

June 18, 2018

Senator Jerry Moran, Chairman
Senator Richard Blumenthal, Ranking Member
Senate Committee on Commerce, Science and Transportation
Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security
512 Dirksen Senate Building
Washington, D.C. 20510

Dear Chairman Moran and Ranking Member Blumenthal:

We write to you regarding the hearing this week on “Cambridge Analytica and Other Facebook Partners: Examining Data Privacy Risks.”¹ We appreciate your interest in this important issue. For many years, the Electronic Privacy Information Center (“EPIC”) has worked with the Commerce Committee to help protect the privacy rights of Americans.² EPIC has also played a leading role at the Federal Trade Commission, bringing to the Commission’s attention emerging privacy and civil liberties. And EPIC is the group that brought the complaint in 2009 to the FTC regarding Facebook’s data practices that resulted in the 2011 Consent Order.³ And EPIC is the group that sued the FTC for its failure to enforce a similar order against Google.⁴

In this statement we outline the history of the 2011 Consent Order, point to subsequent developments (including the recently disclosed user data-disclosure agreements with device

¹ *Cambridge Analytica and Other Facebook Partners: Examining Data Privacy Risks: Hearing Before the S. Comm. on Commerce, Science, & Transportation, Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security*, 115th Cong. (2018), <https://www.commerce.senate.gov/public/index.cfm/2018/6/subcommittee-to-hold-hearing-examining-social-media-data-use-and-privacy-concerns> (June 19, 2018).

² See, e.g., *An Examination of Children’s Privacy: New Technologies and the Children’s Online Privacy Protection Act (COPPA): Hearing Before the S. Comm. on Commerce, Science, and Transportation*, 111th Cong. (2010) (statement of Marc Rotenberg, Exec. Dir. EPIC), (C-SPAN video at <https://www.c-span.org/video/?293245-1/childrens-privacy>), https://epic.org/privacy/kids/EPIC_COPPA_Testimony_042910.pdf; *Impact and Policy Implications of Spyware on Consumers and Businesses: Hearing Before the S. Comm. on Commerce, Science, and Transportation* 110th Cong. (2008) (statement of Marc Rotenberg, Exec. Dir. EPIC) (C-SPAN video at <https://www.c-span.org/video/?205933-1/computer-spyware>), https://www.epic.org/privacy/dv/Spyware_Test061108.pdf.

³ *In the Matter of Facebook, Inc.* (EPIC, Complaint, Request for Investigation, Injunction, and Other Relief) before the Federal Trade Commission, Washington, D.C. (filed Dec. 17, 2009), <http://www.epic.org/privacy/infacebook/EPIC-FacebookComplaint.pdf>.

⁴ *EPIC v. FTC*, 844 F. Supp. 2d 98 (D.D.C. 2012), <https://epic.org/privacy/ftc/google/EPICvFTC-CtMemo.pdf>.

makers⁵), and make several recommendations. Our assessment is that the Cambridge Analytica breach, as well as the disclosure of users' personal information to device makers, could have been prevented if the Commission had enforced the Order.

EPIC would welcome the opportunity to testify, to provide more information, and to answer questions you may have. Our statement follows below.

EPIC, the 2011 FTC Consent Order, and Earlier Action by the FTC

Facebook's transfer of personal data to Cambridge Analytica was prohibited by a Consent Order the FTC reached with Facebook in 2011 in response to an extensive investigation and complaint pursued by EPIC and several US consumer privacy organizations.⁶ The FTC's failure to enforce the order we helped obtain has resulted in the unlawful transfer of 87 million user records to a controversial data mining firm to influence a presidential election as well as the vote in Brexit. The obvious question now is "why did the FTC fail to act?" The problems were well known, widely documented, and had produced a favorable legal judgement in 2011.

Back in 2007, Facebook launched Facebook Beacon, which allowed a Facebook user's purchases to be publicized on their friends' News Feed after transacting with third-party sites.⁷ Users were unaware that such features were being tracked, and the privacy settings originally did not allow users to opt out. As a result of widespread criticism, Facebook Beacon was eventually shutdown.

