epic.org | ELECTRONIC PRIVACY INFORMATION CENTER

Testimony and Statement for the Record of

Marc Rotenberg
President, EPIC
Adjunct Professor, Georgetown University Law Center

Hearing on Consumer Data Security and the Credit Bureaus

Before the

Committee on Banking, Housing, and Urban Affairs
United States Senate

October 17, 2017
538 Dirksen Senate Office Building
Washington, DC, 20002

Mister Chairman and Members of the Committee, thank you for the opportunity to testify today concerning consumer data security and the credit bureaus. My name is Marc Rotenberg. I am President of the Electronic Privacy Information Center ("EPIC"). EPIC is an independent nonprofit research organization in Washington, DC, established in 1994 to focus public attention on emerging privacy and civil liberties issues. I have also taught information privacy law at Georgetown University Law Center since 1990 and I am the author of several leading books on privacy law.[1] I testified before this Committee in 2011 following the spate of data breaches in the financial services sector.[2] And in a recent article for the *Harvard Business Review*, I outlined several steps that Congress could take in response to the Equifax data breach.[3]

I will say at the outset that the Equifax data breach is one of the most serious in the nation's history, on par with the breach at the Office of Personnel Management in 2015 that impacted 22.5 million federal employees, their friends and family members. The Equifax breach poses enormous challenges to the security of American families, as well as our country's national security. Privacy, more precisely described as "data protection," is no longer simply about the concern that large companies misuse personal data. Today our country is facing cyber attacks from foreign adversaries and it is the personal data stored by companies that is the target. When these companies engage in lax security practices or freely disclose consumer data without consent, they are placing not only consumers, but also our nation at risk.

There is no simple solution to these challenges, but in my testimony today I will outline the steps that I believe Congress could take to minimize the risk flowing from this breach and address the risk of future breaches in the data broker industry. In brief, current laws do not protect consumers. Legislation should (1) give consumers greater control of their personal data held by others; (2) limit the use of the Social Security Number in the private sector; (3) minimize the collection of personally identifiable information; (4) improve breach notification; and (5) change the defaults in the credit reporting industry with (a) default credit "freezes" that give consumers opt-in control over the release of their credit report, (b) free, routine monitoring services, and (c) free access at any time for any purpose to a consumer who wants to see the complete contents of a credit report or other similar information product made available for sale.

---

[1] ANITA ALLEN AND MARC ROTENBERG, PRIVACY LAW AN SOCIETY (West 2016); MARC ROTENBERG, THE PRIVACY LAW SOURCEBOOK: UNITED STATES LAW, INTERNATIONAL LAW, AND RECENT DEVELOPMENTS (EPIC 2016); MARC ROTENBERG, ET AL, PRIVACY AND THE MODERN AGE: THE SEARCH FOR SOLUTIONS (The New Press 2015).

[2] *Cybersecurity and Data Protection in the Financial Services Sector: Hearing Before the S. Comm. on Banking, Housing, and Urban Affairs*, 112th Cong. (2011) (statement of Marc Rotenberg, Exec. Dir., EPIC), https://epic.org/privacy/testimony/EPIC_Senate_Banking_Testimony%20_6_21_11.pdf.

[3] Marc Rotenberg, *Equifax, the Credit Reporting Industry, and What Congress Should Do Next*, Harv. Bus. Rev. (Sept. 20, 2017), https://hbr.org/2017/09/equifax-the-credit-reporting-industry-and-what-congress-should-do-next.

I. The Implications of the Equifax Breach

A. This breach was unprecedented in scope

The Equifax data breach is one of the most significant in the history of the United States. Over 145 million American consumers were impacted.[4] More than four months passed from the time the Equifax failed to install critical software updates till the time the time the problem was addressed. And the data that was disclosed is precisely the information that individuals rely upon to open bank accounts, get car loans, seek employment, buy cellphones, and even issue checks online. The data included:

- Names
- Social Security Numbers
- Birth Dates
- Addresses, and
- Driver's License Numbers.[5]

This data is a gold mine for identity thieves. The widespread availability of this personal data poses an ongoing risk to American families and creates problems for those who suffer identity theft that will take months, if not years, to resolve.

The Equifax breach also has implications for U.S. trade relations. According to the Canadian Broadcast Corporation, the data of 100,000 Canadians was seized in the breach.[6] The British Broadcasting Corporation reported that 400,000 UK consumers were affected by the Equifax breach.[7] Equifax has since stated that 15,200,000 million UK consumers were impacted by the breach.[8] And all of this at a time when foreign government are carefully scrutinizing U.S. data protection to determine to determine whether it is safe to transfer personal data to the United States. Equifax has given other countries good reason to fear their data being entrusted to U.S. companies. That could harm U.S. trade.

