epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

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

September 22, 2020

The Honorable Roger Wicker, Chairman
The Honorable Maria Cantwell, Ranking Member
U.S. Senate Committee on Commerce, Science, and Transportation
512 Dirksen Senate Office Building
Washington, DC 20510

Dear Chairman Wicker and Ranking Member Cantwell:

We write to you in advance of the hearing "Revisiting the Need for Federal Data Privacy Legislation," where you will hear from multiple former Federal Trade Commissioners and industry advocates about the need for congressional action on privacy and data protection. We appreciate your interest in the role of the FTC and consumer protection. For more than two decades, EPIC has worked to support the FTC in its efforts to safeguard the privacy of American consumers.[1] But it is our view today that the FTC does not function as an effective privacy agency and that Congress should establish an independent Data Protection Agency in the United States.[2] The Committee should schedule a hearing on S. 3300, which would create a Data Protection Agency, and give it a favorable report without delay.

From EPIC's perspective, the FTC has not done enough to address the growing threats to consumer privacy. Our federal laws do not create adequate data protection standards and do not give the FTC authority to impose meaningful data protection obligations. And the FTC has failed to use the authorities that it does have to bring necessary enforcement against bad actors and prevent widespread privacy harm to consumers. Meanwhile the collection, aggregation, and monetization of personal data has expanded at a rapid pace. Americans have no meaningful choice in limiting the collection and use of their personal data online; and they can't simply "log off" services that have become central to our modern society. The monetization of Americans' personal data has an acute impact on economically disadvantaged and minority communities and has created an architecture of surveillance that is also being leveraged by law enforcement and national security agencies to circumvent constitutional privacy protections. And because so many U.S. companies offer global services that involve the collection of personal data online, including from European consumers, the

[1] Letter from EPIC to FTC Comm'r Christine Varney (Dec. 14, 1995), http://epic.org/privacy/internet/ftc/ftc_letter.html; *See also* EPIC, *In the Matter of DoubleClick, Complaint and Request for Injunction, Request for Investigation and for Other Relief, before the Federal Trade Comm'n* (Feb. 10, 2000), http://epic.org/privacy/internet/ftc/DCLK_complaint.pdf; EPIC, *In the Matter of Microsoft Corp., Complaint and Request for Injunction, Request for Investigation and for Other Relief*, before the Federal Trade Comm'n (July 26, 2001), http://epic.org/privacy/consumer/MS_complaint.pdf; EPIC, *In re Facebook, (Complaint, Request for Investigation, Injunction, and for Other Relief),* Dec. 17, 2009, https://epic.org/privacy/inrefacebook/.

[2] EPIC, *The U.S. Urgently Needs a Data Protection Agency*, https://epic.org/dpa.

failure to implement a comprehensive federal privacy regime threatens economic interests and the viability of international trade.

Many of the privacy bills before this Committee would either expand the FTC's authority or simply maintain the status quo.[3] Neither of those options will lead to meaningful change in the practices of internet firms or adequately protect the privacy of Americans. The Committee should consider whether the Commission is actually capable of establishing and enforcing rigorous data protection standards, or whether a new agency focused solely on data protection is necessary to address the threats that consumers face today.

The FTC Privacy Playbook: Consent Decrees, Infrequent Penalties, and No Meaningful Changes in Business Practices

The FTC does not have the motivation or the tools necessary to enforce meaningful privacy and data protection rights in 2020. Over the last twenty years, the FTC has taken on a role as a regulator of companies' data collection practices, but the Commission's focus has been limited and its impact has been minimal. Several of the FTC's most significant settlements followed complaints that EPIC and other consumer advocates filed with the Commission, but these settlements have not improved the privacy practices of the companies involved or of the industry writ large. For example, in 2011, the FTC entered into a Consent Order with Facebook, following an extensive investigation and complaint pursued by EPIC and several U.S. consumer privacy organizations. The Consent Order prohibited Facebook from transferring personal data to third parties without user consent, which was only one of numerous privacy violations identified in EPIC's complaints.[4] And while Facebook agreed in the consent decree to implement a "comprehensive" privacy program and to subject itself to independent privacy assessments, Facebook's harmful data collection practices continued. Indeed, the transfer of personal data on 87 million Facebook users to Cambridge Analytica was a direct outgrowth of one of the privacy violations that EPIC identified in its original complaints. The FTC Consent Order did not ultimately protect Facebook users from privacy violations, and prior to Cambridge Analytica they had not brought any enforcement actions for violations of that (or similar) consent orders.[5] ***The obvious question is "why did the FTC fail to act as the problem got worse?"***

