epic.org | ELECTRONIC PRIVACY INFORMATION CENTER

September 26, 2016

The Honorable John Thune, Chairman
The Honorable Bill Nelson, Ranking Member
U.S. Senate Committee on Commerce, Science, & Transportation
512 Dirksen Senate Building
Washington, DC 20510

RE: Hearing on "Oversight of the Federal Trade Commission"

Dear Chairman Thune and Ranking Member Nelson:

We write to you regarding the upcoming hearing on "Oversight of the Federal Trade Commission." Simply put, the Federal Trade Commission ("FTC") is not doing enough to protect the personal data of American consumers. Identity theft, data breaches, and financial fraud are increasing. The damage to American consumers and families is escalating. Rather than curtailing the Commission's enforcement efforts, you must determine why the agency is not doing more. The FTC's continued failure to act against the growing threats to consumer privacy and security could be catastrophic.

The Electronic Privacy Information Center ("EPIC") is a public interest research center established more than 20 years ago to focus public attention on emerging privacy and civil liberties issues. EPIC has a particular interest in protecting consumer privacy, and has played a leading role in developing the authority of the FTC to address emerging privacy issues and to safeguard the privacy rights of consumers.[1] EPIC is involved in a wide range of activities involving the FTC, from consumer privacy and antitrust to rulemaking, enforcement of consent orders, and participation in public workshops.[2] Most recently, EPIC and the Center for Digital

[1] *See, e.g.*, Letter from EPIC Exec. Dir. Marc Rotenberg to FTC Comm'r Christine Varney (Dec. 14, 1995) (urging the FTC to investigate the misuse of personal information by the direct marketing industry), http://epic.org/privacy/internet/ftc/ftc_letter.html; DoubleClick, Inc., FTC File No. 071- 0170 (2000) (Complaint and Request for Injunction, Request for Investigation and for Other Relief), http://epic.org/privacy/internet/ftc/DCLK_complaint.pdf; Microsoft Corporation, FTC File No. 012 3240 (2002) (Complaint and Request for Injunction, Request for Investigation and for Other Relief), http://epic.org/privacy/consumer/MS_complaint.pdf; Press Release, Federal Trade Comm'n, FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network (Mar. 30, 2011), http://ftc.gov/opa/2011/03/google.shtm ("Google's data practices in connection with its launch of Google Buzz were the subject of a complaint filed with the FTC by the Electronic Privacy Information Center shortly after the service was launched."); *In the Matter of Facebook, Inc.*, (2009) (EPIC Complaint, Request for Investigation, Injunction, and Other Relief), https://epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf; *In the Matter of Facebook, Inc.*, (2010) (EPIC Complaint, Request for Investigation, Injunction, and Other Relief), https://epic.org/privacy/facebook/EPIC_FTC_FB_Complaint.pdf.

[2] *See* EPIC, *Federal Trade Commission*, https://epic.org/privacy/internet/ftc/.

Democracy ("CDD") filed a complaint with the FTC over WhatsApp's decision to transfer user data to Facebook in violation of commitments both companies previously made to subscribers.[3] At the time Facebook acquired WhatsApp, the FTC stated clearly that the companies must honor their privacy promises to users.[4]

American Consumers Face Unprecedented Privacy and Security Challenges

The unregulated collection of personal data has led to staggering increases in identity theft, security breaches, and financial fraud in the United States.[5] The recent Yahoo! data breach that exposed the personal information of at least half-a-billion users[6] is the latest in a growing number of high-profile hacks that threaten the privacy, security, and financial stability of American consumers. Far too many organizations collect, use, and disclose detailed personal information with too little regard for the consequences.