B. Equifax was at fault

Equifax is clearly responsible this breach. The company was notified of the vulnerability in its software but failed to make the required fixes. Hackers accessed the Equifax database by

---

[4] Equifax, *Equifax Announces Cybersecurity Incident Involving Consumer Information* (Sept. 7, 2017), https://investor.equifax.com/tools/viewpdf.aspx.
[5] *Id*.
[6] Matthew Braga, *100,000 Canadian victims: What We Know About the Equifax Breach—and What We Don't*, CBC News (Sept. 19, 2017), http://www.cbc.ca/news/technology/equifax-canada-breach-sin-cybersecurity-what-we-know-1.4297532.
[7] *Equifax Says Almost 400,000 Britons hit in Data Breach*, BBC News (Sept. 15, 2017), http://www.bbc.com/news/technology-41286638.
[8] Equifax., *Equifax Ltd (UK): UPDATE REGARDING THE ONGOING INVESTIGATION INTO US CYBER SECURITY INCIDENT* (Oct. 10, 2017), https://www.equifax.co.uk/about-equifax/press-releases/en_gb/-/blogs/equifax-ltd-uk-update-regarding-the-ongoing-investigation-into-us-cyber-security-incident.

exploiting a known security vulnerability.[9] The Apache Software Foundation issued a statement in March announcing the vulnerability, and the patch was made available the same day.[10] The Department of Homeland Security also contacted the three credit reporting agencies back in March to notify them of the vulnerability. Yet Equifax left the vulnerability unpatched until July 29. By that time the attackers had already seized millions of records over several months.

It is also worth emphasizing that Equifax chose to collect this data on American customers – American consumers did not choose to provide their personal data to Equifax. Also, Equifax pursued a security strategy that allowed a single point of failure to permit the breach of more than half of the nation's credit reports.

Equifax's response to the breach also demonstrated the company's incompetence and indifference to data security. Equifax created a separate domain -- "equifaxsecurity2017.com" — where consumers were required to enter their name and the last six digits of their social security number to find out if their information was compromised. The domain was not registered to Equifax and was running on WordPress, causing many browsers to flag it as a phishing threat.

To demonstrate how easily this domain could be spoofed, a developer bought the domain "securityequifax2017.com" and made it look exactly like the real Equifax support page.[11] The Equifax even tweeted a link of the fraudulent website, thinking it was their own.

Security researchers later discovered that Equifax's website has also been hacked, and contained false Adobe Flash download links that trick users into downloading malware that displays unwanted ads online.[12] Furthermore, consumers who contacted Equifax to freeze their credit were given PINs to use when they wanted to unfreeze their credit. These pins were based on the time and date of the freeze, making them easier to guess.[13] These actions after the breach reveal how poorly prepared the company was to assist consumers. The company's efforts to mitigate damage caused by the breach have exposed millions of Americans to even more risk.

C. Equifax breach increases the likelihood of identity theft in the United States

The Equifax breach will cause unprecedented harm to consumers. When hackers get access to credit card numbers they can rack up fraudulent charges, but consumers are able to cancel their credit cards and get new numbers. By contrast, consumers cannot change their social

---

[9] The Apache Software Foundation Blog, *MEDIA ALERT: The Apache Software Foundation Confirms Equifax Data Breach Due to Failure to Install Patches Provided for Apache® Struts™ Exploit* (Sept. 14, 2017), https://blogs.apache.org/foundation/entry/media-alert-the-apache-software.

[10] *Id.*

[11] Alfred NG, *Equifax Sends Breach Victims to Fake Support Site*, CNET (Sept. 20, 2017), https://www.cnet.com/news/equifax-twitter-fake-support-site-breach-victims/.

[12] Dan Goodin, *Equifax Website Borked Again, This Time to Redirect to Fake Flash Update*, ArsTechnica (Oct. 12, 2017), https://arstechnica.com/information-technology/2017/10/equifax-website-hacked-again-this-time-to-redirect-to-fake-flash-update/.

