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

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

FEDERAL TRADE COMMISSION

"FTC Releases Draft Strategic Plan for Fiscal Years 2018 to 2022"

December 5, 2017

In response to the Federal Trade Commission's request for public comment on its "Draft Strategic Plan for Fiscal Years 2018-2022," the Electronic Privacy Information Center ("EPIC") offers the following recommendations for how the FTC can accomplish its mission of protecting consumers and promoting competition in the 21st century. EPIC's recommendations build on the earlier comments submitted to the FTC by leading consumer and privacy organizations. In *FTC 2017: 10 Steps for Protecting Consumers, Promoting Competition and Innovation,* EPIC, the Center for Digital Democracy, Consumer Federation of America, Consumer Watchdog, and U.S. PIRG set out a series of steps to protect the privacy interests of American consumers.[1] As we stated:

> American consumers today are at great risk of identity theft, financial fraud, and data breaches. Sensitive personal information is collected by many companies that simply do not do enough to safeguard consumer privacy. We also believe that proactive efforts to strengthen data protection will spur innovation and support business models that are sustainable over time.

[1] Letter to Acting FTC Chair Maureen Ohlhausen, FTC 2017: 10 Steps for Protecting Consumers, Promoting Competition and Innovation (Feb. 15, 2017), https://epic.org/privacy/internet/ftc/EPIC-et-al-ltr-FTC-02-15-2017.pdf.

> The Federal Trade Commission plays a critical role today safeguarding American consumers. To advance the agency's mission on behalf of consumers, we recommend the following concrete proposals to protect consumers and promote competition and innovation.[2]

Based upon the recommendations in that earlier statement to the FTC, EPIC offers the following ten proposals for the FTC's 2018-2022 Strategic Plan. These proposals identify systemic concerns concerning the FTC's ability to fulfill its mission.

1. The FTC Should Enforce Its Consent Orders and Publish Findings on Compliance

The effectiveness of the FTC depends primarily upon the agency's willingness to enforce the legal judgments it obtains. However, the FTC routinely fails to enforce its consent orders, which promotes industry disregard for the FTC.[3] Companies under consent decree have no incentive to protect consumer data if they do not anticipate the FTC to hold them accountable when they violate consent decrees. Beginning in 2018, the FTC should review substantial changes in business practices that implicate the privacy and data protection interests of consumers, determine whether they comply with existing consent orders, and publish a finding on the agency website.

EPIC has repeatedly pressed the FTC to enforce its consent orders. In February 2012, EPIC filed a lawsuit to compel the FTC to enforce the Google consent order and block Google's proposed consolidation of user data from over 60 products and services without users' consent.[4] EPIC argued that this change in business practice was in clear violation of the consent order that Google entered into on October 13, 2011.[5] The Federal District Court for the District of Columbia ultimately ruled that, because courts lack jurisdiction over agency enforcement

[2] *Id.*
[3] *See* EPIC v. FTC, No. 12-206 (D.D.C. Feb. 24, 2012).
[4] *Id*.
[5] Fed. Trade Comm'n, *In re Google Buzz*, Decision and Order, FTC File No. 102-3136 (Oct. 13, 2011).

actions, it was unable to compel the FTC to enforce the consent order. The D.C. Circuit Court affirmed.[6] However, the District Court did find "serious concerns" with Google's change in business practices.[7]

Google's decision to consolidate user data generated widespread consternation. In 2013, European data protection authorities ordered Google to comply with data protection law or face fines over their consolidation of user data.[8] In 2014, the Dutch Data Protection Authority found that Google's change in business practices violated national privacy law.[9] Google's decision to consolidate user data also prompted rebuke from Members of Congress, state Attorneys General, and IT managers in the government and private sector.[10]

In addition, EPIC has called attention to the numerous changes Facebook has made to its privacy settings without obtaining users' affirmative consent, in violation of the terms of its FTC consent decree.[11] In 2012, Facebook entered into a 20-year consent order with the FTC in which it agreed that it "shall not misrepresent … the extent to which it maintains the privacy or security of covered information," and would provide disclosure separate from its privacy policy.[12] But in 2014, Facebook made a dramatic shift in its business practices and began tracking user activity on third party websites across the internet for use in targeted advertising, without disclosing this change to consumers separate from its privacy policy or obtaining affirmative consent.[13] The Trans-Atlantic Consumer Dialogue wrote a letter to the FTC commissioners asking them to investigate Facebook's new business practices as a possible violation of the 2012 consent

[6] *EPIC v. Federal Trade Commission,* Case No. 12-5054 (D.C. Cir. Filed Feb. 24, 2012).
[7] EPIC v. FTC, No. 12-206.
[8] *See* EPIC, *EPIC v. FTC (Enforcement of the Google Consent Order)*, https://epic.org/privacy/ftc/google/consent-order.html.
[9] *Id*.
[10] *Id.*
[11] *See* EPIC, *Smith v. Facebook*, https://epic.org/amicus/facebook/smith/.
[12] Fed Trade Comm'n, *In re Facebook*, Decision and Order, FTC File No. 092-3184 (Jul. 27, 2012).
[13] *See* EPIC, *Smith v. Facebook*, https://epic.org/amicus/facebook/smith/.

order.[14] Subsequently, Facebook was subjected to a lawsuit alleging that its tracking of users on third party medical websites violated consumers' right to privacy under California law.[15] Facebook has made numerous changes to its business practices following its 2012 consent decree with the FTC, many of which likely violate the terms of the order.

Companies and consumer organizations may disagree as to whether a significant change in business practices violates a consent order. That is a decision ultimately for the Commission. But it is incumbent upon the FTC to develop a process that ensures a reasoned decision, subject to public review. At present, there is no meaningful public process to ensure compliance with FTC consent orders.

