epic.org | ELECTRONIC PRIVACY INFORMATION CENTER

Testimony and Statement for the Record of

Marc Rotenberg
President, EPIC
Adjunct Professor, Georgetown Law

Hearing on

"Examining the EU Safe Harbor Decision and Impacts for Transatlantic Data Flows"

Joint Hearing Before the

United States House of Representatives Energy & Commerce Subcommittees on Commerce, Manufacturing, and Trade and Communications and Technology

November 3, 2015
2123 Rayburn House Office Building
Washington, DC

## Testimony Summary

Safe Harbor was an industry-developed self-regulatory trade strategy that simply did not work. Consumer groups and scholars long criticized the Safe Harbor framework, noting that almost a decade passed before the Federal Trade Commission brought an enforcement action against a US company. The decision of the European Court of Justice to strike down the Safe Harbor was not a surprise: transatlantic data transfers without legal protections were never safe.

The Court ruling reflects (1) the weakness of Safe Harbor regime, (2) developments in EU law, and (3) lack of progress on the US side to update domestic privacy law safeguards. The Court's decision reflects the recognition that both privacy (Article 7) and data protection (Article 8) are fundamental rights. The ruling also makes clear that independent national privacy agencies will have the authority to enforce these rights. Enforcement actions are already underway.

But this is not simply a trade issue. The decision of the European Court is also a reminder that US law needs to be updated. American consumers today confront skyrocketing identity theft, data breaches, and financial fraud. All of the polls point to broad-based support, within the United States, for updating privacy safeguards.

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 transborder data flows to continue and protects the interests of US consumers and US businesses.

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 our privacy law is imposing an enormous cost on American consumers.

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. Congress should take this opportunity to carry "the American tort" forward into the Information age. This is not simply a matter of trade policy. It is a matter of fundamental rights.

Chairman Burgess, Chairman Waldman, and members of the House Subcommittees, thank you for the opportunity to testify today regarding EU Safe Harbor decision. My name is Marc Rotenberg, and I am President of the Electronic Privacy Information Center ("EPIC"). EPIC is an independent, non-profit research organization focused on emerging privacy and civil liberties issues. We work closely with a distinguished advisory board, with leading experts in law, technology, and public policy.[1] In 2006, EPIC in conjunction with Privacy International, a London-based human rights organization and several hundred privacy experts and NGOs around the world, published the most extensive survey of international privacy law ever produced.[2]

I have also taught Information Privacy Law at Georgetown Law since 1990 and am the coauthor of a forthcoming casebook on privacy law.[3] Much of my scholarly work over the last two decades has been on comparative approaches to privacy protection. I have written extensively on the development of the EU privacy law and also made recommendation on how the US and Europe could move forward to address shared concerns about the protection of privacy.[4]

---

1 EPIC Advisory Board, https://epic.org/epic/advisory_board.html

2 EPIC and Privacy International, PRIVACY AND HUMAN RIGHTS: AN INTERNATIONAL SURVEY OF PRIVACY LAWS AND DEVELOPMENTS (EPIC 2006) (The report is over 1,100 pages and contains almost 6,000 footnotes).

3 ANITA L. ALLEN & MARC ROTENBERG, PRIVACY LAW AND SOCIETY (WEST 2016). *SEE ALSO*, MARC ROTENBERG, JULIA HORWITZ, & JERAMIE SCOTT, EDS. PRIVACY IN THE MODERN AGE: THE SEARCH FOR SOLUTIONS (THE NEW PRESS 2015).

4 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

## I. Safe Harbor was Never an Effective Basis for EU-US Data Flows.

The Safe Harbor Framework is an industry-developed self-regulatory approach to privacy protection that simply does not work.[5] Coordinated by the Department of Commerce, the Safe Harbor program allows US companies to self-certify privacy policies in lieu of complying with legal requirements for the processing of data of Europeans. The Safe Harbor arrangement developed in response to the European Union Data Directive, a comprehensive legal framework that established essential privacy safeguards for consumers across the European Union.[6] The Federal Trade Commission has been tasked with overseeing Safe Harbor compliance, but only "sanctions" companies by proscribing them from future misrepresentations when they make false representations.

