual, potential, and nascent rivals, it is vital to

⁸ Six4Three, at 12-15. See also Betsy Morris & Deepa Seetharaman, *The New Copycats: How Facebook Squashes Competition from Startups*, WALL ST. J. (Aug. 9, 2017), <https://www.wsj.com/articles/the-new-copycats-how-facebook-squashes-competition-from-startups-1502293444>.

⁹ Six4Three, at 12-15.

¹⁰ Charlie Warzel & Ryan Mac, *These Confidential Charts Show Why Facebook Bought WhatsApp*, BUZZFEED (Dec. 5, 2018), <https://www.buzzfeednews.com/article/charliewarzel/why-facebook-bought-whatsapp>.

¹¹ Facebook, WHATSAPP BLOG (Feb. 19, 2014), <https://blog.whatsapp.com/499/Facebook>; Jim Edwards, *Zuckerberg: 'It's The Only App We've Ever Seen With Higher Engagement Than Facebook Itself*, BUS. INSIDER (Feb. 19, 2014), <https://www.businessinsider.com/facebooks-investor-call-on-whatsapp-acquisition-2014-2> ("No, [Zuckerberg] said, monetization was not an issue. Facebook isn't even thinking about that right now. And no, Facebook would not run ads on WhatsApp.").

¹² EPIC, *Facebook to Collect WhatsApp Data, Violating FTC Order and Privacy Promises* (Aug. 25, 2016), <https://epic.org/2016/08/facebook-to-collect-whatsapp-u.html> ("WhatsApp's recent announcement indicates users will have 30 days to opt-out of data transfers to Facebook, in violation of the law and the FTC's Order.").

¹³ Users who decided to quit Facebook in light of its privacy breaches discovered that cutting it out entirely would require also deleting Instagram and WhatsApp. See Will Oremus, *If You Delete Facebook, Do You Also Have to Delete Instagram and WhatsApp?*, SLATE (Dec. 22, 2018), <https://slate.com/technology/2018/12/can-you-deletefacebook-if-you-dont-also-delete-instagram-and-whatsapp.html>; see also *id.* ("After all, the unfortunate reality is that there aren't a lot of prominent social networks that Facebook doesn't own."). See also <https://marketingland.com/facebook-lost-15-million-users-marketers-remain-unfazed-258164>. It's also worth noting that Facebook collects data even on non-Facebook users. Kurt Wagner, *This Is How Facebook Collects Data on You Even If You Don't Have an Account*, RECODE (Apr. 20, 2018), <https://www.recode.net/2018/4/20/17254312/facebook-shadow-profiles-data-collection-non-users-mark-zuckerberg> ("There is no way to opt out of this kind of data collection.").

examine whether any of Facebook’s acquisitions—including of smaller social networks—unlawfully lessened competition.¹⁴

Second, the agency should investigate whether Facebook has engaged in exclusionary conduct in violation of Section 5 of the Federal Trade Commission Act.¹⁵ Documents reveal that Facebook has responded to competitive threats by cutting them from its network. For example, when Vine, a social application through which users can make short videos, attempted to let users find friends through Facebook’s platform, Facebook quickly shut down the feature.¹⁶ The Commission should examine whether Facebook has weaponized application programming interfaces (APIs) to undermine competition.

Finally, the Commission should consider whether Facebook has abused its monopoly power in violation of Section 5 of the Federal Trade Commission Act.¹⁷ Experts have noted that while Facebook faced competition, it was not able to condition use of its network on constant surveillance; in fact, users expressly rejected this bargain.¹⁸ It was only after Facebook achieved a dominant position that it could successfully backtrack on privacy commitments and initiate widespread commercial surveillance of users.¹⁹ This dramatic decrease in privacy has amounted to quality degradation of Facebook’s service. The Commission should investigate whether Facebook is using its monopoly power to degrade quality below what a competitive marketplace would allow.

Thank you for your attention to this important matter. It is critical that the Commission robustly enforce the antitrust laws to prevent anticompetitive acquisitions and anticompetitive conduct.

¹⁴ For example, in 2017 Facebook acquired *tbh*, a small yet fast-growing startup that had proved popular with high school students and teenagers. Hamza Shaban, *What is TBH, Facebook’s newly acquired anonymous teen compliment app?*, WASH. POST (Oct. 17, 2017), <https://www.washingtonpost.com/news/the-switch/wp/2017/10/17/tbh-facebooks-new-anonymous-teen-compliment-app-explained>. For an analysis of why the FTC should have scrutinized this acquisition, see Ben Thompson, *Why Facebook Shouldn’t Be Allowed to Buy tbh*, STRACHERY (Oct. 23, 2017), <https://stratechery.com/2017/why-facebook-shouldnt-be-allowed-to-buy-tbh/>. Less than a year after the acquisition, Facebook shut down *tbh*, citing “low usage.” Kaya Yurieff, *Facebook shuts the teen app it just bought*, CNN (July 3, 2018), <https://money.cnn.com/2018/07/03/technology/facebook-tbh-app-shut-down/index.html>.

¹⁵ 15 U.S.C. § 45(a)(1) (2019).

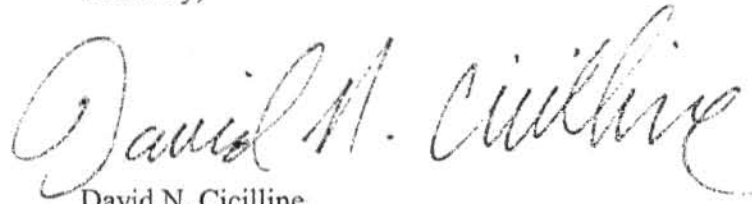
¹⁶ *Six4Three*, at 15, 43.

¹⁷ 15 U.S.C. § 45(a)(1).

¹⁸ Srinivasan, *supra* note 3, at 48-62.

¹⁹ *Id.* at 69-81.

Sincerely,

A handwritten signature in black ink that reads "David N. Cicilline". The signature is written in a cursive, flowing style.

David N. Cicilline
Chairman
Subcommittee on Antitrust,
Commercial and Administrative Law
Committee on the Judiciary

cc: The Honorable Jerrold Nadler, Chairman, Committee on the Judiciary
The Honorable Doug Collins, Ranking Member, Committee on the Judiciary
The Honorable F. James Sensenbrenner, Ranking Member, Subcommittee on Antitrust,
Commercial and Administrative Law
The Honorable Makan Delrahim, Assistant Attorney General, Department of Justice

COMMITTEE ON
APPROPRIATIONS
SUBCOMMITTEE ON
COMMERCE, JUSTICE, SCIENCE,
AND RELATED AGENCIES

SUBCOMMITTEE ON
STATE, FOREIGN OPERATIONS,
AND RELATED PROGRAMS

<http://www.meng.house.gov>
www.facebook.com/repgracemeng
twitter: @repgracemeng



Grace Meng

Congress of the United States

Sixth District, New York

February 25, 2019

CONGRESSIONAL ASIAN PACIFIC
AMERICAN CAUCUS
EXECUTIVE BOARD MEMBER

CHAIR
TASK FORCE ON
APPROPRIATIONS

SENIOR AND
REGIONAL WHIP

CONGRESSIONAL KIDS
SAFETY CAUCUS
CO-CHAIR

The Honorable Joseph J. Simons
Chairman
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Dear Commissioner Simons:

I write to request that the Federal Trade Commission (FTC) launch an investigation into Facebook Inc.'s collection of personal health information from smartphone users. A recent investigation by the Wall Street Journal found that Facebook has been collecting information on millions of users' most sensitive health data – unbeknownst to those users and even if said users have no connection to Facebook. This invasive practice must be stopped immediately.

A recent analysis by the Wall Street Journal (WSJ)¹ found that Facebook installed analytics software inside thousands of apps, including apps that track users' ovulation, menstrual cycles and their blood pressures. As soon as the user opens and logs their sensitive health data, the pre-installed software promptly sends the data to Facebook by creating a "custom app event." For instance, in the WSJ's testing, the Instant Heart Rate: HR Monitor and Flo Health Inc.'s Flo Period & Ovulation Tracker, the latter which claims 25 million active users, sent heart rate data and ovulation and menstrual tracking data to Facebook, respectively. That data would then be available to Facebook users and developers, leading to the creation of targeted ads towards the users of those apps. The companies running the applications have no ability to remove or disable the software Facebook had installed and none of the apps gave users the option to stop their personal information from being sent to Facebook. Collection of such data is an egregious violation of privacy.

Facebook did not obtain clear consent from users to accumulate personal health data that users provided to the app. The FTC must investigate this intrusive and invasive practice, and put an end to it immediately. Smartphone users must be protected from this encroachment into their personal lives; they must know their personal information is safe. I look forward to working with you on this matter.

Sincerely,

Grace Meng
Member of Congress

¹ Schechener, S. and Secada, M. (2019). You Give Apps Sensitive Personal Information. Then They Tell Facebook. *The Wall Street Journal*. Retrieved from https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636?mod=article_inline

RICHARD BLUMENTHAL
CONNECTICUT

COMMITTEES:

AGING

ARMED SERVICES

COMMERCE, SCIENCE, AND TRANSPORTATION

JUDICIARY

VETERANS' AFFAIRS

United States Senate

WASHINGTON, DC 20510

706 HART SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-2823
FAX: (202) 224-9673

90 STATE HOUSE SQUARE, TENTH FLOOR
HARTFORD, CT 06103
(860) 258-6940
FAX: (860) 258-6958

915 LAFAYETTE BOULEVARD, SUITE 304
BRIDGEPORT, CT 06604
(203) 390-0698
FAX: (203) 330-0658

<http://blumenthal.senate.gov>

December 19, 2018

The Honorable Joseph J. Simons
Chairman
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Dear Chairman Simons:

Exactly eight months ago, I wrote to you to draw your attention to evidence that Facebook may have violated its 2011 consent decree. Since then, there has been mounting and incontrovertible evidence that Facebook not only breached users' trust, but also disregarded key provisions in the consent decree. The stunning new investigation by the *New York Times* released last night confirms that Facebook violated its consent order with its data-sharing deals, and that those at the very top, including Mark Zuckerberg, were aware of it.¹ Facebook's seemingly unrestrained sharing of user data, the lengths it will go to justify its doing so, and the fact that it has not been forthcoming with consumers or Congress makes it imperative that the FTC act swiftly to prevent further consumer harm. I write urging you to take actions necessary to renew and refresh the FTC's urgency in pursuing strong legal remedies and major penalties on behalf of the consumers harmed by Facebook's conduct.

Instead of acting to protect consumers after its original breach of consumer privacy, Facebook appears to have defiantly violated its consent order. While news of Facebook's conduct continues to unfold, I am concerned that the FTC seems to be sitting on the sidelines, allowing Facebook and its handpicked auditing companies to vouch for the company. Meanwhile, reporters have aggressively pursued this story and uncovered significant new facts.

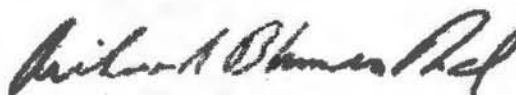
The new report by Gabriel J.X. Dance, Michael LaForgia, and Nicholas Confessore in the *New York Times*—the culmination of interviews with over 60 individuals, including former employees of Facebook and its partners, former government officials, and privacy advocates—paints a disturbing picture of how Facebook was responsible for the massive data sharing of millions of Americans without their consent. According to the report, Facebook justified its development of data-sharing relationships across a wide range of industries, and including foreign companies like the Russian search giant Yandex, by deliberately misinterpreting a "service provider" exemption in the FTC consent decree, which outlined Facebook's oversight of third parties. As a result, Facebook thought that it could skirt requirements in the consent decree that Facebook take steps to "verify the privacy or security protections that any third party

¹ <https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html>

provides” and “obtain the user’s affirmative express consent” for the sharing of any user’s information.²

Thank you in advance for your prompt attention to this matter. I respectfully request a response by January 11, 2018.

Sincerely,

A handwritten signature in black ink, appearing to read "Richard Blumenthal". The signature is fluid and cursive, with the first name being the most prominent.

Richard Blumenthal
United States Senate

² <https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookagree.pdf>

RICHARD BLUMENTHAL
CONNECTICUT

COMMITTEES

AGING

ARMED SERVICES

COMMERCE, SCIENCE, AND TRANSPORTATION

JUDICIARY

VETERANS' AFFAIRS

United States Senate

WASHINGTON, DC 20510

706 HART SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-2823
FAX: (202) 224-8673

90 STATE HOUSE SQUARE, TENTH FLOOR
HARTFORD, CT 06103
(860) 253-6940
FAX: (860) 253-6969

915 LAFAYETTE BOULEVARD, SUITE 804
BRIDGEPORT, CT 06604
(703) 330-0698
FAX: (203) 330-0608

<http://blumenthal.senate.gov>

April 19, 2018

The Honorable Maureen Ohlhausen
Acting Chairman
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Dear Acting Chairman Ohlhausen,

I am pleased that the Federal Trade Commission (FTC) has opened an investigation into the privacy practices and policies at Facebook. Recent revelations about the illegitimate harvesting of personal data on tens of millions of Americans have shed new light on the systemic failure of Facebook to address privacy risks and keep its promises to users. Despite Mark Zuckerberg's recent apology tour, Facebook's history of negligence demonstrates that the company can no longer be trusted to self-regulate. I write to draw attention to information that may be relevant to your investigation, including evidence that Facebook may have violated its consent decree. I also encourage the FTC to pursue strong legal remedies to compensate consumers harmed and set enforceable rules on its future conduct.

In November 2011, Facebook agreed to a proposed settlement containing a consent decree after the FTC found that the company had deceived consumers by sharing personal data with advertisers and making public information previously designated as private. Under the settlement, Facebook was barred from misrepresenting the privacy of personal information and was required to obtain affirmative express consent before enacting changes would override privacy preferences. The FTC also required Facebook to establish "a comprehensive privacy program that is reasonably designed to (1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the privacy and confidentiality of covered information."

Facebook's adherence to the consent decree has been called into question based on recent reports that the political consulting firm Cambridge Analytica and Global Science Research (GSR) had harvested a large-scale dataset of Facebook users based on a third-party app. The GSR app would collect demographic details, private communications, and other profile metrics of those who installed the app and their friends. Based on Facebook's permissive, default privacy settings, Cambridge Analytica was able to obtain information from up to 87 million profiles based on only about 300,000 users installing the GSR app.

This should have never happened. The FTC put Facebook on notice about the privacy risks of third-party apps in its complaint. Three of the FTC's claims concerned the misrepresentation of verification and privacy preferences of third-party apps. In 2008, shortly after the launch of its developer platform, Facebook introduced a "Verified Apps" program, which would provide a badge that Facebook had certified the security, privacy, trustworthiness, and transparency of an app.¹ When Facebook announced it would be ending the program the following year, it claimed that it would be extending these trust standards into *all* apps. However, in its 2011 complaint, the FTC found that despite claims of auditing, Facebook took no steps to verify either the security or protections for collected user information. Seven years later, exactly how Facebook verifies third-party apps is still murky.

The Cambridge Analytica revelations demonstrate that Facebook continued to turn a blind eye to third-party apps despite the FTC mandated privacy program. Facebook should have been aware that GSR was planning to violate developer platform rules based on the policies that developers are required to submit. GSR's terms of service ("Attachment 1") stated explicitly that it reserved the right to sell user data and would collect profile information from friends. These terms of service should have put Facebook on notice that GSR may be seeking to sell user data. At this month's Senate hearing on Facebook, Mr. Zuckerberg informed me that its app review team would have been responsible for vetting the policy and acknowledged that Facebook "should have been aware that this application developer submitted a [terms of service] that was in conflict with the rules of the platform."

Even the most rudimentary oversight would have uncovered these problematic terms of service. Moreover, Facebook knew as early as 2010 that third-party app developers were selling information to data brokers.² The fact that Facebook did not uncover these non-compliant terms strongly suggests that its "comprehensive privacy program" established pursuant to the FTC consent decree was either inadequate to address threats or not followed in practice. This willful blindness left users vulnerable to the actions of Cambridge Analytica.

The Cambridge Analytica matter also calls into question Facebook's compliance with the consent decree's requirements to respect privacy settings and protect private information. Three years after Facebook agreed to the consent decree, Facebook by default continued to provide broad access to personal data to third party apps, data that may not have been marked as public. In evaluating claims of deception and misrepresentation of privacy controls, the FTC has typically considered what a consumer would have reasonably understood their settings to mean. No information was readily provided to users about this permissive sharing to third-party apps or how to opt out. Nor were users informed about which apps accessed their profiles or given the ability to resolve unwanted intrusions. While users could be judicious about their privacy settings and the apps they installed, the actions of only one friend could thwart their efforts without their knowledge. The ease with which the GSR app was able to harvest data on 87 million users

¹ "Guiding Principles." Facebook Developers.

https://web.archive.org/web/20080902015608/http://developers.facebook.com/get_started.php?tab=principles

² "Facebook Shuts Down Apps That Sold User Data, Bans Rapleaf." AdAge. October 29, 2010.

www.adweek.com/digital/facebook-shuts-down-apps-that-sold-user-data-bans-rapleaf/

demonstrates that third parties were effectively able to override privacy preferences without express consent.