Not surprisingly, the privacy concerns of Americans are increasing at a rapid rate. Industry expert Mary Meeker's most recent Internet Trend report said simply, "[a]s data explodes . . . data security trends explode." According to Meeker, 45 percent of users "are more worried about their online privacy than one year ago" and 74 percent have limited their online activity in the last year due to privacy concerns."[7] Public opinion polls show that 91 percent of Americans believe they have lost control of how companies collect and use their personal information.[8] And a recent government study found that nearly half of American internet users refrain from online activities due to privacy and security concerns.[9]

The threats to consumer privacy and security are growing as new challenges emerge. Protecting consumer privacy will become increasingly difficult as the Internet of Things becomes more prevalent.[10] The ubiquity of connected devices enables collection of data about sensitive behavior patterns, which could be used in unauthorized ways or by unauthorized individuals. Another significant risk to consumers in the Internet of Things is security, of both the users' data and their physical person.

---

[3] *In the Matter of WhatsApp, Inc.*, (Aug. 29, 2016) (EPIC, CDD Complaint, Request for Investigation, Injunction, and Other Relief), https://epic.org/privacy/ftc/whatsapp/EPIC-CDDFTC-WhatsApp-Complaint-2016.pdf.
[4] Letter from Jessica Rich, Director of FTC Bureau of Consumer Protection, to WhatsApp and Facebook (Apr. 10, 2014) https://www.ftc.gov/system/files/documents/public_statements/297701/140410facebookwhatappl tr.pdf.
[5] *See, e.g.,* Fed. Trade Comm'n, *Consumer Sentinel Network Data Book* (Feb. 2016), https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2015/160229csn-2015databook.pdf.
[6] Yahoo!, *An Important Message to Yahoo Users on Security* (Sept. 22, 2016), https://investor.yahoo.net/releasedetail.cfm?ReleaseID=990570.
[7] Mary Meeker, *Internet Trends 2016 – Code Conference*, KPCB (June 1, 2016), http://www.kpcb.com/internet-trends.
[8] Lee Rainie, *The State of Privacy in Post-Snowden America,* PEW RESEARCH CENTER (Sept. 21, 2016), http://www.pewresearch.org/fact-tank/2016/01/20/the-state-of-privacy-in-america.
[9] Rafi Goldberg, *Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities*, NAT'L TELECOMM. AND INFO. ADMIN. (May 13, 2016), https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities.
[10] *See, e.g.*, EPIC, Comments on the Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things, NTIA Docket No. 160331306-6306-01 (June 2, 2016), https://epic.org/apa/comments/EPIC-NTIA-on-IOT.pdf.

The increased use of drones for commercial purposes also raises unique privacy issues for American consumers. Drones are designed to undertake constant, persistent surveillance to a degree that former methods of video surveillance were unable to achieve. The FTC recently held a workshop that explored privacy issues related to the commercial uses of drones, but more must be done to protect consumers from this invasive technology.

The American Public Supports and Deserves Baseline Consumer Privacy Legislation

The United States has been slow to update its privacy laws, and companies have been reluctant to implement Privacy Enhancing Technologies. Thus, neither an appropriate legal nor technical framework has been implemented to consistently safeguard individual privacy in the United States. Many of the current laws are no longer suited to protect the privacy of American consumers in the digital age. It is critical that privacy protections for consumers keep pace with advances in technology.

The American public supports updating U.S. privacy safeguards. According to a recent study by the Pew Research Center, "68% of internet users believe current laws are not good enough in protecting people's privacy online; and 64% believe the government should do more to regulate advertisers."[11] 91 percent of Americans believe they have lost control of how companies collect and use their personal information.[12] The overwhelming majority want that control, with 74 percent of Americans saying it is "very important" to control who gets their information and 65 percent saying it is "very important" to control what information gets collected.[13] Americans also consistently express a lack of confidence in the privacy and security of their online communications.[14] Pew also found that "young adults are more focused than elders when it comes to online privacy," and many have tried to protect their privacy, removed their names from tagged photos, and taken steps to mask their identity.