In testimony before the Senate Commerce Committee in 2008, we warned about Facebook's data practices:

Users of social networking sites are also exposed to the information collection practices of third party social networking applications. On Facebook, installing applications grants this third-party application provider access to nearly all of a user's information. Significantly, third party applications do not only access the information about a given user that has added the application. Applications by default get access to much of the information about that user's friends and network members that the user can see. This level of access is often not necessary. Researchers at the University of Virginia found that 90% of applications are given more access privileges than they need.⁸

⁵ Gabriel J.X. Dance, Nicholas Confessore and Michael LaForgia, *Facebook Gave Device Makers Deep Access to Data on Users and Friends*, N.Y. Times (June 3, 2018), <https://www.nytimes.com/interactive/2018/06/03/technology/facebook-device-partners-users-friends-data.html>.

⁶ Fed. Trade Comm'n., *In re Facebook*, Decision and Order, FTC File No. 092 3184 (Jul. 27, 2012) (Hereinafter "Facebook Consent Order"), <https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf>.

⁷ EPIC, *Social Networking Privacy*, <https://epic.org/privacy/socialnet/>.

⁸ *Impact and Policy Implications of Spyware on Consumers and Businesses: Hearing Before the S. Comm. on Commerce, Science, and Transportation* 110th Cong. (2008) (statement of Marc Rotenberg, Exec. Dir. EPIC) (C-SPAN video at <https://www.c-span.org/video/?205933-1/computer-spyware>), https://www.epic.org/privacy/dv/Spyware_Test061108.pdf.

Nonetheless in February 2009, Facebook changed its Terms of Service. The new TOS allowed Facebook to use anything a user uploaded to the site for any purpose, at any time, even after the user ceased to use Facebook. Further, the TOS did not provide for a way that users could completely close their account. Rather, users could “deactivate” their account, but all the information would be retained by Facebook, rather than deleted.

EPIC planned to file an FTC complaint, alleging that the new Terms of Service violated the FTC Act Section 5, and constituted “unfair and deceptive trade practices.” In response to this planned complaint, and a very important campaign organized by the “Facebook Users Against the New Terms of Service,” Facebook returned to its previous Terms of Service. Facebook then established a comprehensive program of Governing Principles and a statement of Rights and Responsibilities.⁹

As we reported in 2009:

Facebook has announced the results of the vote on site governance. The initial outcome indicates that approximately 75 percent of users voted for the new terms of service which includes the new Facebook Principles and Statement of Rights and Responsibilities. Under the new Principles, Facebook users will "own and control their information." Facebook also took steps to improve account deletion, to limit sublicenses, and to reduce data exchanges with application developers. EPIC supports the adoption of the new terms. For more information, see EPIC's page on Social Networking Privacy.¹⁰

However, Facebook failed to uphold its commitments to a public governance structure for the company.

From mid-2009 through 2011, EPIC and a coalition of consumer organizations pursued comprehensive accountability for the social media platform.¹¹ When Facebook broke its final

⁹ *Facebook takes a Democratic Turn*, USA Today, Feb. 27, 2009, at 1B, <https://www.pressreader.com/usa/usa-today-us-edition/20090227/281887294213804>

¹⁰ EPIC, *Facebook Gets Ready to Adopt Terms of Service* (Apr. 24, 2009) <https://epic.org/2009/04/facebook-gets-ready-to-adopt-t.html>

¹¹ There is a longer history of significant events concerning the efforts of Facebook users to establish democratic accountability for Facebook during the 2008-2009 period. The filing of the 2009 complaint came about after it became clear that Facebook would not uphold its commitments to the Statement of Right and Responsibilities it had established. It would also be worth reconstructing the history of the “Facebook Users Against the New Terms of Service” as Facebook destroyed the group and all records of its members and activities after the organizers helped lead a successful campaign against the company. Julius Harper was among the organizers of the campaign. A brief history was written by Ben Popken in 2009 for *The Consumerist*, “What Facebook's Users Want In The Next Terms Of Service,” <https://consumerist.com/2009/02/23/what-facebooks-users-want-in-the-next-terms-of-service/>. Julius said this in 2012: “Most people on Facebook don’t even know they can vote or even that a vote is going on. What is a democracy if you don’t know where the polling place is? Or that a vote is even being held? How can you participate? Ignorance becomes a tool that can be used to disenfranchise people.”

