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 3, 2017

The Honorable Michael Crapo, Chairman
The Honorable Sherrod Brown, Ranking Member
Senate Committee on Banking, Housing, & Urban Affairs
534 Dirksen Senate Office Building
Washington, DC 20510

Dear Chairman Crapo and Ranking Member Brown:

We write to you regarding the upcoming hearing entitled "An Examination of the Equifax Cybersecurity Breach."[1] The Equifax data breach is one of the most serious in U.S. history. The sensitive personal data, including Social Security Numbers, of nearly half the country was compromised. We have recently outlined a strategy for Congress in *the Harvard Business Review*.[2] We provide that article and the comments below for your consideration.

EPIC is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC has long advocated for cybersecurity safeguards for consumer information held by financial and commercial organizations. EPIC has previously testified before Congress on the need for financial institutions and companies to protect consumers against data breaches and the need to limit the use of Social Security Numbers.[3]

---

[1] *An Examination of the Equifax Cybersecurity Breach,* 115th Cong. (2017), S. Comm. on Banking, Housing, & Urban Affairs, https://www.banking.senate.gov/public/index.cfm/hearings?ID=B61BB78D-CF34-4D54-B7F2-F7F982D77D6F.

[2] Marc Rotenberg, *Equifax, the Credit Reporting Industry, and What Congress Should Do Next,* Harvard Business Review, Sep. 20, 2017, https://hbr.org/2017/09/equifax-the-credit-reporting-industry-and-what-congress-should-do-next [hereinafter "Equifax and What Congress Should Do Next"]

[3] *See, e.g.*, Testimony and Statement for the Record of Marc Rotenberg, Executive Director, Electronic Privacy Information Center on "Cybersecurity and Data Protection in the Financial Sector," Before the Senate Committee on Banking, Housing, and Urban Affairs, June 21, 2011, https://epic.org/privacy/testimony/EPIC_Senate_Banking_Testimony%20_6_21_11.pdf; Testimony and Statement for the Record of Marc Rotenberg, Executive Director, Electronic Privacy Information Center, Hearing on the Discussion Draft of H.R. ____, A Bill to Require Greater Protection for Sensitive Consumer Data and Timely Notification in Case of Breach, Before the House Committee on Energy and Commerce Subcommittee on Commerce, Manufacturing, and Trade, June 15, 2011, http://epic.org/privacy/testimony/EPIC_Testimony_House_Commerce_6-11_Final.pdf; EPIC Statement to the U.S. House Committee on Energy & Commerce, Testimony and Statement for the Record of Marc Rotenberg, President and Executive Director, Electronic Privacy Information Center on "Social Security Number High-Risk Issues," Before the House Committee on Ways and Means Subcommittee on Social Security, Mar. 16, 2006, https://epic.org/privacy/ssn/mar_16test.pdf.

Equifax and the Data Breach Epidemic

Equifax is perhaps the most significant data breach in American history affecting nearly half of the United States population.[4] This data breach highlights the need for change in how companies prevent data breaches from occurring and how consumers are notified in the event of a data breach. Equifax was aware of the breach on July 29th. However, the public was not informed of the breach until September 7th.[5] Equifax then directed consumers to a fake website to see if they had been affected.[6]

The seriousness of the Equifax data breach is highlighted by the millions of Social Security Numbers ("SSN") that were compromised. Despite the fact that SSNs were never intended to be used for identification purposes in the private sector, credit grantors rely on the SSN to authenticate a credit applicant's identity. As a result identity theft occurs when thieves obtain stolen SSNs. The root of this problem is that the SSN is used not only to tell the credit issuer who the applicant is, but also to verify the applicant's identity.

The Equifax data breach is simply the latest in a series of breaches to impact consumers across a number of industries. The data breach at the Office of Personnel Management compromised the personal information of more than 20 million people, many with active security clearances.[7] Data breaches have affected numerous private companies including Yahoo, which had over 1 billion user accounts compromised,[8] and Chipotle, Home Depot, and Target who combined had more than 100 million credit cards compromised.[9] Data breaches have also

---

[4] EPIC, "143 Million US Consumers Suffer Massive Data Breach, Equifax at Fault," https://epic.org/2017/09/143-million-us-consumers-suffe.html; Lee Matthews, *Equifax Data Breach Impacts 143 Million Americans,* Forbes, Sep. 7, 2017, https://www.forbes.com/sites/leemathews/2017/09/07/equifax-data-breach-impacts-143-million-americans/#5dd854a4356f.

[5] *Equifax Was Aware of the Breach 6 Weeks Prior, Pennsylvania AG Says,* Fox Business, Sep. 15, 2017, http://www.foxbusiness.com/markets/2017/09/15/equifax-was-aware-breach-6-weeks-prior-pennsylvania-ag-says.html.