*Weaknesses of Safe Harbor Were Known at the Start*

Consumer groups and scholars have long criticized the Safe Harbor Framework, noting that almost a decade passed before the Federal Trade Commission ("FTC") brought an enforcement action against a US company with respect to the Safe Harbor.[7] Furthermore, three studies of the Safe Harbor Framework, conducted in 2001, 2004, and 2008, found numerous deficiencies, with the most recent study finding that "the growing

[5] U.S. Dep't of Commerce, Safe Harbor Privacy Principles, http://export.gov/safeharbor/eu/eg_main_018475.asp (last updated Jan. 30, 2009).
[6] Directive 95/46/EC of the European Parliament and of the Council of Oct. 24, 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.
[7] Anita Ramasastry, *EU-US Safe Harbor Does Not Protect US Companies with Unsafe Privacy Practices*, FINDLAW (Nov. 17, 2009), http://writ.news.findlaw.com/ramasastry/20091117.html. See also TACD, Safe Harbor Proposal and International Convention on Privacy Protection (1999) http://test.tacd.org/wp-content/uploads/2013/09/TACD-ECOM-08-99-Safe-Harbor-Proposal-and-International-Convention-on-Privacy-Protection.pdf; TACD, Safe Harbor, 1999 http://test.tacd.org/wp-content/uploads/2013/09/TACD-ECOM-18-00-Safe-Harbor.pdf

number of false claims made by organisations regarding the Safe Harbor represent a new and significant privacy risk to consumers."[8] In 2010, a German state Data Protection and Privacy Commissioner demanded termination of the Safe Harbor agreement, citing low levels of enforcement by the United States.[9] In 2013, the European Commission outlined thirteen changes to strengthen the Safe Harbor protections.[10] The suggested modifications included changes to Safe Harbor's transparency, redress procedures, enforcement procedures, and the extent to which companies allow US law enforcement to access their data.[11]

These Safe Harbor framework problems were widely known at the time of adoption. Consequently, the European Court of Justice's decision to strike down the Safe Harbor arrangement was the culmination of what many experts had warned about all along: transatlantic data flows under the framework were never safe.[12]

---

[8] World Privacy Forum, The US Department of Commerce and International Privacy Activities: Indifference and Neglect, 18 (Nov. 22, 2010), *available at* http://www.worldprivacyforum.org/wp-content/uploads/2009/12/USDepartmentofCommerceReportfs.pdf. *See also* Chris Connolly, Galexia, The US Safe Harbor – Fact or Fiction? (Dec. 2, 2008), *available at* http://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safe_harbor_fact_or_fiction.pdf.

[9] *Id.* at 19.

[10] Communication from the Commission to the European Parliament and the Council—Rebuilding Trust in EU-US Data Flows, COM (2013) 846 (Nov. 26, 2013), available at http://ec.europa.eu/justice/data-protection/files/com_2013_846_ en.pdf; Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, COM (2013) 847 (Nov. 26, 2013), available at http://ec.europa.eu/justice/data-protection/files/com_ 2013_847_en.pdf.

[11] *Id*.

[12] See generally, Max Schrems v Irish Data Protection Commissioner (Safe Harbor), EPIC (2015) https://epic.org/privacy/intl/schrems/default.html.

*The Federal Trade Commission Failed to Pursue Meaningful Enforcement*

The FTC is charged with enforcing the US-EU Safe Harbor Framework against US companies that fail to abide by the framework. To date, the FTC has not meaningfully exercised its enforcement powers against US companies that violate the Safe Harbor framework. EPIC has previously urged the FTC to take more aggressive action in Safe Harbor settlements. In 2014, EPIC submitted comments to the FTC after the agency published settlement agreements with 12 companies that misrepresented Safe Harbor compliance. Each of the companies had self-certified to the Safe Harbor Framework, but according to the FTC investigation, failed to renew self-certification while continuing to represent to consumers that they were current members of the Safe Harbor Framework. The FTC's settlement agreements prohibited the companies from making those representations and required them to provide annual reports about their compliance with the agreements, but did not impose any other penalty.

EPIC recommended that the FTC revise the proposed orders to, among other things, require the companies to comply with the Consumer Privacy Bills of Rights. The Consumer Privacy Bill of Rights is a comprehensive framework of seven substantive privacy protections for consumers that would ensure that consumers' personal data is protected throughout the data lifecycle. EPIC explained that by requiring companies to comply with the Consumer Privacy Bill of Rights, the FTC would put in place a baseline set of privacy standards that are widely recognized around the world and necessary to protect the interests of consumers.