The FTC also brought a significant action against Google in 2011 following EPIC's complaint concerning the disastrous roll-out of Google "Buzz."[6] In that case, the FTC established a consent order after Google enrolled Gmail users into a social networking service without obtaining meaningful consent.[7] But the Google Consent Order languished in the same way as the Facebook

[3] *See e.g.* S. 4626, 116th Cong. (2020); S. 1214, 116th Cong. (2019); S. 584, 116th Cong. (2019); S. 189, 116th Cong. (2019).
[4] Fed. Trade Comm'n., *In re Facebook*, Decision and Order, FTC File No. 092 3184 (July 27, 2012), https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf.
[5] *See*, Letter from EPIC to S. Comm. on the Judiciary and S. Comm on Commerce, Sci. and Trans. (Apr. 9, 2018), https://epic.org/testimony/congress/EPIC-SJC-Facebook-Apr2018.pdf.
[6] *In the Matter of Google, Inc.*, EPIC Complaint, Request for Investigation, Injunction, and Other Relief, before the Federal Trade Comm'n, Washington, D.C. (filed Feb. 16, 2010), https://epic.org/privacy/ftc/googlebuzz/GoogleBuzz_Complaint.pdf.
[7] Press Release, 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*

Order, and users continued to suffer privacy violations as the FTC took no enforcement actions under the orders. Both Facebook and Google wasted no time in testing the FTC's willingness to stand behind its judgments: the companies made dramatic changes in their data collection practices and expanded their advertising models to leverage invasive tracking of Internet users and user behaviors both online and offline. Both Google and Facebook expanded their data collection empires through mergers and acquisitions, ignoring user privacy preferences and merging data that users had been promised would remain secure and private. And the FTC did nothing.

EPIC and many others repeatedly pointed out to the FTC that 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 FTC took no action. And the "independent" third party audits that the companies obtained pursuant to the consent orders remained hidden from the public until EPIC sued the Commission to obtain their public release.[8] Once we obtained copies of the assessments, it became clear that they did not meaningfully probe Facebook's privacy practices, but merely rubber stamped them.

In March 2018, after the Cambridge Analytica scandal became public, the FTC finally reopened the investigation of Facebook.[9] On July 24, 2019, after a 16-month investigation, the FTC announced a proposed settlement to end its investigation into Facebook. This was the first fine against Facebook since the 2009 EPIC complaint. But the monetary penalty alone was too little, too late. In the nearly 10-years between EPIC's first complaint and the FTC penalty, Facebook established itself as a dominant entity in the internet advertising space and spread its data collection and tracking infrastructure across much of the Internet. The FTC succeeded in fining Facebook $5 billion in 2019, but ***the Commission did not require any no meaningful changes to the business practices***, and it forgave all past privacy violations by Facebook. No accountability for the leaders at Facebook who authorized privacy violations. No expanded injunctive relief against the company's profiling, brokering, and manipulation of internet users.

Large fines do not establish meaningful data protection standards. EPIC, Color of Change, the Open Markets Institute and others wrote to the FTC in January 2019 explaining that more extensive enforcement was necessary in the Facebook case.[10] Our groups called for equitable remedies, including reforming hiring and management practices at Facebook. EPIC called for the FTC to require Facebook to unwind the acquisition of both WhatsApp and Instagram,[11] a view that is now widely shared by many experts in the antitrust field. Our groups also recommended that the FTC require Facebook to add an independent director who represents the interest of users and also examine the civil rights impacts of Facebook's products and policies.