[13] Ron Lieber, *After Equifax, Here's Your Next Worry: Weak PINs*, N.Y. Times (Sept. 10, 2017), https://www.nytimes.com/2017/09/10/your-money/identity-theft/equifax-breach-credit-freeze.html?rref=collection%2Fbyline%2Fron-lieber.

security numbers or dates of birth. Equifax's victims are exposed to ongoing identity theft and fraud, and the full effects of the damage will not be known for years.

Identity theft is an enormous problem for consumers. The Federal Trade Commission reported 399,225 cases of identity theft in the United States in 2016.[14] 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.[15] The same report estimated the cost to the U.S. economy at $15.4 billion.

Identity theft can completely derail a person's financial future. Criminals who have gained access to others' personally identifiable information can open bank accounts and credit cards, take out loans, and conduct other financial activities using someone else's identity. Identity theft has severe consequences for consumers, including:[16]

- Being denied of credit cards and loans
- Being unable to rent an apartment or find housing
- Paying increased interest rates on existing credit cards
- Having greater difficulty getting a job
- Suffering severe distress and anxiety

II. The Equifax Breach Underscores the Need for Reform

The credit reporting industry is in urgent need of reform. An industry that collects the most sensitive data of Americans and has such a great impact on the U.S. economy must use state of the art security measures and must give consumer control over the personal data. Instead, credit bureaus cut corners on security, capture the upside value of selling credit reports, and transfer the risk to consumers for breaches and errors. As companies increasingly rely on complex consumer profiling techniques, credit bureaus have amassed vast amounts of personal data. Without comprehensive legislation, the data breach problem will only get worse.

A. Data breaches are an epidemic in the United States

The scope of the data breach problem extends well beyond Equifax. Data breaches are occurring more frequently across a number of industries. According to the Identity Theft Resource Center, data breaches in the United States increased by 40 percent in 2016 to a record

---

[14] Fed. Trade Comm'n, *FTC Releases Annual Summary of Consumer Complaints* (March 3, 2017), https://www.ftc.gov/news-events/press-releases/2017/03/ftc-releases-annual-summary-consumer-complaints.
[15] Erika Harrell, Bureau of Justice Statistics, *Victims of Identity Theft, 2014* (Sept. 27, 2015), https://www.bjs.gov/index.cfm?ty=pbdetail&iid=5408.
[16] Identity Theft Resource Center, *Identity Theft: The Aftermath 2017*, http://www.idtheftcenter.org/images/page-docs/Aftermath2017Finalv1.pdf.

high of 1,093.[17] As companies collect more data, the risk of identity theft is almost certain to increase.

- The 2013 Yahoo breach, in which hackers stole names, birth dates, phone numbers, and passwords, is now estimated to have impacted all 3 billion users, making it the largest data breach on record[18]

- In 2015, a data breach at the Office of Personnel Management compromised the personal data, including biometric identifiers, of more than 20 million people, many of them with security clearances.[19]

- Recent data breaches have affected Chipotle, Home Depot, and Target, impacting over 100 million stolen credit card numbers combined.[20]

- Data breaches have also impacted large banks, educational institutions, healthcare providers, and many other businesses.[21]

Data breaches in the credit reporting industry pose an enormous threat to consumers. Credit reporting agencies maintain an extraordinary amount of personal data, including Social Security numbers, birthdates, home addresses, telephone numbers, and driver's license records—information that is the holy grail for identity thieves.

B. Consumers lack control over their credit reports

Despite these risks, consumers cannot protect themselves. The relationship between the credit reporting industry and the consumer is skewed. The industry was built to serve the companies that collect and use consumer information and not the consumers themselves. Businesses have easy access to credit reports while consumers do not. By law, consumers are

---

[17] Identity Theft Resource Center, *Data Breaches Increase 40 Percent in 2016, Finds New Report* (Jan. 19, 2017), http://www.idtheftcenter.org/2016databreaches.html.

[18] Nicole Pelroth, *All 3 Billion Yahoo Accounts Were Affected by 2013 Attack*, New York Times (Oct. 3, 2017), https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html.

[19] Ellen Nakashima, *Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say*, Wash. 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/.

[20] 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 Million Card Breach Bigger Than Target's*, Wall Street J. (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.