2. The FTC Should Incorporate Public Comments on Proposed Settlement Agreements

Beginning in 2018, the FTC should incorporate the public comments it requests on proposed settlement agreements in final orders. The agency has thus far failed to incorporate important suggestions from consumer advocates that would strengthen proposed settlements. The FTC's failure to make any changes is: (1) contrary to the explicit purpose of the statutory provision that allows the Commission to request comments from the public;[16] (2) contrary to the broader purpose of the Commission to police unfair and deceptive trade practices;[17] and (3) contrary to the interests of American consumers.

[14] Letter from the Trans Atlantic Consumer Dialogue to Charwoman Edith Ramirez, Fed. Trade Comm'n, and Commissioner Billy Hawkes, Data Protection Comm'nr, Ireland (Jul. 29, 2014), http://tacd.org/wp-content/uploads/2014/07/TACDletter-to-FTC-and-Irish-Data-Protection-Commissioner-re-Facebook-data-collection.pd.
[15] *See* EPIC, *Smith v. Facebook*, https://epic.org/amicus/facebook/smith/.
[16] Commission Rules of Practice, 16 C.F.R. § 2.34 (C) (2014).
[17] Federal Trade Commission Act, 15 U.S.C. § 46 (2006).

The Commission's authority to solicit public comment is pursuant to agency regulations. Commission Rules of Practice, 16 C.F.R. § 2.34 states:

> **(c) Public comment.** Promptly after its acceptance of the consent agreement, the Commission will place the order contained in the consent agreement, the complaint, and the consent agreement on the public record for a period of 30 days, or such other period as the Commission may specify, for the receipt of comments or views from any interested person.
> **(e) Action following comment period. (2**) The Commission, following the comment period, may determine, on the basis of the comments or otherwise, that a Final Decision and Order that was issued in advance of the comment period should be modified. Absent agreement by respondents to the modifications, the Commission may initiate a proceeding to reopen and modify the decision and order in accordance with § 3.72(b) of this chapter or commence a new administrative proceeding by issuing a complaint in accordance with § 3.11 of this chapter.

The provision allows private parties to withdraw from proposed consent orders. As one court has explained, "[s]ince the Commission can withdraw its acceptance, two contract principles permit consent order respondents to withdraw their consent so long as the withdrawal occurs prior to a final decision by the Commission"[18] A failure by the Commission to pursue modifications to proposed orders pursuant to public comment would therefore reflect a lack of diligence on the part of the Commission. If the Commission chooses not to incorporate the comments it receives, it should provide a "reasoned response."[19]

EPIC has submitted numerous comments to the Commission over the years on proposed orders that implicate the privacy interests of consumers.[20] However, to date the Commission has not once modified its consent orders to adopt any of the recommendations of consumer privacy

[18] Johnson Prod. Co. v. F.T.C., 549 F.2d 35, 37 (7th Cir. 1978).
[19] *See* Interstate Nat. Gas Ass'n of Am. v. F.E.R.C., 494 F.3d 1092, 1096 (D.C. Cir. 2007).
[20] *See,* e.g. Comments of EPIC, *In the Matter of Snapchat, Inc.,* FTC File No. 132 3078, Jun. 9, 2014, https://epic.org/apa/comments/FTC-Snapchat-Cmts.pdf; Comments of EPIC, *In the Matter of Myspace LLC,* FTC Docket No. 102 3058, Jun. 8, 2012, https://epic.org/privacy/socialnet/EPIC- Myspace-comments-FINAL.pdf; Comments of EPIC, *In the Matter of Facebook, Inc.* FTC Docket No. 092 3184, Dec. 27, 2011, https://epic.org/privacy/facebook/Facebook-FTC- Settlement-Comments-FINAL.pdf; Comments of the EPIC, *In the Matter of Google,* FTC Docket No. 102 3136, May 2, 2011, https://epic.org/privacy/ftc/googlebuzz/EPIC_Comments_to_FTC_Google_Buzz.pdf.

groups. In 2011, EPIC submitted comments to the FTC on a proposed consent order with Google regarding its "Google Buzz" service.[21] The FTC alleged that "Google deceived consumers about their ability to decline enrollment in certain features of Buzz," and in addition, "Google failed to disclose adequately that certain information would become public by default through the Buzz product."[22] EPIC originally brought the Google Buzz matter to the attention of the FTC, and provided detailed recommendations for how to improve the settlement.[23] EPIC recommended that the order require Google to (1) incorporate Fair Information Practices for all of its products and services, (2) build a "Do Not Track" mechanism into the company's Chrome web browser, (3) encrypt all of its cloud computing services, and (4) cease tracking mobile phone users' locations or web-browsing habits without explicit opt-in permission.[24] EPIC also called the FTC's attention to numerous other comments submitted over the course of the Google Buzz proceeding by consumer privacy advocates recommending further steps that the FTC should take to protect Google users' privacy.[25] The Commission failed to incorporate any of these recommendations into its final order.

In addition, EPIC submitted detailed comments regarding the FTC's proposed settlement with Facebook in 2011.[26] As with Google Buzz, the Facebook settlement arose from a complaint filed by EPIC and a collation of privacy and civil liberties organizations, and a supplemental

---

[21] *See* FTC, *Google, Inc.; Analysis of Proposed Consent Order to Aid Public Comment,* File No. 102-3136, 76 Fed. Reg. 18762 (Apr. 5, 2011), *available at* http://www.ftc.gov/os/caselist/1023136/110405googlebuzzfrn.pdf.
[22] *Id*.
[23] *See* Comments of the EPIC, *In the Matter of Google,* FTC Docket No. 102 3136, May 2, 2011, https://epic.org/privacy/ftc/googlebuzz/EPIC_Comments_to_FTC_Google_Buzz.pdf.
[24] *Id*.
[25] *Id*.
[26] Facebook, Inc.; Analysis of Proposed Consent Order to Aid Public Comment, 76 Fed. Reg. 75883 (proposed Dec. 5, 2011), http://www.ftc.gov/os/fedreg/2011/12/111205facebookfrn.pdf.

complaint filed by EPIC in 2010.[27] EPIC alerted the FTC's to changes in Facebook's business practices and urged the Commission to (1) require Facebook to restore its original privacy settings prior to the Commission's Complaint, (2) allow users to access all of the data that Facebook keeps about them, (3) cease creating facial recognition profiles without users' affirmative consent, (4) make Facebook audits publicly available and (5) cease secret post-log out tracking of users across the web.[28] Since EPIC's comments, Facebook has repeatedly come under scrutiny for the very practices EPIC urged the Commission to prohibit. Despite EPIC's recommendations, the Commission adopted the proposed order without any modifications.

