epic.org

1718 Connecticut Ave NW
Suite 200
Washington DC 20009
USA
+1 202 483 1140 [tel]
+1 202 483 1248 [fax]
www.epic.org

January 26, 2015

Representative Fred Upton, Chairman
Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515

Representative Frank Pallone, Jr., Ranking Member
Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20215

Dear Chairman Upton and Ranking Member Pallone,

We write today in anticipation of your upcoming hearing, "What are the Elements of Sound Data Breach Legislation?," to bring your attention to the work of EPIC and to urge you to pursue strong measures that safeguard consumers and that do not preempt state law. We appreciate your work and the work of other Committee Members to address an issue of paramount concern to American consumers.

The Electronic Privacy Information Center ("EPIC") is a non-partisan research organization established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC has a particular interest in safeguarding personal privacy and preventing harmful data practices.[1]

EPIC has previously testified before Congress on data breach notification.[2] We urged Members to enact federal baseline legislation for breach notification that would allow the states to adopt more stringent safeguards if they wish.[3] In 2011, we stated:

---

[1] EPIC routinely submits administrative comments, urging federal agencies to uphold the data security protections in the Privacy Act and protect individual privacy in mass government databases. See, e.g., EPIC, Comments on Big Data and the Future of Privacy, FR Doc. 2014-04660 (Apr. 4, 2014), available at http://epic.org/privacy/big-data/EPIC-OSTP-Big-Data.pdf; See also, EPIC: Big Data and the Future of Privacy, https://www.epic.org/privacy/big-data/; EPIC, Comments on National Privacy Research Strategy (Oct. 17, 2014), available at https://www.epic.org/apa/comments/EPIC-NITRD-Privacy-Research-Strategy.pdf.

[2] Testimony of Marc Rotenberg, EPIC President, "Requiring Greater Protection for Sensitive Consumer Data and Timely Notification in Case of Breach: Discussion Draft" before the House Commerce Committee (June 15, 2011), available at https://epic.org/privacy/testimony/EPIC_Testimony_House_Commerce_6-11_Final.pdf.; see also Testimony of Marc Rotenberg, EPIC President, "Cybersecurity and Data Protection in the Financial Sector," before the House Financial Services Committee (Sept. 14, 2011), available at http://financialservices.house.gov/uploadedfiles/091411rotenberg.pdf

[3] *Id.* at 6 (testimony of EPIC President Marc Rotenberg).

> Because states enjoy a unique perspective that allows them to craft innovative programs to protect consumers, they should be permitted to continue to operate as 'laboratories of democracy' in the privacy and data security arena. State legislatures are closer to their constituents and the entities they regulate; they are the first to see trends and problems, and are well-suited to address new challenges and opportunities that arise from evolving technologies and business practices.[4]

Since that time, the data breach problem has only grown worse. In the past 18 months, 70 million Target customers, 38 million Adobe users, 76 million JPMorgan Chase & Co. users, 4.6 million Snapchat users, and potentially all 148 million eBay users had their personal information exposed by database breaches.[5] There have been approximately 4,478 publicly disclosed data breaches since 2005, with 43% of companies experiencing a data breach this past year.[6]

More needs to be done. To protect consumers there must be strong measures, including data-breach transparency and the mandatory use of Privacy Enhancing Techniques.[7] Federal legislation that does not preempt state safeguards is critical.

EPIC also supports enactment of the Consumer Privacy Bill of Rights and urges the Committee to promptly begin legislative hearings on the President's proposal.[8] The White House proposal reflects widely established standards currently found in U.S. Privacy Law. Enactment of the Consumer Privacy Bill of Rights would establish new baseline consumer data safeguards, promoting consumer trust and confidence in the digital economy.[9]

---

[4] *Id.* at 8 (testimony of EPIC President Marc Rotenberg).

[5] Reuters Video, EBay says client information stolen in hacking attack (May 22, 2014), http://uk.reuters.com/video/2014/05/29/ebay-says-client-information-stolen-in-h?videoId=313044013&videoChannel=2603 (EBay); BBC News, Snapchat Hack Affects 4.6 Million Users (January 1, 2014), http://www.bbc.com/news/technology-25572661 (Snapchat); Krebs on Security, Adobe Breach Impacted at Least 38 Million Users (Oct. 29, 2013), http://krebsonsecurity.com/2013/10/adobe-breach-impacted-at-least-38-million-users/ (Adobe). See Ponemon Institute, 2014: A Year of Mega Breaches (January 2015), http://www.ponemon.org/local/upload/file/2014%20The%20Year%20of%20the%20Mega%20Breach%20FINAL3.pdf (cataloging the statistics of the worst data breaches of 2014).

[6] Privacy Rights Clearinghouse, "Chronology of Data Breaches," https://www.privacyrights.org/data-breach/new; Ponemon Institute, Is your Company Ready for a Big Data Breach? The Second Annual Study on Data Breach Preparedness (Sept. 2014), available at http://www.experian.com/assets/data-breach/brochures/2014-ponemon-2nd-annual-preparedness.pdf.

[7] Comments on National Privacy Research Strategy, supra note 1, at 6, 12 (discussing consumer protection safeguards and defining Privacy Enhancing Techniques as technologies and practices that minimize or eliminate the collection of personally identifiable information).

[8] The White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy (Feb. 2012), http://www.whitehouse.gov/sites/default/files/privacy-final.pdf (articulating the Consumer Privacy Bill of Rights).

[9] *See* EPIC, Comments on Big Data and the Future of Privacy, supra note 1, at 8-11 (discussing the elements of the Consumer Privacy Bill of Rights)

EPIC would also like to draw the Committee's attention to the need to promote "algorithmic transparency." We must end the secret profiling of American consumers that excludes many from economic opportunity. It is not sufficient for companies to reveal the circumstances when breaches have occurred, companies should also be required to disclose the basis of automated decisionmaking

Previous work by EPIC has made clear the risk of "risk-based" algorithmic profiling: it encourages companies to collect far more data than they can safely and securely store.[10] In recent comments to the Office of Science and Technology Policy, we explained that, "[t]he 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."[11]

It is within the Committee's jurisdiction to address the growing threats to American consumers that impact threat personal safety and economic opportunity.

EPIC looks forward to working with your staff on this matter.

Sincerely,

Marc Rotenberg
EPIC President

Julia Horwitz, Director
EPIC Consumer Privacy Project

Brooke Olaussen
Brooke Olaussen
EPIC Consumer Privacy Counsel

CC: Attorney General Jim Hood (MS), President, National Association of Attorneys General (NAAG)
Attorney General Marty Jackley (SD), President-Elect, NAAG

[10] *See, e.g.,* EPIC et al., Comments Urging the Department of Homeland Security to (A) Suspend the "Automated Targeting System" as Applied to Individuals, or in the Alternative, (B) Fully Apply All Privacy Act Safeguards to Any Person Subject to the Automated Targeting System (Dec. 4, 2006), available at http://epic.org/privacy/pdf/ats_comments.pdf; EPIC, Comments on Automated Targeting System Notice of Privacy Act System of Records and Notice of Proposed Rulemaking, Docket Nos. DHS-2007-0042 and DHS-2007-0043 (Sept. 5, 2007), available at http://epic.org/privacy/travel/ats/epic_090507.pdf.
See also, Automated Targeting System, EPIC, https://epic.org/privacy/travel/ats/.

[11] Comments on National Privacy Research Strategy, supra note 1, at 2.