The consequences of inadequate data protection in the U.S. implicate the interests of U.S. consumers and businesses.[15] The competitiveness of American technology companies in the global market also requires strong U.S. legal protections for communications privacy.[16] Officials in Europe are reviewing the "ePrivacy Directive" as internet users in Europe face challenges

[11] Lee Rainie, *The State of Privacy in Post-Snowden America,* PEW RESEARCH CENTER (Sept. 21, 2016), http://www.pewresearch.org/fact-tank/2016/01/20/the-state-of-privacy-in-america.
[12] *Id*.
[13] *Id*.
[14] *Id.*
[15] *See* Marc Rotenberg, Testimony before the U.S. House of Representatives Energy & Commerce Subcommittees on Commerce, Manufacturing, and Trade and Communications and Technology, *Examining the EU Safe Harbor Decision and Impacts for Transatlantic Data Flows* (Nov. 3, 2015), https://epic.org/privacy/intl/schrems/EPIC-EU-SH-Testimony-HCEC-11-3-final.pdf.
[16] *See* Aarti Shahani, *A Year After Snowden, U.S. Tech Losing Trust Overseas*, NPR (June 5, 2014), http://www.npr.org/sections/alltechconsidered/2014/06/05/318770896/a-year-after-snowden-u-s-tech-losing-trust-overseas; Claire Caine Miller, *Revelations of N.S.A. Spying Cost U.S. Tech Companies*, NY TIMES (Mar. 21, 2014), http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html.

similar to those faced by American consumers.[17] A framework for baseline consumer privacy protections may provide a good starting point to build a common approach to online privacy and to avoid the dramatic divergence that has arisen.[18]

The common refrain that greater privacy protections are contrary to innovation is simply wrong. According to a recent report by the World Economic Forum, three of the top five countries that benefit most from technology innovation are members of the European Union: Finland, Sweden, and Norway.[19] The United States ranked fifth in this report. These European countries are subject to robust EU data protection laws, yet foster greater technology innovation than that of the United States. Privacy and innovation are not mutually exclusive.

Moreover, strong privacy protections are also a necessary and pragmatic part of risk mitigation in the age of the ubiquitous cybersecurity breach. Failure to protect user privacy frequently stems from failure to adequately protect user data, which can result in enormous liability for companies.[20] The more data a company stores, the more valuable a target its database is for hackers; and the more stored data, the greater the company's losses in the event of a breach.[21]

The FTC's Current Approach is Insufficient to Protect Consumer Privacy and Security

EPIC has fought for privacy rights for internet users at the FTC for more than two decades. We filed landmark complaints about privacy violations by Microsoft, Facebook, and Google.[22] While we respect the efforts of the Commission to protect consumers, the reality is that the FTC lacks the statutory authority, the resources, and the political will to adequately protect the online privacy of American consumers.

The FTC's privacy framework – based largely on "notice and choice"– is simply not working. Research shows that consumers rarely read privacy policies; when they do, these complex legal documents are difficult to understand. Moreover, emphasizing notice or disclosure

[17] *ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation*, European Commission (June 10, 2015), https://ec.europa.eu/digital-agenda/en/news/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data.
[18] EPIC, *Examining the EU Safe Harbor Decision and Impacts for Transatlantic Data Flows*, EPIC (Nov. 3, 2015) https://epic.org/privacy/intl/schrems/EPIC-EU-SH-Testimony-HCEC-11-3-final.pdf.
[19] WORLD ECONOMIC FORUM, *Global Information Technology Report 2016*, http://reports.weforum.org/global-information-technology-report-2016/report-highlights/.
[20] *2016 Cost of Data Breach Study: United States*, PONEMON INST., 1 (June 2016).
[21] Bruce Schneier, *Data Is A Toxic Asset*, SCHNEIER ON SECURITY, (March 4, 2016), https://www.schneier.com/blog/archives/2016/03/data_is_a_toxic.html ("saving [data] is dangerous because failing to secure it is damaging. It will reduce a company's profits, reduce its market share, hurt its stock price, cause it public embarrassment, and—in some cases—result in expensive lawsuits and occasionally, criminal charges. All this makes data a toxic asset, and it continues to be toxic as long as it sits in a company's computers and networks.").
[22] *See* Complaint and Request for Injunction, Request for Investigation and for Other Relief, *In the Matter of Microsoft Corporation*, (July 26, 2001), https://www.epic.org/privacy/consumer/MS_complaint.pdf. *See also* Complaint, Request for Investigation, Injunction, and Other Relief, *In the Matter of Facebook, Inc*, (Dec. 17, 2009), https://epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf; Complaint, Request for Investigation, Injunction, and Other Relief, *In the Matter of Google, Inc*, (Feb. 16, 2010), https://epic.org/privacy/ftc/googlebuzz/GoogleBuzz_Complaint.pdf.

favors the interests of businesses over consumers and fails to establish meaningful privacy safeguards. Nor can industry self-regulatory programs provide realistic privacy protections when they are not supported by enforceable legal standards.