It is also noteworthy that the relaxation of data retention policies for third party developers may have contributed to the illegitimate collection of data. In a version of its Developer Principles and Policies dated December 1, 2009, Facebook mandated that developers “must not store or cache any data you receive from us for more than 24 hours” and “must not give data you receive from us to any third party.”³ In April 2010, Facebook changed this policy to permit developers to keep user information with significantly reduced restrictions on the sharing of data.⁴ There is no indication that Facebook informed its users that third parties would now be allowed to store their data or share it.

Facebook had multiple opportunities to prevent this harvesting and notify users before March 2018, but failed to do so. According to former Cambridge Analytica employee Christopher Wylie, the GSR app had collected data so aggressively that it triggered Facebook’s security protocols.⁵ However, there is no indication Facebook took steps to investigate or limit the collection despite the problematic terms of service.

Facebook finally acted on the GSR app after *The Guardian* reported on Cambridge Analytica’s plans in December 2015. While Facebook removed the application and contacted both companies to request the destruction of user information, its response continued to be inadequate. Facebook did not take any steps to prevent Cambridge Analytica and its partners from continuing to use its platform for advertising or analytics services, even working alongside the company within campaigns. It did not provide notice to users about how their information has been harvested by Cambridge Analytica, nor did it inform the FTC about the collection of data without user consent. Facebook did not contact Christopher Wylie to request the deletion of user data until the following August – at least nine months after the initial report. Facebook took no further action to assess whether data had been deleted. The ineffective response calls into question how seriously the company took this incident and others like it.

Former Facebook employees have told me that its staff were not empowered to effectively enforce privacy policies. For example, Sandy Parakilas, who led efforts to fix privacy problems on its developer platform from June 2011 to August 2012, describes Facebook as a company that would not commit resources or attention to protecting users against violations from third-party apps. Mr. Parakilas’ letter to me (“Attachment 2”) along with his November 19, 2017 *New York Times* op-ed and April 10, 2018 interview with *New York Magazine*, highlight a deeply disturbing pattern of disregard by Facebook to the privacy risks posed by third-party apps. Mr. Parakilas recounts how one executive told him, after proposing a deeper audit of

³ “Developer Principles and Policies.” Facebook Developers. December 1, 2009. <https://web.archive.org/web/20091223051700/http://developers.facebook.com/policy/>

⁴ “A New Data Model.” Facebook. April 21, 2010. <https://web.archive.org/web/20120502125823/http://developers.facebook.com/blog/post/378/>

⁵ Cadwalladr, Carole. “I made Steve Bannon’s psychological warfare tool’: meet the data war whistleblower.” *The Observer*. March 17, 2018. <https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-facebook-nix-bannon-trump>

developers' use of data, "Do you really want to see what you'll find?" Had Facebook taken such requests more seriously at the time, the GSR app might have been caught earlier.

Facebook has acknowledged it has neglected its privacy controls, which had non-functional settings and often outdated descriptions did not reflect how the platform operates.⁶ Overall Facebook's privacy controls were arcane and difficult to navigate, preventing users from effectuating their preferences. Such deficiencies indicate that Facebook did not maintain an adequate privacy program that was sufficient to protect users and enable them to exercise informed consent.

We may never know the full extent of the damage caused by the failure to provide adequate controls and protection to users. A month after the recent Cambridge Analytica reports, Facebook has not disclosed information on how many applications engaged in similar data collection, but has stated that it expects to have to audit thousands of suspicious applications. As before, it remains only externally reactive to public reports, for example suspending the company CubeYou after media covered its commercial activities. The Facebook developer platform was launched in 2007 and stronger protections for consumers were not implemented until 2015. Presumably many of those companies that developed platform application have shut down, contact details changed, and record trails lost. While Mr. Zuckerberg has committed to audit suspicious apps, it is clear that Facebook will never be able to fully assess the impact of its years of neglect.

Facebook now bears little resemblance to the company it was at the time of the consent decree, necessitating a vigorous investigation into its privacy practices across its range of products and activities. Since November 2011, its expansion and acquisitions have strengthened the company's dominance in the social networking market and increased the significance of the challenges posed to consumers. Consumers, civil society, and members of Congress have raised an expansive set of privacy concerns, including its collection of Internet traffic for surveilling competitors; purchase of personal information from data brokers; tracking of non-Facebook users across the web; and harvesting of communications metadata from phones. These allegations raise new issues relevant to the consent decree that should be in the scope of the FTC's review.

The FTC ordered the consent decree in response to Facebook's repeated failures to address privacy risks, and put into place rules on how the company should act to protect users. If its investigation find that Facebook has violated the consent decree or engaged in further unfair or deceptive acts and practices, it should seek both monetary penalties that provide redress for consumers and impose stricter oversight on Facebook. The FTC should consider further measures that rigorously protects consumers, such as:

- data minimization standards that requires Facebook to retain and use data only for services expressly requested by users;
- limits on the combining and sharing of data between Facebook-owned services;

⁶ "It's Time to Make Our Privacy Tools Easier to Find." Facebook. March 28, 2018. <https://newsroom.fb.com/news/2018/03/privacy-shortcuts/>

- transparency on the types of data that Facebook collects from users and from other sources, and to publicly account for how that data is used;
- restrictions on collection of data from its “social plug-ins,” cross-device tracking, and or data brokers;
- appointment of a third-party monitor to oversee changes to Facebook’s privacy and data use policies and practices, with periodic reinvestigation; and,
- organizational changes to ensure that privacy and data use is protected at all levels.

While the Cambridge Analytica revelations have raised awareness to Facebook’s failure to provide users with adequate information or safeguards to protect privacy, many have raised legitimate and broad-reaching concerns about the company’s practices beyond a single ‘bad actor’ problem. Mr. Zuckerberg has acknowledged that the incident was a breach of trust between Facebook and its users, a broken promise that requires redress for consumers and enforceable commitments that deter further breaches. It is time for the FTC to thoroughly and rigorously reassess Facebook’s privacy practices and put into place rules that finally protect consumers.

Thank you for your attention to this important matter.

Sincerely,



Richard Blumenthal
United States Senate

Attachment 1

Global Science Research (GSR) Terms of Service

GSRApp APPLICATION END USER TERMS AND CONDITIONS

1. **The Parties:** This Agreement (“Agreement”) is between Global Science Research (“We”, “Us” or “GSR”), which is a research organisation registered in England and Wales (Number: 9060785) with its registered office based at Magdelene College, Cambridge, UK CB3 0AG, and the User of the Application (“You” or “User”).
2. **Agreement to Terms:** By using GSRApp APP (“Application”), by clicking “OKAY” or by accepting any payment, compensation, remuneration or any other valid consideration, you consent to using the Application, you consent to sharing information about you with us and you also accept to be bound by the Terms contained herein.
3. **Purpose of the Application:** We use this Application as part of our research on understanding how people's Facebook data can predict different aspects of their lives. Your contribution and data will help us better understand relationships between human psychology and online behaviour.
4. **Data Security and Storage:** Data security is very important to us. All data is stored on an encrypted server that is compliant with EU Directive 95/46/EC on the protection of individuals with regard to the processing of personal data.
5. **Your Statutory Rights:** Depending on the server location, your data may be stored within the United States or in the United Kingdom. If your data is stored in the United States, American laws will regulate your rights. If your data is stored within the United Kingdom (UK), British and European Union laws will regulate how the data is processed, even if you live in the United States. Specifically, data protection and processing falls under a law called the Data Protection Act 1998. Under British and European Union law, you are considered to be a “Data Subject”, which means you have certain legal rights. These rights include the ability to see what data is stored about you. Where data held in the EU is transferred to the United States, GSR will respect any safe harbour principles agreed between the United States Department of Commerce and the European Commission. The GSR Data Controller can be contacted by e-mail at alexbkogan@gmail.com.
6. **Information Collected:** We collect any information that you choose to share with us by using the Application. This may include, inter alia, the name, demographics, status updates and Facebook likes of your profile and of your network.
7. **Intellectual Property Rights:** If you click “OKAY” or otherwise use the Application or accept payment, you permit GSR to edit, copy, disseminate, publish, transfer, append or merge with other databases, sell, licence (by whatever means and on whatever terms) and archive your contribution and data. Specifically, agreement to these Terms also means you waive any copyright and other intellectual property rights in your data and contribution to GSR, and grant GSR an irrevocable, sublicenseable, assignable, non-

exclusive, transferrable and worldwide license to use your data and contribution for any purpose. You acknowledge that any and all intellectual property rights and database rights held in your data or contribution that is acquired by GSR or the Application will vest with GSR and that you will not have any claim in copyright, contract or otherwise. Nothing in this Agreement shall inhibit, limit or restrict GSR's ability to exploit, assert, transfer or enforce any database rights or intellectual property rights anywhere in the world. You also agree not attempt to appropriate, assert claim to, restrict or encumber the rights held in, interfere with, deconstruct, discover, decompile, disassemble, reconstruct or otherwise reverse-engineer the Application, the data collected by the Application or any other GSR technology, algorithms, databases, methods, formulae, compositions, designs, source code, underlying ideas, file formats, programming interfaces, inventions and conceptions of inventions whether patentable or un-patentable.

8. **Informed Consent:** By signing this form, you indicate that you have read, understand, been informed about and agree to these Terms. You also are consenting to have your responses, opinions, likes, social network and other related data recorded and for the data collected from you to be used by GSR. If you do not understand these Terms, or if you do not agree to them, then we strongly advise that you do not continue, do not click "OKAY", do not use the Application and do not to collect any compensation from us.
9. **Variation of Terms:** You permit GSR to vary these Terms from time to time to comply with relevant legislation, for the protection of your privacy or for commercial reasons. If you choose to provide us with your e-mail address, notice of any variation will be sent to that e-mail address. If you do not provide us with an e-mail address, you waive your right to be notified of any variation of terms.
10. **Rights of Third Parties:** A person who is not a Party to this Agreement will not have any rights under or in connection with it.

THISISYOURDIGITALLIFE APP APPLICATION END USER TERMS AND CONDITIONS

1. The Parties: This Agreement ("Agreement") is between Global Science Research ("We", "Us" or "GSR"), which is a research organisation registered in England and Wales (Number: 9060785) with its registered office based at St John's Innovation Centre, Cowley Road, Cambridge, CB4 0WS, and the User of the Application ("You" or "User").
2. Agreement to Terms: By using THISISYOURDIGITALLIFE APP ("Application"), by clicking "OKAY" or by accepting any payment, compensation, remuneration or any other valid consideration, you consent to using the Application, you consent to sharing information about you with us and you also accept to be bound by the Terms contained herein.
3. Purpose of the Application: We use this Application to (a) provide people an opportunity to see their predicted personalities based on their Facebook information, and (b) as part of our research on understanding how people's Facebook data can predict different aspects of their lives. Your contribution and data will help us better understand relationships between human psychology and online behaviour.
4. Data Security and Storage: Data security is very important to us. All data is stored on an encrypted server that is compliant with EU Directive 95/46/EC on the protection of individuals with regard to the processing of personal data.
5. Your Statutory Rights: Depending on the server location, your data may be stored within the United States or in the United Kingdom. If your data is stored in the United States, American laws will regulate your rights. If your data is stored within the United Kingdom (UK), British and European Union laws will regulate how the data is processed, even if you live in the United States. Specifically, data protection and processing falls under a law called the Data Protection Act 1998. Under British and European Union law, you are considered to be a "Data Subject", which means you have certain legal rights. These rights include the ability to see what data is stored about you. Where data held in the EU is transferred to the United States, GSR will respect any safe harbour principles agreed between the United States Department of Commerce and the European Commission. The GSR Data Controller can be contacted by e-mail at info@globalscienceresearch.com.

6. Information Collected: We collect any information that you choose to share with us by using the Application. This may include, inter alia, the name, demographics, status updates and Facebook likes of your profile and of your network.

7. Intellectual Property Rights: If you click "OKAY" or otherwise use the Application or accept payment, you permit GSR to edit, copy, disseminate, publish, transfer, append or merge with other databases, sell, licence (by whatever means and on whatever terms) and archive your contribution and data. Specifically, agreement to these Terms also means you waive any copyright and other intellectual property rights in your data and contribution to GSR, and grant GSR an irrevocable, sublicenceable, assignable, non-exclusive, transferrable and worldwide license to use your data and contribution for any purpose. You acknowledge that any and all intellectual property rights and database rights held in your data or contribution that is acquired by GSR or the Application will vest with GSR and that you will not have any claim in copyright, contract or otherwise. Nothing in this Agreement shall inhibit, limit or restrict GSR's ability to exploit, assert, transfer or enforce any database rights or intellectual property rights anywhere in the world. You also agree not attempt to appropriate, assert claim to, restrict or encumber the rights held in, interfere with, deconstruct, discover, decompile, disassemble, reconstruct or otherwise reverse-engineer the Application, the data collected by the Application or any other GSR technology, algorithms, databases, methods, formulae, compositions, designs, source code, underlying ideas, file formats, programming interfaces, inventions and conceptions of inventions whether patentable or un-patentable.

8. Informed Consent: By signing this form, you indicate that you have read, understand, been informed about and agree to these Terms. You also are consenting to have your responses, opinions, likes, social network and other related data recorded and for the data collected from you to be used by GSR. If you do not understand these Terms, or if you do not agree to them, then we strongly advise that you do not continue, do not click "OKAY", do not use the Application and do not to collect any compensation from us.

9. Variation of Terms: You permit GSR to vary these Terms from time to time to comply with relevant legislation, for the protection of your privacy or for commercial reasons. If you choose to provide us with your e-mail address, notice of any variation will be sent to that e-mail address. If you do not provide us with an e-mail address, you waive your right to be notified of any variation of terms. 10. Rights of Third Parties: A person who is not a Party to this Agreement will not have any rights under or in connection with it.

- [Privacy Policy](#)

- Powered by **Global Science Research**

© 2014 Global Science Research LTD. All content is copyrighted. St John's Innovation Centre,
Cowley Road, Cambridge, CB4 0WS

Email: info@globalscienceresearch.com

Attachment 2

Sandy Parakilas Letter

Sandy Parakilas

Dear Senator Blumenthal,

In 2011 and 2012, I led the team responsible for overseeing Facebook's data policy enforcement efforts governing third-party application developers who were using Facebook's App Platform, and responding to violations of that policy.

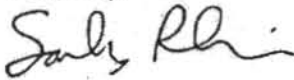
In my first week on the job, I was told about a troubling feature of the App Platform: there was no way to track the use of data after it left Facebook's servers. That is, once Facebook transferred user data to the developer, Facebook lost all insight into or control over it. To prevent abuse, Facebook created a set of platform policies that forbade certain kinds of activity, such as selling the data or passing it to an ad network or data broker such as Cambridge Analytica.

Facebook had the following tools to deal with developers who abused the platform policies: it could call the developer and demand answers; it could demand an audit of the developer's application and associated data storage, a right granted in the platform policies; it could ban the developer from the platform; it could sue the developer for breach of the policies; or it could do some combination of the above. During my sixteen months at Facebook, I called many developers and demanded compliance, but I don't recall the company conducting a single audit of a developer where the company inspected the developer's data storage. Lawsuits and outright bans for data policy violations were also very rare.

Despite the fact that executives at Facebook were well aware that developers could, without detection, pass data to unauthorized fourth parties (such as what happened with Cambridge Analytica), little was done to protect users. A similar, well-publicized incident happened in 2010, where Facebook user IDs were passed by apps to a company called Rapleaf, which was a data broker. Despite my attempts to raise awareness about this issue, nothing was done to close the vulnerability. It was difficult to get any engineering resources assigned to build or maintain critical features to protect users.

Unfortunately, Facebook's failure to address this clear weakness, during my time there or after I left, led to Cambridge Analytica's misappropriation of tens of millions of Americans' data.

Sincerely,

A handwritten signature in black ink, appearing to read "Sandy Parakilas". The signature is written in a cursive, flowing style.

Sandy Parakilas

JOSH HAWLEY
MISSOURI

KYLE PLOTKIN
CHIEF OF STAFF

DIRKREIN OFFICE BUILDING
508 40A
TELEPHONE: (202) 224-6164
FAX: (202) 225-0526
WWW.HAWLEY.SENATE.GOV

United States Senate

WASHINGTON, DC 20510-2509

COMMITTEES
JUDICIARY
ARMED SERVICES
HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS
SMALL BUSINESS
AND ENTREPRENEURSHIP
AGING

March 11, 2019

Joseph J. Simons
Chairman
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Dear Chairman Simons:

This week, the Senate Judiciary Committee will hold a hearing on the approaches to privacy that California and the European Union have taken in recent months and how those approaches have affected competition.

For too long our nation has put off accounting for the price we paid in return for the benefits of the online platforms that now dominate American culture and industry. These debates cross party lines, implicating election integrity, free speech, privacy, competition, and many other issues. But these debates include a central, shared concern that the new custodians of once-diffuse information have abused the power they amassed and neglected their responsibilities.