*Consequences of Inadequate Data Protection in the United States Implicate the Interests of US Consumers and US Businesses*

The ongoing collection of personal information in the United States without sufficient privacy safeguards has led to staggering increases in identity theft, security breaches, and financial fraud. These privacy problems have skyrocketed since 2000, but one only needs to look at this year of disastrous data breaches to confirm the magnitude of the problem. This summer a number of retailers, including CVS and Walgreens, lost their customers data through a breach of a common third-party vendor that managed the photo service sites for each retailer. The data breach compromised customer credit card information, names, phone numbers, email addresses, usernames, and passwords.[13] CareFirst BlueCross BlueShield was hit by a data breach that compromised the personal information of over 1 million users. Healthcare insurers Anthem and Premera Blue Cross also suffered major data breaches this year. Overall, these healthcare insurers have lost the data on more than 90 million Americans.[14] Experian, the largest American consumer credit bureau, suffered a breach that compromised the Social Security Numbers of 15 million people. The sensitive information of 21.5 million people was compromised with the data theft from the Office of Personnel Management.[15] The data breach included the loss of Social Security Numbers as well as security clearance applications.

[13] Taryn Luna, *CVS Confirms Data Breach at Photo Site This Summer*, Boston Globe (Sept. 11, 2015), https://www.bostonglobe.com/business/2015/09/11/cvs-confirms-data-breach-photo-site-this-summer/xc7mG3YFVgkKLYBQHfrIwI/story.html.
[14] Bryan Krebs, *Carefirst Blue Cross Breach Hits 1.1M*, Krebs on Security Blog (May15, 2015, 9:03 AM), http://krebsonsecurity.com/2015/05/carefirst-blue-cross-breach-hits-1-1m/.
[15] Jim Sciutto, *OPM Government Data Breach Impacted 21.5 Million*, CNN (July 10, 2015), http://www.cnn.com/2015/07/09/politics/office-of-personnel-management-data-breach-20-million/.

These data breaches only represent a subset of the breaches in 2015 and continue a rising trend in data theft—data theft that often leads to identity theft. It is no wonder that identity theft continues to be the top consumer complaint to the Federal Trade Commission and has been for a decade and a half.[16] The rise in data breaches in US companies and identity theft since the implementation of the Safe Harbor has diminished US and EU citizen confidence that their data will remain private and secure. A PEW research poll last fall showed little confidence that the US government or commercial entities would keep data secure.[17] No serious person today believes that the United States has adequate protections in place for personal data.

A "Safe Harbor 2.0" merely repackages the previous framework that the European Court of Justice struck down, and it would not adequately safeguard personal data US companies routinely fail to protect. To encourage transatlantic data flows, Congress must modernize and enforce US privacy law.

## II. The Schrems Decision is Far-reaching and the Consequences Could Be Severe if the US Fails to Act

The European Court of Justice struck down Safe Harbor because EU personal data transferred to the United States does not receive the same legal protection in the

[16] Press Release, FTC, Identity Theft Tops FTC's Consumer Complaint Categories Again in 2014 (Feb. 27, 2015), https://www.ftc.gov/news-events/press-releases/2015/02/identity-theft-tops-ftcs-consumer-complaint-categories-again-2014.

[17] Mary Madden and Lee Rainie, *Americans' Attitudes About Privacy, Security and Surveillance*, Pew Research Center (May 20, 2015), http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/.

United States as it does in Europe. Specifically, according to the European standard, the level of protection should be "adequate"[18] and "essentially equivalent."[19]

*EU Regulatory Approach for Data Protection is Similar to US Regulatory Approach for Drugs, Foods, Consumer Products, and Cars – Consumers in Domestic Markets are Protected by Meaningful Safeguards*

This is a very familiar idea in many US regulatory domains. We do not permit the import of drugs, foods, consumer products, or cars that are not safe for American consumers. It would not be fair to our companies to expect them to comply with our regulatory requirements while allowing non-US firms to ignore the same legal obligations. The same applies to European companies in Europe. It is not fair to expect them to comply with European privacy and data protection laws if the American companies do not have to comply with the same rules. Data transfers to the US are not safe for non-US individuals because the lack of adequate privacy safeguards.[20]

Essentially, the Safe Harbor regime created a legal ground for US companies to circumvent European data protection standards while European companies are bound by those obligations. This has resulted in lower level of protection for Europeans when their data is transferred to the US. The level of privacy protection in the US is lower for Europeans from two perspectives. First, US privacy protections are not as stringent as

[18] Article 25(6) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31), as amended by Regulation (EC) No 1882/2003 of the European Parliament and of the Council of 29 September 2003 (OJ 2003 L 284, p. 1) ('Directive 95/46'). See also Marc Rotenberg, Letter to the Editor, The New York Times (October 13, 2015). http://www.nytimes.com/2015/10/13/opinion/digital-privacy-in-the-us-and-europe.html?_r=0

[19] Paragraph 73 of C-362/14, Maximillian Schrems v Data Protection Commissioner, 2015.