commitment, we went ahead with a complaint to the Federal Trade Commission. Our complaint alleged that Facebook had changed user privacy settings and disclosed the personal data of users to third parties without the consent of users.¹² EPIC and others had conducted extensive research and documented the instances of Facebook overriding the users' privacy settings to reveal personal information and to disclose, for commercial benefit, user data, and the personal data of friends and family members, to third parties without their knowledge or affirmative consent.¹³

We explained our argument clearly in the 2009 EPIC complaint with the Commission (attached in full to this statement):

This complaint concerns material changes to privacy settings made by Facebook, the largest social network service in the United States, which adversely impact users of the Facebook service. Facebook's changes to users' privacy settings disclose personal information to the public that was previously restricted. Facebook's changes to users' privacy settings also disclose personal information to third parties that was previously not available. These changes violate user expectations, diminish user privacy, and contradict Facebook's own representations. These business practices are Unfair and Deceptive Trade Practices, subject to review by the Federal Trade Commission (the "Commission") under section 5 of the Federal Trade Commission Act.¹⁴

We should also make clear that the 2009 complaint that EPIC filed with the Federal Trade Commission about Facebook was not the first to produce a significant outcome. In July and August 2001, EPIC and a coalition of fourteen leading consumer groups filed complaints with the Federal Trade Commission (FTC) alleging that the Microsoft Passport system violated Section 5 of the Federal Trade Commission Act (FTCA), which prohibits unfair or deceptive practices in trade.¹⁵

EPIC and the groups alleged that Microsoft violated the law by linking the Windows XP operating system to repeated exhortations to sign up for Passport; by representing that Passport protects privacy, when it and related services facilitate profiling, tracking and monitoring; by signing up Hotmail users for Passport without consent or even the ability to opt-out; by representing that the system complies with the Children's Online Privacy Protection Act; by not allowing individuals to delete their account; and by representing that the system securely holds individuals' data.

Facebook upsets some by seeking to take away users' voting rights, San Jose Mercury News, Nov. 30, 2012, <https://www.mercurynews.com/2012/11/30/facebook-upsets-some-by-seeking-to-take-away-users-voting-rights/>.

¹² *In re Facebook*, EPIC.org, <https://epic.org/privacy/inrefacebook/>.

¹³ *FTC Facebook Settlement*, EPIC.org, <https://epic.org/privacy/ftc/facebook/>.

¹⁴ *In the Matter of Facebook, Inc.* (EPIC, Complaint, Request for Investigation, Injunction, and Other Relief) before the Federal Trade Commission, Washington, D.C. (filed Dec. 17, 2009), <http://www.epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf>.

¹⁵ EPIC, *Microsoft Passport Investigation Docket*, <https://epic.org/privacy/consumer/microsoft/passport.html>.

We requested that the FTC initiate an investigation into the information collection practices of Windows XP and other services, and to order Microsoft to revise XP registration procedures; to block the sharing of Passport information among Microsoft properties absent explicit consent; to allow users of Windows XP to gain access to Microsoft web sites without disclosing their actual identity; and to enable users of Windows XP to easily integrate services provided by non-Microsoft companies for online payment, electronic commerce, and other Internet-based commercial activity.

The Federal Trade Commission undertook the investigation we requested and issued an important consent order. As the Commission explained announcing its enforcement action in 2002:

Microsoft Corporation has agreed to settle Federal Trade Commission charges regarding the privacy and security of personal information collected from consumers through its "Passport" web services. As part of the settlement, Microsoft will implement a comprehensive information security program for Passport and similar services. . . .

The Commission initiated its investigation of the Passport services following a July 2001 complaint from a coalition of consumer groups led by the Electronic Privacy Information Center (EPIC).

According to the Commission's complaint, Microsoft falsely represented that:

- It employs reasonable and appropriate measures under the circumstances to maintain and protect the privacy and confidentiality of consumers' personal information collected through its Passport and Passport Wallet services, including credit card numbers and billing information stored in Passport Wallet;
- Purchases made with Passport Wallet are generally safer or more secure than purchases made at the same site without Passport Wallet when, in fact, most consumers received identical security at those sites regardless of whether they used Passport Wallet to complete their transactions;
- Passport did not collect any personally identifiable information other than that described in its privacy policy when, in fact, Passport collected and held, for a limited time, a personally identifiable sign-in history for each user; and
- The Kids Passport program provided parents control over what information participating Web sites could collect from their children.

