epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

April 9, 2018

Senator Chuck Grassley, Chairman
Senator Dianne Feinstein, Ranking Member
Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, D.C. 20510

Senator John Thune, Chairman
Senator Bill Nelson, Ranking Members
Committee on Commerce, Science and Transportation
512 Dirksen Senate Building
Washington, D.C. 20510

Dear Members of the Senate Judiciary Committee and the Senate Commerce Committee:

We write to you regarding the joint hearing this week on "Facebook, Social Media Privacy, and the Use and Abuse of Data."[1] We appreciate your interest in this important issue. For many years, the Electronic Privacy Information Center ("EPIC") has worked with both the Judiciary Committee and the Commerce Committee to help protect the privacy rights of Americans.[2]

In this statement from EPIC, we outline the history of Facebook's 2011 Consent Order with the Federal Trade Commission, point to key developments (including the failure of the FTC to enforce the Order), and make a few preliminary recommendations. Our assessment is that the Cambridge Analytica breach, as well as a range of threats to consumer privacy and democratic institutions, could have been prevented if the Commission had enforced the Order.

---

[1] *Facebook, Social Media Privacy, and the Use and Abuse of Data: Hearing Before the S. Comm. on the Judiciary*, 115th Cong. (2018), https://www.judiciary.senate.gov/meetings/facebook-social-media-privacy-and-the-use-and-abuse-of-data (April 10, 2018).

[2] *See, e.g.*, *The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century: Hearing Before the S. Comm on the Judiciary*, 112th Cong. (2012) (statement of Marc Rotenberg, Exec. Dir., EPIC), https://epic.org/privacy/vppa/EPIC-Senate-VPPA-Testimony.pdf; *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.

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.[3] 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.[4] 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.[5]

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.

---

[3] 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.

[4] EPIC, Social Networking Privacy, https://epic.org/privacy/socialnet/.

[5] *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.

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.[6]

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.[7]

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.[8] When Facebook broke its final 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.[9] EPIC and others had conducted extensive research

---

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

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

[8] 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." *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/.

[9] *In re Facebook*, EPIC.org, https://epic.org/privacy/inrefacebook/.

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.[10]

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.[11]

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.[12]

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.

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.

---

[10] *FTC Facebook Settlement*, EPIC.org, https://epic.org/privacy/ftc/facebook/.
[11] *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.
[12] EPIC, *Microsoft Passport Investigation Docket,* https://epic.org/privacy/consumer/microsoft/passport.html.

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.[13]

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

[13] 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.

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."[14]

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.[15] 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.[16]

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.[17] 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."[18]

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;"

---

[14] *Id.*
[15] EPIC, ChoicePoint, https://www.epic.org/privacy/choicepoint/
[16] 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.
[17] Facebook Consent Order.
[18] 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.

- "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."[19]

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 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

[19] *Id*.

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.[20]

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
>
> 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

[20] Facebook Consent Order.

> 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.[21]

EPIC expressed support for the Consent Order but also believed it could be improved.[22] 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.

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."[23] The FTC Chair called Mr.

---

[21] *Id.* at 6–7.
[22] 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.
[23] 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

Zuckerberg's post a "good sign" and said, "He admits mistakes. That can only be good for consumers."[24]

Commissioners and staff of the FTC later testified before Congress, citing the Facebook Consent Order as a major accomplishment for the Commission.[25] 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 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

---

Rights and Responsibilities for the site has also disappeared. This is the original link: http://blog.facebook.com/blog.php?post=54746167130.

[24] 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.

[25] 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/120509privacytestimony.pdf.

> 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.[26]

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

The Google Consent Order and the FTC's Subsequent Failure to Enforce Consent Orders

In 2011, we also had also obtained a significant consent order at the FTC against Google after the disastrous roll-out of Google "Buzz." In that case, the FTC established a consent order after Google tried to enroll Gmail users into a social networking service without meaningful consent. The outcome was disastrous. Personal contact information was made publicly available by Google as part of its effort to establish a social network service to compete with Facebook. EPIC filed a detailed complaint with the Commission in February that produced a consent order in 2011, comparable to the order for Facebook.[27]

But a problem we did not anticipate became apparent almost immediately: the Federal Trade Commission was unwilling to enforce its own consent orders. Almost immediately after the settlements, both Facebook and Google began to test the FTC's willingness to stand behind its judgements. Dramatic changes in the two companies' advertising models led to more invasive tracking of Internet users. Online and offline activities were increasingly becoming merged.