[20] Douwe Korff , EU-US Umbrella Data Protection Agreement : Detailed analysis, FREE Group (October 14, 2015). http://free-group.eu/2015/10/14/eu-us-umbrella-data-protection-agreement-detailed-analysis-by-douwe-korff/

Europeans privacy protections. Second, EU citizens do not enjoy the same Privacy Act protections that Americans do. The Privacy Act, as adopted in 1974, defines an "individual" entitled to protection under the Act as a citizen of the United States or an alien lawfully admitted for permanent residence.[21] In recognizing the fact that the US routinely collects data on EU citizens, Congress is considering updating the Privacy Act to extend protections to EU citizens.[22]

The European Court of Justice's holdings were driven in part by the National Security Agency's mass surveillance programs and the failure to establish meaningful regulation of Internet companies, almost all based in the United States. The judgment of the Court reflects also the incorporation of Article 7 and Article 8 of the Charter of Fundamental Rights in EU law. These provisions state

**Article 7**
*Respect for private and family life*

> Everyone has the right to respect for his or her private and family life, home and communications.

**Article 8**
*Protection of personal data*

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

[21] 5 U.S.C. § 552a(a)(2). *See generally, The Privacy Act 1974*, EPIC (2015), https://epic.org/privacy/1974act/.
[22] EPIC's letter to the U.S. House of Representatives Committee on the Judiciary on H.R. 1428, the Judicial Redress Act of 2015 (September 16, 2015). https://epic.org/foia/umbrellaagreement/EPIC-Statement-to-HJC-on-HR1428.pdf

3. Compliance with these rules shall be subject to control by an independent authority.

The Court ruling reflects (1) the weakness of Safe Harbor regime, (2) developments in EU law and (3) lack of progress on US side to develop meaningful and comprehensive privacy safeguards.

The Court also highlighted the enforcement power of the national data protection officials of EU Member States. This means that although they are not entitled to declare an adequacy decision of the European Commission – such as Safe Harbor – invalid, they can and should enforce privacy and data protection rights. This type of enforcement capability[23] is not a new power provided by the Court decision, but it is certainly strengthened and has become more visible[24] after the judgment. This development also reflects the ongoing negotiations about the General Data Protection Reform in Europe.[25] The European Court of Justice's holdings are far-reaching and of global significance. Following the Safe Harbor decision, Israel and Switzerland suspended data flows under Safe Harbor.[26]

Other countries too have taken actions against American firms because we have not yet updated our privacy laws. Jennifer Stoddart, former Privacy Commissioner of

[23] Dutch DPA Signs Agreement GPEN Alert System, International Privacy Conference Amsterdam 2015 (October 26, 2015). https://www.privacyconference2015.org/dutch-dpa-signs-agreement-gpen-alert-system/

[24] European Commission Press Release, Speech/15/5916, Commissioner Jourová's remarks on Safe Harbour EU Court of Justice judgment before the Committee on Civil Liberties, Justice and Home Affairs (Libe) (October 26, 2015). http://europa.eu/rapid/press-release_SPEECH-15-5916_en.htm

[25] European Commission Factsheet, Reform of the data protection legal framework in the EU (Last update: October 13, 2015). http://ec.europa.eu/justice/data-protection/reform/index_en.htm

[26] No Easy Way Forward for EU-US transfers of personal data, Privacy Laws (October 28, 2015). http://www.privacylaws.com/Int_enews_28_10_15

Canada said "this is the age of big data where personal information is the currency that Canadians and others around the world freely give away."[27]As a result of her continuous investigation and other enforcement actions against Facebook, the company agreed to make changes to better protect users' personal information on the social networking site and comply with Canadian laws. These changes mean that that the privacy of 200 million Facebook users in Canada and around the world will be far better protected.[28]

In Asia, there is growing concern about privacy issues, new, comprehensive privacy laws in Singapore and Malaysia, the amendment of China's consumer protection law to include data privacy principles, and increased financial penalties in South Korea.[29] The Korean Communications watchdog previously fined Google for unauthorized data collection for Street View[30] and the company is now facing business suspension in Korea because of the firm's participation in the Prism program.[31]

---

[27]Meagan Fitzpatrick, Social media websites ignoring privacy laws, watchdog says, CBCNews(May 29, 2012) http://www.cbc.ca/news/politics/social-media-websites-ignoring-privacy-laws-watchdog-says-1.1197586.