[6] Merrit Kennedy, *After Massive Data Breach, Equifax Directed Customers To Fake Site,* NPR, Sep. 21, 2017, http://www.npr.org/sections/thetwo-way/2017/09/21/552681357/after-massive-data-breach-equifax-directed-customers-to-fake-site.

[7] Ellen Nakashima, *Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say,* Washington Post, Jul. 9, 2015, https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/?utm_term=.305e75d6db3d.

[8] Vindue Goel, Nicole Perlroth, *Yahoo Says 1 Billion Users Accounts Were Hacked,* New York Times, Dec. 14, 2016, https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html.

[9] Lisa Baertlein, *Chipotle Says Hackers Hit Most Restaurants In Data Breach,* Reuters, May 26, 2017, https://www.reuters.com/article/us-chipotle-cyber/chipotle-says-hackers-hit-most-restaurants-in-data-breach-idUSKBN18M2BY; Robin Sidel, *Home Depot's 56 Milion Card Breach Bigger Than Target's,* Wall Street Journal, Sep. 18, 2014, https://www.wsj.com/articles/home-depot-breach-bigger-than-targets-1411073571; *Target: 40 Million Credit Cards Compromised,* CNN, Dec. 19, 2013, http://money.cnn.com/2013/12/18/news/companies/target-credit-card/index.html.

impacted educational institutions with the personal information of hundreds of thousands students and faculty exposed.[10]

Solutions to the Data Breach Problem

The scope of the data breach epidemic cannot be overstated, but there are several solutions that Congress should consider to prevent the breaches from occurring and to protect consumers after they occur. As we explained recently, the current practice of delayed notification and credit monitoring services is not sufficient to remedy to the harm done. [11]

Consumers must be promptly notified once a data breach has been discovered. Companies should minimize the amount of personal data they collect and only retain it for as long as necessary to provide their product or service. Congress has previously established data minimization and deletion requirements.[12] EPIC has long argued that the best way to prevent the misuse of sensitive personal data is to avoid gathering it in the first place.[13] Minimizing stored user data reduces incentives for hackers to attack data storage systems by reducing the amount of data available to steal. This practice also reduces the costs of data breaches.

Congress should also consider privacy enhancing technologies ("PETs") as part of any solution to the data breach epidemic..[14] These technologies also reduce the risk of a data breach and minimize the harm should a breach occur.

Far more needs to be done to safeguard the personal information American consumers. Harmful data breaches have become commonplace for American consumers and action must be taken to prevent future breaches and to protect consumers in the event of a data breach.

---

[10] UMD Data Breach, University of Maryland, http://www.umd.edu/datasecurity/.; Janet Gilmore, *Campus Alerting 80,000 Individuals to Cyberattack*, Berkley News, Feb. 26, 2016, http://news.berkeley.edu/2016/02/26/campus-alerting-80000-individuals-to-cyberattack/; Natasha Singer, *Data Security Is a Classroom Worry, Too*, New York Times, Jun. 22, 2013, http://www.nytimes.com/2013/06/23/business/data-security-is-a-classroom-worry-too.html.

[11] Equifax and What Congress Should Do Next

[12] *See e.g.* Video Privacy Protection Act of 1988, Pub. L. No. 100-618, 102 Stat. 3195 (Nov. 5, 1988), codified at 18 U.S.C. 2710 (stating that businesses must, "d]estroy personally identifiable information as soon as practicable, but no later than one year from the date the information is no longer necessary for the purpose for which it was collected . . . ."

[13] *See, e.g.*, Reply Comments of EPIC, *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services* 11-12, WC Docket NO. 16-106 (July 6, 2016), https://epic.org/apa/comments/EPIC-FCC-Privacy-NPRM-Reply-Comments-07.06.16.pdf; Comments of EPIC, Request for Information: Big Data and the Future of Privacy (April 4, 2014), https://epic.org/privacy/big-data/EPIC-OSTP-Big-Data.pdf; Brief of Amicus Curiae Electronic Privacy Information Center in Support of Respondent, *City of Ontario v. Quon*, 560 U.S. 746 (2010), https://epic.org/privacy/quon/Quon_Brief_Draft_final.pdf.

[14] *EPIC Online Guide to Practical Privacy Tools,* EPIC, https://www.epic.org/privacy/tools.html.