Finally, EPIC submitted comments to the FTC regarding its settlement with Snapchat in 2014.[29] The Snapchat matter also arose from a complaint EPIC filed with the FTC.[30] The FTC found that Snapchat had made misrepresentations to users regarding whether Snapchat messages are permanently deleted.[31] EPIC urged the Commission to strengthen the settlement by requiring Snapchat to implement the Consumer Privacy Bill of Rights and make Snapchat's independent privacy assessments available to the public. As with Google Buzz and Facebook, the FTC again failed to incorporate any of these proposals.

---

[27] Facebook, Inc., (2009) (EPIC Complaint, Request for Investigation, Injunction, and Other Relief), https://epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf; Facebook, Inc., (2010) (EPIC Supplemental Materials in Support of Pending Complaint and Request for Injunction, Request for Investigation and for Other Relief); Facebook, Inc., (2010) (EPIC Complaint, Request for Investigation, Injunction, and Other Relief) , https://epic.org/privacy/facebook/EPIC_FTC_FB_Complaint.pdf.

[28] Comments of EPIC, *In the Matter of Facebook, Inc.* FTC Docket No. 092 3184, Dec. 27, 2011, https://epic.org/privacy/facebook/Facebook-FTC- Settlement-Comments-FINAL.pdf

[29] Comments of EPIC, *In the Matter of Snapchat, Inc.,* FTC File No. 132 3078, Jun. 9, 2014, https://epic.org/apa/comments/FTC-Snapchat-Cmts.pdf.

[30] *In the Matter of Snapchat, Inc*., (2013) (EPIC Complaint, Request for Investigation, Injunction, and Other Relief), http://epic.org/privacy/ftc/EPIC-Snapchat-Complaint.pdf.

[31] *In the Matter of Snapchat, Inc.,* FTC File No. 132 3078 (2014) (Agreement Containing Consent Order), http://www.ftc.gov/system/files/documents/cases/140508snapchatorder .pdf.

3. The FTC Should Mandate Fair Information Practices in Consumer Privacy Settlements

Beginning in 2018, the FTC should require compliance with Fair Information Practices under the terms of consent orders with companies in consumer privacy settlements. The Code of Fair Information Practices ("FIPs") sets out responsibilities in the collection and use of personal data.[32] It serves as the starting point for modern privacy law and was incorporated into the Privacy Act of 1974.[33] The FIPs are also found in other privacy laws and frameworks, such as the Organization for Economic Cooperation and Development ("OECD") Privacy Guidelines[34] and the European Commission's Data Protection Regulation.[35] This common approach to privacy protection helps enable international data transfer.

Today, U.S. technology and business practices have outpaced our legal protection, which is why we are experiencing skyrocketing levels of data breach, identity theft, and financial fraud. That is also why our trading partners are increasingly apprehensive about sending the personal data of their citizens to the United States. The Equifax data breach in particular highlighted the U.S.'s inadequate approach to data security and underscored why the FIPs should be extended to the private sector.

In accordance with the FIPs, the Commission's orders should require companies to (1) adopt privacy-enhancing techniques, (2) limit the use of data for the original purpose for which it was collected, (3) prohibit companies from using secret consumer scoring systems, (4) prohibit

---

[32] EPIC, The Code of Fair Information Practices, https://epic.org/privacy/consumer/code_fair_info.html.
[33] Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy*, 2001 Stan. Tech. L. Rev. 1.
[34] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, *available at* http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.
[35] Proposal for a Regulation of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and the free movement of such data (General Data Protection Regulation), E.C. COM (2012) final, (Jan. 25, 2012), available at http://ex.europa/eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

companies from transferring personal data to third parties without explicit opt-in consent, and (5) mandate comprehensive data security measures. The FTC has the legal authority to impose these requirements and doing so will have the effect of raising industry standards.

First, as part of the 2018-2022 Strategic Plan, the FTC should require companies to adopt privacy-enhancing techniques (PETs) such as data minimization to limit the amount of personal data a company collects and the length of time that it retains that data. The FTC should also require companies to encrypt and anonymize data to make it harder for hackers to steal the identities of the consumers whose data was breached. In addition, the FTC should require companies to disgorge data it unlawfully obtained.

Second, under the Privacy Act of 1974, when data is collected by federal agencies, it is generally for a specific purpose and its use is limited to that purpose. When data is collected by private entities, however, it is often sold to third-parties and used by many entities for a multitude of purposes that differ vastly from the original purpose for which it was collected. For example, information originally collected by a student loan servicer will then appear on a person's credit report, and it might then be sold to employment agencies and can eventually serve as the basis to deny that person a job.[36] The FTC's orders should limit the use of data in the private sector to only the purpose for which it was originally collected.

Third, the Privacy Act prohibits the existence of secret government databases and requires government agencies to show an individual any records kept on him or her (with broad exceptions for law enforcement activities).[37] In the private sector, companies increasingly rely on secret algorithms and scoring systems that make it impossible for consumers to know what information is collected about them and how it is used. Today, consumers confront a "black box

[36] Cathy O'Neil, *Weapons of Math Destruction* (2016).
[37] EPIC, *The Privacy Act*, https://epic.org/privacy/1974act/.

society" in which companies from all sectors of the economy engage in ubiquitous data collection and profiling without consumers' knowledge or control.[38] In accordance with the FIPs, consumers should have access to all the data that is collected about them and should be entitled to know how that data is used.