These companies have failed us. Washington has failed us. The FTC has a special role to play in protecting consumers, but it too has failed us. Any robust definition of consumer welfare must acknowledge that these companies have harmed consumers by conditioning participation in the modern public square on giving away enormous—and growing—amounts of personal information and by leveraging scale to cripple emerging competitors in their infancy. Yet the approach the FTC has taken to these issues has been toothless.

Even a brief snapshot of the track-record for Google and Facebook is alarming:

- According to a recent lawsuit based on 80,000 pages of internal Facebook records, Facebook appears to have fraudulently inflated—by as much as 900%—metrics about how much users were interacting with video ads, prompting widespread layoffs in the news media industry that harmed consumers. Until this controversy, the company had long resisted demands for third-party ad metric auditing.
- In 2011, Facebook entered into a settlement with the FTC after the FTC charged Facebook with massive deception about how it was collecting data. Substantial evidence indicates that Facebook breached this agreement.

- When Facebook acquired its competitor WhatsApp, it promised to maintain separation between the two platforms. It later broke that promise, prompting a \$122 million fine from the European Union.
- When Facebook purchased Onavo, it began to use the application to monitor how persons were using other apps, including Facebook's competitor Snapchat. Apple recently banned the app from its app store because Facebook's misuse of that application violated Apple's terms of service. Google recently disabled its similar Screenwise Meter app.
- Google has consistently misinformed users about its use of geolocation data, continuing to collect data even when users disabled location services and even when phones are turned off and lack SIM cards.
- Google adopts definitions contrary to what regular consumers would expect, enabling them to continue to collect personal information even when users tell Google not to. For example, Google continues to track geolocation information even when users disable "Location Services" and "Location History" because it chooses to define certain geolocation information under a different category—"Web and App Activity"—a title that includes no reference to geolocation.
- Google also uses misleading terms like "location" when it collects a much broader category of non-location data, including the type of motion (*e.g.*, walking, biking, or driving), barometric pressure, Wi-Fi connectivity, MAC addresses, and battery charge status.
- Google has misled consumers by selling products embedded with data-collection devices inessential to product functionality and never disclosed on product packaging, like the secret microphone Google installed in its Nest Guard home alarm system without alerting purchasers.
- Platforms have often allowed data to fall into the hands of unaccountable third parties, shattering the illusion of data anonymity. Third parties demonstrated that they could track staff members for President Trump based on their positions on the inaugural podium. And recent reports suggest that nearly anybody can purchase on the black market real-time location information with nothing more than a phone number.

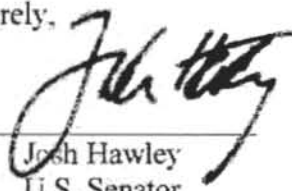
There is a common pattern to these discoveries: Big tech companies adopt an "ask forgiveness rather than seek permission" mentality to their repeated deceptions of consumers and encroachments on user privacy. A handful of their most egregious practices are discovered long after they are initiated—usually by the media—and the companies offer only half-hearted apologies. Occasionally, clear lines are breached, as with Facebook's violation of the FTC consent decree. Too often, though, public shaming is the only consequence.

This is not what Americans were promised. These companies provide benefits to consumers, but those benefits can be secured without so deep a cost.

I appreciate well the limits of the FTC, and Congress bears primary responsibility for this and other matters. But I am concerned that the FTC has not investigated these companies and enforced the law as vigorously as it should. I am cautiously optimistic about the creation of an FTC task force to address these issues, and I hope that this task force will have more substance than show.

I urge you to investigate and act to stop the abuses I have documented, and myriad others I have left unmentioned, with all appropriate speed. At the earliest possible date, alert Congress to all apparent gaps in your authority that stymie such work. There is no excuse for inaction, by the Commission or by Congress. I hope to work together with you to address these challenges.

Sincerely,



Josh Hawley
U.S. Senator

United States Senate

WASHINGTON, DC 20510

March 22, 2018

The Honorable Maureen K. Ohlhausen
Acting Chairman
Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580

Dear Acting Chairman Ohlhausen:

We write in response to recent reports that the Federal Trade Commission (FTC) will investigate Facebook for the breach involving the personal data of 50 million Americans and to express our view that such an action would be a positive step toward determining whether the media company violated a 2011 FTC consent decree. We urge the FTC to conduct a thorough investigation—which should include examining any and all potential violations of users’ privacy—to assess whether Facebook violated the decree or any other applicable laws.

As you know, the 2011 consent decree was negotiated to settle FTC complaints that Facebook was deceiving consumers by sharing or publicizing private user information after assuring users that the information would be kept private. In particular, the consent decree required that Facebook obtain users’ “affirmative express consent” before sharing a user’s nonpublic information with any third party. It also mandated that Facebook establish a comprehensive privacy program to address privacy risks associated with the development and management of new and existing products and services.

Recent reports concerning Cambridge Analytica’s access to the Facebook user data of millions of Americans raise serious questions about whether Facebook is in compliance with the terms of the consent decree. Two former FTC Bureau of Consumer Protection officials have suggested that Facebook may have violated the terms of that decree. One commented that each violation of the consent decree could carry a \$40,000 fine, which could result in an aggregate fine amounting to billions of dollars.

Facebook plays an important role in our society. Roughly two-thirds of American adults now report that they are Facebook users, and roughly three-quarters of those users access Facebook on a daily basis.^[1] Facebook has a legal responsibility to ensure user data is secure and that its policies are transparent—which includes upholding the privacy rights of its users and keeping its promises when it comes to notifying them if there has been a violation.

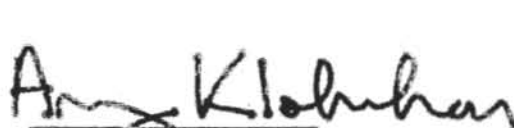
Accordingly, we respectfully request responses to the following questions by April 13, 2018:

^[1] Aaron Smith & Monica Anderson, Pew Research Center, Social Media Use in 2018 (Mar. 1, 2018), at <http://www.pewinternet.org/2018/03/01/social-media-use-in-2018/>.

- Will the FTC's investigation include an inquiry into whether Facebook's release of user data to Cambridge Analytica constitutes a violation of Facebook's obligations under its 2011 consent decree or under any other law?
- Will the FTC's investigation address any other unconsented releases of Facebook user data that may have occurred since the execution of the 2011 consent decree and whether any such releases violate the terms of the consent decree or any other law?
- Will the FTC's investigation look into whether the comprehensive privacy program that Facebook was required to establish under the 2011 consent decree was and remains adequate (1) to address privacy risks associated with the development and management of new and existing products and services, and (2) to protect the privacy and confidentiality of consumers' information?
- Will the FTC commit to giving a confidential briefing on the progress of the FTC's investigation to members of the Senate Judiciary Committee, as well as Judiciary Committee staff, at an appropriate point in the investigation?
- Will the FTC commit to issuing a public statement concerning the outcome of the investigation upon its conclusion, so that the public can be made aware of the circumstances surrounding this significant breach?

Thank you for your consideration of this matter.

Sincerely,



Amy Klobuchar
United States Senator



Kamala D. Harris
United States Senator

United States Senate

WASHINGTON, DC 20510

April 8, 2019

The Honorable Joseph J. Simons
Chairman
Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, DC 20580

The Honorable Noah Joshua Phillips
Commissioner
Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, DC 20580

The Honorable Rohit Chopra
Commissioner
Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, DC 20580

The Honorable Rebecca Kelly Slaughter
Commissioner
Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, DC 20580

The Honorable Christine S. Wilson
Commissioner
Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, DC 20580

Dear Chairman Simons and Commissioners Phillips, Chopra, Slaughter, and Wilson:

We write to urge the Federal Trade Commission (FTC) to take action in response to concerns regarding potential privacy, data security, and antitrust violations involving online platforms. We also call on the FTC to provide additional transparency into its ongoing investigations to ensure that consumers are protected from harmful conduct relating to digital markets.

In the past few years, rapid changes in technology have reshaped our economy and transformed the daily lives of millions of Americans—in many ways for the better. But during that same time, a small number of firms have grown to dominate key digital markets. For example, in digital search, Google, Inc. now has approximately 90 percent of web search volume, and in digital advertising, Google and Facebook account for nearly 60 percent of U.S. digital ad spending, with Amazon a distant third at just under 9 percent. This type of market dominance has amplified concerns about how those companies protect consumers' online information and about possible anticompetitive conduct that could harm consumers, innovation, and small business growth.

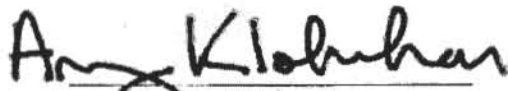
The intensive collection and monetization of consumers' personal data by digital platforms, as well as reported breaches of consumer data held by these companies, has raised significant questions regarding privacy and data security. In particular, some have expressed concern that

Facebook's recently announced plans to integrate its three messaging platforms—WhatsApp, Instagram, and Messenger—may lead to Facebook sharing user data between its platforms. As Congress considers legislation to enact stronger safeguards for consumers' online privacy, we urge the FTC to use its existing authority to protect the privacy and security of consumers' online data.


We understand that the FTC does not typically comment on nonpublic investigations, but the public discussion surrounding Google and other companies' conduct have made this a uniquely important national issue. Accordingly, we respectfully request that the FTC consider publicly disclosing whether it is conducting an investigation of Google and/or other major online platforms and describe, in general terms, the nature of the conduct under examination in any such investigations. Going forward, we also encourage the FTC to disclose the existence of non-public investigations that may be of significant public interest, consistent with the FTC's legal obligations.

Thank you for your attention to these critical issues.

Sincerely,



Amy Klobuchar
United States Senator



Marsha Blackburn
United States Senator

EDWARD J. MARKEY
MASSACHUSETTS

COMMITTEES:

ENVIRONMENT AND PUBLIC WORKS

FOREIGN RELATIONS

RANKING MEMBER:

SUBCOMMITTEE ON EAST ASIA, THE PACIFIC,
AND INTERNATIONAL CYBERSECURITY POLICY

COMMERCE, SCIENCE, AND TRANSPORTATION

RANKING MEMBER:

SUBCOMMITTEE ON
SPACE, SCIENCE, AND COMPETITIVENESS

SMALL BUSINESS AND ENTREPRENEURSHIP

CHAIRMAN:

U.S. SENATE CLIMATE CHANGE TASK FORCE

United States Senate

May 3, 2018

SUITE SD-255
DIRKSEN BUILDING
WASHINGTON, DC 20510-2117
202-224-2742

975 JFK FEDERAL BUILDING
15 NEW SLIDBURY STREET
BOSTON, MA 02202
617-565-8519

222 MILLIKEN BOULEVARD, SUITE 312
FALL RIVER, MA 02721
508-677-0523

1550 MAIN STREET, 4TH FLOOR
SPRINGFIELD, MA 01103
413-785-4610

The Honorable Joseph Simons
Chairman
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20530

The Honorable Maureen Ohlhausen
Commissioner
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20530

The Honorable Noah Phillips
Commissioner
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20530

The Honorable Rohit Chopra
Commissioner
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20530

The Honorable Rebecca Slaughter
Commissioner
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20530

Dear Chairman Simons, Commissioner Ohlhausen, Commissioner Phillips, Commissioner Chopra, and Commissioner Slaughter:

In your leadership positions at the Federal Trade Commission (FTC), each of you has the significant responsibility of protecting American consumers from a vast set of threats, including privacy infringement online. Recent reporting regarding the social media platform Facebook points to a disturbing record of failure to protect users' privacy and misuse of Americans' personal data. These revelations strongly suggest that Facebook violated a 2011 settlement with the FTC. I support the FTC's decision to launch an investigation into Facebook's privacy policies and practices. I write to request information about your agency's role in ensuring the privacy of Facebook users and to suggest additional safeguards Facebook should be required to implement.

According to recent media coverage and Facebook CEO Mark Zuckerberg's testimony before the United States Senate, in 2013, Aleksandr Kogan, a Lecturer at Cambridge University,

developed an app that collected Facebook user data for psychological profiling.¹ The application, “thisisyourdigitallife,” obtained information from tens of millions of Facebook users, while only 270,000 users installed the application themselves and explicitly consented to sharing their data. Kogan was able to collect this data after telling Facebook that information would be used for academic purposes. However, he later shared this private data with the political consulting firm Cambridge Analytica, which utilized the information without users’ knowledge or consent to target political messages online.

Additionally, Facebook recently announced that “malicious actors” took advantage of Facebook’s search function to amass information about and discover the identities of most of Facebook’s two billion users. These hackers collected phone numbers and email addresses on the “Dark Web,” a corner of the internet where criminals post illicit content, and used Facebook’s system for recovering accounts to build comprehensive profiles of Facebook users.²

These invasions of privacy and breeches of user trust are unacceptable and amount to compelling evidence that Facebook violated the 2011 settlement with the FTC. The consent decree included in this settlement prohibited Facebook from misrepresenting privacy or security of consumers’ personal information; required Facebook to obtain users’ affirmative express consent prior to making changes that override user privacy preferences; required Facebook to prevent access to user data more than 30 days after the user has deleted her account; required Facebook to establish and maintain a comprehensive privacy program; and required Facebook to obtain independent audits confirming that its privacy protections comply with the FTC order.

I am concerned that Facebook failed to comply with this consent decree. I urge the FTC to use all necessary resources to investigate Facebook, demand that Facebook pay all monetary penalties it owes as a result of any transgressions of the 2011 order, and instruct Facebook to institute additional safeguards. They should include:

- Require Facebook to make future audits of Facebook’s privacy practices, as required by the 2011 consent decree, readily available to the public upon request when possible;
- Require Facebook to cease all tracking of users across websites after users have logged out of their Facebook accounts;
- Require Facebook to suspend deployment of facial recognition tools pending completion of the FTC investigation;
- Prohibit Facebook from repealing or weakening its current policy prohibiting applications from collecting users’ data based on their “friends” permission;
- Take all necessary steps to ensure the independence of the entity or entities conducting required privacy audits under the 2011 order;

¹ Matthew Rosenberg, Nicholas Confessore & Carole Cadwalladr, *How Trump Consultants Exploited the Facebook Data of Millions*, N.Y. Times (Mar. 17, 2018), <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>.

² Craig Timberg, Tony Romm, and Elizabeth Dwoskin, *Facebook: ‘Malicious actors’ used its tools to discover identities and collect data on a massive global scale*, Washington Post (April 4, 2018), [https://www.washingtonpost.com/news/the-switch/wp/2018/04/04/facebook-said-the-personal-data-of-most-its-2-billion-users-has-been-collected-and-shared-with-outsiders/?hpid=hp_hp-top-table-main-facebook-data%3Ahomepage%2Ft%3Afacebook&hpid=hp_hp-top-table-main-facebook-data%3Ahomepage%2Ft%3Afacebook&utm_term=.3ede52a719e7](https://www.washingtonpost.com/news/the-switch/wp/2018/04/04/facebook-said-the-personal-data-of-most-its-2-billion-users-has-been-collected-and-shared-with-outsiders/?hpid=hp_hp-top-table-main-facebook-data%3Ahomepage%2Ft%3Afacebook%3Ahomepage%2Ft%3Afacebook&hpid=hp_hp-top-table-main-facebook-data%3Ahomepage%2Ft%3Afacebook&utm_term=.3ede52a719e7).

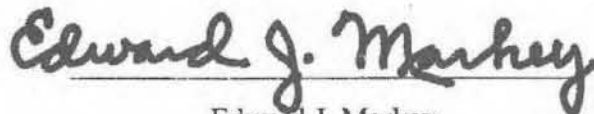
- Require Facebook to release publicly and automatically transmit to the FTC any consumer complaints or records that contradict, qualify, or call into question Facebook's compliance with the consent decree; and
- Require Facebook leadership to routinely brief its employees on the company's rights to review third party applications and its obligations to protect users' privacy under law and its own policies.

In addition, I request answers to the following questions by May 24, 2018:

- Has Facebook provided the FTC with all audits required by the 2011 consent order?
 - If yes, what entity or entities currently conduct these audits? Please provide all relevant information about this entity's independence and ability to conduct unbiased analyses. If no, why not?
 - Who at the FTC is currently responsible for reviewing these audits?
- What steps is the FTC taking as part of its current investigation to ensure Facebook's compliance with the 2011 order that the FTC was not taking before it initiated the current investigation?
- When will the findings of the FTC's investigation be made available to the public?

Thank you for your attention to these important matters.