We ask that this letter and the accompanying article be entered in the hearing record. EPIC looks forward to working with the Committee 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/ *Kim Miller*
Kim Miller
EPIC Policy Fellow

Attachment

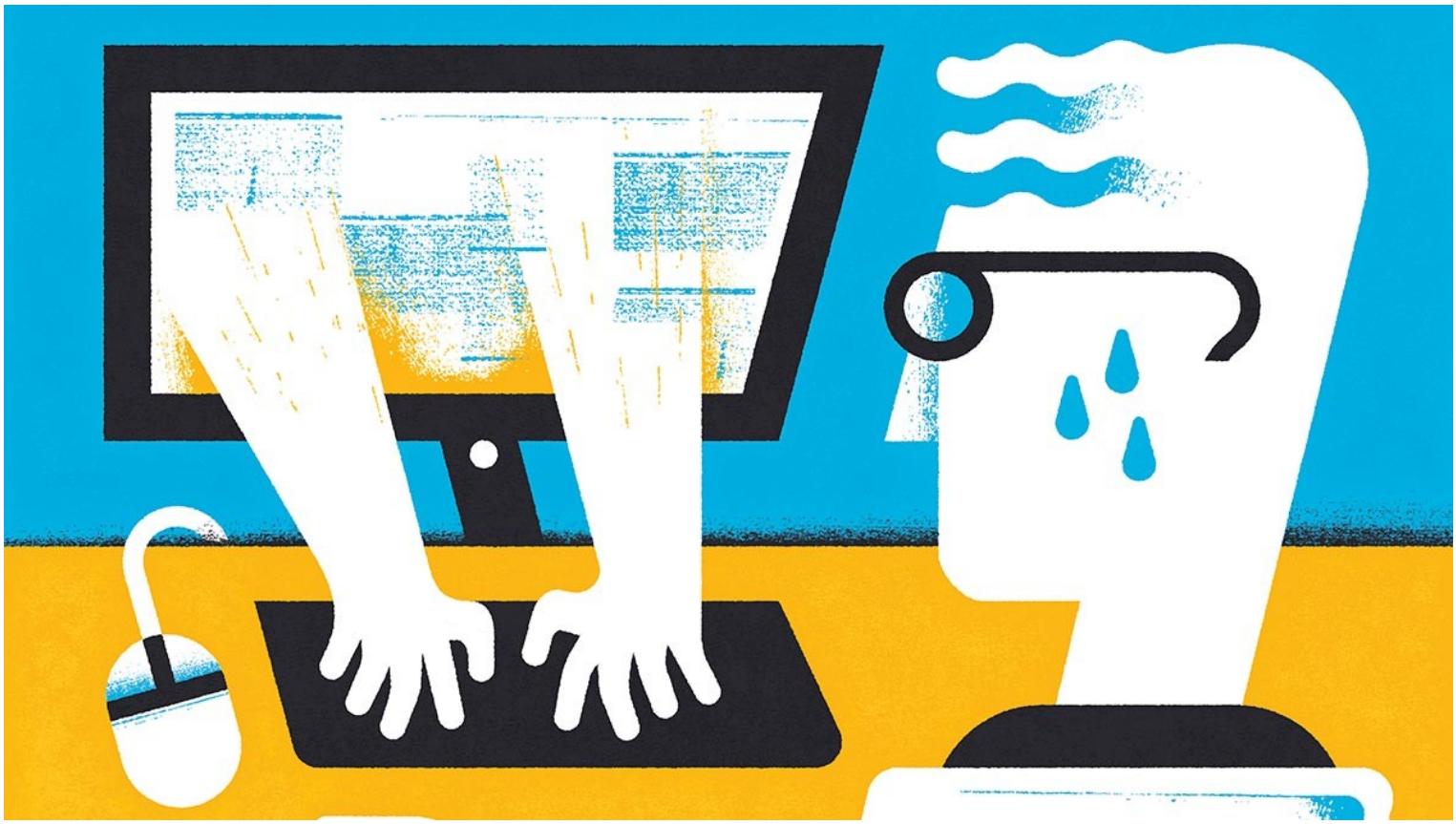
Harvard Business Review

SECURITY & PRIVACY

Equifax, the Credit Reporting Industry, and What Congress Should Do Next

by Marc Rotenberg

SEPTEMBER 20, 2017



Even for the experts, the recent data breach at Equifax was staggering. The data that undergirds the credit records of 143 million consumers was compromised. Social Security numbers, dates of birth, and drivers' license records are used to authenticate identity. It is not difficult to change a credit card number, but changing Social Security numbers and birth dates is a whole different matter. Data breaches are on the rise in the United States. It's time for Congress to act. Why does this require action by Congress? There are at least five major reasons that the private sector cannot handle this issue

on its own:

Identity theft is one of the top consumer complaints. The Federal Trade Commission reported 399,225 cases of identity theft in the United States in 2016. Of that number, 29% involved the use of personal data to commit tax fraud. More than 32% reported that their data was used to commit credit card fraud, up sharply from 16% in 2015. A 2015 report from the Department of Justice found that 86% of the victims of identity theft experienced the fraudulent use of existing account information, such as credit card or bank account information. The same report estimated the cost at $15.4 billion.