[21] Greg Farrell & Patricia Hurtado, *JPMorgan's 2014 Hack Tied to Largest Cyber Breach Ever*, Bloomberg (Nov. 10, 2015), https://www.bloomberg.com/news/articles/2015-11-10/hackers-accused-by-u-s-of-targeting-top-banks-mutual-funds; Brendan Pierson, *Anthem to Pay Record $115 Million to Settle U.S. Lawsuits Over Data Breach*, Reuters (June 23, 2017), https://www.reuters.com/article/us-anthem-cyber-settlement/anthem-to-pay-record-115-million-to-settle-u-s-lawsuits-over-data-breach-idUSKBN19E2ML; UMD Data Breach, University of Maryland, http://www.umd.edu.datasecurity/.

entitled to only one free credit report per year, and the process of obtaining one is cumbersome.[22] Consumers have no control over what information credit reporting agencies collect. Information is often out of date, incomplete, or inaccurate, and it is often impossible for consumers to correct inaccurate information.[23] Consumers are then wrongfully denied jobs, housing, and credit as a result. In these circumstances, consumers are almost always left in the dark about how their data was used.

Under current law and industry practices, when data breaches occur, consumers bear the burden. Consumers only learn of the breach once the company decides to notify the public, and then must take costly steps to obtain a credit freeze or credit monitoring services.[24] And because consumers cannot choose which companies collect their data, they have no control over how vulnerable their information is to identity thieves. In sum, the current model is broken, and only Congress can fix it.[25]

C. Consumer profiling is growing more complex and lacks transparency

An invisible system of consumer profiling has emerged.[26] We now face the specter of a "scored society" where consumers do not have access to the most basic information about how they are evaluated.[27] Data brokers now use secret algorithms to build profiles on every American citizen whether they have allowed their personal data to be collected or not.[28] These secret algorithms can be used to determine the interest rates on mortgages and credit cards, raise consumers' insurance rates, or even deny people jobs.[29] Data brokers even scrape social media and score consumers based on factors such as their political activity on Twitter.[30]

In one recent complaint to the Federal Trade Commission, EPIC highlighted the practice of the secret scoring of young athletes.[31] It may seem to odd to think that an activity such as high school athletics is now being taken over by proprietary algorithms, but that is in fact the case. Once you could say that a runner completed a mile in 4:28, a high school basketball player shot 92% from the line, or a softball player hit .352 for the season. Now it is the secret scoring of young athletes that could determine their future.

---

[22] Fed. Trade Comm'n., *Free Credit Reports*, March 2013, https://www.consumer.ftc.gov/articles/0155-free-credit-reports.
[23] *Id*.
[24] Fed. Trade Comm'n, *Credit Freeze FAQs* (2017), https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs.
[25] Bruce Schneier, *Don't Waste Your Breath Complaining to Equifax About Data Breach*, CNN, Sep. 11, 2017, http://www.cnn.com/2017/09/11/opinions/dont-complain-to-equifax-demand-government-act-opinion-schneier/index.html.
[26] *Id*.
[27] Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 Wash. L. Rev. 1 (2014).
[28] *Id*.
[29] *Exploring the Fintech Landscape: Hearing Before the S. Comm. on Banking, Housing, and Urban Affairs*, 115th Cong. 7 (2017) (written testimony of Frank Pasquale, Professor of Law, University of Maryland).
[30] *Id*.
[31] EPIC, *EPIC Asks FTC to Stop System for Secret Scoring of Young Athletes* (May 17, 2017), https://epic.org/2017/05/epic-asks-ftc-to-stop-system-f.html.

Determinations about whether we get a job, a home, or an athletic scholarship should not be left to the "secret judgments of software," especially when this type of machine learning can lead to discrimination.[32] We not only lack knowledge of the methods being used to score us, but we do not even know what underlying information about us is being collected. For example, EPIC just filed an amicus brief in a case involving a company that scrapes data from user profiles on LinkedIn to create scores to evaluate "flight risk."[33] The consumer scoring industry -- not just the credit reporting agencies -- needs oversight, accountability, and transparency.[34]

III. Next Steps to Protect Consumers Following the Equifax Breach

In the wake of the Equifax breach, immediate action should be taken to reform not only the credit reporting industry, but also to address the broader problem of secret profiling and mishandling of consumers' personal data. It is time to change the defaults and time to put consumers back in control of both their credit reports and their personal information. Consumers must have free and easy access to their credit information, and control over when and how that information is disclosed. Companies collecting consumers' personal data must establish effective safeguards, including requirements for prompt disclosure of any data breach. Congress should end the use of the social security number as a general-purpose identifier. And Congress should promote the use of innovative technology to minimize the collection of personal data.

A. Reform the industry by giving consumers control over their credit reports

The essential problem with the credit reporting industry is that it does not work. Consumers have no control over the collection and use of their credit reports and bear all the risk when credit reporting agencies mishandle their personal information. Data brokers operate in the shadows and consumers are left in the dark. That structure is backward. Consumers should have free access to their credit information and, by default, no credit report should be released to a third party without the consumer's express authorization.