Sincerely,



Edward J. Markey
United States Senator

ROBERT J. WITTMAN
1ST DISTRICT, VIRGINIA

WASHINGTON OFFICE:

2055 Rayburn House Office Building
Washington, DC 20515
(202) 225-4261

HOUSE ARMED SERVICES COMMITTEE
CHAIRMAN, READINESS SUBCOMMITTEE
SEAFORCE AND PROJECTION FORCES
SUBCOMMITTEE

NATURAL RESOURCES COMMITTEE
ENERGY AND MINERAL
RESOURCES SUBCOMMITTEE
WATER, POWER, AND OCEANS SUBCOMMITTEE

CO-CHAIR, CONGRESSIONAL
SPORTSMEN'S CAUCUS

CO-CHAIR, CONGRESSIONAL
SHIPBUILDING CAUCUS

CO-CHAIR, CONGRESSIONAL
CHESAPEAKE BAY CAUCUS

Congress of the United States
House of Representatives
Washington, DC 20515

DISTRICT OFFICES:

Stafford Office
95 Dunn Drive Suite 201
Stafford, VA 22556
(540) 659-2734

Hanover Office
6501 Mechanicsville Turnpike
Suite 102
Mechanicsville, VA 23111
(804) 730 - 6595

Middle Peninsula Office
508 Church Lane
P.O. Box 3106
Tappahannock, VA 22560
(804) 443-0668

www.wittman.house.gov

April 24, 2019

Ms. Jeanne Bumpus
Director, Office of Congressional Relations
Federal Trade Commission
600 Pennsylvania Ave NW Rm 404
Washington, DC 20580-0001

Dear Ms. Bumpus:

Enclosed is a copy of correspondence I received from my constituent (b)(6) I believe you will find the letter self-explanatory.

I would appreciate you reviewing the enclosed documentation and providing me with any information that may be helpful to my constituent. Please direct your response to my office at:

95 Dunn Drive, Ste. 201
Stafford, VA 22556
(540) 659-2734 phone (540) 659-2737 fax

I am grateful for any assistance you may be able to provide in this matter.

Sincerely,



Rob Wittman
Member of Congress

RJW/kk

PATRICK J. TOOMEY
PENNSYLVANIA

COMMITTEES:
BANKING, HOUSING, AND
URBAN AFFAIRS
COMMERCE, SCIENCE, AND
TRANSPORTATION
BUDGET
JOINT ECONOMIC COMMITTEE

United States Senate

WASHINGTON, DC 20510

March 7, 2012

Bureau of Consumer Protection
Office of the Attorney General
Via facsimile: 717 787 8242

CC: Federal Trade Commission
Via facsimile: 202 326 3585

Dear whom it may concern,

My constituent, (b)(6) has contacted me regarding his concern with spam emails to his private email address after the closing of his Facebook account.

(b)(6) enclosed statement details the situation. I bring this to your attention for your comment on whatever action you deem necessary, and to the attention of the FTC for pattern tracking.

Please provide me with whatever information you feel may help address my constituent's concerns. Please address your response to my Constituent Service Advocate, Imani Johnson, at:
1628 John F. Kennedy Blvd
Suite 1702
Philadelphia, PA 19103
Phone: 215 241 1090
Fax: 215 241 1095
Email: imani_johnson@toomey.senate.gov

Thank you for your attention to this matter. I look forward to hearing from you.

Sincerely,



Pat Toomey
U. S. Senator

From: Veale, Adam <Adam.Veale@mail.house.gov>
Sent: Thursday, May 09, 2019 11:54 AM
To: Congressional Relations <congressionalrelations@ftc.gov>
Subject: Congressional Inquiry (b)(6)

To whom it may concern,

Please see the attached privacy release form from our constituent (b)(6). (b)(6) is a business owner who filed a complaint with the FTC regarding Facebook's use of demographic statistics. Essentially, the constituent is unhappy with her market reach when she pays for Facebook advertising and has been refused documentation from Facebook to assist her with her advertising. She would like a response from FTC on letterhead describing FTC's role (or lack thereof) in this matter. Thank you very much for providing a response that Congresswoman McBath can share with her constituent.

I would also like to direct this message to the attention of Derrick, who indicated he would be sending information re: a district event with FTC. Thanks so much!

All the best,

Adam Veale
Constituent Services Representative
Congresswoman Lucy McBath (GA-6)
E: adam.veale@mail.house.gov
P: 470.773.6330

Hope M. Babcock
Angela J. Campbell
Directors
Andrew Jay Schwartzman
Benton Senior Counselor
James T. Graves
Ariel Nelson
Adam Riedel
Staff Attorneys

600 New Jersey Avenue NW
Suite 312
Washington, DC 20001-2075
Telephone: 202-662-9535
Fax: 202-662-9634



GEORGETOWN LAW
INSTITUTE FOR PUBLIC REPRESENTATION

October 3, 2018

VIA E-MAIL

Donald S. Clark, Secretary of the Commission
Andrew Smith, Director, Bureau of Consumer Protection
Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, DC 20580

Dear Mr. Clark and Mr. Smith,

Campaign for a Commercial-Free Childhood (CCFC), by its counsel, the Institute for Public Representation, together with the undersigned organizations, write to ask the Federal Trade Commission to investigate and take enforcement action against Facebook for violating the Children’s Online Privacy Protection Act. Facebook’s messaging application for children under 13, Messenger Kids, is the first major social media platform designed specifically for young children—as young as five years of age. Messenger Kids violates COPPA by collecting personal information from children without obtaining verifiable parental consent or providing parents with clear and complete disclosures of Facebook’s data practices.

In January 2018, CCFC asked Facebook to discontinue its Messenger Kids app because of the developmental risks it poses to children. In a letter signed by 118 public health advocates and organizations, CCFC said “a growing body of research demonstrates that excessive use of digital devices and social media is harmful to children and teens, making it very likely this new app will undermine children’s healthy development.”¹

In addition to these serious child development issues, Facebook’s Messenger Kids application does not comply with COPPA—despite Facebook’s claims to the contrary.² Messenger Kids

¹ Letter from Campaign for a Commercial-Free Childhood *et al.* to Mark Zuckerberg, Facebook (Jan. 30, 2018), <http://www.commercialfreechildhood.org/sites/default/files/develop-generate/gaw/FBMessengerKids.pdf>.

² Messenger Kids, <https://messengerkids.com/> (“Is Messenger Kids COPPA compliant? Yes. Messenger Kids is designed to be compliant with important child privacy laws like the Children’s Online Privacy Protection Act (COPPA).”).

falls short of COPPA compliance in at least two ways. First, the application’s parental consent mechanism is not reasonably calculated to ensure that the person providing consent is the child’s parent—or even an adult. In fact, it employs a mechanism similar to one that the FTC has previously rejected. Second, Facebook’s privacy notice for Messenger Kids³ is confusing and incomplete, preventing parents from making informed decisions about whether to allow Facebook to collect their children’s sensitive personal information.

A. Facebook Messenger Kids does not have a COPPA-compliant mechanism for obtaining verifiable parental consent.

COPPA requires operators of online services directed at children to obtain verifiable parental consent before collecting, using, or disclosing sensitive information about children under 13.⁴ The consent mechanism must be reasonably calculated, in light of available technology, to ensure that the person providing consent is the child’s parent.⁵ Messenger Kids does not meet this requirement.

The Messenger Kids application allows anyone who has a Facebook account and claims to be an adult to create and “verify” an account for a child. The verification process works as follows: After the app is downloaded to a child’s device, someone (ostensibly the child’s parent) authenticates to the app with his or her Facebook username and password. That person can then create an account for the child and add contacts to the child’s contact list through the “parent’s” own Facebook account.⁶ The child is then able to send messages to the person who created the account and any of the child’s contacts.

This method is not “reasonably calculated, in light of available technology, to ensure that the person providing consent is the child’s parent.”⁷ The only prerequisites to creating a Messenger Kids account for a child are a Facebook account of a user who claims to be 18 or older and physical access to a child’s device. Because Facebook does not verify ages, the mere existence of a Facebook account is insufficient to establish that a person is an adult, much less that the supposed adult is a child’s parent or guardian.

The FTC has previously denied approval for a similar “verifiable parental consent” mechanism under COPPA.⁸ In 2013, the FTC rejected the application of AssertID, which proposed to use Facebook’s social graph as a method of authentication. AssertID’s product would have “ask[ed] a parent’s ‘friends’ on a social network to verify the identity of the parent and the existence of the parent-child relationship.” The method would have been “premised on verification by a

³ Facebook, *Messenger Kids Privacy Policy* (Dec. 4, 2017), <https://www.facebook.com/legal/messengerkids/privacypolicy>.

⁴ 15 U.S.C. § 6502(b)(1)(A)(ii).

⁵ 16 C.F.R. § 312.4.

⁶ Messenger Kids, <https://messengerkids.com/>.

⁷ 16 C.F.R. § 312.5(b)(1).

⁸ Under 16 C.F.R. § 312.12, companies may apply for the Commission’s approval of parental consent mechanisms not enumerated in Section 312.5(b).

minimum number of verifiers” and would have required “that a minimum ‘trust score’ be met” for approval.⁹

The Commission held that approval would be premature “without relevant research or marketplace evidence demonstrating the efficacy of social-graph verification and that such a method is reasonably calculated to ensure the person providing consent is the child’s parent.” The Commission was also “persuaded by commenters’ concerns about the reliability of social-graph verification.” It recognized that “users can easily fabricate Facebook profiles,” noted that about 8.7% of Facebook’s accounts at the time were fake, and cited comments “highlighting the fact that children under 13 have falsified their age information to establish social media accounts, including very active accounts with significant age-inflation.”¹⁰

Facebook’s parental consent mechanism for Messenger Kids is even less trustworthy than what AssertID proposed. Instead of relying on a person’s social graph, Facebook relies solely on a single user’s unverified assertions. As was the case with AssertID, Facebook has not shown any research or evidence that its verification method is reasonably calculated to ensure that the person providing consent is the child’s parent—or is even an adult.

Five years after the FTC rejected AssertID’s application, Facebook still cannot prevent fake accounts. Facebook reported last year that up to 270 million users were either “user-misclassified and undesirable” or duplicates of real accounts.¹¹ It is easy enough to create fake accounts that Russia used hundreds of them to interfere with the 2016 election.¹²

Our own testing shows that it is not difficult to create a fake account that can approve a Messenger Kids user. We created a brand new Facebook account for a fictional 18 year-old. We then used that account to approve a fictional Messenger Kids user. The entire process took five minutes.

What the FTC found in 2013 is still true: a Facebook account is insufficient to ensure that a person providing consent is the child’s parent.

⁹ Letter from Donald S. Clark, Secretary, FTC, to Keith Dennis, President, AssertID, Inc., FTC Matter No. P135415 (Nov. 12, 2013), <https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-denies-assertids-application-proposed-coppa-verifiable-parental-consent-method/131113assertid.pdf>.

¹⁰ *Id.*

¹¹ James Titcomb, *Facebook Admits up to 270m Users are Fake and Duplicate Accounts*, Telegraph (U.K.) (Nov. 2, 2017), <https://www.telegraph.co.uk/technology/2017/11/02/facebook-admits-270m-users-fake-duplicate-accounts/>

¹² Scott Shane, *The Fake Americans Russia Created to Influence the Election*, N.Y. Times (Sept. 7, 2017), <https://www.nytimes.com/2017/09/07/us/politics/russia-facebook-twitter-election.html>.

B. Facebook’s privacy policy for Messenger Kids is confusing and incomplete

The COPPA Rule also requires that notice to parents “must be clearly and understandably written, complete, and must contain no unrelated, confusing, or contradictory material.”¹³ Facebook’s notice fails this standard for two reasons. First, the notice is not clearly written or complete because it does not adequately inform parents about Facebook’s data-sharing practices. Second, the policy is incomplete because it does not clearly disclose how long Facebook retains children’s data.

Facebook’s privacy notice includes the following description of its third-party disclosure policy:

Our vendors and service providers. We may transfer information we collect to third party service providers that support our business, such as companies that provide technical infrastructure or support (like a content delivery network), provide customer service, or analyze how Messenger Kids is being used to help us improve the service. . . .

Facebook Family of Companies. Messenger Kids is part of Facebook, and we may share the information we collect in Messenger Kids within the family of companies that are part of Facebook to support the uses described above, and to improve the services provided by the FB family of companies. For example, parents use Facebook Messenger to communicate with their children on Messenger Kids, and Facebook uses information from Messenger Kids to support seamless cross-service communication.¹⁴

This language is vague and incomplete. It states that Facebook may transfer information to third parties to “support [its] business.” That phrase might be interpreted to cover almost anything, including transfers to advertising networks, data brokers, and analytics firms. Although Facebook lists non-exclusive examples of service providers that would support Facebook’s business, those examples could be interpreted narrowly or broadly. A parent reading that policy might reasonably assume a narrower interpretation of “support our business” while Facebook takes a broader view of the term. That ambiguity is confusing and potentially misleading.

The language in Facebook’s policy stating that data may be disclosed “to improve the services provided by the Facebook family of companies” is similarly vague.

¹³ 16 C.F.R. § 312.4(a).

¹⁴ Facebook, *Messenger Kids Privacy Policy* (Dec. 4, 2017), <https://www.facebook.com/legal/messengerkids/privacypolicy>.

Facebook’s reference to the “Facebook Family of Companies” is likewise confusing and incomplete. Facebook has acquired or merged with 66 different companies.¹⁵ Parents may not know which companies Facebook owns, and the Messenger Kids privacy policy does not say. Parents who want to know how widely Facebook might share their children’s data must find out for themselves by searching for a separate page that lists some, but not all, of the companies Facebook has bought. The Messenger Kids privacy policy does not even link to this page.

Facebook’s distinction between “the family of companies” and subsidiaries creates further confusion. According to Facebook’s “Help Center,” the “Facebook Family of Companies” includes Facebook Payments, the Onavo analytics company, WhatsApp, Oculus VR, Masquerade (whose products include face-tracking technologies), and the CrowdTangle social analytic platform.¹⁶ Missing from that list are “Facebook Products” such as Instagram, Messenger, Moments, Bonfire, Audience Network, and “other features, apps, technologies, software, products, or services.”¹⁷ Thus, even parents who manage to find the “Facebook Family of Companies” page would lack the information needed to give meaningful consent to the disclosure of their children’s sensitive personal information.

If Facebook does disclose information to third parties, its privacy notice may be incomplete by not naming them. Under the FTC’s COPPA Rule, a privacy notice must list “all operators collecting or maintaining personal information from children through the Web site or online service.”¹⁸ The FTC has long viewed “affiliates and subsidiaries” as third parties unless the affiliate relationship is clear to consumers.¹⁹ Thus, both third parties and companies owned by Facebook must be named.

Other required disclosures are also missing. For example, a privacy notice must tell parents that the operator “won’t require a child to disclose more information than is reasonably necessary to participate in an activity,” that parents “can agree to the collection and use of their child’s information, but still not allow disclosure to third parties unless that’s part of the service,” and

¹⁵ Steve Toth, *66 Facebook Acquisitions – The Complete List (2018)*, TechWyse (Jan. 24, 2018), <https://www.techwyse.com/blog/infographics/facebook-acquisitions-the-complete-list-infographic/>.

¹⁶ Facebook, *The Facebook Companies*, <https://www.facebook.com/help/111814505650678> (last visited Sept. 15, 2018).

¹⁷ Facebook, *What are the Facebook Products?*, <https://www.facebook.com/help/1561485474074139> (last visited Sept. 15, 2018).

¹⁸ 16 C.F.R. § 312.4(d)(1).

¹⁹ *Protecting Consumer Privacy in an Era of Rapid Change* 42, FTC (Mar. 2012), <http://ftc.gov/os/2012/03/120326privacyreport.pdf> (“The Commission maintains the view that affiliates are third parties, and a consumer choice mechanism is necessary unless the affiliate relationship is clear to consumers”).

that parents have the right to direct the operator to delete their child’s personal information.²⁰ These disclosures are either missing or incomplete in the Messenger Kids privacy notice.

The disclosures regarding parents’ rights to have their children’s personal information deleted are especially confusing and incomplete. The COPPA Rule requires that “an operator shall retain personal information collected online from a child for only as long as is reasonably necessary to fulfill the purpose for which the information was collected.”²¹ But the Messenger Kids privacy notice does not clearly indicate that Facebook deletes personal information on children when it is no longer needed.

Every message a child sends with Messenger Kids is “personal information.” Personal information protected by COPPA includes “information concerning the child or the parents of that child that the website collects online from the child and combines with an identifier described in [15 U.S.C. § 6501(8)].”²² A message from a child necessarily contains some “information concerning the child.” Each message on Messenger Kids is associated with the name of the child who sent or received the message. Thus, messages sent or received on Messenger Kids are personal information that Facebook must delete at a parent’s direction.

Facebook’s policy does not comply with that requirement. According to the Messenger Kids privacy notice, parents who want to stop Facebook from collecting their child’s personal information must delete their child’s account, at which time Facebook “will delete [the child’s] Messenger Kids registration information, information about their activity and contacts, and device information.”²³ The privacy notice does not state how long Facebook retains this information if a parent has not deleted his or her child’s account. The privacy notice also tells parents that “the messages and content your child sent to and received from others before their account was deleted may remain visible to those users.”²⁴ It is unclear how long those messages, which must remain on Facebook’s servers to be visible to any users, will stay visible.