The proposed consent order prohibits any misrepresentation of information practices in connection with Passport and other similar services. It also requires Microsoft to implement and maintain a comprehensive information security program. In addition, Microsoft must have its security program certified as

meeting or exceeding the standards in the consent order by an independent professional every two years.¹⁶

FTC Chairmen Timothy J. Muris said at the time, "Good security is fundamental to protecting consumer privacy. Companies that promise to keep personal information secure must follow reasonable and appropriate measures to do so. It's not only good business, it's the law. Even absent known security breaches, we will not wait to act."¹⁷

Then in December 2004, EPIC filed a complaint with the Federal Trade Commission against databroker Choicepoint, urging the Commission to investigate the compilation and sale of personal dossiers by data brokers such as Choicepoint.¹⁸ Based on the EPIC complaint, in 2005, the FTC charged that Choicepoint did not have reasonable procedures to screen and verify prospective businesses for lawful purposes and as a result compromised the personal financial records of more than 163,000 customers in its database. In January 2006, the FTC announced a settlement with Choicepoint, requiring the company to pay \$10 million in civil penalties and provide \$5 millions for consumer redress. EPIC's Choicepoint complaint produced the largest civil fine at the time in the history of the FTC.¹⁹

The Microsoft order led to user-centric identity scheme that, if broadly adopted, could have done much to preserve the original open, decentralized structure of the Internet. The Choicepoint order led to significant reforms in the data broker industry. And it is worth noting that both investigations were successfully pursued with Republican chairmen in charge of the federal agency and both actions were based on unanimous decisions by all of the Commissioners.

The Facebook complaint should have produced an outcome even more consequential than the complaints concerning Microsoft and Choicepoint. In 2011, the FTC, based the materials we provided in 2009 and 2010, confirmed our findings and recommendations. In some areas, the FTC even went further. The FTC issued a Preliminary Order against Facebook in 2011 and then a Final Order in 2012.²⁰ In the press release accompanying the settlement, the FTC stated that Facebook "deceived consumers by telling them they could keep their information on Facebook private, and then repeatedly allowing it to be shared and made public."²¹

¹⁶ Fed. Trade Comm'n, *Microsoft Settles FTC Charges Alleging False Security and Privacy Promises: Passport Single Sign-In, Passport "Wallet," and Kids Passport Named in Complaint Allegations*, Press Release, (Aug. 8, 2002), <https://www.ftc.gov/news-events/press-releases/2002/08/microsoft-settles-ftc-charges-alleging-false-security-privacy>.

¹⁷ *Id.*

¹⁸ EPIC, ChoicePoint, <https://www.epic.org/privacy/choicepoint/>

¹⁹ Fed. Trade Comm'n., *ChoicePoint Settles Data Security Breach Charges; to Pay \$10 Million in Civil Penalties, \$5 Million for Consumer Redress: At Least 800 Cases of Identity Theft Arose From Company's Data Breach* (Jan. 26, 2006), <https://www.ftc.gov/news-events/press-releases/2006/01/choicepoint-settles-data-security-breach-charges-pay-10-million>.

²⁰ Facebook Consent Order.

²¹ Fed. Trade Comm'n., *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>.

According to the FTC, under the proposed settlement Facebook is:

- “barred from making misrepresentations about the privacy or security of consumers’ personal information;”
- “required to obtain consumers’ affirmative express consent before enacting changes that override their privacy preferences;”
- “required to prevent anyone from accessing a user’s material more than 30 days after the user has deleted his or her account;”
- “required to establish and maintain a comprehensive privacy program designed to address privacy risks associated with the development and management of new and existing products and services, and to protect the privacy and confidentiality of consumers’ information; and”
- “required, within 180 days, and every two years after that for the next 20 years, to obtain independent, third-party audits certifying that it has a privacy program in place that meets or exceeds the requirements of the FTC order, and to ensure that the privacy of consumers’ information is protected.”²²

The reporting requirements are set out in more detail in the text of the Final Order. According to the Final Order:

[The] Respondent [Facebook] shall, no later than the date of service of this order, establish and implement, and thereafter maintain, 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. Such program, the content and implementation of which must be documented in writing, shall contain controls and procedures appropriate to Respondent’s size and complexity, the nature and scope of Respondent’s activities, and the sensitivity of the covered information, including:

- A. the designation of an employee or employees to coordinate and be responsible for the privacy program.
- B. the identification of reasonably foreseeable, material risks, both internal and external, that could result in Respondent’s unauthorized collection, use, or disclosure of covered information and an assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this privacy risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management, including training on the requirements of this order, and (2) product design, development, and

²² *Id.*

research.