[28] Facebook to make privacy changes, CBCNews (August 27, 2009) http://www.cbc.ca/news/technology/facebook-to-make-privacy-changes-1.780164.

[29]Mark Parsons and Peter Colegate, 2015: The Turning Point for Data Privacy Regulation in Asia?, Hogan Lovells Chronicle of Data Protection (February 18, 2015) http://www.hldataprotection.com/2015/02/articles/international-eu-privacy/2015-the-turning-point-for-data-privacy-regulation-in-asia/.

[30]Jack Purcher, Korea's Communication Watchdog Fines Google $198,000, Patently Apple (January 29, 2014) http://www.patentlyapple.com/patently-apple/2014/01/koreas-communication-watchdog-fines-google-198000.html.

[31] Bahk Eun-ji, Google faces business suspension in Korea, The Korea Times (July 2, 2015) http://www.koreatimes.co.kr/www/news/tech/2015/07/133_182052.html.

*European Privacy Officials Will Take Enforcement Action*

Since the Safe Harbor judgment was issued last month, we can anticipate many privacy cases.[32] Data protection authorities across Europe are preparing enforcement actions.[33] Some of the European privacy officials will go beyond Safe Harbor and look more closely at alternative data transfer strategies, such as Binding Corporate Rules and Model Contract Clauses.[34] According to the Schrems judgment, they have a legal responsibility to safeguard fundamental rights. Therefore, not even the European Commission—the US negotiating party—has the legal authority to prevent these investigations. [35]

Neither consumers nor businesses want to see the disruption of transborder 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. A "Safe Harbor 2.0" does not solve this problem. The US will need to do more to reform privacy law to enable transborder dataflows. It is a well-

[32] EPIC, European Data Protection Authorities Conclude Data Transfers under Safe Harbor Now Unlawful (October 17, 2015). https://epic.org/2015/10/european-data-protection-autho.html
[33] Press Release, Statement of the Article 29 Working Party (October 16, 2015). http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf
[34] Unabhängige Landeszentrum für Datenschutz, Positionspapier des ULD zum Urteil des Gerichtshofs der Europäischen Union vom 6. Oktober 2015, C-362/14 (October 14, 2015). https://www.datenschutzzentrum.de/uploads/internationales/20151014_ULD-Positionspapier-zum-EuGH-Urteil.pdf
[35] Monika Kuschewsky, Schrems (Safe Harbor) Judgment – German Data Protection Authorities Issue Position Paper, Inside Privacy (October 26, 2015). http://www.insideprivacy.com/international/european-union/schrems-safe-harbor-judgment-german-data-protection-authorities-position/

known paradox that promoting the free flow of personal data across national boundaries requires comprehensive privacy protection.[36]

## III. To Support Transatlantic Data Flows, Congress Must Modernize US Privacy Law

Never has the need to update the privacy laws of the United States been more urgent. Identity theft, data breaches, and financial fraud are skyrocketing. Americans today worry about retailers who lose their credit card information, intelligence agencies that gather their phone records, and data brokers that sell their family's medical information to strangers. Industry "self-regulation" has failed and opt-out techniques force consumers to check their privacy settings every time a company changes its business model.[37]

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 transborder 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

[36] 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/

[37] Coalition Letter to President Obama, On the Second Anniversary of the Consumer Privacy Bill of Rights (February 24, 2014) https://epic.org/privacy/Obama-CPBR.pdf.

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, particularly after the terrible data breach that compromised 21.5 million employment records, 5 million digitized finger print files, and even the most sensitive SF-86 forms. 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.[38]

The application of the Privacy Act for non-US Persons is the cornerstone of the E.U.-US Umbrella Agreement.[39] But the current proposed changes to the Privacy Act will not solve the problem as the right of judicial redress is far too attenuated. The much better approach would be to simply revise the definition of "individual" to mean "natural person." This would immediately address the concerns that have been raised outside the United States about the scope of coverage of the Act. Further changes to the Privacy Act would be beneficial for US citizens as well.