C. Conclusion

Messenger Kids poses developmental risks for children. It also violates COPPA. Facebook does not obtain verifiable parental consent via a mechanism reasonably calculated to ensure that the person giving consent is the child’s parent, or even an adult. And Facebook does not give parents sufficient notice of its data practices to allow parents to make an informed choice whether to allow Facebook to access children’s personal information. We ask the Commission

²⁰ FTC, *Children’s Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business* (June, 2017), <https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance>. See also 16 C.F.R. § 312.4(d).

²¹ 16 C.F.R. § 312.10.

²² 15 U.S.C. § 6501(8)(G).

²³ Facebook, *Messenger Kids Privacy Policy* (Dec. 4, 2017), <https://www.facebook.com/legal/messengerkids/privacypolicy>.

²⁴ *Id.*

to investigate Facebook's violations of COPPA and to take all enforcement actions necessary to ensure compliance with the law.

Respectfully Submitted,

James T. Graves*
Angela J. Campbell
Institute for Public Representation
Georgetown University Law Center
600 New Jersey Ave NW, Suite 312
Washington, DC 20001
James.Graves@law.georgetown.edu
202-662-9545
*Counsel for Campaign for a Commercial-Free
Childhood*

Campaign for a Commercial-Free Childhood	Parents Across America
Badass Teachers Association	Parents Television Council
Centre for Child Honouring	Peace Educators Allied for Children Everywhere (P.E.A.C.E.)
Consumer Federation of America	Public Citizen
Defending the Early Years	The Story of Stuff
Electronic Privacy Information Center	TRUCE (Teachers Resisting Unhealthy Childhood Entertainment)
Media Education Foundation	United Opt Out National
MomsRising/MamásConPoder	USPIRG
New Dream	
Parent Coalition for Student Privacy	

* This letter was drafted primarily by Jae Ahn, a law student in the Institute for Public Representation Communication & Technology Clinic, under the supervision of clinic attorneys.

Center for Digital Democracy
Common Sense Kids Action
Constitutional Alliance
Consumer Action
Consumer Federation of America
Consumer Watchdog
Defending Rights & Dissent
Patient Privacy Rights
Privacy Rights Clearinghouse
Privacy Times
Public Citizen
U.S. Public Interest Research Group

June 11, 2018

Chairman Simons
Commissioner Ohlhausen
Commissioner Phillips
Commissioner Chopra
Commissioner Slaughter
Federal Trade Commission
600 Pennsylvania Ave., N.W.
Washington, D.C. 20580

Dear Chairman and Commissioners,

Common Sense is the nation's leading organization dedicated to helping kids and families thrive in a digital world. For over a decade, we have helped parents, teachers, and policymakers by providing unbiased information, trusted advice, and innovative tools to help them harness the power of media and technology as a positive force in all kids' lives. Common Sense has an uncommon reach, with more than 68 million users, half a million educators, and advocates in all fifty states supporting our policy initiatives. We write to follow up on our April 10 request (attached), where we asked that as you investigate Facebook's disclosure of the personal information of 87 million users to Cambridge Analytica and potential violations of the 2011 Consent Order, you in particular: (1) investigate how teens were affected, and (2) include specific provisions protecting users under 18 in any future decrees or orders.

Teens were potentially disproportionately harmed by Facebook's allowing apps to scrape friends' information; teen online behavior often includes significant sharing and use of third party apps (games). This disproportionate harm is particularly concerning given teens' special vulnerability online, as detailed in our April 10 request, and as recognized by the Commission as well as the U.S. legal framework (which in general prohibits teens from entering binding contracts).

Further reports have revealed that Facebook gave access to Facebook users' and their friends' information to device makers, including foreign and domestic mobile phone and gaming console companies, without a user's consent and sometimes despite a user's denial.¹ (Unfortunately, ignoring users' privacy settings does not appear to be an isolated incident--just yesterday another instance was reported where Facebook made private posts public.²) Given this news we are even more concerned about disproportionate harm to young people. Young people are likely to access or have accessed Facebook and "Facebook-like experiences" on mobile and other devices, the very same devices for which Facebook built

¹ Gabriel J.X. Dance et al., *Device Companies Have Vast Access to Facebook Data*, N.Y. Times, June 4, 2018, at A1.

² Sheera Frankel, *Facebook Bug Changed Privacy Settings of Up to 14 Million Users*, N.Y. Times, June 8, 2018, at B2.

device-integrated APIs that enabled data-sharing with device makers. Teens, especially lower-income teens, are more likely to have access to phones than computers³, and a 2015 Common Sense report found that teens spent over four hours a day on mobile media.⁴ The report also found that teens were 2.5 times more likely to access social media via a smartphone than a computer, and 3 times more likely to have video game consoles as opposed to desktop computers in their bedroom.⁵ The means and methods teens use to access social media appear to put them at greater risk.

The sharing of information with device makers is yet another reason why the Commission should pay special attention to how Facebook's mishandling of user information impacted teens, with respect to Cambridge Analytica, Huawei, and a growing number of third-parties. How did device usage affect user privacy? Were teens more affected because of their device usage? Were lower-income teens more affected because of their device usage?

Moreover, that this sharing was not disclosed during multiple Congressional hearings, but rather unearthed by reporters, underscores how much of what Facebook does continues to be extremely opaque. It is therefore extremely important that the Federal Trade Commission act to protect Americans' privacy and ensure that companies are transparent--not only with Congress but with consumers as well--so consumers know what to expect. Teens especially need additional help in understanding how companies collect and use their information. According to recent Common Sense and SurveyMonkey polling, very few teens read the terms of service, compared to adults, and most almost never or never do. And only a third of teens think social networks do a good job of explaining what they do with user data, though almost all believe such networks *should* clearly label how they collect and use information.⁶ Not reading terms of service, and not understanding them, makes perfect sense for a young teen--a Georgia Tech study last year found that sites like Facebook had terms of service written, on average, for a college sophomore's reading level.⁷ This is not a document most 13-year-olds could be expected to understand.

We respectfully request that the Commission look carefully into how Facebook has communicated its practices to teens, handled teens' information, and respected teens' privacy preferences, especially with request to sharing information with device makers. We further respectfully request that the Commission craft any future decree or relief with teens in mind.

³ Monica Anderson et al., *Teens, Social Media & Technology 2018*, Pew Research Center, 14 (2018), http://assets.pewresearch.org/wp-content/uploads/sites/14/2018/05/31102617/PI_2018.05.31_TeensTech_FINAL.pdf

⁴ Common Sense Media, *The Common Sense Census: Media Use by Tweens and Teens*, 13 (2015), https://www.common sense media.org/sites/default/files/uploads/research/census_researchreport.pdf

⁵ *Id.*, at 22

⁶ *Quarterly Survey Series*, Common Sense Media and SurveyMonkey (June 11, 2018), <https://www.common sense media.org/research/quarterly-survey-series>

⁷ Casey Fiesler & Amy Bruckman, *Copyright Terms in Online Creative Communities*, CHI '14 Extended Abstracts on Human Factors in Computing Systems, 2551 (2014), <https://www.cc.gatech.edu/elc/copyright/pdf/p2551-fiesler.pdf>

As noted previously, the Commission's investigation into Facebook's apparent violations of the 2011 Consent Order and Section 5 of the Federal Trade Commission Act provides an opportunity to ensure that Facebook takes steps to provide protective measures to teens that are not available to other people.⁸ The Commission has long recognized that teens are especially vulnerable to privacy harms such as identity theft and reputational damage that can affect education and employment opportunities. We ask that you take full advantage of this chance to protect them, no matter what devices they use.

Respectfully,

James P. Steyer

James P. Steyer, CEO & Founder

Ariel Fox Johnson, Senior Counsel, Policy & Privacy

Common Sense Media

650 Townsend St.

San Francisco, CA 94103

(415) 863-0600

⁸ Federal Trade Commission, *Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises*, Press Release (Nov. 29, 2011), <https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep>

ATTACHMENT

April 10, 2018

Acting Chairman Maureen Ohlhausen
Commissioner Terrell McSweeney
Federal Trade Commission
600 Pennsylvania Ave., N.W.
Washington, D.C. 20580

Dear Acting Chairman Ohlhausen and Commissioner McSweeney,

Common Sense is the nation's leading organization dedicated to helping kids and families thrive in a digital world. We write to request that, as you investigate Facebook's disclosure of the personal information of 87 million users to Cambridge Analytica and potential violations of the 2011 Consent Order, you: (1) investigate how teens in particular were affected, and (2) include specific provisions protecting users under 18 in any future decrees or orders. Given teens' tendencies to share and engage online and to be friends with other teens, it seems likely they were disproportionately harmed by Facebook's allowing apps to scrape friends' information. The Commission has recognized that teens are uniquely vulnerable; this is an opportunity to protect them.

For over a decade, Common Sense has helped parents, teachers, and policymakers by providing unbiased information, trusted advice, and innovative tools to help them harness the power of media and technology as a positive force in all kids' lives. Common Sense has an uncommon reach among parents and teachers, with more than 68 million users and half a million educators across its network. We also have advocates in all fifty states supporting our policy initiatives.

We have long advocated for stronger privacy protections for kids and families across all platforms and services, especially those young men and women below the age of legal consent. We have supported updates to COPPA that would include teens. And we spearheaded California student privacy legislation, the Student Online Personal Information Protection Act (SOPIPA) that has become a model across the nation. Further, we have worked with industry and other partners to encourage them to build in privacy by design. We have researched media and technology use by young people from a variety of perspectives, and we are particularly attuned to the privacy challenges young people face.

As the Commission itself has recognized, teens are particularly vulnerable online, and prone to behavior that could lead to identity theft or adversely affect employment or educational opportunities.¹ Social and neuroscience research tells us that they are more likely to share information without thinking, focusing on the present and not considering or understanding long

¹ Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change*, 70 (Mar. 2012); *see also* FTC, *Data Brokers: A Call for Transparency and Accountability* 55 (May 2014) (noting that that teens often fail to appreciate long-term consequences of posting data online).

term consequences.² Young people are more susceptible to advertising, and less able to assess content critically.³ While this is especially true for kids, it is also true for teens—particularly ones under 16—as studies have shown commercial literacy increases between 12 and 15.⁴ This has caused academic experts to question whether such teens, who may not be able to distinguish between an ad and content, can grasp the myriad ways in which companies use their personal information.⁵ And these vulnerabilities in comprehension and understanding are exacerbated by the sheer amount of time young people spend online and the activities they partake in. Teens have to go online in order to get an education, and many view it as a primary means to connect with friends. Over three-quarters of teens are on social media.⁶ And all teens, on average, spent over an hour a day on social media in 2015.⁷ That number has likely only grown.

Our legal framework reflects this reality of teens' differences and vulnerabilities—in general, they are unable to enter into binding legal contracts. Given the special legal and ethical considerations regarding young people, we believe it is important for the Commission to look carefully into how teens' information has been handled, and privacy preferences respected, and to craft any future decree or relief with teens in mind.

During its investigation, we ask that the Commission pay special attention to how teens were impacted by Facebook's mishandling of user information, both with respect to Cambridge Analytica and any other third-parties. Given teens' propensity to take personality quizzes, play games, and share viral content, and to be friends with other teens, it seems likely they were disproportionately affected by Facebook's allowing apps to scrape friends' information. How many teens were affected? Were teens more affected? Have affected teens been informed by Facebook in language they can understand and act upon?

We also ask that any future decrees or orders provide special protections for teens. These should be tailored to address teens' specific vulnerabilities. For example, privacy policies and terms of service are notoriously dense for adults, let alone for youth, calling into question teens' abilities

² See, e.g., Adriana Galván et al, Earlier Development of the Accumbens Relative to Orbitofrontal Cortex Might Underlie Risk-Taking Behavior in Adolescents, *Journal of Neuroscience* (June 21, 2006); Adriana Galván and Kristine M. McGlennen, Enhanced striatal sensitivity to aversive reinforcement in adolescents versus adults, *Journal of Cognitive Neuroscience* (2013).

³ Workgroup on Children's Online Privacy Protection, Report to the Maryland General Assembly on Children's Online Privacy, 16 (Dec. 30, 2013); Ofcom, Children and Parents: Media Use and Attitudes Report 2015 (Nov. 20, 2015), <http://stakeholders.ofcom.org.uk/market-data-research/other/research-publications/childrens/children-parentsnov-15/>.

⁴ Livingstone, Sonia and Kjartan Ólafsson, Children's Commercial Media Literacy: New Evidence Relevant to UK Policy Decisions Regarding the GDPR, Media Policy Project (Jan. 26, 2017), blogs.lse.ac.uk/mediapolicyproject/2017/01/26/childrens-commercial-media-literacy-new-evidence-relevant-to-uk-policy-decisions-regarding-the-gdpr/.

⁵ See, e.g., Livingstone, Sonia et al, If Children Don't Know an Ad from Information, How Can They Grasp How Companies Use Their Personal Data?, Media Policy Project (July 19, 2017), blogs.lse.ac.uk/mediapolicyproject/2017/07/18/if-children-dont-know-an-ad-from-information-how-can-they-grasp-how-companies-use-their-personal-data/.

⁶ NORC at the University of Chicago, New survey: Snapchat and Instagram are most popular social media platforms among American teens: Black teens are the most active on social media and messaging apps, *ScienceDaily* (April 21, 2017), www.sciencedaily.com/releases/2017/04/170421113306.htm.

⁷ Common Sense Media, Common Sense Census: Media Use by Tweens and Teens, Executive Summary (Nov. 3, 2015), https://www.commonsensemedia.org/sites/default/files/uploads/research/census_executivesummary.pdf.

to understand all of the nuances that may be buried in them. Teens deserve clear policies written for their age and level of understanding. Otherwise, they are unable to understand what they are allegedly agreeing to or give anything resembling informed consent. Teens also deserve privacy protective defaults. Given teens' propensity to share and act impulsively, protective defaults can provide an important speedbump. Facebook itself has actually recognized this with respect to some settings the Facebook site has for teens vis-à-vis sharing with the public, but it does not appear to have taken any such steps vis-à-vis sharing with apps and advertisers.

These are just some of the ways that Facebook can better respect and protect its teenage users in the future. After learning more about how teens were impacted—which the Commission has the power to do during its investigation—there will likely be additional safeguards that are appropriate to put in place.

The Commission's investigation into Facebook's apparent violations of the 2011 Consent Order⁸ and Section 5 of the Federal Trade Commission Act provides an opportunity to ensure that Facebook takes steps to provide protective measures to teens that are not available to other people. As noted, the Commission has long recognized that teens are especially vulnerable to privacy harms such as identity theft and reputational damage that can affect education and employment opportunities. We ask that you take full advantage of this chance to protect them.

Respectfully,

James P. Steyer
James P. Steyer, CEO & Founder
Ariel Fox Johnson, Senior Counsel, Policy & Privacy
Common Sense Media
650 Townsend St.
San Francisco, CA 94103
(415) 863-0600

⁸ Federal Trade Commission, Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises, Press Release (Nov. 29, 2011), <https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep>.

Before the
FEDERAL TRADE COMMISSION
WASHINGTON, DC 20580

In the Matter of)
)
Request to Investigate Facebook, Inc.'s)
Misrepresentations of its Face Recognition)
Setting for Violating the Federal Trade)
Commission Act and the 2011)
Consent Agreement)
)

Submitted by

Consumer Reports

Katie McInnis
Policy Counsel
Consumer Reports
1101 17th Street NW
Suite 500
Washington, DC 20036
(202) 462-6262

May 20, 2019

Table of Contents

Summary.....2

I. Background.....4

 A. Tag Suggestions Control.....4

 B. Face Recognition Control.....6

 C. Instances of Consumers Lacking Important Face Recognition Control Documented.....8

 D. Consumers who lack Face Recognition control also faced increased difficulty navigating to their available facial recognition control: Tag Suggestions.....10

II. Facebook’s practices are deceptive under the Federal Trade Commission Act.....12

 A. Facebook represents to consumers that they would have access to the Face Recognition Setting and this setting would be “off” by default or align with the user’s older Tag Suggestions setting.....12

 B. Facebook’s representations mislead consumers.....16

 C. Facebook’s misleading representations are material to the consumer.....18

 D. Under the precedent of *Chitika*, *InMobi*, *Nomi*, and the *Google/Safari* settlements, the Commission should investigate Facebook’s conduct.....18

III. Facebook’s practices violate the 2011 *Consent Agreement*.....20

IV. Conclusion and Request for Relief21

Summary

Consumer Reports¹ (CR) asks the Federal Trade Commission (FTC) to investigate whether Facebook, Inc. is violating the Federal Trade Commission Act (FTC Act) and the 2011 *Consent Agreement* in connection with its Face Recognition control provided to users on their Facebook platform.

