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

October 11, 2017

The Honorable Robert Latta, Chairman
The Honorable Janice Schakowsky, Ranking Member
U.S. House Committee on Energy and Commerce
Subcommittee on Digital Commerce & Consumer Protection
2125 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Latta and Ranking Member Schakowsky:

We write to you regarding the "21st Century Trade Barriers: Protectionist Cross Border Data Flow Policy's Impact on U.S. Jobs" hearing.[1] We appreciate the Committee's interest in this important topic, but hope that you will consider the urgent need to update privacy laws in the United States as you examine the reasons that foreign governments may be reluctant to permit the transfer of personal data.

EPIC is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues.[2] EPIC has previously testified before this Committee on this issue and has made recommendations on how the US and Europe could move forward to address shared concerns about the protection of privacy.[3] Those recommendations have gained greater force over time.

American consumers today face unprecedented privacy threats and security risks. The unregulated collection of personal data has led to staggering increases in identity theft, security

[1] *21st Century Trade Barriers: Protectionist Cross Border Data Flow Policy's Impact on U.S. Jobs*, 115th Cong. (2017), H. Comm. on Energy & Commerce, Subcomm. on Digital Commerce and Consumer Protection, https://energycommerce.house.gov/hearings/21st-century-trade-barriers-protectionist-cross-border-data-flow-policies-impact-u-s-jobs/ (Oct. 12, 2017).
[2] *See* EPIC, *About EPIC*, https://epic.org/epic/about.html.
[3] Marc Rotenberg, EPIC Executive Director, Testimony before the House Comm. on Energy & Commerce, Subcomm. on Communications and Technology, *Examining the EU Safe Harbor Decision and Impacts for Transatlantic Data Flows* (November 13, 2015), https://epic.org/privacy/intl/schrems/EPIC-EU-SH-Testimony-HCEC-11-3-final.pdf; Marc Rotenberg, "They're Right to Distrust U.S. Data Security", Wall Street Journal (March 22, 2016); Marc Rotenberg, "Digital Privacy, in US and Europe," N.Y. Times, Oct. 13, 2015; Marc Rotenberg, "On International Privacy: A Path Forward for the US and Europe," *Harvard International Review* (Spring 2014); Marc Rotenberg & David Jacobs, "Updating the Law of Information Privacy: The New Framework of the European Union," *Harvard Journal of Law and Public Policy* (Spring 2013); Marc Rotenberg, "Better Privacy Laws: Priority for America and Germany," N.Y. Times, Sept. 3, 2013.

breaches, and financial fraud in the United States.[4] The Equifax data breach revealed last month that exposed the personal information of approximately 145.5 million Americans[5] 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.

The United States should take four steps to update domestic privacy law: (1) enact the Consumer Privacy Bill of Rights, (2) modernize the Privacy Act, (3) establish an independent data protection agency, and (4) ratify the International Privacy Convention. This is the strategy that enables cross border data flows to continue and protects the interests of US consumers and US businesses.

The Federal Trade Commission Has Failed to Pursue Meaningful Enforcement

The FTC is simply not doing enough to safeguard the personal data of American consumers. 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. 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.[6] 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.

Last month, the FTC announced a settlement with three companies that misrepresented their participation in the Privacy Shield arrangement.[7] The Privacy Shield[8] allows companies to transfer the personal data of European consumers to the United States based on a system of industry self-certification. The FTC settlement prohibits the companies from making future false claims about compliance with Privacy Shield, but does not impose any penalty. The FTC settlement also fails to provide any remedy to the EU consumers whose personal data was

[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.
[5] Equifax, *Cybersecurity Incident & Important Consumer Information*, https://www.equifaxsecurity2017.com/frequently-asked-questions/.
[6] *See EPIC v. FTC*, No. 12-206 (D.C. Cir. Feb. 8, 2012).
[7] Press Release, Federal Trade Comm'n, Three Companies Agree to Settle FTC Charges They Falsely Claimed Participation in EU-US Privacy Shield Framework (Sept. 8, 2017), https://www.ftc.gov/news-events/press-releases/2017/09/three-companies-agree-settle-ftc-charges-they-falsely-claimed.
[8] EPIC, *Privacy Shield EU-U.S. Data Transfer Arrangement*, https://epic.org/privacy/intl/privacy-shield/.

wrongfully obtained, nor does it require the companies to disgorge the data they fraudulently obtained.

Privacy Shield Is Not an Effective Basis for EU-US Data Flows

EPIC and many others are concerned about the adequacy of the Privacy Shield and the protection of consumer data.[9] 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. Specifically, 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.[10]

Neither consumers nor businesses want to see the disruption of cross border data flows. But the problems of inadequate data protection in the United States can no longer be ignored. US consumers are suffering from skyrocketing problems of identity theft, data breach, and financial fraud. Not surprisingly, European governments are very concerned about what happens to the personal information of their citizens when it is transferred to the United States. Privacy Shield does not solve this problem. The US will need to do more to reform privacy law to enable cross border data flows. It is a well- known paradox that promoting the free flow of personal data across national boundaries requires comprehensive privacy protection.[11]

The Schrems II Decision Could Have Far-reaching Consequences if the US Fails to Act

