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

March 20, 2018

The Honorable Kevin Brady, Chairman
The Honorable Richard Neal, Ranking Member
U.S. House Committee on Ways & Means
1102 Longworth HOB
Washington D.C. 20515

Dear Chairman Brady and Ranking Member Neal:

We write to you regarding the Hearing with Commerce Secretary Ross[1] and the critical issue of privacy protection, perhaps the most important issue that the Secretary of Commerce will confront over the next several years.

EPIC is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues.[2] EPIC is a leading advocate for consumer privacy and has appeared before this Committee on several occasions, and has actively participated in the proceedings of the Federal Trade Commission ("FTC") and the Federal Communications Commission ("FCC").[3]

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.[4] The recent Equifax data breach that exposed the personal information of more than 145 million Americans 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.

---

[1] *FY19 Budget Hearing - Department of Commerce*, 115th Cong. (2018), H. Comm. on Appropriations, Subcomm. on Commerce, Justice, Science, and Related Agencies, https://appropriations.house.gov/calendar/eventsingle.aspx?EventID=395131 (Mar. 20, 2018).
[2] *See* EPIC, *About EPIC*, https://epic.org/epic/about.html.
[3] *See, e.g,* Marc Rotenberg, EPIC Executive Director, Testimony before the U.S. Senate Committee on Commerce, Science, and Transportation, Commerce Committee, *Internet Privacy and Profiling* (June 13, 2000), https://epic.org/privacy/internet/senate-testimony.html; Letter from EPIC to the U.S. Senate Committee on Commerce, Science, and Transportation on Oversight of the FTC (Sept. 26, 2016), https://epic.org/privacy/consumer/EPIC-Letter-Sen-Comm-CST-FTC-Oversight.pdf; Letter from EPIC to the U.S. House of Representatives Committee on Energy and Commerce on FCC Privacy Rules (June 13, 2016), https://epic.org/privacy/consumer/EPIC-FCC-Privacy-Rules.pdf.
[4] 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.

Secretary Ross must back strong privacy safeguards for American consumers. At this time, the FTC is simply not doing enough to safeguard the personal data 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. And companies remain free to changes the terms and conditions whenever they wish. Nor can industry self-regulatory programs provide meaningful privacy protections without enforceable legal standards.

Even when the FTC reaches a consent agreement with a privacy-violating company, the Commission rarely enforces the Consent Order terms.[5] Just this week, we learned that the FTC's failure to enforce a 2011 Consent Order with Facebook has resulted in the unlawful transfer of 50 million Facebook user records to a controversial data mining firm to influence the 2016 U.S. presidential election.[6] The 2011 Facebook Order was the result of an extensive complaint filed by EPIC and a coalition of consumer organizations in 2009, following Facebook's repeated changes to its privacy settings that overrode user preferences and allowed third parties to access private information without users' consent.[7] The FTC has an obligation to the American public to ensure that companies comply with existing Consent Orders. It is unconscionable that the FTC allowed this unprecedented disclosure of Americans' personal data to occur. The FTC's failure to act imperils not only privacy but democracy as well.

EPIC has also repeatedly warned the FTC that it has an affirmative duty to undertake a review of substantial changes in business practices of a company subject to a consent order that implicates the privacy of Internet users.[8] The FTC's apparent failure to pursue such review has led to a downward spiral in the protection for American consumers.

The FCC must also do more to safeguard American consumers. Last year, in the context of a public rulemaking, EPIC urged the FCC to adopt comprehensive privacy rules that would apply to both Internet Service Providers ("ISPs") and so-called "edge" providers, such as Google and Facebook, that dominate much of the Internet economy.[9] However, the FCC adopted a modest rule that only applied to ISPs and that rule was subsequently repealed by Congress, with the support of the current FCC Chairman Ajit Pai. Instead of moving forward to safeguard consumers, the FCC is moving backwards, leaving users of new communications services exposed to unprecedented levels of identity theft, financial fraud, and security breaches.[10]

---

[5] *See EPIC v. FTC*, No. 12-206 (D.C. Cir. Feb. 8, 2012).
[6] Craig Timberg, et al., *U.S. and European Officials Question Facebook's Protection of Personal Data*, Washington Post, (Mar. 18, 2018), https://www.washingtonpost.com/business/economy/us-and-european-officials-question-facebooks-protection-of-personal-data/2018/03/18/.
[7] EPIC, et al, In the Matter of Facebook, Inc. (Complaint, Request for Investigation, Injunction, and Other Relief) (Dec. 17, 2009), https://epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf.
[8] Letter to Acting FTC Chair Maureen Ohlhausen, "FTC 2017: 10 Steps for Protecting Consumers, Promoting Competition and Innovation" (Feb. 15, 2017) ("*1. The FTC Must Enforce Existing Consent Orders")*, https://epic.org/privacy/internet/ftc/EPIC-et-al-ltr-FTC-02-15-2017.pdf
[9] EPIC Statement, *FCC Overreach: Examining the Proposed Privacy Rules*, hearing before the House Committee on Energy and Commerce, Subcommittee on Communications and Technology, Jun. 13, 2016.
[10] Federal Trade Comm'n, *Consumer Sentinel Network Data Book,* Mar. 2017, https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2016/csn_cy-2016_data_book.pdf.

Of particular urgency for Secretary Ross is the "Privacy Shield," which permits the flow of data on European consumers to firms located in the United States that would otherwise be subject to European privacy law. EPIC and many others are concerned about the adequacy of the Privacy Shield and the protection of consumer data.[11] Without more substantial reforms to ensure protection for fundamental rights of individuals on both sides of the Atlantic, the Privacy Shield will put users at risk and undermine trust in the digital economy. There is also a growing sense that European leaders may simply withdraw from the transborder data sharing arrangement if certain steps are not taken:

- Appoint the Privacy Shield "ombudsman" at the Department of Commerce
- Reform Section 702 surveillance authority
- Stand up the privacy and Civil Liberties Oversight Board with five commissioners
- Stand up the Federal Trade Commission with five commissioners
- Limit excessive data gathering and surveillance at the border

The United States must commit to protecting the data privacy of both US-persons and non-US-persons in order to protect users and instill trust in the digital economy.[12]

Secretary Ross should make clear his commitment to a comprehensive approach to data protection, based in law. If he fails to do this, there is a real risk that the transatlantic flow of personal data will be disrupted, and consumer privacy, as well as business opportunity and innovation will suffer. *He should be asked specifically about the US efforts to uphold Privacy Shied.*

We ask that this letter be submitted into the hearing record. EPIC looks forward to working with the Subcommittee on Commerce, Justice, Science, and Related Agencies on this issue.

Sincerely,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

/s/ *Caitriona Fitzgerald*
Caitriona Fitzgerald
EPIC Policy Director

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

/s/ *Sunny Kang*
Sunny Kang
EPIC International Consumer Counsel

[11] *See, e.g.*, Testimony of Marc Rotenberg, EPIC Executive Director, Testimony before the U.S. House of Representatives Energy & Commerce Comm., *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.

[12] *See, e.g.*, Letter from EPIC, et al., to Article 29 Working Party Chairman Isabelle Falque-Pierrotin, et al., on Privacy Shield (Mar. 16, 2016), https://epic.org/privacy/intl/schrems/Priv-Shield-Coalition-LtrMar2016.pdf.