The Federal Trade Commission Act makes it unlawful for one to engage in “unfair or deceptive acts or practices in or affecting commerce.”² Under the Federal Trade Commission’s Deception Statement, for an act to be deceptive, it must be a representation, omission or practice that is likely to mislead a reasonable consumer and this representation, omission, or practice must be material. The FTC clarified that materiality is assessed on the basis of whether or not the practice is “likely to affect the consumer’s conduct or decision with regard to a product or service.”³

In 2011, Facebook entered into a settlement agreement with the Federal Trade Commission to settle charges “that it deceived consumers by telling them they could keep their information on Facebook private, and then repeatedly allowing it to be shared and made public.”⁴ The *Consent Agreement* reached between Facebook and the Commission states that Facebook:

...shall not misrepresent in any manner, expressly or by implication, the extent to which it maintains the privacy or security of covered information, including, but not limited to:

- A. Its collection or disclosure of any covered information;
- B. The extent to which a consumer can control the privacy of any covered information maintained by [Facebook] and the steps a consumer must take to implement such controls;⁵

Under the *Agreement*, “covered information” is defined to include “information from or about an individual consumer, including but not limited to...(e) photos and videos.”⁶

¹ Consumer Reports is the world’s largest independent product-testing organization. It conducts its advocacy work in the areas of privacy, telecommunications, financial services, food and product safety, health care, among other areas. Using its dozens of labs, auto test center, and survey research department, the nonprofit organization rates thousands of products and services annually. Founded in 1936, Consumer Reports has over 6 million members and publishes its magazine, website, and other publications.

² Federal Trade Commission Act, 15 U.S.C. § 45(a)(1).

³ Fed. Trade Comm’n, FTC Policy Statement on Deception (1983), <http://www.ftc.gov/bcp/policystmt/ad-decept.htm> [hereinafter FTC Deception Policy].

⁴ *Facebook Settles FTC Charges That It Deceived Consumers by Failing to Keep Privacy Promises*, FED. TRADE COMM’N (Nov. 29, 2011), <https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep> [hereinafter *Facebook Settles*].

⁵ In the Matter of Facebook, Inc., Decision and Order, No. C-4365, p. 3-4, <https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf> [hereinafter 2011 Consent Agreement].

⁶ *Id.*

Facebook provides an online social media platform that allows users to upload their own content to the site, including photos and videos. From December 2011, Facebook has provided users with a control called “Tag Suggestions” that allows users to decide whether or not other users on the site will be served with suggested tags for photos that appear to match the physical characteristics of the individual user. Facebook’s Tag Suggestions feature uses facial recognition technology to identify whether or not a particular user is in the photo or video that is uploaded to the site.

In December 2017, Facebook announced a new setting, “Face Recognition,” which would replace the older Tag Suggestions control for consumers in the US. With this new control, US-based users are able to control whether or not the company’s facial recognition technology is used on the content they upload to the site. This setting, unlike the prior one, also allows the user to opt out of future applications of facial recognition technology on the site.

Since at least May 1, 2019, but perhaps as early as June 2018, Facebook has not provided access to the Face Recognition tool to all US-based users. Consumer Reports first noticed that some profiles lacked access to the Face Recognition control, but instead had the older Tag Suggestions setting, in June 2018. At that time, Facebook declined to provide a comment on the record about this inconsistency in access to privacy controls. However, in early May 2019, Consumer Reports conducted a study with 31 participants across the United States, finding that 8 out of 31, or 26 percent, of those users lacked access to the new Face Recognition tool. These users instead could access the older, and less protective opt-out, Tag Suggestions tool.

Facebook deceived their users by representing that US-based consumers over the age of 18 would have access to the new, and more protective opt-out control of Face Recognition. However, some consumers lack this control. In addition, Facebook represented to consumers that this new control would reflect their prior facial recognition preferences, as indicated by the Tag Suggestions setting. Therefore, if a consumer opted-out of the Tag Suggestions setting they could reasonably assume that they have already opted-out of Facebook’s facial recognition processing, when in fact all they opted-out of was allowing their friends to get tag suggestions for them. Further, these users faced greater difficulty navigating to even the less protective opt-out of facial recognition processing because the new interface and help pages do not provide clear links to the Tag Suggestions system.

Facebook also deceived their users by representing that the new Face Recognition setting would be set to “off”/“no” by default or would align with the user’s past expressed preferences with regards to facial recognition as indicated by whether they changed their default Tag Suggestions setting (i.e., by changing the setting from “Friends” to “No one,” thus opting out of this narrow control on facial recognition technology). First, our study documented that new accounts are initially given the older Tag Suggestions setting, which is on by default. For those users, they have no previous settings to inherit and have no facial recognition protection by default, despite Facebook’s representations. Further, even if they eventually get the new Face Recognition setting,

which would be “on”/“yes” by default, Facebook’s public statements that the default for the Face Recognition control is “off”/“no” leaves them in the position of assuming that they are protected when they are not

In light of these findings, we respectfully request the Commission to investigate these practices and assess civil penalties that demonstrate that violations of the Federal Trade Commission Act and 2011 *Consent Agreement* are impermissible.

I. Background

A. Tag Suggestions Control

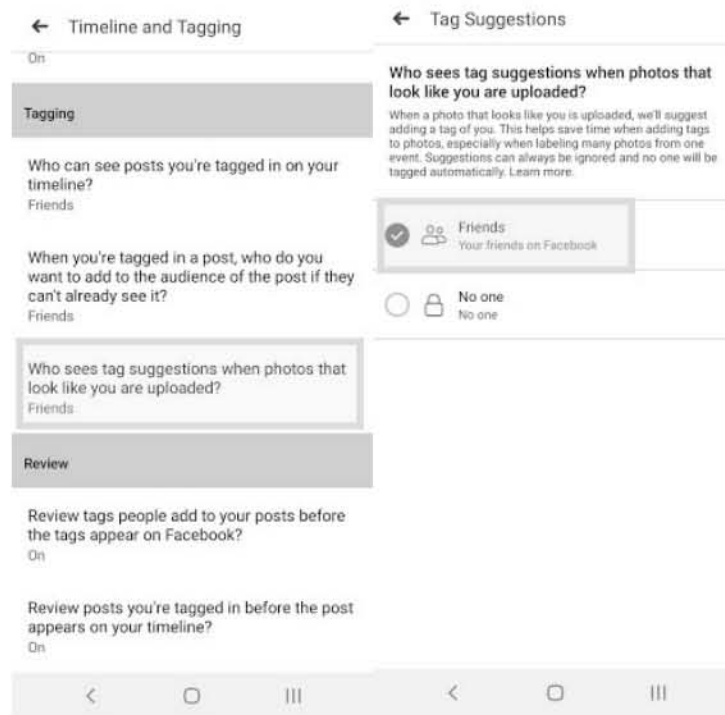
On December 15, 2010, Facebook first announced its “Tag Suggestions” feature, which uses “face recognition software—similar to that found in many photo editing tools—to match your new photos to other photos you're tagged in.”⁷ The setting was on by default,⁸ meaning that users were automatically opted into Facebook’s facial recognition technology recommending tags to connections if the user’s face was identified in a photo or video uploaded to Facebook. However, Facebook did provide the ability to opt out.⁹

⁷ Matt Hicks, *Making Photo Tagging Easier*, FACEBOOK (June 30, 2011, 5:16 PM), <https://www.facebook.com/notes/facebook/making-photo-tagging-easier/467145887130/> [hereinafter *Making Photo Tagging*].

⁸ “If for any reason you don't want your name to be suggested, you will be able to disable suggested tags in your Privacy Settings.” *Id.*; and, see, Ian Paul, *Facebook Photo Tagging: A Privacy Guide*, PC WORLD (June 9, 2011), https://www.pcworld.com/article/229870/Facebook_Photo_Tagging_A_Privacy_Guide.html.

⁹ “If for any reason you don't want your name to be suggested, you will be able to disable suggested tags in your Privacy Settings. Just click “Customize Settings” and “Suggest photos of me to friends.” Your name will no longer be suggested in photo tags, though friends can still tag you manually. You can learn more about this feature in our Help Center.” *Making Photo Tagging*, *supra* note 7.

A user's default Tag Suggestions setting



The Tag Suggestions featured on Facebook uses a four-step facial recognition process:

Initially, the software tries to detect faces (the “detection” step) and standardizes any detected faces for qualities like orientation and size (the “alignment step”). For each face that is detected and aligned, Facebook computes a “face signature,” which is a “string of numbers that represents a particular image of a face” (the “representation” step). Face signatures are then run through a stored database of user “face templates” to look for matches (the “classification” step). A face template is “a string of numbers that represents a boundary” between the face signatures of a given Facebook user and the face signature of others, and is calculated based on that user’s photographs. If a computed face signature falls within the boundary described by a user’s face template, Facebook suggests tagging the user. Facebook represents, with no challenge from plaintiffs, that face signatures are not stored. Only face templates are kept by Facebook.¹⁰

With this tool, the site’s users are not able to stop Facebook from scanning photos, creating “templates” of each face, and retaining the data. However, this setting did allow users to prevent Facebook’s facial recognition system from suggesting that others tag you in photos.¹¹ According

¹⁰ Citations omitted. Order re Class Certification, In Re Facebook Biometric Information Privacy Litigation, No. 3:15-cv-03747-JD, (N.D. Cal. Apr. 16, 2018), available at <https://docs.justia.com/cases/federal/district-courts/california/candce/3:2015cv03747/290385/333>.

¹¹ *Making Photo Tagging*, *supra* note 7.

to Facebook, if you untag a photo or video, “information from those photos and videos is no longer used in the face template.”¹²

B. Face Recognition Control

On December 19, 2017, Facebook announced that they updated the privacy settings on the site to allow users to turn off the use of facial recognition technology on their photos:

We also decided to update Facebook’s settings. Concerns about updated settings are as old as Facebook, so we didn’t take the decision lightly. But we learned in our research that people want a way to completely turn off face recognition technology rather than on a feature-by-feature basis. We knew that as we introduced more features using this technology, most people would find it easier to manage one master setting rather than navigate a long list of products deciding what they want and what they don’t. Our new setting is an on/off switch. Some may criticize this as an “all or nothing” approach, but we believe this will prevent people from having to make additional decisions among potentially confusing options.¹³

The underlying facial recognition technology for both the Face Recognition and Tag Suggestions settings appears to be the same,¹⁴ but the new tool seems to have been designed to allay consumer concerns, while also introducing new features.¹⁵ Furthermore, if a user sets their face recognition setting to “off”/“no,” Facebook “delete[s] the template”¹⁶ and opts the user out of all facial recognition features, including any new features based on this technology that the site might introduce in the future. By contrast, the older tool (Tag Suggestions) only allowed users to prevent Facebook from recommending that others tag them in photos, and did not prevent Facebook from: scanning photos and videos; creating face templates and retaining that data; or any further

¹² *Tagging Photos*, Facebook, <https://www.facebook.com/help/463455293673370> (last visited May 16, 2019).

¹³ Rob Sherman, *Hard Questions: Should I Be Afraid of Face Recognition Technology?*, FACEBOOK NEWSROOM (Dec. 19, 2017), <https://newsroom.fb.com/news/2017/12/hard-questions-should-i-be-afraid-of-face-recognition-technology/> [hereinafter *Hard Questions*].

¹⁴ “But how does this technology really work? It starts with showing a computer photos of the same person. The computer analyzes the pixels in each image and generates a string of numbers to represent a person’s face. Then, the computer analyzes images of other people and creates strings for each of them too. So whenever the system is presented with a new photo, it can quickly find matches on the photos it already has.” Transcript of *Hard Questions: Face Recognition* Animated Video, FACEBOOK (Dec. 17, 2019), <https://www.facebook.com/facebook/videos/10156872585996729/> [hereinafter *Hard Questions Video*]; “On Facebook, face recognition helps people tag photos with the names of their friends. When you have face recognition enabled, our technology analyzes the pixels in photos you’re already tagged in and generates a string of numbers we call a template. When photos and videos are uploaded to our systems, we compare those images to the template.” *Hard Questions*, *supra* note 13.

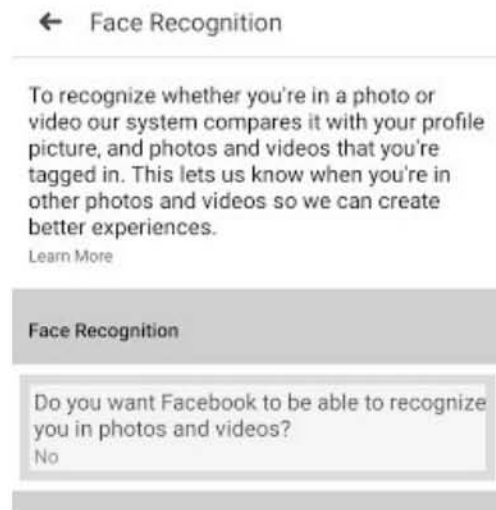
¹⁵ “We recently announced new features that use face recognition technology. People can now find photos of themselves even when they aren’t tagged in them, making it possible for people to manage their privacy in new ways. They may also know when someone is using their image as a profile photo — which can help stop impersonation. In addition, those with vision impairments can now hear aloud who’s in the photos they come across on Facebook. Just as in 2010, we had to evaluate how we’d inform people and give them choice over these new uses of the technology.” *Hard Questions*, *supra* note 13.

¹⁶ *Tagging Photos*, *supra* note 12.

application of facial recognition technology to their photos or videos or those uploaded by others.

The new Face Recognition setting is set to “off”/“no” by default, meaning that users are not automatically opted into allowing Facebook’s facial recognition technology to scan their photos and videos uploaded to the site.¹⁷

Screenshot of the default Face Recognition setting

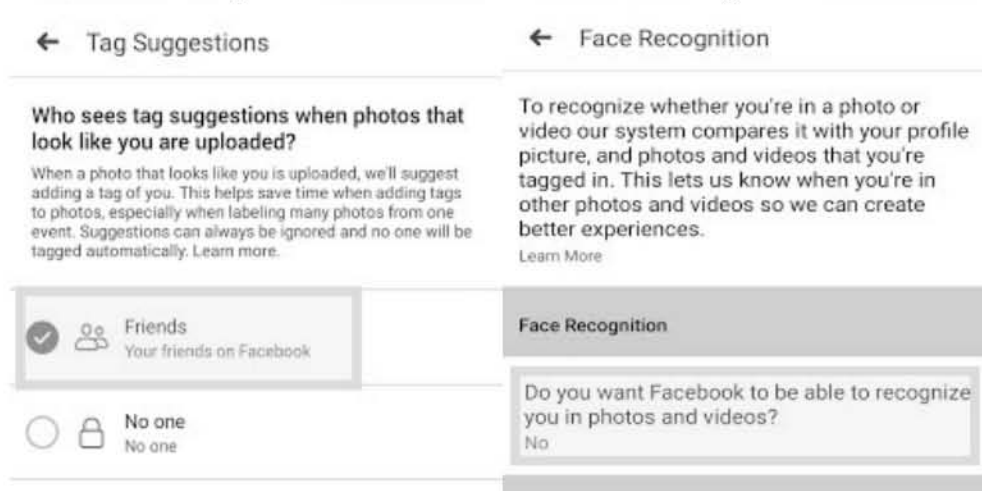


However, in order to respect a user's present privacy practices, Facebook stated that the default Face Recognition control would reflect the settings users had chosen with the older Tag Suggestions feature (i.e., if a person set their Tag Suggestions setting to “off”/“no one” in the past, their Face Recognition setting would be set to “off”/“no” automatically, opting the user out of the use of facial recognition technology).¹⁸

¹⁷ Lily Hay Newman, *How to Turn Off Facebook’s Face Recognition Features*, WIRED (Feb, 28, 2018), <https://www.wired.com/story/how-to-turn-off-facebook-face-recognition-features/> [hereinafter *Facebook’s Face Recognition*].

¹⁸ *Id.*

If a user changed their Tag Suggestions setting to “off”/“no one” previously, the new Face Recognition control would also be set to “off”/“no”



C. Instances of Consumers Lacking Access to Important Face Recognition Control Documented

Consumer Reports documented through a small, qualitative study of US-based Facebook users that some of the site’s users lack the Face Recognition setting that was introduced in December 2017. We first spotted this issue in June 2018. Although we contacted Facebook about this possible anomaly, Facebook did not comment on the record at that time. In early May 2019, Consumer Reports conducted an online study with 31 Facebook users across the United States.

Consumer Reports utilized a service called UserTesting to conduct our study. Participants are paid a nominal fee for their time, and can be directed to perform various tasks and answer questions about their experiences. As participants complete tasks, the service captures video of their screens. The videos, along with recordings of written and verbal responses to questions are sent to the organization conducting the study.

Our study consisted of 34 Facebook users. Two users from our initial pool of participants reported that they lived outside the United States, and were excluded from our final results, as laws regarding biometrics or privacy writ large may affect Facebook’s practices in those countries and the distribution of its privacy settings. We also excluded one user who did not complete the study, for a final pool of 31 participants.

UserTesting lets its clients design tests and establish qualifications in order to target specific groups of consumers. Participants who meet those qualifications are then selected at random from among the service’s pool of consumers. Participants were required to use the Chrome web browser, which UserTesting recommends in order to ensure the proper functioning of the UserTesting

platform.

After running a small test of five participants to confirm that our protocol would be easy to follow, we added more participants with additional requirements: We excluded participants from outside the United States, and targeted some users who were residents of Illinois. The goal with that requirement was to research whether a state law, the Illinois Biometrics Information Privacy act, has any effect on the availability of the setting. Our findings did not indicate that the Facebook platform treats Illinois residents any differently when it comes to the availability of the Face Recognition setting.