The Irish High Court's decision[12] released last week calls into question the viability of the current data transfer scheme between the US and EU. As a general principle, EU law prohibits data transfers outside of the EU where strict EU privacy laws do not apply, but there are exceptions. One exception was Safe Harbor, but two years ago, the Court of the Justice of the European Union invalidated it.[13] This case originated from a complaint brought my Max Schrems against Facebook Ireland Ltd. before the Irish Data Protection Commissioner in 2013. After it could no longer use Safe Harbor, Facebook used another legal mechanism—Standard Contractual Clauses (also known as Model Clauses)—to facilitate data transfers to the US. Standard Contractual Clauses are contracts between European and American companies whereby American companies agree to abide by European privacy law. The Irish Data Protection Commissioner has taken the position that Standard Contractual Clauses are invalid under EU

[9] *See, e.g.*, Testimony of Marc Rotenberg, EPIC Executive Director, 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.

[10] *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.

[11] Marc Rotenberg, On International Privacy: A Path Forward for the US and Europe, Harvard International Review (June 15, 2014), http://hir.harvard.edu/on-international-privacy-a-path- forward-for-the-us-and-europe/.

[12] Data Protection Commissioner v. Facebook Ireland Limited and Maximilian Schrems [2017] (Ir.).

[13] Maximilian Schrems v. Data Protection Commissioner [2015] (E.C.J.).

law, referred the case to the Court of the Justice of the European Union to resolve this question. Once again, the highest European court will have the opportunity to invalidate a mechanism commonly used to facilitate transfers between American and European companies.

This case highlights the urgency of the need for the US to take action to protect user privacy. The United States should not update its privacy law because of a judgment of the European Court. The United States should update its privacy law because it is long overdue, because it is widely supported, and because the ongoing failure to modernize privacy law is imposing enormous costs on American consumers.

To Support Cross Border Data Flows, Congress Must Modernize US Privacy Law

There are at least four steps that Congress needs to take to address concerns about data protection in the United States. This is the strategy that enables cross border data flows to continue and protects the interests of US consumers and US businesses.

First, Congress should enact the Consumer Privacy Bill of Rights. The Consumer Privacy Bill of Rights is a sensible framework that would help establish fairness and accountability for the collection and use of personal information. It is based on familiar principles for privacy protection that are found in many laws in the United States. This framework would establish baseline safeguards for the development of innovative services that take advantage of technology while safeguarding privacy. But the key to progress is the enactment by Congress. Only enforceable privacy protections create meaningful safeguards.

Second, Congress should modernize the Privacy Act, revise the scope of the Act's coverage and clarify the damages provision. There are many changes that need to be made to the law to protect the interests of Americans. The Judicial Redress Act does not provide adequate protection to permit data transfers and it does not address the many provisions in the Privacy Act that need to be updated.[14]

Third, Congress should create an independent privacy agency, as Congress contemplated in 1974 when it enacted the Privacy Act.[15] EPIC has previously recommended the establishment of a privacy agency to ensure independent enforcement of the Privacy Act, develop additional recommendations for privacy protection, and provide permanent leadership within the federal government on this important issue.[16] This independent privacy agency would be charged with enforcing privacy laws. Enforcement should not be assigned to the FTC, as the FTC has missed many opportunities to strengthen US privacy law.

---

[14] *See generally*, EPIC, EU-US Data Transfer Agreement (2015), https://epic.org/privacy/intl/data-agreement/index.html.

[15] Staff of S. Comm. on Gov't Operations, 93d Cong., Materials Pertaining to S. 3418 and Protecting Individual Privacy in Federal Gathering, Use and Disclosure of Information (Comm. Print 1974) (collecting materials on S. 3418, a bill to establish a Federal Privacy Board).

[16] *See, e.g.*, Marc Rotenberg, *In Support of a Data Protection Board in the United States*, 8 *Gov't Info. Q.* 79 (1991); *Communications Privacy: Hearing Before the Subcomm. on Courts and Intellectual Prop. of H. Comm. on the Judiciary*, 105th Cong. (1998) (testimony of Marc Rotenberg), available at https://www.epic.org/privacy/internet/rotenberg-testimony-398.html.

Fourth, the final step to address the growing EU-US divide is to ratify the international Privacy Convention 108, the most-well established legal framework for international data flows.[17] The Privacy Convention would establish a global bias to safeguard personal information and enable the continued growth of the Internet economy. In the absence of a formal legal agreement, it is likely that other challenges to self- regulatory frameworks will be brought.

This is not simply a matter of trade policy. It is a matter of fundamental rights. There is today a growing consensus on both sides of the Atlantic, supported by consumer groups and business leaders, to recognize that privacy is a fundamental human right.

As a general proposition, we support the free flow of information and oppose protectionist barriers. But the failure of the United States to ensure meaningful privacy protection for personal data is the reason that a growing number of countries are concerned about trans-border data flows. Until that problem is addressed, concerns about data transfers to the United States will remain.

We ask that this Statement from EPIC be entered in the hearing record. We look forward to working with you on these issues of vital importance to the American public.

Sincerely,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

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

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

[17] *See generally*, EPIC, Council of Europe Privacy Convention (2015), https://epic.org/privacy/intl/coeconvention/.