To EPIC and many others, these changes violated the terms of the consent orders. We urged the FTC to establish a process to review these changes and publish its findings so that the public could at least evaluate whether the companies were complying with the original orders. But the Commission remained silent, even as it claimed that its model was working well for these companies.

In 2012, EPIC sued the Commission when it became clear that Google was proposing to do precisely what the FTC said it could not – consolidate user data across various services that came with diverse privacy policies in order to build detailed individual profiles. The problem was widely understood. Many members of Congress in both parties, state attorneys general, and Jon Leibowitz, the head of the FTC itself, warned about the possible outcome. Even the federal

---

[26] 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

[27] *In the Matter of Google, Inc.*, EPIC Complaint, Request for Investigation, Injunction, and Other Relief, before the Federal Trade Commission, Washington, D.C. (filed Feb. 16, 2010), https://epic.org/privacy/ftc/googlebuzz/GoogleBuzz_Complaint.pdf; Fed. Trade Comm'n., *FTC Charges Deceptive Privacy Practices in Googles Rollout of Its Buzz Social Network: Google Agrees to Implement Comprehensive Privacy Program to Protect Consumer Data*, Press Release, (Mar. 30, 2011), https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz.

court, which ruled that it could not require the agency to enforce its order, was sympathetic. "EPIC – along with many other individuals and organizations – has advanced serious concerns that may well be legitimate, and the FTC, which has advised the Court that the matter is under review, may ultimately decide to institute an enforcement action," wrote the judge.[28]

But that enforcement action never came. Even afterward, EPIC and other consumer privacy organizations have continued to urge the Federal Trade Commission to enforce its consent orders. In our most recent comments to the Federal Trade Commissioner, we said simply "The FTC Must Enforce Existing Consent Orders." We wrote:

> The effectiveness of FTC enforcement is determined by the agency's willingness to enforce the legal judgments it obtains. The FTC should review substantial changes in business practices for companies under consent orders that implicate the privacy interests of consumers. Multiple prominent internet firms have been permitted to alter business practices, without consequence, despite being subject to 20-year consent orders with the FTC. This has harmed consumers and promoted industry disregard for the FTC.[29]

The Senate Commerce Committee should be specifically concerned about the FTC's ongoing failure to enforce its consent orders. This agency practice poses an ongoing risk to both American consumers and American businesses.

Cambridge Analytica Breach

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] Last week, Facebook announced that the number of users who had their data unlawfully harvested was actually closer to 87 million.[32]

This is 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]

---

[28] *EPIC v. FTC,* 844 F. Supp. 2d 98 (D.D.C. 2012), https://epic.org/privacy/ftc/google/EPICvFTC-CtMemo.pdf.
[29] EPIC Statement to FTC (Feb. 2017), https://epic.org/privacy/internet/ftc/EPIC-et-al-ltr-FTC-02-15-2017.pdf.
[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.

takes or has taken to verify the privacy or security protections that any third party provides."[33] 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."[34] 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."[35]

Response of EPIC and Consumer Privacy Organizations, Compliance with GDPR

After the news broke of the Cambridge Analytica breach, EPIC and a consumer coalition urged the FTC to reopen the Facebook investigation.[36] We stated, "Facebook's admission that it disclosed data to third parties without users' consent suggests a clear violation of the 2011 Facebook Order." We further said:

> The FTC has an obligation to the American public to ensure that companies comply with existing Consent Orders. It is unconscionable that the FTC allowed this unprecedented disclosure of Americans' personal data to occur. The FTC's failure to act imperils not only privacy but democracy as well.