We had participants log in to Facebook.com, and directed them to navigate to different areas of the site in order to document whether the Face Recognition setting was available. We also had users show us the availability of a Tag Suggestions setting, to test our hypothesis that users are granted access to one of those two settings, but not both. We documented whether these settings were turned on or off, and asked whether users had adjusted them in the past.

We found that the Face Recognition setting to be available to most users, but the setting was missing from eight out of the final pool of 31 accounts we documented.

As part of our test, we asked users a number of questions to research whether demographic or behavioral patterns had any effect on the availability of the setting. Questions included how often participants use Facebook, what kind of phones and computers they use, whether or not they use the Facebook mobile app, and whether the participants had ever used Facebook while traveling outside of the United States. In addition, we had users navigate to certain pages that would allow us to document how many “friends” they had, when their accounts were created, and whether or not the users’ “profile pictures” were photographs of their faces. We also gathered information about each user’s age and gender from self-reported information through the UserTesting platform. None of these factors seemed to affect the availability of the Face Recognition setting.

In addition to our formal test, we asked members from two Consumer Reports Facebook groups to check if the setting was available. Among hundreds of replies, a number of users reported that the Face Recognition setting is unavailable to them. While this anecdotal evidence reinforces the findings of our study, we did not include these results in our analysis as we did not have documentation to confirm the accuracy of these responses.

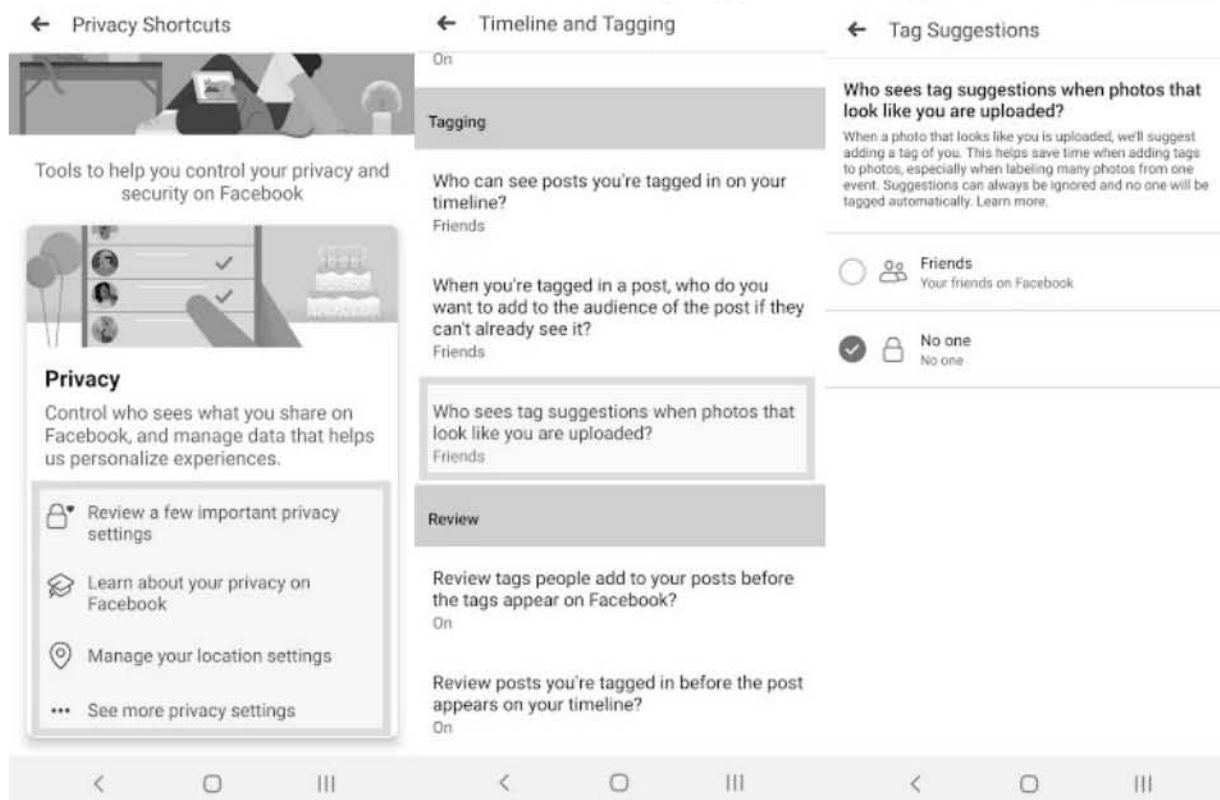
In a separate experiment, Consumer Reports tried to see whether the Face Recognition setting worked. We downloaded archives of Facebook data from user accounts that did have the Facial Recognition setting. If the feature had been turned on for several days, the archive included a file labeled Face Recognition containing a long string of characters that may have been the facial recognition template. If Facial Recognition had been turned off, that file did not appear in our

archive, indicating the setting is likely working when it is available.

D. Consumers who lack Face Recognition control also faced increased difficulty navigating to their available facial recognition control: Tag Suggestions

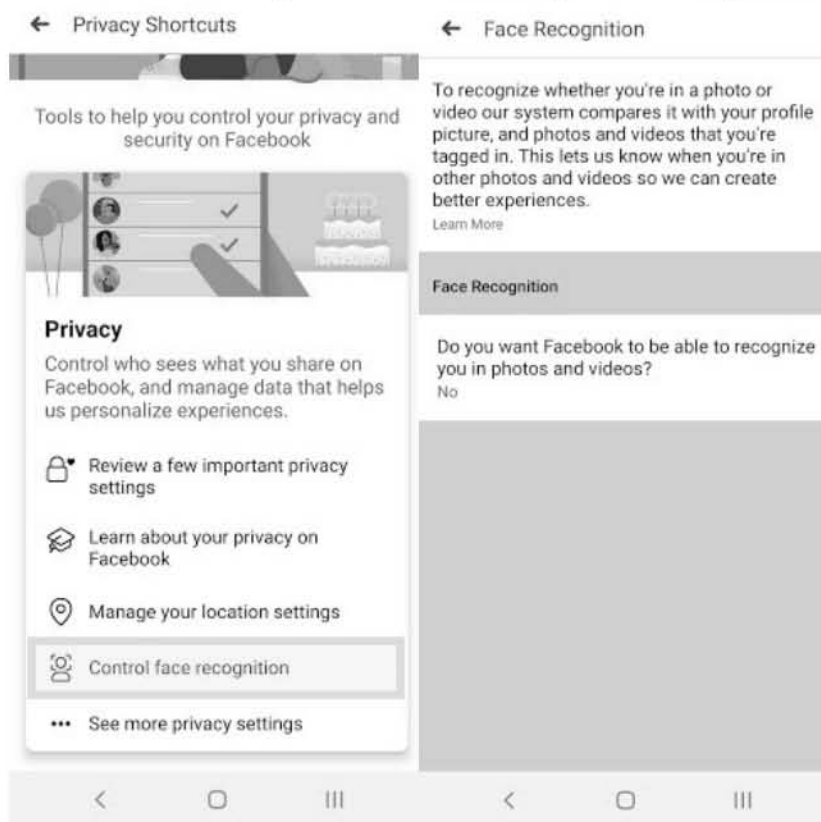
As shown in the screenshots below, the privacy shortcuts page for users who do not have the new Face Recognition setting lacks any shortcut to modify their Tag Suggestions control. A user must instead find their Tag Suggestions setting by navigating to their main account settings page through a different menu.

Screenshots of A User's Tag Suggestions Setting



As documented in the screenshots below, a user who does have access to the Face Recognition setting Facebook introduced in December 2017 can easily access and change their facial recognition control from their privacy shortcuts page. This ease of navigation is contrasted with the relative difficulty with which a user who only has the older Tag Suggestions control would have finding their Tag Suggestions setting.

Screenshots of a User's Face Recognition Setting



If a user was presented with the older Tag Suggestions control and not the newer Face Recognition control, it was harder for the user to navigate to the appropriate setting. A slide show on Facebook's "Privacy Basics"¹⁹ page explains how the Face Recognition control works and provide illustrations of what the setting looks like, and how to use it. The penultimate informational final slide reads, "You can turn the setting on or off at any time, which will also apply to any features we add later," and includes a link²⁰ which directs users to the page where they can adjust the setting.²¹

¹⁹ *Manage Your Privacy: Face Recognition*, FACEBOOK, <https://www.facebook.com/about/basics/manage-your-privacy/face-recognition> (last visited May 20, 2019).

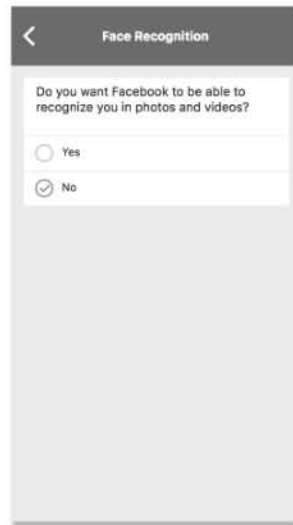
²⁰ *Settings: Face Recognition*, FACEBOOK, <https://www.facebook.com/settings?tab=facerec> (last visited May 20, 2019).

²¹ *Id.*

Screenshot of the penultimate informational slide

< Manage Your Privacy

MENU >



You can turn the setting on or off at any time, which will also apply to any features we add later.

But if the user does not have the Face Recognition control, that link just takes them to their main account settings page. Then it is up to the user to figure out that, on their account, the setting does not exist. Aside from concerns about the availability of this important control, the lack of usable links in these explanations for consumers about Facebook’s face recognition technology makes the process of changing one’s privacy settings even more complicated and onerous. Consumers already have a hard time utilizing the few privacy controls they do have, and this broken disclosure system only serves to exacerbate the problem.

II. Facebook’s practices are deceptive under the Federal Trade Commission Act

The Federal Trade Commission has the ability under the Federal Trade Commission Act to prevent the use of “unfair or deceptive acts or practices in or affecting commerce.”²² Under the Federal Trade Commission’s Deception Statement, for an act to be deceptive, it must be a representation, omission or practice that is likely to mislead a reasonable consumer and this representation, omission, or practice must be material. The FTC clarified that materiality is assessed on the basis of whether or not the practice is “likely to affect the consumer’s conduct or decision with regard to a product or service.”²³

A. Facebook represents to consumers that they would have access to the Face

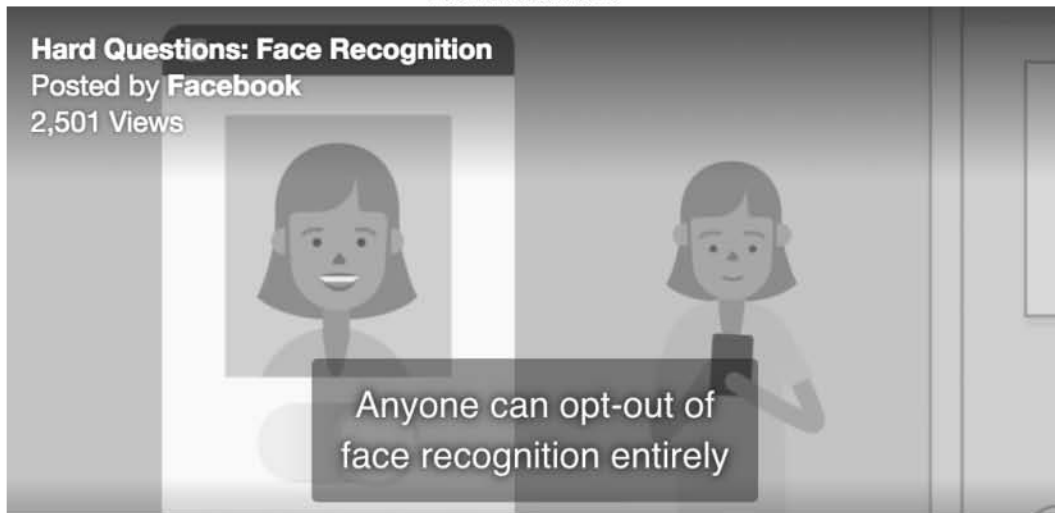
²² Federal Trade Commission Act, 15 U.S.C. § 45(a)(1).

²³ FTC Deception Policy, *supra* note 3.

Recognition Setting and this setting would be “off” by default or align with the user’s older Tag Suggestions setting

From at least December 2017 to the present, Facebook represented to US-based consumers that they would be able to turn off facial recognition on the site. In an animated video in the post announcing the new Face Recognition control the company says: “Anyone can opt out of face recognition entirely through their Facebook account settings.”²⁴

A Screenshot of the Animated Video by Created and Hosted by the Company on their Facebook Newsroom site²⁵



Facebook also states in their blog post announcing this new setting that “when it comes to face recognition, control matters.”²⁶

Screenshot from the blog post in the Facebook Newsroom site announcing the new Face Recognition Control

Our Responsibility

When it comes to face recognition, control matters. We listen carefully to feedback from people who use Facebook, as well as from experts in the field. We believe we have a responsibility to build these features in ways that deliver on the technology’s promise, while avoiding harmful ways that some might use it.

²⁴ *Hard Questions Video*, *supra* note 14.

²⁵ *Id.*

²⁶ *Hard Questions*, *supra* note 13.

In addition, in Facebook’s Help Center, the company provides consumers with explanations on how to turn off facial recognition for their account. These instructions represent that these users should be able to turn off the use of this technology, despite the fact that Consumer Reports documented that some consumers lack this control entirely.²⁷

Screenshot of a section of the Facebook Help Center page


How do I turn face recognition on or off for my account?

Computer Help Mobile Help ▾

➔ Share Article

Face recognition helps Facebook recognize you in photos or videos based on your profile picture and photos or videos you are tagged in. Learn about how face recognition may be used on Facebook.

To turn face recognition on or off for your account:

- 1 Click  in the top right of Facebook and select **Settings**.
- 2 In the left column, click **Face Recognition**.
- 3 Go to **Do you want Facebook to be able to recognize you in photos and videos?** and click **Edit**.
- 4 Select **Yes** or **No** to confirm your choice.

When Face Recognition is set to off, templates are deleted.

Note: This setting isn't available in all countries, and will only appear in your profile if you are at least 18 years old.

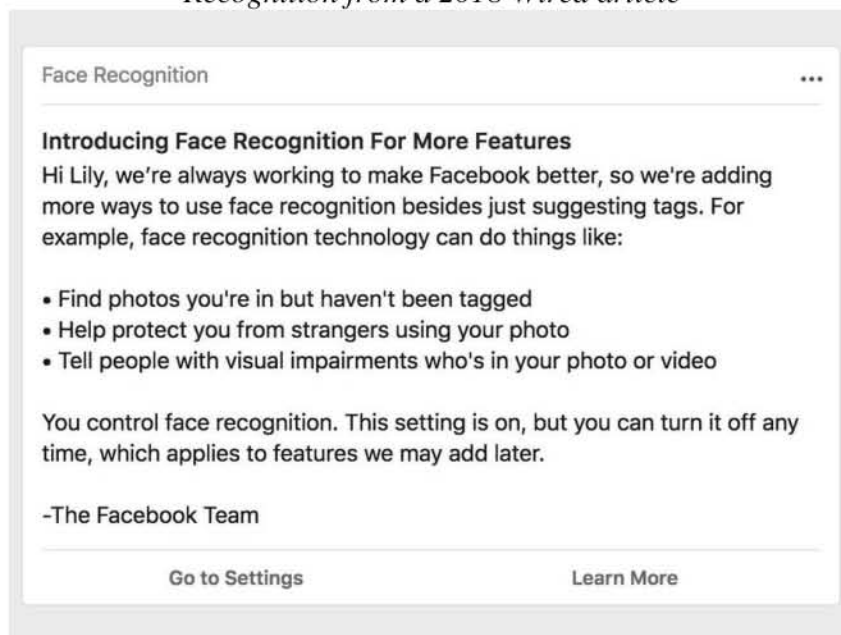
Users who visited their Facebook home page following the release of the new setting in December 2017 were alerted to this new control via a pop-up dialogue box in their newsfeed,²⁸ similar to one that was included in a Wired story²⁹ in February 2018.

²⁷ *How do I turn face recognition on or off for my account?*, FACEBOOK HELP CENTER, https://www.facebook.com/help/187272841323203?helpref=uf_permalink (last visited May 18, 2019).

²⁸ “People asked us to explain how face recognition works more clearly, and to provide more prominent information about how we might use it on Facebook. To address this feedback, we’re informing people about updates to face recognition in News Feed – the doorstep of Facebook.” *Hard Questions*, *supra* note 13.

²⁹ *Facebook’s Face Recognition*, *supra* note 17.

Screenshot of a Facebook pop-up dialogue box that gives users more information about the Face Recognition from a 2018 Wired article



This dialogue box tells users “You control face recognition...you can turn it off at any time.” Although CR has not documented instances where a user was presented with this disclosure even though they lacked the setting, this dialogue box is another instance where Facebook represented that users can control this setting and turn off the application of facial recognition technology “at any time.”