Data (Mar. 30, 2011), https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles- rollout-its-buzz.

[8] *EPIC v. FTC (Facebook Assessments)*, https://epic.org/foia/ftc/facebook/.

[9] Press Release, Fed. Trade Comm'n., Statement by the Acting Director of FTC's Bureau of Consumer Protection Regarding Reported Concerns About Facebook Privacy Practices (Mar. 26, 2018), https://www.ftc.gov/news-events/press-releases/2018/03/statement-acting-director-ftcs-bureau-consumer-protection.

[10] Letter from EPIC et al. to Joseph Simons, Chairman, Federal Trade Comm'n (Jan. 24, 2019), https://epic.org/privacy/facebook/2011-consent-order/US-NGOs-to-FTC-re-FB-Jan-2019.pdf.

[11] *See* Tim Wu, *The Curse of Bigness: Antitrust in the New Gilded Age* 132-33 (2018).

Despite the clear need for a transformation of Facebook's practices, the settlement did not change Facebook's business model or impose restrictions on its collection and use of consumer data. The settlement permits Facebook to continue to make its own determinations about user privacy and data collection if it produces additional records about those choices. It also does not meaningfully change the company's structure or financial incentives. The large settlement amount, while flashy, constitutes only 7% of Facebook's projected global ad revenue for 2019 of $67.37 billion. Given the comparative ease with which Facebook can pay fines of this degree, the company can retain its business model and its profitability under the settlement. Facebook is incentivized to continue to operate as it currently does, merely risking paying future fines out of its revenue. 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.

The FTC has proven to be incapable of reigning in the data collection of Facebook and Google, and that is just the tip of the iceberg. Below are just a few examples of recent actions where the FTC found violations of a consent order but failed to impose meaningful changes in business practices to protect consumers:

- **YouTube (2019):** Following a comprehensive complaint launched by the Campaign for a Commercial Free Childhood and the Center for Digital Democracy concerning children's privacy,[12] the FTC reached a settlement with YouTube and parent company Google. The companies agreed to pay $170 million to settle claims that they violated the Children's Online Privacy Protection Act, but little will change in the companies business model. Writing in dissent, Commissioner Slaughter said, "YouTube and Google were knowingly profiting off of the unlawful tracking of children," and that the Commission should have required a "technological backstop" to ensure that behavioral advertising of children would not continue.[13]

- **Equifax (2019):** The CFPB, the FTC, and 48 State AGs reached a settlement with Equifax arising from the 2017 data breach that compromised personal data of 143 million Americans. Equifax failed to safeguard the names, addresses, dates of birth and SSNs of 147 million Americans, and then failed to act once aware of the breach. Equifax agreed to pay $700 million, an insufficient amount for the number of individuals affected, and extinguished all victims' rights via class action. The Equifax settlement required third-party assessments that would not be made public, and, again, no meaningful changes to business practices.

[12] Center for Digital Democracy, Campaign for a Commercial-Free Childhood, EPIC, et al. Complaint to the FTC, *In the Matter of Request to Investigate Google's YouTube Online Service and Advertising Practices for Violating COPPA* (2018), https://commercialfreechildhood.org/wp-content/uploads/archive/devel-generate/tiw/youtubecoppa.pdf.
[13] Dissenting Statement of Commissioner Rebecca Kelly Slaughter, *In Matter of Google LLC and YouTube LLC.*, FTC File No. 172 3083 (September 4, 2019).