- C. the design and implementation of reasonable controls and procedures to address the risks identified through the privacy risk assessment, and regular testing or monitoring of the effectiveness of those controls and procedures.
- D. the development and use of reasonable steps to select and retain service providers capable of appropriately protecting the privacy of covered information they receive from Respondent and requiring service providers, by contract, to implement and maintain appropriate privacy protections for such covered information.
- E. the evaluation and adjustment of Respondent's privacy program in light of the results of the testing and monitoring required by subpart C, any material changes to Respondent's operations or business arrangements, or any other circumstances that Respondent knows or has reason to know may have a material impact on the effectiveness of its privacy program.²³

Moreover, the Final Order stated:

Respondent shall obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. A person qualified to prepare such Assessments shall have a minimum of three (3) years of experience in the field of privacy and data protection. All persons selected to conduct such Assessments and prepare such reports shall be approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, in his or her sole discretion. Any decision not to approve a person selected to conduct such Assessments shall be accompanied by a writing setting forth in detail the reasons for denying such approval. The reporting period for the Assessments shall cover: (1) the first one hundred and eighty (180) days after service of the order for the initial Assessment, and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:

- A. set forth the specific privacy controls that Respondent has implemented and maintained during the reporting period;
- B. explain how such privacy controls are appropriate to Respondent's size and complexity, the nature and scope of Respondent's activities, and the sensitivity of the covered information;
- C. explain how the privacy controls that have been implemented meet or exceed the protections required by Part IV of this order; and

²³ Facebook Consent Order.

- D. certify that the privacy controls are operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information and that the controls have so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Respondent shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by Respondent until the order is terminated and provided to the Associate Director of Enforcement within ten (10) days of request.²⁴

EPIC expressed support for the Consent Order but also believed it could be improved.²⁵ In response to the FTC's request for public comments on the proposed order we wrote:

EPIC supports the findings in the FTC Complaint and supports, in part, the directives contained in the Consent Order. The Order makes clear that companies should not engage in unfair and deceptive trade practices, particularly in the collection and use of personal data. However, the proposed Order is insufficient to address the concerns originally identified by EPIC and the consumer coalition, as well as those findings established by the Commission. Consistent with this earlier determination, to protect the interests of Facebook users, and in light of recent changes in the company's business practices, EPIC urges the Commission to require Facebook to:

- Restore the privacy settings that users had in 2009, before the unfair and deceptive practices addressed by the Complaint began;
- Allow users to access all of the data that Facebook keeps about them;
- Cease creating facial recognition profiles without users' affirmative consent;
- Make Facebook's privacy audits publicly available to the greatest extent possible;
- Cease secret post-log out tracking of users across web sites.

²⁴ *Id.* at 6–7.

²⁵ Comments of EPIC, *In the Matter of Facebook, Inc.*, FTC File No. 092 3184, (Dec. 27, 2011), <https://epic.org/privacy/facebook/Facebook-FTC-Settlement-Comments-FINAL.pdf>.

At the time, the FTC settlement with Facebook was widely viewed as a major step forward for the protection of consumer privacy in the United States. The Chairman of the FTC stated, “Facebook is obligated to keep the promises about privacy that it makes to its hundreds of millions of users. Facebook's innovation does not have to come at the expense of consumer privacy. The FTC action will ensure it will not.” Mark Zuckerberg said at the time of the Consent Order that the company had made “a bunch of mistakes.”²⁶ The FTC Chair called Mr. Zuckerberg’s post a “good sign” and said, “He admits mistakes. That can only be good for consumers.”²⁷

Commissioners and staff of the FTC later testified before Congress, citing the Facebook Consent Order as a major accomplishment for the Commission.²⁸ And U.S. policymakers held out the FTC’s work in discussions with trading partners for the proposition that the US could provide privacy protections to those users of US-based services. For example, former FTC Chairwoman wrote this to Věra Jourová, Commissioner for Justice, Consumers and Gender Equality, European Commission:

As part of its privacy and security enforcement program, the FTC has also sought to protect EU consumers by bringing enforcement actions that involved Safe