There are already several commonsense proposals that the Congress should enact into law:

Free Credit "Freezes" and "Thaws" (Change the default for report disclosure to "opt-in")

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, with free and easy access for consumers who wish to disclose their report for a specific purpose. A credit freeze is one of the only mechanisms available to prevent "new account identity theft" before it happens.[35] But only four states (Indiana, Maine, North Carolina, and South Carolina) mandate

---

[32] FRANK PASQUALE, THE BLACK BOX SOCIETY 8 (2015); Citron & Pasquale, *supra*.
[33] EPIC, *hiQ Labs, Inc. v. LinkedIn Corp.*, https://epic.org/amicus/cfaa/linkedin/.
[34] Citron & Pasquale, *supra*, at 5.
[35] *See* U.S. PIRG, *Security Freeze and Identity Theft Tips*, http://uspirg.org/sites/pirg/files/resources/Security%20Freeze%20and%20Identity%20Theft%20Tips.pdf.

free consumer access to credit freezes and thaws, while four additional states "provide free freezes but charge for thaws."[36] This means that "[a]pproximately 158 million consumers between 18-65 in 42 states and DC must pay a fee to get credit freezes."[37]

Provide Free Monitoring and Easy Access to Credit History

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. Instead, Equifax and other credit reporting agencies profit from the very problems they create. The Consumer Financial Protection Bureau also fined Equifax and TransUnion earlier this year after finding that the companies "lured consumers into costly recurring payments for credit-related products with false promises."[38] Credit reporting agencies should provide life-long credit monitoring services to consumers at no cost. Some credit card companies already offer similar services for free.[39] The credit other reporting agencies should do so as well.

Mandatory Disclosure of Secret Scores and Algorithms

Congress should move quickly to address the risks to consumers in the credit reporting industry. But the problems in the credit reporting industry arise in other industries. We face the specter of a "scored society" where consumers don't have access to the most basic information about how they are evaluated.[40] "Algorithmic transparency" is key to accountability.[41] Absent rules requiring the disclosure of these secret scores, lists, and the underlying data and algorithms upon which they are based, consumers will have no way to even know, let alone solve, these problems.

B. Improve Breach Notification

The epidemic of data breaches, and failure of companies to be held accountable, cannot continue. Identity theft has reached an unprecedented level, yet the companies that amass troves of personal data expect consumers to bear the costs of breaches. After a data breach occurs, companies such as Equifax urge consumers to check a website to find out whether they were

---

[36] U.S. PIRG, *Interactive Map Shows Consumers in 42 States Have No Access to Free Credit Freezes* (Oct. 2, 2017), https://uspirg.org/news/usp/interactive-map-shows-consumers-42-states-have-no-access-free-credit-freezes.
[37] *Id*.
[38] Consumer Fin. Prot. Bureau, *CFPB Orders TransUnion and Equifax to Pay for Deceiving Consumers in Marketing Credit Scores and Credit Products* (Jan. 3, 2017), https://www.consumerfinance.gov/about-us/newsroom/cfpb-orders-transunion-and-equifax-pay-deceiving-consumers-marketing-credit-scores-and-credit-products/.
[39] *See, e.g.*, Discover, *Social Security Alerts* (2017), https://www.discover.com/credit-cards/member-benefits/security/ssn-newaccount-alerts/.
[40] *Id*.
[41] EPIC, *Algorithmic Transparency,* https://epic.org/algorithmic-transparency/.

affected.[42] But even these vague warnings come weeks or months after the breach has occurred.[43] That is not a workable business response or sensible public policy.

It has become clear that these companies cannot effectively police themselves. Congress should set national, baseline standards to limit the damage caused by data breaches.

Federal Baseline Data Breach Notification Standard

At a bare minimum, the Equifax breach underscores the need for a baseline federal data breach notification standard for all companies that store personal information.[44] The only federal law with a breach notification rule is the Health Insurance Portability and Accountability Act, which only applies to protected health information.[45] Florida currently has one of the most comprehensive data breach laws, providing a mandatory 30-day notification rule, a broad scope, and proactive requirements for reasonable data protection measures.[46] A federal baseline notification standard should go even further, requiring immediate and efficient notification of impacted consumers, regulators, and the public.[47] Companies are increasingly interacting with consumers on social media and via automated text and e-mail messages, so it is reasonable to expect that companies can notify consumers within 48-72 hours of a breach.