Third, Congress should create an independent privacy agency, as Congress contemplated in 1974 when it enacted the Privacy Act.[40] EPIC has previously recommended the establishment of a privacy agency to ensure independent enforcement

[38] H.R. 1428 114th Congress Judicial Redress Act of 2015
[39] *See generally*, EPIC, EU-US Data Transfer Agreement (2015), https://epic.org/privacy/intl/data-agreement/index.html.
[40] 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).

of the Privacy Act, develop additional recommendations for privacy protection, and provide permanent leadership within the federal government on this important issue.[41] 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. The FTC has failed to enforce its own orders when companies have breached settlement agreements.[42] The Commission routinely fails to require companies found to have violated privacy rules to comply with the Consumer Privacy Bill of Rights. The Commission has made no recommendations for legislation following several, in-depth workshops exploring privacy obstacles consumers confront, including Internet of Things and facial recognition. These missed opportunities, coupled with the fact that the FTC infrequently undertakes enforcement actions, make clear that consumers desperately need a new, independent privacy enforcement agency.

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.[43] 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.

---

[41] *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.
[42] EPIC, EPIC v. FTC (Enforcement of the Google Consent Order) (2015), https://epic.org/privacy/ftc/google/consent-order.html.
[43] *See generally*, EPIC, Council of Europe Privacy Convention (2015), https://epic.org/privacy/intl/coeconvention/.

**Conclusion**

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 our privacy is imposing an enormous cost on American consumers. According to a Pew survey earlier this year, 74% of Americans believe control over personal information is "very important," yet only 9% believe they have such control.[44] In a Pew survey last year, 80% of adults "agree" or "strongly agree" that Americans should be concerned about the government's monitoring of phone calls and internet communications.[45] 64% believe there should be more regulation of advertisers.[46]

Remarkably, the leaders of US Internet companies have also called for stronger privacy protection and have described privacy, much as the European Court did, as a fundamental human right. Microsoft President Brad Smith recently said, "Legal rules that were written at the dawn of the personal computer are no longer adequate for an era with ubiquitous mobile devices connected to the cloud. In both the United States and Europe, we need new laws adapted to a new technological world."[47] Mr. Smith said simply,

---

[44] Mary Madden and Lee Rainie, *Americans' Views About Data Collection and Security*, Pew Research Center (May 20, 2015), http://www.pewinternet.org/2015/05/20/americans-views-about-data-collection-and-security/.

[45] Mary Madden, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, Pew Research Center (Nov. 12, 2014), http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/.

[46] *Id.*

[47] Brad Smith, *The Collapse of the US-EU Safe Harbor: Solving the New Privacy Rubik's Cube*, Microsoft on the Issues Blog (Oct. 20, 2015), http://blogs.microsoft.com/on-the-issues/2015/10/20/the-collapse-of-the-us-eu-safe-harbor-solving-the-new-privacy-rubiks-cube/.

"Privacy is a fundamental human right."[48] Earlier this year, Apple CEO Tim Cook said, "If those of us in positions of responsibility fail to do everything in our power to protect the right of privacy, we risk something far more valuable than money, we risk our way of life."[49] And then just two weeks ago, Mr. Cook told NPR "privacy is a fundamental human right."[50]

In the realm of regulatory policy, we call this "convergence." 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. I urge the Congress to take this opportunity to carry "the American tort" forward into the Information age.[51] This is not simply a matter of trade policy. It is a matter of fundamental rights.

---

[48] *Id.*

[49] Caroline Moss, *Apple CEO Tim Cook Delivers a Fantastic, Touching Speech About Why Online Privacy Matters*, Business Insider (Feb. 14, 2015), http://www.businessinsider.com/tim-cook-on-online-privacy-2015-2.

[50] NPR, Apple CEO Tim Cook: 'Privacy Is A Fundamental Human Right' (Oct. 1, 2015), http://www.npr.org/sections/alltechconsidered/2015/10/01/445026470/apple-ceo-tim-cook-privacy-is-a-fundamental-human-right.

[51] Following the publication of the famous Brandeis Warren article in 1890, European scholars referred to the privacy claim as "the American tort."