In Facebook’s Data Policy, the company has a section entitled “How do we use this information?” Under the subsection titled “Provide, personalize and improve our Products” Facebook has a separate bullet about their facial recognition technology. In this section, Facebook includes links to their site’s privacy settings. However, the section on facial recognition technology does not mention that some users may have an older Tag Suggestions setting. In addition, the section specifically states that users can: “...control our use of this technology in Facebook settings.” This statement would lead users to believe that they have the ability to change how Facebook uses this technology, when in fact some users lack this control entirely.

Screenshot of the section on Face Recognition in Facebook's Data Policy

- **Face recognition:** If you have it turned on, we use face recognition technology to recognize you in photos, videos and camera experiences. The face-recognition templates we create may constitute data with special protections under the laws of your country. Learn more about how we use face recognition technology, or control our use of this technology in Facebook Settings. If we introduce face-recognition technology to your Instagram experience, we will let you know first, and you will have control over whether we use this technology for you.

As documented by Consumer Reports, from at least May 1, 2019, but perhaps as early as June 2018, some consumers *did not* have access to this control. Specifically, eight out of 31, or 26 percent, of participants did not have the new Face Recognition setting, but rather the older Tag Suggestions setting, despite the fact that Facebook indicated to consumers that access to this control would be ubiquitous for adults in the United States.³⁰ Although this study only examined a small subset of Facebook users, since we could not find any clear commonalities between these users, we can infer that many more users in the US likely also lack this control. As of April 2019, Facebook has approximately 190 million users in the US,³¹ a significant proportion of which are adults.³²

B. Facebook's representations mislead consumers

Most consumers do not change the default settings in their accounts.³³ Facebook spokesperson Rochelle Nadhiri publicly stated that the Face Recognition setting “is not on by default.”³⁴ In

³⁰ A Facebook spokesman told Wired: “Anyone can opt out of face recognition entirely through their Facebook account settings.” (*Facebook's Face Recognition*, *supra* note 17.) However, the company did make it clear that the control was only available to individuals over the age of 18 and was not available in all countries: “Note: This setting isn't available in all countries, and will only appear in your profile if you are at least 18 years old.” (*Tagging Photos*, *supra* note 12); *see, also*: “Even in this renewed push to incorporate face recognition, people in Canada and the European Union won't have access to the features at all, because those regions have regulations about how companies can collect and store biometric data.” (*Facebook's Face Recognition*, *supra* note 17.)

³¹ *Leading countries based on number of Facebook users as of April 2019 (in millions)*, STATISTA, <https://www.statista.com/statistics/268136/top-15-countries-based-on-number-of-facebook-users/> (last visited May 20, 2019).

³² A Pew Research Center study found: “Facebook is no longer the dominant online platform among teens...In 2018, three online platforms other than Facebook – YouTube, Instagram and Snapchat – are used by sizable majorities of this age group. Meanwhile, 51% of teens now say they use Facebook.” Monica Anderson & Jingjin Jiang, *Teens, Social Media & Technology 2018*, PEW RESEARCH CTR. (May 31, 2018), <https://www.pewinternet.org/2018/05/31/teens-social-media-technology-2018/>.

³³ Len V. Groeger, *Set It and Forget It: How Default Settings Rule the World*, PROPUBLICA (July 27, 2016), <https://www.propublica.org/article/set-it-and-forget-it-how-default-settings-rule-the-world>.

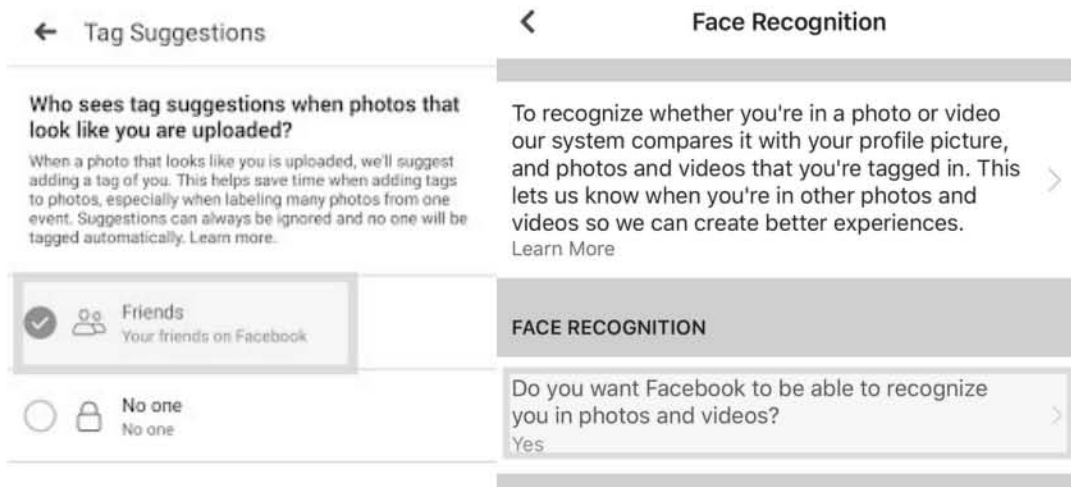
³⁴ “The new setting is not on by default,” says Facebook spokesperson Rochelle Nadhiri. True, but not so simple. “The new setting respects people's existing choices, so if you've already turned off tag suggestions then your new

addition, the same spokesman stated: "The new setting respects people's existing choices, so if you've already turned off tag suggestions then your new face recognition setting will be off by default. If your tag suggestions setting was set to 'friends' then your face recognition setting will be set to on."³⁵

Therefore, consumers who previously changed their setting for Tag Suggestions to "off"/"no one" would reasonably assume that their Face Recognition setting was likewise set to "off"/"no." However, since some consumers lack the Face Recognition setting, their Face Recognition has not been set to off, despite Facebook's claim. Such consumers could therefore incorrectly expect that their previous actions already opted them out of Facebook's facial recognition technology collection and processing of their data when in fact they lack the tool.

However, consumers who never changed their Tag Suggestions setting from the default of "on"/"friends" would then be opted-in to new Face Recognition setting and thus the setting for this new control would be "on"/"yes." This automatic opt-in is in contradiction with the statement from Facebook spokesperson Rochelle Nadhiri who states that the setting "is not on by default."³⁶

If a user previously had their Tag Suggestions setting set to "Friends," then the new Face Recognition setting would be set to "Yes," in accordance with Facebook's statements



This means that, despite the public affirmation made by Facebook spokesperson Rochelle Nadhiri that this setting "is not on by default,"³⁷ new users who never changed the default setting on their Tag Suggestions control will automatically be opted-in to allowing facial recognition processing on their photos and videos.

face recognition setting will be off by default. If your tag suggestions setting was set to 'friends' then your face recognition setting will be set to on," Nadhiri explains." *Facebook's Face Recognition*, *supra* note 17.

³⁵ *Id.*

³⁶ *Id.*

³⁷ *Id.*

This misrepresentation could lead some consumers to assume, in error, that they do not need to change their settings. In addition, on all four new accounts Consumer Reports created in early May 2019, the Tag Suggestion was set to “on” by default (i.e., the setting was set to “friends” in response to the setting “Who sees tag suggestions when photos that look like you are uploaded?,” as opposed to “no one”), which implies that if the Face Recognition is rolled out to these accounts, the new setting will be set “on” by default as well.

C. Facebook’s misleading representations are material to the consumer

Finally, the gap in understanding between the privacy controls each consumer has access to on the Facebook site is material to a consumers’ choices. If a consumer knows that they lack the newer and stronger opt-out of the Face Recognition setting, the consumer might reconsider uploading personal photos or videos to the site in order to protect their privacy and the privacy of the people featured, including children. In addition, if a subset of consumers lacks a stronger opt-out that is provided to other consumers, consumers in that subset may reconsider their relationship to the social media company, especially in light of the company’s recent privacy violations and controversies.³⁸

D. Under the precedent of *Chitika*, *InMobi*, *Nomi*, and the *Google/Safari* settlements, the Commission should investigate Facebook’s conduct

The results of our research indicate that Facebook may be misrepresenting the ability of their users to control what data is collected and processed by the company using their facial recognition technology. The misrepresentations made by Facebook can be compared to the *Chitika*, *InMobi*, *Nomi*, and *Google/Safari* settlements.

The Federal Trade Commission has brought enforcement cases against companies that misrepresent the extent to which consumers can control the collection, use, or sharing of their data in violation of the Federal Trade Commission Act. For instance, in the *Chitika, Inc.* settlement,³⁹ the Commission found that the company had violated the FTC Act by misleading users about the extent to which they could control the collection, use, or sharing of their data because the online site offered users an opt-out that served to only opt the consumer out for a period of ten days, due to a self-expiring cookie. The opt-out control offered by Chitika resulted in an opt-out cookie being placed on the user’s computer that prevented other cookies from being placed from the site. If the user navigated to view whether or not they were opted out of such tracking, the website attested that the consumer was “currently opt-ed out.” However, and unbeknownst to the user, the opt-out

³⁸ See Alyssa Newcomb, *A Timeline of Facebook’s Privacy Issues—and Its Responses*, NBC NEWS (Mar. 24, 2018), <https://www.nbcnews.com/tech/social-media/timeline-facebook-s-privacy-issues-its-responses-n859651>.

³⁹ In the Matter of Chitika, Inc., FED. TRADE COMM’N (June 7, 2011), <https://www.ftc.gov/sites/default/files/documents/cases/2011/06/110617chitikacmpt.pdf>.

cookie was set to self-expire after ten days, thus preventing the consumer from effectively opting out.⁴⁰

Likewise, in the case of *InMobi*, the FTC brought an enforcement action against the company for misrepresenting that its advertising software would only track consumers' locations when they opted in and in a manner consistent with their privacy settings. The FTC complaint alleges that the company used a database of the locations of wireless networks created from opted-in users to infer the physical locations of consumers who had opted out of sharing their location.⁴¹ In order to settle this charge and others, the FTC and the company reached a settlement under which InMobi was required to pay almost a million dollars in civil penalties and implement a comprehensive privacy program.⁴²

In addition, the FTC has found that it is unlawful under the FTC Act for a company to misrepresent the choices consumers have to control data collection by a company. Specifically, the Commission alleged in the *Nomi* case that the company misled consumers with promises that it would provide an in-store mechanism for consumers to opt out of tracking.⁴³ However, the company did not provide such controls and thus the Commission approved a final order in 2015 against Nomi for this misrepresentation and other allegations.⁴⁴

In the case of the Facebook Face Recognition setting, the company similarly misrepresented to consumers that consumers are able to restrict the extent to which the company collects information about them, in possible violation of the FTC Act. Facebook has represented to their users for at least 18 months that “[a]nyone can opt out of face recognition entirely through their Facebook account settings,”⁴⁵ despite the fact that 26 percent of our participants cannot because they lack access to this control. These users are distributed across the US and our researchers could not find any commonalities between the users that could explain this discrepancy. Under the history of *Chitika*, *InMobi*, and *Nomi* cases, the Federal Trade Commission should bring an enforcement action against Facebook for this misrepresentation.

⁴⁰ *Id.*

⁴¹ “The complaint alleges that InMobi created a database built on information collected from consumers who allowed the company access to their geolocation information, combining that data with the wireless networks they were near to document the physical location of wireless networks themselves. InMobi then would use that database to infer the physical location of consumers based on the networks they were near, even when consumers had turned off location collection on their device.” *Mobile Advertising Network InMobi Settles FTC Charges It Tracked Hundreds of Millions of Consumers' Locations Without Permission*, FED. TRADE COMM’N (June 22, 2016), <https://www.ftc.gov/news-events/press-releases/2016/06/mobile-advertising-network-inmobi-settles-ftc-charges-it-tracked>.

⁴² *United States v. InMobi Pte Ltd.*, No. 3:16-cv-03474, (N.D. Cal. June 22, 2016) (Stipulated Order for Permanent Injunction and Civil Penalty Judgment), *available at* <https://www.ftc.gov/system/files/documents/cases/160622inmobistip.pdf>.

⁴³ *In the Matter of Nomi Technologies, Inc.*, No. C-4538, FED. TRADE COMM’N (Aug. 28, 2015), <https://www.ftc.gov/enforcement/cases-proceedings/132-3251/nomi-technologies-inc-matter>.

⁴⁴ *FTC Approves Final Order in Nomi Technologies Case*, FED. TRADE COMM’N (Sept. 3, 2015), <https://www.ftc.gov/news-events/press-releases/2015/09/ftc-approves-final-order-nomi-technologies-case>.

⁴⁵ *Hard Questions Video*, *supra* note 14.

Facebook also made misrepresentations about the availability of their Face Recognition setting in their Help Center. Facebook’s misrepresentations in their Help Center about the availability and use of the Face Recognition tool can be compared to Google’s misrepresentations of Safari’s settings in the 2012 settlement between the FTC and Google.⁴⁶ In that case, Google told Safari browser users that they would automatically be opted out of third-party cookies like Google’s on their Advertising and Privacy page, which was located in the consumer help/frequently-asked-questions center.⁴⁷ Similarly, in Facebook’s Help Center, the site tells users how to “turn face recognition on or off for my account.” However, for the users that do not have access to this control, these explainers misrepresent what settings they have for they lack access to the Face Recognition control entirely. In addition, the links in the Help Center on this setting fail to navigate users who lack the Face Recognition control to settings that they can use to modify what information Facebook can collect about them. The links instead take users without this setting to the main account settings page, leaving it up to the user to figure out that they lack this control.

III. Facebook’s practices violate the 2011 Consent Agreement

The misrepresentations documented in this letter are also possible violations of the *Consent Agreement* reached by Facebook and the Federal Trade Commission in 2011. Under the *Agreement*, Facebook:

...shall not misrepresent in any manner, expressly or by implication, the extent to which it maintains the privacy or security of covered information, including, but not limited to:

- C. Its collection or disclosure of any covered information;
- D. The extent to which a consumer can control the privacy of any covered information maintained by [Facebook] and the steps a consumer must take to implement such controls;⁴⁸

Under the terms of this *Consent Agreement*, photos or videos are included within the definition of “covered information.”⁴⁹ Since Facebook made misrepresentations of the extent to which a consumer could control the privacy of their photos and videos under the privacy settings provided by Facebook, the instances reported in this letter are covered by said *Agreement*.⁵⁰ Therefore, the Commission should explore whether or not to bring an enforcement action against Facebook due to this violation of the 2011 *Consent Agreement*.

⁴⁶ *Google Will Pay \$22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple’s Safari Internet Browser*, FED. TRADE COMM’N (Aug. 9, 2012), <https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented>.

⁴⁷ *United States v. Google, Inc.*, No. 12-04177 (N.D. Cal. Aug. 8, 2012) (Complaint for Civil Penalties and Other Relief), p. 8, <https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809googlecmptexhibits.pdf>.

⁴⁸ 2011 Consent Agreement, *supra* note 5.

⁴⁹ 2011 Consent Agreement, *supra* note 5.

⁵⁰ The agreement extends until 2032. *See* 2011 Consent Agreement, *supra* note 3.

IV. Conclusion and Request for Relief

Facebook misrepresented the extent to which their users can control the amount of information that is collected and processed about them under the company’s facial recognition technology, in violation of the Federal Trade Commission Act⁵¹ and the 2011 *Consent Agreement*.⁵² The public statements made and Help Center resources provided by Facebook could mislead consumers to believe that they have certain privacy protections when they in fact lack those protections. Our research with 31 of Facebook users demonstrates that this new setting has not been deployed to all users. Therefore, many users of this site could be misled to think they have this control when in fact they do not, leading them to a false sense of control and privacy of their data. Furthermore, since the links in the Help Center page and in the Facebook Newsroom announcement fail to navigate to the correct setting for those individuals who lack the new Face Recognition setting, consumers could be additionally confused and unable, without extra effort, to find out they do not have this new setting.

Finally, Facebook also deceived their users by representing that the new Face Recognition setting would be set to “off”/“no” by default or would align with the user’s past expressed preferences with regards to facial recognition as indicated by whether they changed their default Tag Suggestions setting (i.e., by changing the setting from “Friends” to “No one,” thus opting out of this narrow control on facial recognition technology). But in fact, most users never change their default settings, so many users likely were opted-in to Facebook’s facial recognition processing of their photos due to the default setting of the older Tag Suggestions feature (which was on by default). Additionally, we found that new accounts are often given the older Tag Suggestions feature initially (which is on by default) and thus these accounts, when they do receive the newer Face Recognition control, will be opted into facial recognition processing of their photos.

These misrepresentations by Facebook potentially constitute violations of the FTC Act and the 2011 *Consent Order*. We therefore urge the FTC to investigate these practices.

Respectfully submitted,

/s/ Katie McInnis

Katie McInnis
Policy Counsel
Consumer Reports
Suite 500
1101 17th Street NW
Washington, DC 20036
(202) 462-6262

⁵¹ 15 U.S.C. § 45(a)(1).

⁵² *Facebook Settles*, *supra* note 3.