²⁶ Somini Sengupta, *F.T.C. Settles Privacy Issue at Facebook*, N.Y. Times, at B1 (Nov. 29, 2011), <https://www.nytimes.com/2011/11/30/technology/facebook-agrees-to-ftc-settlement-on-privacy.html>. There was also a “lengthy blog post” from Mr. Zuckerberg in the N.Y. Times article but the link no longer goes to Mr. Zuckerberg’s original post. Mr. Zuckerberg’s post in 2009 that established the Bill of Rights and Responsibilities for the site has also disappeared. This is the original link: <http://blog.facebook.com/blog.php?post=54746167130>.

²⁷ Julianne Pepitone, *Facebook settles FTC charges over 2009 privacy breaches*, CNN Money (Nov. 29, 2011), http://money.cnn.com/2011/11/29/technology/facebook_settlement/index.htm.

²⁸ According to the statement of the FTC Commissioners who testified before the Senate Commerce Committee in 2012:

Similar to the Google order, the Commission’s consent order against Facebook prohibits the company from deceiving consumers with regard to privacy; requires it to obtain users’ affirmative express consent before sharing their information in a way that exceeds their privacy settings; and requires it to implement a comprehensive privacy program and obtain outside audits. In addition, Facebook must ensure that it will stop providing access to a user’s information after she deletes that information.

The Need for Privacy Protections: Perspectives from the Administration and the Federal Trade Commission: Hearing Before the S. Comm on Commerce, Science and Transportation, at 18, 112th Cong. (May 9, 2012) (statement of Fed. Trade Comm’n.),

https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-need-privacy-protections-perspectives-administration-and/120509privacyprotections.pdf; see also, *The Need for Privacy Protections:*

Perspectives from the Administration and the Federal Trade Commission, Hearing before the S. Comm. on Commerce, Science, and Transportation, 112th Cong. (May 19, 2012) (statement of Maureen K. Ohlhausen, Commissioner, Fed. Trade Comm’n) (“We have also charged companies with failing to live up to their privacy promises, as in the highly publicized privacy cases against companies such as Google and Facebook, which together will protect the privacy of more than one billion users worldwide. As a Commissioner, I will urge continuation of this strong enforcement record.”),

https://www.ftc.gov/sites/default/files/documents/public_statements/statement-commissioner-maureen-k.ohlhausen/120509privacystatement.pdf.

Harbor violations. . . . Twenty-year consent orders require Google, Facebook, and Myspace to implement comprehensive privacy programs that must be reasonably designed to address privacy risks related to the development and management of new and existing products and services and to protect the privacy and confidentiality of personal information. The comprehensive privacy programs mandated under these orders must identify foreseeable material risks and have controls to address those risks. The companies must also submit to ongoing, independent assessments of their privacy programs, which must be provided to the FTC. The orders also prohibit these companies from misrepresenting their privacy practices and their participation in any privacy or security program. This prohibition would also apply to companies' acts and practices under the new Privacy Shield Framework. . . . Consequently, these FTC orders help protect over a billion consumers worldwide, hundreds of millions of whom reside in Europe.²⁹

Yet the Federal Trade Commission never charged Facebook with a single violation of the 2011 Consent Order.

Facebook's Repeated Disclosures of Personal Information to Third Parties

On March 16, 2018, Facebook admitted the unlawful transfer of 50 million user profiles to the data mining firm Cambridge Analytica, which harvested the data obtained without consent to influence the 2016 U.S. presidential election.³⁰ Relying on the data provided by Facebook, Cambridge Analytica was able to collect the private information of approximately 270,000 users and their extensive friend networks under false pretenses as a research-driven application.³¹ Facebook now says that the number of users who had their data unlawfully harvested was actually closer to 87 million.³²

But the Cambridge Analytica breach, it turns out, is only the beginning. In the weeks since Facebook CEO Marc Zuckerberg told this Committee “[e]very piece of content that you share on Facebook you own. You have complete control over who sees it and how you share it,” we have learned that that is far from the truth. On June 3, 2018, the New York Times reported that Facebook has “data-sharing partnerships” with at least 60 device makers.³³ “Data-sharing partnership” is a nice way of saying that Facebook was giving your personal information, and the personal information of all your friends, to companies like Apple, Amazon, BlackBerry,

²⁹ Letter from FTC Chairwoman Edith Ramirez to Věra Jourová, Commissioner for Justice, Consumers and Gender Equality, European Commission, at 4-5 (Jul. 7, 2016), <https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q0v>

³⁰ Press Release, Facebook, *Suspending Cambridge Analytica and SCL Group from Facebook* (Mar. 16, 2018), <https://newsroom.fb.com/news/2018/03/suspending-cambridge-analytica/>.