Fourth, one of the most important aspects of the Privacy Act is that it restricts the transfer of information between government agencies. It does this by limiting "matching programs," which it defines as the computerized comparison of databases in order to determine the status, rights, or benefits of the individuals within those systems of records. In the private sector, however, personal data is freely transferred between entities without any regard to individual privacy. The FTC should not permit companies to sell or disclose data to third parties without explicit opt-in consent by the consumer.

And fifth, beginning in 2018, the FTC should begin mandating comprehensive data security measures in its consent orders. For instance, in the FTC's complaint against Uber, the Commission found that the company allowed unauthorized access to its trove of personal data stored in the Amazon S3 Datastore.[39] However, as EPIC pointed out, the FTC's consent order failed to establish any affirmative data security requirements beyond mandating that Uber develop a "comprehensive privacy program."[40] It makes little sense for the Commission to bring enforcement actions against companies for failing to maintain adequate data security without imposing any data security requirements.

[38] Frank Pasquale, THE BLACK BOX SOCIETY 8 (2015); Danielle Keats Citron & Frank Pasquale, The Scored Society: Due Process for Automated Predictions, 89 Wash. L. Rev. 1 (2014).
[39] Fed. Trade Comm'n, *In the Matter of Uber Technologies, Inc*. (Complaint).
[40] Comments of EPIC, *In the Matter of Uber Technologies, Inc*., FTC File No. 152-3054 (Sep. 15, 2017).

4. The FTC Should Promote Transparency

The FTC's Strategic Plan should also reflect a commitment to transparency in how the Commission handles complaints received from organizations representing consumers' interests. Specifically, the FTC should promptly confirm receipt of such complaints and notify the complainants in a timely fashion if it decides not to bring formal action and provide the reasons for that decision. The Commission should also establish a formal and transparent process to assess significant changes in business practices by a company subject to an FTC consent order.

EPIC has called for the FTC to make privacy audits publicly available to the greatest extent possible.[41] In the past, the Commission has stated that similar privacy assessments by other companies would be available to the public, subject to applicable laws. After finalizing a consent order with Google that required similar independent assessments, the Commission wrote to EPIC and stated that "[t]o the extent permissible under law, the public may have access to the submissions required pursuant to the order."[42] Furthermore, the experience of the international community provides evidence of the feasibility of such transparency. For example, in 2011 the Irish Data Protection Commissioner's investigation into Facebook produced a 150-page report and 77 pages of "technical analysis" that were made publicly available.[43] The Data Protection

[41] *See, e.g.*, Comments of EPIC to the FTC, *In the Matter of Uber Technologies, Inc.*, FTC File No. 152-3054 (Sept. 17, 2017), https://epic.org/apa/comments/EPIC-FTC-Uber-Settlement.pdf; Comments of EPIC to the FTC, *In the Matter of Myspace, LLC*, FTC File No. 102 3058 (June 8, 2012); https://epic.org/privacy/socialnet/EPIC-Myspace-comments-FINAL.pdf.

[42] Letter from Federal Trade Comm'n, Office of Secretary, to EPIC (Oct. 13, 2011), http://www.ftc.gov/os/caselist/1023136/111024googlebuzzepic.pdf.

[43] *See* Data Protection Comm'r, Report of Audit (2011), http://dataprotection.ie/documents/facebook%20report/report.pdf/report.pdf.

Commissioner also released a report of their re-audit of Facebook the following year.[44] The FTC should commit to transparency in its complaint and settlement enforcement procedures.

5. The FTC Should Seek Greater Authority to Protect American Consumers

In 2018, the FTC should seek legislative authority to protect consumer privacy and to reduce the risks of identity theft, security breaches, and financial fraud. We face a data protection crisis in the United States, and the FTC currently lacks the statutory authority to effectively deal with the problem.[45] Fundamentally, the FTC is not a data protection agency because it does not enforce a general data protection law. Other federal agencies have taken the misguided position that the FTC is the sole agency responsible for protecting consumer privacy,[46] but the FTC does not have the proper authority to fulfill this role. Relying on the FTC's current framework to address all consumer privacy concerns is not in the best interest of U.S. consumers.

The FTC is currently ill-equipped to handle the scale of the privacy and data security challenges faced by today's consumers. The FTC states in its draft Strategic Plan that "complaints are an integral component when determining the areas of greatest concern and injury to consumers."[47] Identity theft has consistently been the number one complaint to the FTC, and it is the number one concern of American consumers.[48] The FTC reported 399,225 cases of identity

---

[44] *See* Data Protection Comm'r, Report of Re-Audit (2012), https://www.dataprotection.ie/documents/press/Facebook_Ireland_Audit_Review_Report_21_Sept_2012.pdf.

[45] Marc Rotenberg, Equifax, the Credit Reporting Industry, and What Congress Should Do Next, Harv. Bus. Rev. (Sept. 20, 2017), https://hbr.org/2017/09/equifax-the-credit-reporting-industry-and-what-congress-should-do-next.

[46] *See, e.g.*, NHTSA, *Automated Driving Systems FAQs: What is NHTSA's approach to privacy?*, https://www.nhtsa.gov/manufacturers/automated-driving-systems#automated-driving-systems-topic.

[47] Fed. Trade Comm'n, FTC Strategic Plan FY 2018-2022, (Nov. 1, 2017), https://www.ftc.gov/system/files/attachments/press-releases/ftc-releases-draft-strategic-plan-fiscal-years-2018-2022/draftstratplanfy18-22.pdf.