Reasonable Data Security Measures

Prompt breach notifications are necessary to ensure that consumers and regulators can quickly deal with a data breach after it happens. But more needs to be done to prevent these breaches from happening in the first place. For example, the Florida Information Protection Act requires that companies collecting consumer data "take reasonable measures to protect and

---

[42] These post-breach websites can also create new risks to consumers. *See, e.g.*, Merrit Kennedy, *After Massive Data Breach, Equifax Directed Customers to Fake Site*, NPR (Sept. 21, 2017), http://www.npr.org/sections/thetwo-way/2017/09/21/552681357/after-massive-data-breach-equifax-directed-customers-to-fake-site.

[43] *See, e.g.*, Michael Hiltzik, *Here Are All The Ways The Equifax Data Breach Is Worse Than You Can Imagine*, L.A. Times (Sept. 8, 2017), http://www.latimes.com/business/hiltzik/la-fi-hiltzik-equifax-breach-20170908-story.html.

[44] There are currently breach notification laws in "[f]orty-eight states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands." Nat'l Conference of State Legislators, *Security Breach Notification Laws* (Apr. 12, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx#1. *See also* Steptoe & Johnson LLP, *Comparison of US State and Federal Security Breach Notification Laws* (Sept. 1, 2017), https://www.steptoe.com/assets/htmldocuments/SteptoeDataBreachNotificationChart2017.pdf.

[45] 45 C.F.R. §§ 164.400–414. *See* Steptoe, *supra* at 202–08. The Graham-Leach-Bliley Act "Interagency Guidelines" also discuss consumer notice, but the rules do not contain a requirement that notice be given within a specific time period. *See* 12 C.F.R. pt. 224, app. F (Supp. A 2014); 70 Fed. Reg. 15,736 (2005).

[46] EPIC, *State Data Breach Notification Policy* (2017), https://epic.org/state-policy/data-breach/.

[47] *"Discussion Draft of H.R.__, A Bill to Require Greater Protection for Sensitive Consumer Data and Timely Notification in Case of Breach," Hearing before the Subcomm. on Commerce, Manufacturing, and Trade of the H. Comm. on Energy and Commerce*, 112th Cong. (testimony and statement for the record of Marc Rotenberg, Exec. Dir., EPIC) https://epic.org/privacy/testimony/EPIC_Testimony_House_Commerce_6-11_Final.pdf; *see also "H.R. 2221, the Data Accountability and Trust Act and H.R. 1319, the Informed P2P User Act," Hearing before the Subcomm. on Commerce, Trade, and Consumer Prot. of the H. Comm. on Energy and Commerce*, 111th Cong. (2009) (testimony and statement for the record of Marc Rotenberg, Exec. Dir., EPIC), https://epic.org/linkedfiles/rotenberg_house_ctcp2221_1319.pdf.

secure data in electronic form containing personal information."[48] Companies that collect and store sensitive consumer data are in the best position to prevent data breaches, and they should be held liable when they fail to adopt reasonable security measures.[49] This is especially important because the Equifax hack and other major data breaches caused by known vulnerabilities are entirely preventable.[50]

Elimination of Consumer Arbitration Waivers

The most effective way to improve data security is to establish a private right of action for consumers who have suffered a breach of their personal data. This provides a specific remedy for a specific harm. But Equifax did the exact opposite. In response to the data breach, the company tried to trick consumer into an arbitration agreement, guaranteeing that there would be few legal remedies for consumers following the breach.[51] The Consumer Financial Protection Bureau ("CFPB") recently banned arbitration clauses in consumer financial contracts because class action waivers make it prohibitive for any consumers to obtain relief.[52] Credit reporting agencies and other financial institutions should be prohibited from using these arbitration agreements to block consumer actions for breach, improper disclosure, or misuse of their personal data. And a breach of personal data should be sufficient harm to provide a cause of action.