³¹ *Id.*

³² Cecilia Kang and Sheera Frenkel, *Facebook Says Cambridge Analytica Harvested Data of Up to 87 Million Users*, N.Y. Times, (Apr. 4, 2018), <https://www.nytimes.com/2018/04/04/technology/mark-zuckerberg-testify-congress.html>.

³³ Gabriel J.X. Dance, Nicholas Confessore and Michael LaForgia, *Facebook Gave Device Makers Deep Access to Data on Users and Friends*, N.Y. Times (June 3, 2018), <https://www.nytimes.com/interactive/2018/06/03/technology/facebook-device-partners-users-friends-data.html>.

Microsoft and Samsung for the last decade. The New York Times found that “[s]ome device makers could retrieve personal information even from users’ friends who believed they had barred any sharing.”³⁴ Facebook had similar agreements with Chinese phone manufacturers, including Huawei, a company that American intelligence officials have called a national security threat.³⁵ These partnerships pre-dated the 2011 FTC Consent Order and are reportedly still in effect.

Both the Cambridge Analytica breach and the partnerships with device makers are in clear violation of the 2011 Consent Order, which states that Facebook “shall not misrepresent in any manner, expressly or by implication ... the extent to which [Facebook] makes or has made covered information accessible to third parties; and the steps [Facebook] takes or has taken to verify the privacy or security protections that any third party provides.”³⁶ Part II of the proposed order required Facebook to “give its users a clear and prominent notice and obtain their affirmative express consent before sharing their previously-collected information with third parties in any way that materially exceeds the restrictions imposed by their privacy settings.”³⁷ Part IV “requires Facebook to establish and maintain 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, and (2) protect the privacy and confidentiality of covered information. The privacy program must be documented in writing and must contain controls and procedures appropriate to Facebook’s size and complexity, the nature and scope of its activities, and the sensitivity of covered information.”³⁸

Oversight of the Federal Trade Commission and Facebook Compliance with the 2011 Consent Order

Several former FTC commissioners and former FTC staff members have recently suggested that the FTC needs more authority to protect American consumers. At least with regard to enforcement of its current legal authority, we strongly disagree. The FTC could have done far more than it did.

On March 20, 2018, EPIC submitted a request to the FTC under the Freedom of Information Act for the 2013, 2015, and 2017 Facebook Assessments, as well as all records concerning the person(s) approved by the FTC to undertake the Facebook Assessments; and all records of communications between the FTC and Facebook regarding the Facebook Assessments. In 2013, EPIC received redacted version of Facebook’s initial compliance report

³⁴ *Id.*

³⁵ Michael LaForgia and Gabriel J.X. Dance, *Facebook Gave Data Access to Chinese Firm Flagged by U.S. Intelligence*, N.Y. Times (June 5, 2018), <https://www.nytimes.com/2018/06/05/technology/facebook-device-partnerships-china.html>.

³⁶ Federal Trade Commission, *Facebook, Inc.; Analysis of Proposed Consent Order To Aid Public Comment*, 76 Fed. Reg. 75883 (Dec. 5, 2011), https://www.ftc.gov/sites/default/files/documents/federal_register_notices/facebook-inc.analysis-proposed-consent-order-aid-public-comment-proposed-consent-agreement/111205facebookfrm.pdf.

³⁷ *Id.* (emphasis added).

³⁸ *Id.* (emphasis added).

and first independent assessment after a similar FOIA request.³⁹ Cambridge Analytica engaged in the illicit collection of Facebook user data from 2014 to 2016, encompassed by the requested reporting period of the assessments.

EPIC's FOIA request drew attention to a version of the 2017 report available at the FTC website.⁴⁰ The 2017 Facebook Assessment, prepared by PwC, stated that "Facebook's privacy controls were operating with sufficient effectiveness" to protect the privacy of users.⁴¹ This assessment was prepared *after* Cambridge Analytica harvested the personal data of 87 million Facebook users. The report available online is heavily redacted. EPIC is suing now for the release of unredacted report.