Even when the FTC reaches a consent agreement with a privacy-violating company, the Commission rarely enforces the Consent Order terms.[23] American consumers whose privacy has been violated by unfair or deceptive trade practices do not have a private right of action to obtain redress. Only enforceable privacy protections create meaningful safeguards, and the lack of FTC enforcement has left consumers with little recourse.

This is illustrated by the FTC's decision to permit Google to consolidate users' personal information across more than 60 Google services, including search, email, browsing, and YouTube, into single, comprehensive user profiles.[24] Google's plan to consolidate user data without consent was a clear violation of the FTC's 2011 consent order with the company, which bars Google from misrepresenting its privacy practices and sharing user information without affirmative consent.[25] EPIC filed suit seeking to compel the FTC to enforce the terms of its consent order with Google, but the agency succeeded in dismissing the suit and took no action to protect the privacy interests of Google users.[26] As a result of the FTC's inaction, virtually all internet activity now comes under the purview of one company.

The FTC also consistently fails to modify proposed settlement agreements in response to public comments. EPIC has submitted comments to the Commission on numerous proposed orders that implicate the privacy interests of consumers. However, to date the Commission has adopted these consent orders without any modification.[27] The FTC's failure to make any changes to proposed settlements based on comments it has explicitly requested is: (1) contrary to the explicit purpose of the statutory provision that allows the Commission to request comments from the public;[28] (2) contrary to the broader purpose of the Commission to police unfair and deceptive trade practices;[29] and (3) contrary to the interests of American consumers.

The Commission has never required compliance with the Consumer Privacy Bill of Rights ("CPBR"),[30] a basic set of privacy requirements, under its Consent Orders even when

[23] *See EPIC v. FTC*, No. 12-206 (D.C. Cir. Feb. 8, 2012).
[24] *See* EPIC, *EPIC v. FTC (Enforcement of the Google Consent Order)*, https://epic.org/privacy/ftc/google/consent-order.html.
[25] The FTC's 2011 consent order with Google arose from a complaint filed by EPIC in 2010 over the company's introduction of the Google Buzz social network, which automatically enrolled Gmail users and published their contact lists without first notifying users or obtaining their consent. *See* EPIC, *In re Google Buzz*, https://epic.org/privacy/ftc/googlebuzz/.
[26] *See* EPIC, *supra* note 18.
[27] Comments of the Elec. Privacy Info. Ctr., FTC Docket No. 102 3058 (Jun. 8, 2012), https://epic.org/privacy/socialnet/EPIC-Myspace-comments-FINAL.pdf; Comments of the Elec. Privacy Info. Ctr., FTC Docket No. 092 3184 (Dec. 17, 2011), https://epic.org/privacy/facebook/Facebook-FTCSettlement-Comments-FINAL.pdf; Comments of the Elec. Privacy Info. Ctr., FTC Docket No. 102 3136 (May 2, 2011), https://epic.org/privacy/ftc/googlebuzz/EPIC_Comments_to_FTC_Google_Buzz.pdf.
[28] Commission Rules of Practice, 16 C.F.R. § 2.34 (C) (2014).
[29] Federal Trade Commission Act, 15 U.S.C. § 46 (2006).
[30] White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Economy*, Feb. 23, 2012, http://www.whitehouse.gov/sites/default/files/privacy-

companies are found to violate Section 5 of the FTC Act.[31] By requiring compliance with the CPBR, the Commission could ensure that the personal data of consumers is protected throughout the data lifecycle. More importantly, the Commission would be able to put in place the baseline privacy standards that are widely recognized around the world and necessary to protect the interests of consumers.