- **Uber (2017):** Shortly after announcing a settlement[14] over Uber's egregious misuse of personal data in 2017 (following an EPIC complaint[15]), the FTC discovered that Uber had failed to disclose another massive data breach of its third-party cloud storage service.[16] The breach exposed unencrypted files containing more than 25 million names and email addresses, 22 million names and phone numbers, and 600,000 names and driver's license numbers.[17] Uber had waited a full *year* to notify its customers of the breach. Uber also failed to notify the FTC of this breach despite the fact that it occurred during the FTC's investigation. The FTC's resulting modified settlement requires Uber to submit all of its biennial privacy assessments to the FTC, rather than just the initial assessment, but those assessments will not be made public.[18] Despite Uber's repeated failures to protect consumer data, the proposed Order contains no mandatory provisions for how Uber will safeguard consumer data. The FTC imposed no fines.

When a company violates an FTC Order, the Commission should impose new restrictions that will remedy the core problems and avoid future harm. The recent FTC settlement with Facebook is just one example of the Commission's playbook: the FTC's highest profile penalty settlement did not change any data collection practices, avoided any accountability for corporate leadership, and immunized the company against tens of thousands of complaints that the agency did not investigate. As Commissioner Chopra said in his dissent, the FTC's enforcement action "places no meaningful restrictions on Facebook's ability to collect, share, and use personal information. Instead, the order allows Facebook to evaluate for itself what level of user privacy is appropriate, and holds the company accountable only for producing those evaluations. What it does not require is actually respecting user privacy."[19]

The Committee should be specifically concerned about the FTC's ongoing failure to enforce its consent orders and the Commission's failure to require changes to business practices in the face of obvious and recurring unfair and deceptive trade practices. This agency's failure to take meaningful action to curb these privacy violations poses an ongoing risk to both American consumers and American businesses.

---

[14] Agreement Containing Consent Order FILE NO. 1523054, *In the Matter of Uber Technologies, Inc.*, https://www.ftc.gov/system/files/documents/cases/1523054_uber_technologies_agreement.pdf.
[15] EPIC Complaint to the FTC, *In the Matter of Uber Technologies, Inc.* (June 22, 2015), https://epic.org/privacy/internet/ftc/uber/Complaint.pdf.
[16] Press Release, Fed. Trade Comm'n., Uber Agrees to Expanded Settlement with FTC Related to Privacy, Security Claims (Apr. 12, 2018), https://www.ftc.gov/news-events/press-releases/2018/04/uber-agrees-expanded-settlement-ftc-related-privacy-security.
[17] *Id*.
[18] Press Release, Fed. Trade Comm'n., Federal Trade Commission Gives Final Approval to Settlement with Uber (Oct. 26, 2018), https://www.ftc.gov/news-events/press-releases/2018/10/federal-trade-commission-gives-final-approval-settlement-uber.
[19] Dissenting Statement of Comm'r Rohit Chopra, *In re Facebook, Inc.*, FTC File No. 1823109, at 17 (July 24, 2019)

FTC's Failure to Use Existing Authority

The Federal Trade Commission has asked for more authority to regulate privacy,[20] but Congress should be skeptical of that request because the Commission has failed in the past to use the new authorities that it has been given.[21] For example, the Commission already has authority to promulgate trade rules to define unfair practices and issue penalties without consent orders; the Commission already has the authority to regulate smart grid providers; and the Commission already has the authority to regulate data collection practices in the auto industry. The Commission's failure to use its existing authorities to create meaningful privacy protections undermines the claim that it can be an effective privacy regulator if given more authority.

There are plenty of steps that the FTC could take to bolster data protection standards without being given new authority, and the Commission should use its resources to do so rather than convening workshops to discuss policy topics unrelated to the enforcement of consumer protection laws. The FTC should codify definitions of unfair and deceptive trade practices that reflect an understanding of consumer harm presented by companies that fail to enforce strong data protection standards. This would allow the FTC to issue penalties after a first offense rather than relying on violations of consent orders. The agency has the authority to issue these rules and has not done so.[22]

The FTC should use its existing authority to write energy privacy rules,[23] to write rules for concerning data collection by motor vehicle dealers,[24] and to conduct studies on ed tech companies' collection of children's data in schools.[25] The FTC is empowered to impose data protection standards under Section 5 by promulgating trade regulation rules that are directly enforceable.[26] The Commission should also use its rulemaking authority under Section 5 to establish stronger data security standards. If the FTC fails to use these authorities, then the Commission is not capable of protecting Americans' privacy, and the Commission should no longer be trusted to do so.