We will keep both Subcommittee informed of the progress of EPIC's FOIA request for the FTC reports on Facebook compliance. We also urge the Subcommittee to pursue the public release of these documents. They will provide for you a fuller pictures of the FTC's lack of response to the looming privacy crisis in America.

Recommendations

There is a lot of work ahead to safeguard the personal data of Americans. Here are a few preliminary recommendations:

- *Improve oversight of the Federal Trade Commission.* The FTC has failed to protect the privacy interests of American consumer and the Commission's inaction contributed directly to the Cambridge Analytica breach, and possibly the Brexit vote and the outcome of the 2016 Presidential election. Oversight of the Commission's failure to enforce the 2011 consent order is critical, particularly for the Senate Commerce Committee which also bears some responsibility for this outcome.
- *Update US privacy laws.* It goes without saying (though obviously it still needs to be said) that U.S. privacy law is out of date. There has always been a gap between changes in technology and business practices and the development of new privacy protections. But the gap today in the United States is the greatest at any time since the emergence of modern privacy law in the 1960s. The current approach is also unnecessarily inefficient, complex, and ineffective. And many of the current proposals, e.g. better privacy notices, would do little to protect privacy or address the problems arising from Cambridge Analytica debacle.
- *Establish a federal privacy agency in the United States.* The U.S. is one of the few developed countries in the world without a data protection agency. The practical

³⁹ Facebook Initial Compliance Report (submitted to FTC on Nov. 13, 2012), <http://epic.org/foia/FTC/facebook/EPIC-13-04-26-FTC-FOIA-20130612-Production-1.pdf>; Facebook Initial Independent Assessment (submitted to FTC on Apr. 22, 2013), <http://epic.org/foia/FTC/facebook/EPIC-14-04-26-FTC-FOIA-20130612-Production-2.pdf>.

⁴⁰ PwC, *Independent Assessor's Report on Facebook's Privacy Program* (Feb. 11, 2017), <https://epic.org/foia/ftc/facebook/EPIC-18-03-20-FTC-FOIA-20180418-FB-Assessment-2017.pdf>.

⁴¹ *Id.* at 4.

consequence is that the U.S consumers experience the highest levels of data breach, financial fraud, and identity theft in the world. And U.S. businesses, with their vast collections of personal data, remain the target of cyber attack by criminals and foreign adversaries. The longer the U.S. continues on this course, the greater will be the threats to consumer privacy, democratic institutions, and national security.

Conclusion

The 2011 Consent Order against Facebook was issued to protect the privacy of user data. If the FTC had done its job and enforced the Order, the transfer of 87 million user records to Cambridge Analytica could have been avoided.

After this week's hearing, the Subcommittee should ask current and former FTC Commissioners and key staff, "why didn't you enforce the 2011 Consent Order against Facebook and prevent this mess?"⁴²

We ask that this letter be submitted into the hearing record. EPIC looks forward to working with the Subcommittee.

Sincerely,

/s/ Marc Rotenberg

Marc Rotenberg
EPIC President

/s/ Caitriona Fitzgerald

Caitriona Fitzgerald
EPIC Policy Director

/s/ Enid Zhou

Enid Zhou
EPIC Open Government Fellow

/s/ Sunny Kang

Sunny Kang
EPIC International Consumer Counsel

/s/ Sam Lester

Sam Lester
EPIC Consumer Privacy Counsel

Attachment

EPIC, et al. *In the Matter of Facebook, Inc: Complaint, Request for Investigation, Injunction, and Other Relief*, Before the Federal Trade Commission, Washington, DC (Dec. 17, 2009) (29 pages, 119 numbered paragraphs) (signatories include The Electronic Privacy Information Center, The American Library Association, The Center for Digital Democracy, The Consumer Federation of America, Patient Privacy Rights, Privacy Activism, Privacy Rights Now Coalition, The Privacy Rights Clearinghouse, The U.S. Bill of Rights Foundation).

⁴² See Marc Rotenberg, *How the FTC Could Have Prevented the Facebook Mess*, Techonomy (Mar. 22, 2018), <https://techonomy.com/2018/03/how-the-ftc-could-have-avoided-the-facebook-mess/>.