[48] Fed. Trade Comm'n, IDENTITY THEFT AND DATA SECURITY, https://www.ftc.gov/news-events/media-resources/identity-theft-and-data-security ("Identity theft tops the list of consumer complaints that are reported to the FTC and other enforcement agencies every year.").

theft in 2016.[49] The Bureau of Justice Statistics estimates that overall 17.6 million individuals—7% of American consumers—experienced identity theft in 2014, at a cost of $15.4 billion to the U.S. economy.[50] These numbers reflect a data breach epidemic in the United States. According to the Identity Theft Resource Center, data breaches in the United States increased by 40% in 2016 to a record 1,093 cases.[51]

In order to address what is arguably the most important consumer protection issue today, the FTC needs to testify before Congress in support omnibus privacy legislation to safeguard American consumers, as FTC Commissioners have done previously. The proposal could follow similar recommendation from EPIC that would give consumers greater control over their personal information.[52] EPIC has called for (1) mandatory nationwide credit freeze, (2) free and easy access to consumer credit reports, (3) mandatory data breach notification, (4) limiting the use of the Social Security number in the private sector, (5) reasonable data security standards, and (6) "algorithmic transparency" for secret scoring systems so that consumers know how their information is being used.[53]

Today in the United States, there is an over-reliance on industry "self-regulation." Self-regulation does little to protect consumer privacy and invites a "race to the bottom" in which companies pursue ever more invasive collections of personal information.[54] In 2000, then FTC

---

[49] Fed. Trade Comm'n, FTC Releases Annual Summary of Consumer Complaints (March 3, 2017), https://www.ftc.gov/news-events/press-releases/2017/03/ftc-releases-annual-summary-consumer-complaints.

[50] Bureau of Justice Statistics, 17.6 Million U.S. Residents Experienced Identity Theft in 2014, Press Release, (Sep. 27, 2015), https://www.bjs.gov/content/pub/press/vit14pr.cfm.

[51] Identity Theft Resource Center, Data Breaches Increase 40 Percent in 2016, Finds New Report (Jan. 19, 2017), http://www.idtheftcenter.org/2016databreaches.html.

[52] *Consumer Data Security and the Credit Bureaus*: *Hearing Before the S. Comm. on Banking, Housing, and Urban Affairs*, 115th Cong. (2017), (statement of Marc Rotenberg, Exec. Dir., Electronic Privacy Information Center), https://epic.org/privacy/testimony/EPIC-Testimony-SBC-10-17.pdf.

[53] *Id*.

[54] *See*, *Privacy and Data Protection: Hearing Before the Committee on Citizen's Freedoms and Rights, Justice and Home Affairs, and the Committee on Legal Affairs and the Internal Markets European*

Chairman Robert Pitofsky endorsed new privacy legislation in the United States.[55] He warned that "[w]ithout comprehensive federal legislation, it is possible that something of a vacuum will be created and states may enter, not always with consistent proposals, to protect the privacy of their citizens. There may soon come a point when the business community will have to decide whether it prefers a single comprehensive federal rule, or a situation in which a variety of state rules create difficult to follow mandates."[56]

EPIC supports comprehensive federal legislation but such legislation should not preempt state law, allowing states to implement higher standards of data protection if they so choose. Consumer privacy legislation should also support a private right of action, however the FTC's role in enforcing such a statute will be critical, as consumer lawsuits alone are insufficient to deter unlawful activity in the marketplace.

In the wake of the Equifax data breach, lawmakers have begun to introduce proposals for data protection legislation.[57] Now is the time for the FTC to support comprehensive data protection legislation. The United States was once a leader in privacy protection, but we have now fallen behind many other countries, and our inadequate data protection regime threatens trade relations with Europe. As technology increases companies' ability to engage in invasive data collection and profiling, new data protection legislation becomes more and more urgent. The FTC 2018-2022 Strategic Plan should include legislative proposals for Congress to safeguard consumer privacy.

Parliament, (statement of Marc Rotenberg, Exec. Dir., Electronic Privacy Information Center) (Feb. 23, 2000), https://epic.org/privacy/intl/EP_testimony_0200.html.

[55] *Antitrust and Intellectual Property: Unresolved Issues at the Heart of the New Economy*, The Berkeley Center for Law and Technology at the University of California, Berkeley (statement of Robert Pitofsky, Former Chairman, Fed. Trade Comm'n) (Mar. 2, 2001), https://www.ftc.gov/public-statements/2001/03/antitrust-and-intellectual-property-unresolved-issues-heart-new-economy.

[56] *Id*.

[57] *See*, EPIC, *Senator Leahy Introduces Legislation To Protect Consumer Privacy*, (Nov. 15, 2017), https://epic.org/2017/11/senator-leahy-introduces-legis-1.html.

6. The FTC Should Bring More Actions Based on "Unfairness" Authority

As part of the FTC 2018-2022 Strategic Plan, the FTC should plan to bring more enforcement actions over unfair trade practices. Specifically, the Commission should adopt a broader understanding of "consumer harm" caused by companies that fail to implement strong data protection standards.

The Commission recently asked interest groups in advance of its upcoming Workshop on Informational Injury, "how do we quantify injuries?" in the consumer privacy context. These injuries should be obvious, however. The recent Equifax breach exposed the Social Security numbers, dates of birth, addresses and driver's license numbers of over 145 million U.S. consumers.[58] Equifax knew prior to its breach that its database of highly sensitive consumer data was vulnerable to attack, yet failed to take any data security precautions.[59] After any data breach, consumers wishing to protect themselves from identity theft must go through the costly and burdensome process of obtaining credit freezes from all three credit reporting agencies or purchasing credit monitoring services.[60] Credit reporting agencies like Equifax have no incentive to protect consumer data because consumers are not their customers, and the credit bureaus in fact profit from their own security failures when they suffer a breach (while consumers bear the costs).[61] And for the 7% of Americans who fall victim to identity theft, the long-term

---

[58] Equifax, Equifax Announces Cybersecurity Incident Involving Consumer Information (Sept. 7, 2017), https://investor.equifax.com/tools/viewpdf.aspx.

[59] The Apache Software Foundation Blog, MEDIA ALERT: The Apache Software Foundation Confirms Equifax Data Breach Due to Failure to Install Patches Provided for Apache® StrutsTM Exploit (Sept. 14, 2017), https://blogs.apache.org/foundation/entry/media-alert-the-apache-software.

[60] Fed Trade Comm'n, CREDIT FREEZE FAQS, https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs.