---

[20] *Online Platforms and Market Power, Part 4: Perspectives of the Antitrust Agencies,* 116th Cong. (2019), H. Comm. on the Judiciary, Subcomm. on Antitrust, Commercial, and Admin. Law, https://judiciary.house.gov/legislation/hearings/online-platforms-and-market-power-part-4-perspectives-antitrust-agencies (Nov. 13, 2019) (testimony of Joseph Simons, Chairman, Fed. Trade Comm'n) ("So I think if you want us to do more on the privacy front than we need, we need help from you. Our tools - we've done as much as we can do with the tools we have.")

[21] Statement of Comm'r Rohit Chopra, *Regarding the Report to Congress on the FTC's Use of Its Authorities to Protect Consumer Privacy and Security* (June 17, 2020), https://www.ftc.gov/system/files/documents/public_statements/1577067/p065404dpipchoprastatement.pdf.

[22] 15 U.S.C. § 57a

[23] *See Statement of Comm'r Chopra, supra* note 22; 42 U.S.C. 16471 (authorizing the Commission to "issue rules protecting the privacy of electric consumers" without preempting more protective state regulations).

[24] 12 U.S. Code § 5519; FTC, *The Auto Marketplace,* https://www.ftc.gov/news-events/media-resources/consumer-finance/auto-marketplace.

[25] Letter from Campaign for a Commercial-Free Childhood and Center for Digital Democracy to Joseph Simons, Chairman, Fed. Trade Comm'n, et al. re: Request for Public Comment on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule (Mar. 26, 2020), https://commercialfreechildhood.org/wp-content/uploads/2020/03/6B-Letter-3.25.20.pdf.

[26] *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3rd Cir. 2015).

The United States Needs a Data Protection Agency

The Federal Trade Commission helps to safeguard consumers and to promote competition, but the FTC is not an effective data protection agency. The FTC lacks authority to enforce basic data protection obligations and has failed to enforce the orders it has established. The Commission also lacks the ability, authority and expertise to engage the broad range of challenges we now confront—such as Internet of Things, Artificial Intelligence, connected vehicles, and more.

The FTC's problems are not lack of budget or staff. The FTC has not even filled the current post for a Chief Technologist. The FTC has simply failed to use its current resources and current authorities to safeguard consumers. ***Giving the FTC more authority will not solve that issue.***

Given the enormity of the challenge, the U.S. would be best served to do what other countries have done and create a dedicated data protection agency. An independent agency could more effectively utilize its resources to police the current widespread exploitation of consumers' personal information and would be staffed with personnel who possess the requisite expertise to regulate the field of data security.

The U.S. is one of the few advanced economies in the world without a data protection agency. The 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. Meanwhile companies collect vast amounts of personal data about American's without their knowledge and without any meaningful data protection standards. The Cambridge Analytica case is just one illustration of the ways in which that vulnerability threatens not only U.S. citizens, but also our democratic institutions. The longer the U.S. continues on this course, the greater will be the threats to consumer privacy, democratic institutions, and national security.

As the data breach epidemic reaches unprecedented levels and the FTC fails to act again and again, the need for an effective, independent data protection agency has never been greater.

This Committee has a bill before it that would solve this problem. S. 3300, filed by Senator Kirsten Gillibrand, creates an independent Data Protection Agency in the United States to safeguard the personal data of Americans. The Committee should schedule a hearing on S. 3300 and give it a favorable report without delay.

We ask that this letter be entered in the hearing record. EPIC looks forward to working with the Committee on these issues of vital importance to the American public.

Sincerely,

/s/ *Alan Butler*
Alan Butler
EPIC Interim Executive Director
and General Counsel

/s/ *Caitriona Fitzgerald*
Caitriona Fitzgerald
EPIC Interim Associate Director
and Policy Director