Expansion of Gramm-Leach-Bliley Security Rules

The existing data security requirements for consumer-facing financial institutions should extend to credit reporting agencies and other companies that sell consumer profiles. The Gramm-Leach-Bliley Act already provides for oversight of financial institutions' privacy practices by seven regulatory agencies, but the current regime fails to address credit reporting agencies.[53] Specifically, although the Dodd-Frank Act transferred authority over certain privacy provisions to the CFBP, the law did not transfer regulatory authority to establish data security guidelines.[54]

---

[48] Fla. Stat. § 501.171(2) (2017). *See* EPIC, *State Data Breach Notification Policy* (2017).
[49] Brief of Amicus Curiae EPIC in Support of Appellants, *Storm v. Paytime*, No. 15-3690, at 25–30 (3d Cir. filed Apr. 18, 2016), https://epic.org/amicus/data-breach/storm/EPIC-Amicus-Storm-Paytime.pdf.
[50] *See* Lily Hay Newman, *Equifax Officially Has No Excuse*, Wired (Sept. 14, 2017), https://www.wired.com/story/equifax-breach-no-excuse/.
[51] Equifax is the most recent, but not the only, company guilty of forcing consumers into arbitration against their interests. *See* David Lazarus, *The Real Outrage Isn't Equifax's Arbitration Clause—It's All The Others*, L.A. Times (Sept. 12, 2017), http://www.latimes.com/business/lazarus/la-fi-lazarus-equifax-arbitration-clauses-20170912-story.html.
[52] 12 C.F.R. 1040; Consumer Fin. Prot. Bureau, *CFPB Study Finds That Arbitration Agreements Limit Relief For Consumers* (Mar. 10, 2015) https://www.consumerfinance.gov/about-us/newsroom/cfpb-study-finds-that-arbitration-agreements-limit-relief-for-consumers/.
[53] 15 U.S.C. § 6801; *see* 79 Fed. Reg. 37166 (2014) ("Section 501(b) of the Gramm-Leach-Bliley Act (GLB Act) [1] requires the Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and Office of Thrift Supervision (the Agencies), as well as the National Credit Union, the Securities and Exchange Commission, and the Federal Trade Commission, to establish appropriate standards for the financial institutions subject to their respective jurisdictions relating to the administrative, technical, and physical safeguards for customer records and information.").
[54] *Id*.

As it stands, the CFPB can only bring enforcement actions based on a company's affirmative misrepresentations about data security practices.[55] Given that credit reporting agencies hold more sensitive personal data than many of the other financial institutions combined, it makes little sense for those companies to be exempt from the rules.

C. Limit the use of the Social Security Number by private companies

Social security numbers have been asked to do too much. They were never meant to be used as an all-purpose identifier.[56] The unregulated use of the social security number in the private sector has contributed to record levels of identity theft and financial fraud.[57] The recent Equifax breach illustrates this problem, as the social security numbers of nearly half of all Americans were stolen. The solution is not, however, to replace the social security number with a national biometric identifier that raises serious privacy and security risks.[58] Instead, we suggest that the best way to minimize the problem of identity theft is to reduce the industry's reliance on the social security number as a personal identifier.[59] Congress should prohibit the use of the social security number in the private sector without explicit legal authorization.

D. Promote innovative technology to minimize the collection of personal data

The focus should now turn to how companies can minimize the collection of personal data and maximize consumer privacy and control. There are already initiatives to improve privacy protections in the field of data science, and these efforts could be adopted and further developed by the companies responsible for protecting consumer data.[60]

The newly-formed Commission on Evidence-Based Policymaking recently issued a report that urged the adoption of privacy enhancement and preservation techniques, including "differential privacy" algorithms that can be used to glean information from data sets without revealing personal information.[61] We have also seen increasingly secure methods of two-factor authentication that can minimize the risk of phishing and other attempts to compromise personal

---

[55] *See, e.g.*, Consumer Financial Protection Bureau, *CFPB Takes Action Against Dwolla for Misrepresenting Data Security Practices* (Mar. 2, 2016), https://www.consumerfinance.gov/about-us/newsroom/cfpb-takes-action-against-dwolla-for-misrepresenting-data-security-practices/.

[56] Marc Rotenberg, *The Use of the Social Security Number as a National Identifier*, 22 *Comp. & Soc'y* nos. 2, 3, 4 (Oct. 1991).

[57] Marc Rotenberg, *Equifax, The Credit Reporting Industry, And What Congress Should Do Next*, Harv. Bus. Rev., (Sep. 20, 2017).

[58] EPIC, Identity Theft, http://epic.org/privacy/idtheft/ (last visited October 13, 2017)

[59] *"Cybersecurity and Data Protection in the Financial Services Sector," Hearing Before the H. Comm. on Fin. Servs.*, 112th Cong. (2011) (statement of Marc Rotenberg, Exec. Dir., EPIC), https://financialservices.house.gov/uploadedfiles/091411rotenberg.pdf.