[61] Bruce Schneier, Don't Waste Your Breath Complaining to Equifax About Data Breach, CNN, (Sep. 11, 2017), http://www.cnn.com/2017/09/11/opinions/dont-complain-to-equifax-demand-government-act-opinion-schneier/index.html.

consequences can have devastating financial impacts, such as lowered credit scores, higher interest rates, denial of credit or even a job.

The Commission should use its unfairness authority to establish substantive privacy and data security requirements that protect American consumers and reduce the risk of identity theft, data breach, and financial fraud. The Commission's orders routinely prohibit companies from misrepresenting their data security practices, but they rarely impose any affirmative data protection requirements—such as data minimization or comprehensive data security measures.[62] Companies lack the incentive to protect consumer data without affirmative legal requirements.

By contrast, the Commission's unworkable "notice and choice" approach fails to provide meaningful privacy protections, and simply produces vague privacy policies. As the FTC itself acknowledged, notice-and-choice "led to long, incomprehensible privacy policies that consumers typically do not read, let alone understand."[63] Even if consumers do read every privacy policy, companies frequently do not permit consumers to opt-out of data collection. And in the case of data brokers, consumers' information is transferred between third parties without the consumer's knowledge or control.

The FTC is empowered to impose data protection standards under Section 5.[64] It has the legal authority to use Section 5 to build stronger data security standards for industries, and it should expand its unfairness authority to accomplish this goal.

[62] Comments of EPIC, *In the Matter of Uber Technologies, Inc*., FTC File No. 152-3054 (Sep. 15, 2017)
[63] Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change 60 (2012), http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.
[64] *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3rd Cir. 2015).

7. The FTC Should Oppose Mergers that Consolidate User Data and Threaten Consumer Privacy

The risks to consumer privacy and data security posed by mergers and acquisitions cannot be overstated. When companies merge, they combine not only their products, services, and finances, but also their vast troves of personal data. This increases the risk of cyberattacks and data breaches, and also increases the invasiveness of data collection. The FTC should use its antitrust authority to block the merger of companies that consolidate user data and threaten consumer privacy. This should be a key goal in the 2018-2022 FTC Strategic Plan.

EPIC has routinely underscored the consumer privacy risks of high-profile mergers and has urged the FTC to oppose such mergers. Nearly two decades ago, EPIC and a coalition of consumer organizations warned the FTC of the privacy implications of the Time Warner/AOL merger.[65] That merger produced what were, at the time, likely "the most detailed records on consumers ever assembled."[66] Despite both companies' records of non-compliance with privacy laws, the FTC approved the merger without addressing any of the consumer privacy or data security risks.[67] In 2007, EPIC filed a complaint with the FTC contending that Google's proposed acquisition of DoubleClick would enable Google to collect the personal information of billions of users and track their browsing activities across the web to deliver targeted advertisements.[68] EPIC correctly warned that this acquisition would accelerate Google's

[65] TACD, Statement on AOL-Time Warner Merger (Feb. 2000), https://ftc.gov/news-events/press-releases/2000/12/ftc-aproves-aoltime-warner-merger-conditions.
[66] Id.
[67] Press Release, FTC Approves AOL/Time Warner Merger with Conditions, Federal Trade Commission (Dec. 14, 2000), https://www.ftc.gov/news-events/press-releases/2000/12/ftc-approves-aoltime-warner-merger-conditions.
[68] In the Matter of Google Inc. and DoubleClick Inc., (EPIC Complaint, Request for Injunction, Investigation, and Other Relief), (Apr. 20, 2007), https://epic.org/privacy/ftc/google/epic_complaint.pdf.

dominance of the online advertising industry. The FTC ultimately allowed the merger to go forward over the compelling dissent of Commissioner Pamela Jones Harbor.[69]

Most notably, EPIC opposed the merger of Facebook and WhatsApp.[70] WhatsApp attracted users specifically for its privacy commitments, but after it was purchased by Facebook in 2014, WhatsApp began disclosing the personal information of its users to Facebook, including their phone numbers, contradicting its previous promises to honor user privacy.[71] EPIC and the Center for Digital Democracy filed a complaint with the FTC urging the Commission to mandate privacy safeguards for WhatsApp user data before approving the sale.[72]

The merger of Facebook and WhatsApp has prompted countries in Europe to update their competition laws.[73] But the FTC has repeatedly failed to even consider consumer privacy and data security in its merger review process.[74] EPIC emphasized the consequences of this failure in comments to the FTC in 2015, stating, "[i]n every instance, it was clear that the practical consequence of the merger would be to reduce the privacy protections for consumers and expose individuals to enhanced tracking and profiling. The failure of the FTC to take this into account during merger review is one of the main reasons consumer privacy in the United States has

[69] In the Matter of Google/DoubleClick, FTC File No. 070-0170 (2007) (Harbor, C., dissenting), https://www.ftc.gov/sites/default/files/documents/public_statements/statement-matter-google/doubleclick/071220harbour_0.pdf.
[70] EPIC and Center for Digital Democracy, Complaint, Request for Investigation, Injunction, and Other Relief, In the Matter of WhatsApp, Inc., (Mar. 6, 2014), https://epic.org/privacy/ftc/whatsapp/WhatsApp-Complaint.pdf. ("WhatsApp Complaint").
[71] WHATSAPP, Looking Ahead for WhatsApp, WhatsApp Blog, (Aug. 25, 2016), https://blog.whatsapp.com/10000627/Looking-ahead-for-WhatsApp.
[72] WhatsApp Complaint
[73] Fuel of the Future: Data is Giving Rise to A New Economy, The Economist, May 6, 2017, http://www.economist.com/news/briefing/21721634-how-it-shaping-up-data-giving-rise-new-economy.
[74] Nathan Newman, 15 Years of FTC Failure to Factor Privacy Into Merger Reviews, Huffington Post, (Mar. 19, 2015), https://www.huffingtonpost.com/nathan-newman/15-years-of-ftc-failure-t_b_6901670.html.

diminished significantly over the last 15 years."[75] The FTC should explore the privacy implications of mergers and block those proposals that lack sufficient privacy and data security safeguards.