Current measures do not work. When data breaches occur, consumers are urged to check a website to see if they were affected. They are offered time-limited credit monitoring services and encouraged to check credit reports for stray transactions. This protocol has done little to stem the rise in data breaches and identity thefts in the United States. And because most state laws about data breach notification fail to establish strict time limits, consumers learn that their data was stolen long after the crime occurred.

Equifax pulled that script, waited more than a month to notify the public of the breach, and then set up a website to provide information to consumers. Multiple problems ensued. The company asked for still more personal data (the last six of people's Social Security numbers). The site didn't work, and the company tried to use the interaction as an opportunity to disclaim liability.

This is not a workable business response or sensible public policy. Consumers should not carry the burden when data breaches occur. And the lax response imperils global data flows.

Data breaches could hurt U.S. trade with Europe. The announcement of the Equifax breach came the week before top officials from the European Union arrived in the United States to undertake the first annual review of "Privacy Shield," an EU-U.S. data trade agreement that permits the transfer of personal data of European consumers to U.S. firms outside normal legal channels. The agreement is premised on the belief that the United States will provide sufficient data protection for the personal data obtained from across the Atlantic. Privacy Shield is necessary, as the White House explained last week, to "enable the free flow of information, which sustains the nearly $1 trillion dollars in goods and services trade across the Atlantic, and even more around the globe." But Privacy Shield also faced fierce opposition from consumer groups on both sides of the Atlantic, leading European privacy officials, and now possibly European politicians. BBC reported that about 400,000 Britons were hit by the Equifax breach. Politicians in the U.S. and the EU will be looking for solutions, but small measures will not solve the problem.

Social Security numbers have been asked to do too much. It is time to end the use of the Social Security numbers (SSN) as a general-purpose identifier. Today American consumers experience record levels of identity theft and financial fraud, largely traced to the unregulated use of SSN in the private sector. The numbers contribute to insecure password schemes (many accounts still default to the last four digits of the SSN), incorrect identification, and secretive profiling and decision making. The SSN was never intended to be used this way, and we now live with consequences. Future uses of the SSN in the private sector should take place only with legal authority, and Congress also needs to take responsibility. If Congress does not authorize the use of the SSN, a number created by the federal government, then the number should not be used for commercial transactions.

The credit reporting industry is fundamentally flawed. The essential problem with the credit reporting industry is that it does not work. In the best of circumstances, the information provided by data brokers to businesses is inaccurate, incomplete, or out of date. In some circumstances individuals are wrongfully denied jobs, housing, and credit. In other circumstances, the data contributes to identity theft. In almost all circumstances, consumers are left in the dark about the collection and use of their personal data by others.

Next Steps

Reforms should not just fix these issues but also aim to transform the industry for the better. Credit reporting agencies should provide free, life-long credit monitoring services. Next, credit reporting agencies should change the default on access to credit reports by third parties. Instead of the current setting, which allows virtually anyone to pull someone's credit report, credit reporting agencies should establish a credit freeze for all disclosures. Consumers would still retain the ability to disclose report when they choose to do so. Credit reporting agencies should also send a free annual report to all credit card holders, indicating in full the information about consumers that was collected, to whom it was provided, and for what purpose it was used. Current laws allow consumers access to free credit reports, but the process is cumbersome, and few consumers take advantage. A rationalized market would help ensure that consumers have as much information as possible about the use of their personal data by others.

The credit reporting industry is an easy target. It is well known and its problems are widely documented. But the reality is that consumer scoring is a rapidly growing field, with companies now scraping websites to gather profile data that is sold to third parties. Many of the errors familiar from the 50-year history of credit reports — inaccuracy, discrimination — are compounded in the field of consumer scoring. New principles for data protection such as data minimization and algorithmic transparency will be needed for modern regulatory frameworks.

Consumers and businesses face a real crisis. The risk of increased identity theft resulting from the breach is real. Equifax

created this particular problem, and it should be responsible for the clean-up. But this problem is about much more than Equifax.

More transparency ensures more accountability — that is the essential paradox of privacy protection. But consumer privacy is not a goal achieved by markets. It must be mandated by Congress. After all, consumers are also voters.

Marc Rotenberg is President of the Electronic Privacy Information Center (EPIC) in Washington, DC. He frequently testifies before Congress on emerging privacy issues.

This article is about SECURITY & PRIVACY

⊕ **FOLLOW** THIS TOPIC

Related Topics: DATA