[60] *See, e.g.*, Comm. on Nat'l Statistics, Div. of Behavioral and Social Sciences and Education, Nat'l Academies of Science, Engineering, and Medicine, *Combining Data Sources While Protecting Privacy* (National Academies Press 2017); Cynthia Dwork & Aaron Roth, *The Algorithmic Foundations of Differential Privacy*, 9 Found. & Trends in Theoretical Comp. Sci. 211 (2014).

[61] Marc Rotenberg, *Let's Use Government Data to Make Better Policy*, Sci. Am. (Oct. 4, 2017), https://blogs.scientificamerican.com/observations/let-rsquo-s-use-government-data-to-make-better-policy/.

data.[62] Even the consumer-facing financial companies are beginning to develop better mechanisms to enable control and monitoring of accounts, including dedicated applications to limit unauthorized debit card charges.[63] These are the techniques that Equifax and other credit reporting agencies should invest in to limit harm to consumers going forward.

E. Enact baseline privacy legislation and establish a Data Protection Agency

We have urged for many years that the United States update its privacy laws to address the challenges posed by new technologies and new business practices. The United States was once a leader and innovator in privacy protection, but we have now fallen behind many other countries that are seeking to ensure that the rapid adoption of new technologies does not leave them vulnerable to data breach, identity theft, and cyber attack. Certainly, the United States needs to do more.

A good starting point would be to enact the Consumer Privacy Bill of Rights, baseline privacy legislation that would put the responsibilities on companies that collect and use personal data to protect the information they choose to collect. The Consumer Privacy Bill of Rights follows the structure of many privacy laws in the United States and elsewhere. That means it could both harmonize and simplify compliance, and the CPBR could help resolve pending trade disputes with Europe and others about the protections for transborder data flows.

The United States should also establish as Data Protection Agency as has virtually every other advanced economy facing the challenges of the digital age. The current agencies in the United States tasked with protecting consumers and citizens lack the authority and even the personnel to do what needs to be done.

I am aware that these are ambitious recommendations and reach beyond the immediate concerns before this Committee. But U.S. consumers, businesses, and the U.S. government face a genuine threat from the unbounded collection of personal data without adequate legal and technical protections. This data is now the target of foreign adversaries. Two years ago it was the OPM breach. Now it is the Equifax breach. I am reluctant to imagine the consequences for the United States of the next major breach.

---

[62] *See* Letter from Sen. Ron Wyden (D-Ore.), Ranking Member, Comm. on Finance, to Acting Commissioner Nancy A. Berryhill, Social Sec'y Admin. (Oct. 5, 2017) (recommending the use of Universal Second Factor (U2F) tokens to secure social security accounts), https://www.finance.senate.gov/imo/media/doc/100517%20RW%20to%20SSA%20U2F.pdf.

[63] *See, e.g.*, *Ally Card Controls App* (2017) (providing consumers with a way to "turn off" their debit card whenever they are not using it), https://www.ally.com/help/bank/card-controls-app.html. Debit cards pose an acute risk to consumers because consumers are not as well protected from fraudulent charges as they are with credit cards. *See* U.S. PIRG, *Debit Card Facts*, http://www.pirg.org/consumer/banks/debit/debitcards1.htm (last accessed Oct. 13, 2017).

Conclusion

We think it is time now to reform the credit reporting industry and to end the practice of building massive, secretive, profiles on American consumers that are sold to strangers and obtained by hackers, yet are almost impossible for consumers to see or control.

EPIC supports legislation that will give consumers control over their information and establish accountability for companies in the personal data industry. EPIC also support techniques that minimize the collection of personally identifiable information. And we urge the end to the use of the SSN by private companies without legal authority.

It will come as no surprise that consumers across the country favor reform of the credit reporting industry. But I want to end with a story that may be surprising. Earlier this fall, I had the opportunity to speak with leading CEOs from across the country about the Equifax breach. After a brief exchange, the event moderator polled the CEOs. 87% said "the Equifax boss should go" and 95% "want stronger consumer privacy laws."[64]

American consumers favor stronger consumer privacy laws. American businesses favor stronger consumer privacy laws. Now it is time for Congress to Act.

Thank you for the opportunity to testify today. I will be pleased to answer your questions.

---

[64] CEO Summit, Chief Executive Leadership Institute, Yale School of Management, Washington DC (Sept. 9, 2017), http://som.yale.edu/faculty-research-centers/centers-initiatives/chief-executive-leadership-institute/programs/ceo-summit.