8. The FTC Should Produce Concrete Outcomes from Workshops

FTC workshops provide an important opportunity for experts to provide input to the Commission, but the workshops should produce meaningful, actionable outcomes. Looking ahead to future workshops that may proposed in the 2018-2022 Strategic Plan, the FTC should commit to substantive reports and concrete recommendations for future actions. To date, many of the workshops do not produce any tangible result and merely lead to unenforceable suggestions for industry. The FTC should issue effective guidance and propose legislative and regulatory solutions. The FTC should also use its authority to address the consumer privacy issues raised in these workshops.

EPIC has submitted comments in advance of FTC workshops that have led to reports.[76] In 2015, the Commission released a report on the "Internet of Things: Privacy & Security in a Connected World," following a 2013 workshop.[77] EPIC and other consumer privacy advocates participated in the workshop, emphasizing the risks of IoT devices and making a number of

[75] EPIC, Comments of the Electronic Privacy Information Center: Assessing the FTC's Prior Actions on Merger Review and Consumer Privacy, FTC File No. P143100, (Mar. 17, 2015), https://epic.org/privacy/internet/ftc/Merger-Remedy-3-17.pdf.
[76] *See, e.g.*, Comments of EPIC, On the Privacy and Security Implications of the Internet of Things (Jun. 1, 2013), https://epic.org/privacy/ftc/EPIC-FTC-IoT-Cmts.pdf; Comments of EPIC, Cross-Device Tracking Workshop (Dec. 16, 2015), https://epic.org/apa/comments/EPIC-FTC-Cross-Device-Tracking-Comments.pdf.
[77] Fed. Trade Comm'n, Internet of Things: Privacy & Security in a Connected World, FTC Staff Report, (Jan. 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf, ("FTC IoT Report").

recommendations, including adoption of Fair Information Practices.[78] The FTC's final report included several recommendations for how companies could make IoT devices safer for consumers, including EPIC's recommendation that companies build security into their products by design.[79]

The FTC should act on this 2015 report. Specifically, the Commission should require companies to (1) apply FIPs to their data collection practices, (2) incorporate privacy and security by design, (3) comply with COPPA rules for internet-connected toys, and (4) promote transparency and consumer access to their data.

EPIC and other organizations have repeatedly warned the FTC about numerous internet-connected products, but the Commission has failed to act on any of these complaints. In June 2015, EPIC urged the FTC and the Department of Justice to investigate and take action against such devices that may violate federal wiretap laws.[80] In October 2017, EPIC and a coalition of consumer watchdogs sent a letter to the Consumer Product Safety Commission urging it to recall the Google Home Mini "smart speaker" because it contained a serious defect causing it to record all conversations, even when users assumed it was off.[81] EPIC also submitted a complaint to the FTC in 2015 regarding Samsung's "SmartTV," which was equipped with voice-recognition

[78] Comments of EPIC, On the Privacy and Security Implications of the Internet of Things, before the Fed. Trade Comm'n, (Jun. 1, 2013), https://epic.org/privacy/ftc/EPIC-FTC-IoT-Cmts.pdf.
[79] FTC IoT Report.
[80] EPIC, Letter to Attorney General Loretta Lynch and FTC Chairwoman Edith Ramirez, (Jun. 10, 2015) (requesting a workshop and investigation into "always on" consumer devices), https://epic.org/privacy/internet/ftc/EPIC-Letter-FTC-AG-Always-On.pdf.
[81] EPIC, et al, Letter to CPSC Chairman Ann Marie Buerkle, (Oct. 13, 2017), https://epic.org/privacy/consumer/Letter-to-CPSC-re-Google-Mini-Oct-2017.pdf.

technology, enabling it to record users' conversations and transmit those conversations to a third-party.[82]

In 2017, the FTC released a report on "Cross-Device Tracking" following a 2015 workshop.[83] EPIC filed comments with the Commission urging limits on cross-device tracking, which presents significant privacy challenges due to the "lack of transparency and control in this undetectable online tracking scheme."[84] EPIC recommended that the Commission issue regulations on cross-device tracking based on the Consumer Privacy Bill of Rights, and reject the ineffective "notice and choice system."[85] EPIC also recommended that the FTC update its Children's Online Privacy Act rules to reflect cross-device tracking practices that affect minors and use its Section 5 enforcement authority to prevent deceptive cross-device tracking practices.[86] In the Commission's final report, however, it recommends continued industry self-regulation and application of the unworkable "notice and choice" approach.[87]

Finally, EPIC submitted comments to the FTC and NHTSA in June 2017 in advance of a workshop of connected vehicles.[88] EPIC urged rules that limit the amount of personal information that vehicles can collect.[89] Connected cars raise numerous privacy and safety

---

[82] EPIC, Complaint, Request for Investigation, Injunction, and Other Relief, *In the Matter of Samsung Electronics Co., Ltd*. before the Fed. Trade Comm'n, (Feb. 24, 2015), https://epic.org/privacy/internet/ftc/Samsung/EPIC-FTC-Samsung.pdf.
[83] Fed. Trade Comm'n, Cross-Device Tracking, FTC Staff Report, (Jan. 2017), https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf.
[84] Comments of EPIC, Cross Device Tracking Workshop, before the Fed. Trade Comm'n, (Dec. 16, 2015), https://epic.org/apa/comments/EPIC-FTC-Cross-Device-Tracking-Comments.pdf.
[85] *Id*.
[86] *Id*.
[87] Fed. Trade Comm'n, Cross-Device Tracking, FTC Staff Report, (Jan. 2017), https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf.
[88] Comments of EPIC to the FTC & NHTSA, Benefits and Privacy and Security Issues Associated with Current and Future Motor Vehicles, (May 1, 2017), https://epic.org/apa/comments/EPIC-ConnectedCar-Workshop-Comments.pdf.
[89] *Id.*

concerns. They track everywhere a driver has been, and they have become a prime target for hackers.[90] This information can be used to stalk an individual or to determine when someone is not at home in order to commit a robbery. Connected cars also present serious safety risks from hackers gaining control of their systems remotely.[91] A study by the Government Accountability Office observed that "in 2015, hackers gained remote access to a car through its connected entertainment system and were able to cut the brakes and disable the transmission."[92]

These workshops present an opportunity for the FTC to solicit recommendations from leading consumer privacy groups and develop concrete proposals for addressing the challenges of new technologies. The FTC should develop concrete proposals from its workshops and act on them in order to better protect consumers from emerging business practices that threaten privacy.