On March 26, 2018, less than two weeks ago, the FTC announced it would reopen the investigation.[37] The Statement by the Acting Director of FTC's Bureau of Consumer Protection Regarding Reported Concerns about Facebook Privacy Practice, issued on March 26, 2018, was as follows:

> The FTC is firmly and fully committed to using all of its tools to protect the privacy of consumers. Foremost among these tools is enforcement action against

---

[33] 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/111205facebookfrn.pdf.

[34] *Id.* (emphasis added).

[35] *Id.* (emphasis added).

[36] Letter to Acting Chairman Maureen Ohlhausen and Commissioner Terrell McSweeney from leading consumer privacy organizations in the United States (Mar. 20, 2018), https://epic.org/privacy/facebook/EPIC-et-al-ltr-FTC-Cambridge-FB-03-20-18.pdf. *See* "EPIC, Consumer Groups Urge FTC To Investigate Facebook" (Mar. 20, 2018), https://epic.org/2018/03/epic-consumer-groups-urge-ftc-.html.

[37] Fed. Trade Comm'n., *Statement by the Acting Director of FTC's Bureau of Consumer Protection Regarding Reported Concerns about Facebook Privacy Practices* (March 26, 2018), https://www.ftc.gov/news-events/press-releases/2018/03/statement-acting-director-ftcs-bureau-consumer-protection. *See* EPIC, "FTC Confirms Investigation into Facebook about 2011 Consent Order" (Mar. 26, 2018), https://epic.org/2018/03/ftc-confirms-investigation-int.html.

> companies that fail to honor their privacy promises, including to comply with Privacy Shield, or that engage in unfair acts that cause substantial injury to consumers in violation of the FTC Act. Companies who have settled previous FTC actions must also comply with FTC order provisions imposing privacy and data security requirements. Accordingly, the FTC takes very seriously recent press reports raising substantial concerns about the privacy practices of Facebook. Today, the FTC is confirming that it has an open non-public investigation into these practices.

Congress should monitor this matter closely. This may be one of the most consequential investigations currently underway in the federal government.

But others are not waiting for the resolution. State Attorneys General have also made clear their concerns about the Facebook matter.[38]

Also today, a broad coalition of consumer organizations in the United States and Europe, represented by the TransAtlantic Consumer Dialogue ("TACD"), will urge Mr. Zuckerberg to make clear his commitment to compliance with the General Data Protection Regulation. The TACD wrote:

> The GDPR helps ensure that companies such as yours operate in an accountable and transparent manner, subject to the rule of law and the democratic process. The GDPR provides a solid foundation for data protection, establishing clear responsibilities for companies that collect personal data and clear rights for users whose data is gathered. These are protections that all users should be entitled to no matter where they are located.[39]

EPIC supports the recommendation of TACD concerning the GDPR. There is little reason that a U.S. firm should provide better privacy protection to individuals outside the United States than it does to those inside our country.

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

[38] EPIC, "State AGs Launch Facebook Investigation," (Mar. 26, 2018), https://epic.org/2018/03/state-ags-launch-facebook-inve.html.
[39] Letter from TACD to Marck Zuckerberg, CEO, Facebook, Inc., Apr. 9, 2018, http://tacd.org/wp-content/uploads/2018/04/TACD-letter-to-Mark-Zuckerberg_final.pdf.

records of communications between the FTC and Facebook regarding the Facebook Assessments. In 2013, EPIC received redacted version of Facebook's initial compliance report and first independent assessment after a similar FOIA request.[40]

Under the Final Consent Order, Facebook's initial assessment was due to the FTC on April 13, 2013, and the subsequent reporting deadlines were in 2015 and 2017. Cambridge Analytica engaged in the illicit collection of Facebook user data from 2014 to 2016, encompassed by the requested reporting period of the assessments.

We will keep both Committees informed of the progress of EPIC's FOIA request for the FTC reports on Facebook compliance. We also urge both Committees 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 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.

[40] 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.

Conclusion

The transfer of 87 million user records to Cambridge Analytica could have been avoided if the FTC had done its job. The 2011 Consent Order against Facebook was issued to protect the privacy of user data. If it had been enforced, there would be no need for the hearing this week.

After the hearing with Mr. Zuckerberg this week, the Committees 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?"[41]

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

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).

[41] *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/.