Fundamentally, the FTC is not a data protection agency. Without regulatory authority, the FTC is limited to reactive, after-the-fact enforcement actions that largely focus on whether companies honored their own privacy promises. Because the United States currently lacks comprehensive privacy legislation or an agency dedicated to privacy protection, there are very few legal constraints on business practices that impact the privacy of American consumers.

EPIC's Recommendations

Maintaining the status quo imposes enormous costs on American consumers and businesses. Consumers face unprecedented threats of identity theft, financial fraud, and security breach.[32] Privacy protections based on industry self-regulation and burdensome "notice and choice" policies do not provide meaningful safeguards for consumers. The FTC must issue effective guidance and use its Section 5 enforcement authority to ensure adequate protection of consumer privacy in the digital age.

Moreover, the FTC must promptly investigate business practices, pursue complaints, enforce existing Consent Orders, and modify proposed settlements to reflect public comments. The Commission's ongoing failure to fulfill these obligations is (1) contrary to the explicit purpose of the statutory provision that allows the Commission to request comments from the public;[33] (2) contrary to the broader purpose of the Commission to police unfair and deceptive trade practices;[34] and (3) contrary to the interests of American consumers.

We urge Congress to consider the Commission's use of Section 5 authority in the context of the greater American legal landscape. Because the U.S. lacks a comprehensive privacy law or an agency dedicated to privacy protection, there are very few legal constraints on business practices that impact the privacy of Americans. The FTC's already modest Section 5 authority helps to deter and penalize the abuse of data. Any effort to limit the Commission's authority –

---

final.pdf; *see also* EPIC, *White House Sets Out Consumer Privacy Bill of Rights,* https://epic.org/privacy/white_house_consumer_privacy_.html.

[31] EPIC has recommended compliance with the CPBR in numerous settlement proceeding where the FTC has asked for public comment. *See, e.g.*, EPIC Comments, FTC Project No P114506 (Jul. 11, 2012), https://epic.org/privacy/ftc/FTC-In-Short-Cmts-7-11-12-FINAL.pdf; EPIC Comments, FTC Docket No. 102 3058 (Jun. 8, 2012), https://epic.org/privacy/socialnet/EPIC-Myspace-comments-FINAL.pdf; EPIC Comments, FTC Project No P114506 (May 11, 2012), https://epic.org/privacy/ftc/EPIC-FTCAd-Disclosures-FINAL.pdf; EPIC Comments, FTC Docket No. 092 3184 (Dec. 17, 2011), https://epic.org/privacy/facebook/Facebook-FTC-Settlement-Comments-FINAL.pdf; EPIC Comments, FTC Docket No. 102 3136 (May 2, 2011), https://epic.org/privacy/ftc/googlebuzz/EPIC_Comments_to_FTC_Google_Buzz.pdf.

[32] *See, e.g.*, FED. TRADE COMM'N, *Consumer Sentinel Network Data Book* (Feb. 2016), https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-januarydecember-2015/160229csn-2015databook.pdf.

[33] Commission Rules of Practice, 16 C.F.R. § 2.34 (C) (2014).

[34] Federal Trade Commission Act, 15 U.S.C.. § 46 (2006).

coupled with Congress' failure to update America's privacy laws – is a disservice to the vast majority of Americans who are increasingly concerned about their loss of privacy and want their government to do more to protect this important democratic value.

We look forward to working with you to improve the FTC's authority in this field and to develop rules to provide meaningful and much-needed protections for consumer privacy.

Sincerely,

Marc Rotenberg
Marc Rotenberg
EPIC President

Claire Gartland
Claire Gartland
Director, EPIC Consumer Privacy Project

cc: The Honorable Jerry Moran, Chairman, U.S. Senate Subcommittee on Consumer Protection, Product Safety, Insurance & Data Security

The Honorable Richard Blumenthal, Ranking Member, U.S. Senate Subcommittee on Consumer Protection, Product Safety, Insurance & Data Security