9. The FTC Should Enforce Privacy Shield and COPPA

Until there is a replacement for Privacy Shield, the FTC has an obligation to uphold its responsibilities and to bring enforcement action when necessary. The Privacy Shield allows companies to transfer the personal data of European consumers to the United States based on a system of industry self-certification, but one of its major flaws is that it lacks effective safeguards and legal remedies. The FTC recently announced settlements with three companies that misrepresented their participation in the Privacy Shield arrangement. [93] These settlements are inadequate because they merely prohibit companies from making future false claims about compliance with Privacy Shield, and impose no monetary penalties. These settlements also fail

[90] *Id*.
[91] *Id.*
[92] Government Accountability Office, Internet of Things: Status and Implications of an Increasingly Connected World, (May 15, 2017), https://www.gao.gov/products/GAO-17-75.
[93] Fed. Trade Comm'n., *Three Companies Agree to Settle FTC Charges They Falsely Claimed Participation in EU-US Privacy Shield Framework*, Press Release, (Sep. 8, 2017), https://www.ftc.gov/news-events/press-releases/2017/09/three-companies-agree-settle-ftc-charges-they-falsely-claimed.

to provide any remedy to the EU consumers whose personal data was wrongfully obtained, nor do they require the companies to disgorge the data they fraudulently obtained. Without strong enforcement of the Privacy Shield framework, foreign governments are reluctant to permit the transfer of the personal data of their citizens to the U.S.

The FTC should also do more to enforce the Children's Online Privacy Protection Act (COPPA). Beyond the broad concerns raised by the IoT, internet-connected toys pose unique privacy and safety risks to children. Consumer advocates have warned not only of the privacy risks but of the serious childhood development concerns from toys that communicate with children and encourage them to form bonds and friendships with data-collecting devices.[94] In December 2016, EPIC and a coalition of privacy advocates filed a complaint with the FTC against toymaker Genesis Toys and speech recognition firm Nuance Communications over the doll "My Friend Cayla, a "toy that spied" in violation of the Children's Online Privacy Protection Act (COPPA).[95] The complaint emphasized how toys that subject children to ongoing surveillance, without any meaningful data protection standards, pose an immediate threat to their privacy and safety.[96] The FTC acknowledged the complaint but has failed to act on it.[97]

The FTC recently clarified how its COPPA rule applies to the collection of voice recordings by internet-connected toys.[98] The Commission stated that an audio file may only be

[94] Center For Commercial Free Childhood, On the Heels of Congressional Inquiry, Advocates Ask Mattel to Scrap "Aristotle," AI Device Which Spies on Babies & Kids, (Oct. 2, 2017), http://www.commercialfreechildhood.org/heels-congressional-inquiry-advocates-ask-mattel-scrap-%E2%80%9Caristotle%E2%80%9D-ai-device-which-spies-babies-kids.
[95] EPIC, et al, Complaint and Request for Investigation, Injunction, and Other Relief, In the Matter of Genesis Toys and Nuance Communications, before the Fed. Trade Comm'n, (Dec. 6, 2016), https://epic.org/privacy/kids/EPIC-IPR-FTC-Genesis-Complaint.pdf.
[96] Id.
[97] See Letter from Peder Magee, FTC, Division of Identity Protection, to EPIC and IPR, (Jan. 10, 2017), https://epic.org/privacy/kids/FTC-EPIC-Response-ToysThatSpy-Jan2017.pdf.
[98] Fed. Trade Comm'n, FTC Provides Additional Guidance on COPPA and Voice Recordings, Press Release, (Oct. 23, 2017), https://www.ftc.gov/news-events/press-releases/2017/10/ftc-provides-additional-guidance-coppa-voice-recordings.

used "as a replacement for written words," and may only be maintained "for the brief time necessary for that purpose."[99] EPIC supports these guidelines and urges the Commission to begin taking enforcement actions against companies that market toys that continuously record childrens' conversations.

Enforcement of Privacy Shield and COPPA will become more critical over the 2018-2022 period as Europeans bring greater scrutiny to U.S. data protection practices and the possibilities for more internet-connected toys and other products targeted toward children increases.

10. The FTC Should Support Establishment of a Data Protection Agency in the United States

The United States is one of the few democracies in the world that does not have a federal data protection agency, even though the original proposal for such an institution emerged from the U.S. in the 1970s.[100] As data flows increase and the data broker industry proliferates, the need for an effective, independent data protection agency becomes clear. An independent agency can more effectively utilize its resources to police the current widespread exploitation of consumers' personal information. The FTC should back the long overdue establishment of a Data Protection Agency.

Conclusion

The FTC plays a critical role in safeguarding American consumers. American consumers today are at great risk of identity theft, financial fraud, and data breaches. Sensitive personal information is collected by many companies that simply do not do enough to safeguard consumer

[99] Id.
[100] See, EPIC, The Privacy Act of 1974, https://epic.org/privacy/1974act/#history.

privacy. We also believe that proactive efforts to strengthen data protection will spur innovation and support business models that are sustainable over time.

As the FTC shapes a strategic plan for the next five years, we urge the Commission to incorporate the recommendations outlined above. There is a real data protection crisis in the United States. The Commission will need to address this challenge.

Respectfully Submitted,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

/s/*Christine Bannan*
Christine Bannan
EPIC Policy Fellow

/s/ *Sam Lester*
Sam Lester
EPIC Consumer Privacy Fellow