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 "Examining the Current Data Security and Breach Notification Regulatory Regime"

Before the

House Committee on Financial Services
Subcommittee on Financial Institutions and Consumer Credit

February 14, 2018
2128 Rayburn House Office Building
Washington, DC, 20002

Mister Chairman and Members of the Committee, thank you for the opportunity to testify today concerning the current data security and breach notification regulatory regime. 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.[1] 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.[2] I testified before this Committee in 2011 following the spate of data breaches in the financial services sector.[3] 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.[4]

Data breaches pose 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 companies that misuse or fail to protect 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.

The United States also faces growing challenges on the trade front. Many countries are increasingly concerned about the absence of adequate privacy protection for the personal data of their consumers that is collected by Internet firms in the United States. There is a real risk that over the next year, privacy officials in Europe will move to limit the flow of personal information to the United States unless appropriate legal safeguards are established.

In my testimony today I will outline a comprehensive approach to data protection for the United States. EPIC recommends both comprehensive legislation and the establishment of a federal data protection agency. Congress should enact legislation that (1) gives consumers greater control of their personal data held by others; (2) limits the use of the Social Security Number in the private sector; (3) mandates data breach notification; (4) changes 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. In addition, Congress should establish a data protection agency in the United States.

---

[1] *See* EPIC, *About EPIC*, https://epic.org/epic/about.html. EPICs Advisory Board includes distinguished experts in law, technology, and public policy, https://epic.org/epic/advisory_board.html.

[2] 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).

[3] *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.

[4] 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. See also, Christine Bannan, *Equifax's Data Breach Sins Live on to This Year's Tax Season*, The Hill (Feb. 1, 2018), http://thehill.com/opinion/finance/371815-equifaxs-data-breach-sins-live-on-to-this-years-tax-season.

There are several proposals in the House and Senate to strengthen privacy protection for Americans. Given the rapidly increasing risks to consumers from data breaches and identity theft, now is the time for Congress to implement much-needed reforms.

I. The scope of the data breach problem

A. Data breaches are an epidemic in the United States

2017 marked yet another "worst year ever" for data breaches.[5] One report found that the number of data breaches nearly doubled from 2016 to 2017, and 73% of all U.S. companies have now been breached.[6] There were a total of 159,700 cybersecurity incidents in 2017.[7] These figures represent a disturbing lack of data security by U.S. companies.

The data breach epidemic imposes an enormous cost on the U.S. economy. According to the Department of Justice, 17.6 million individuals – 7% of all Americans – experienced identity theft, at a cost of $15.4 billion to the U.S. economy.[8] The Department of Justice found that 86% of identity theft victims experienced the fraudulent use of existing account information.[9] A recent report found that identity fraud increased by 16 percent in 2016, with a total of $16 billion stolen from 15.4 million U.S. consumers.[10] Identity theft continues to be the number one complaint to the FTC.[11]

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:[12]

- Being denied of credit cards and loans
- Being unable to rent an apartment or find housing
- Paying increased interest rates on existing credit cards

---

[5] Online Trust Alliance, *Cyber Incident and Breach Trend Report*, (Jan. 25, 2018), https://www.otalliance.org/system/files/files/initiative/documents/ota_cyber_incident_trends_report_jan2018.pdf.
[6] *Id*; *See also*, Thales, 2018 DATA THREAT REPORT, https://dtr.thalesesecurity.com/.
[7] Online Trust Alliance, *supra*, at 5.
[8] Bureau of Justice Statistics, *17.6 Million U.S. Residents Experienced Identity Theft in 2014*, Press Release, (Sep. 27, 2015), https://www.bjs.gov/content/pub/press/vit14pr.cfm.
[9] *Id*.
[10] Javelin Strategy & Research, *Identity Fraud Hits Record High With 15.4 Million U.S. Victims in 2016, Up 16 Percent According to new Javelin Strategy & Research Study*, Press Release, (Feb. 1, 2017), https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new.
[11] 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.
[12] Identity Theft Resource Center, *Identity Theft: The Aftermath 2017*, http://www.idtheftcenter.org/images/page-docs/Aftermath2017Finalv1.pdf.

- Having greater difficulty getting a job
- Suffering severe distress and anxiety

B. Recent data breaches demonstrate the need for reform

Two recent high-profile data breaches at Equifax and Uber underscore the urgent need for reform. The Equifax data breach was one of the worst in U.S. history. Over 145 million Americans had sensitive personal information stolen, including Social Security numbers, driver's license numbers, dates of birth, and addresses—data that is a gold mine for identity thieves.[13] Equifax was aware of a major security vulnerability in its system but failed to fix the problem for four months.[14] Equifax's data security was so inadequate that a single point of failure exposed the personal data of more than half of American consumers.

Equifax's response to the breach created even further harm for consumers. Equifax waited six weeks to notify the public of the breach.[15] The company then created a website where consumers could find out if their information had been hacked, but the website didn't work, and at one point the company even directed consumers to a phishing website designed to look like Equifax's page.[16] And while Equifax offered free credit monitoring services in the wake of the breach, it initially used this offer to force consumers to sign away their rights to sue Equifax in court, relenting only after public outrage.[17]

EPIC testified before the Senate following the Equifax breach, urging reform of the credit reporting industry.[18] We emphasized in our testimony that as a result of the breach, the incidents of identity theft and financial fraud are likely to increase. The IRS did report that tax-related identity theft fell by 40 percent in 2017—from 401,000 reports to 242,000—in spite of the fact that the rates of identity theft continue to climb overall.[19] However, the Equifax breach creates a risk that the incidents of tax fraud could also climb back up.[20]

---

[13] Equifax, *Equifax Announces Cybersecurity Incident Involving Consumer Information* (Sept. 7, 2017), https://investor.equifax.com/tools/viewpdf.aspx.

[14] 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.

[15] Chris Isidore, *Equifax's Delayed Hack Disclosure Did it Break the Law?*, CNNtech, (Sep. 8, 2017), http://money.cnn.com/2017/09/08/technology/equifax-hack-disclosure/index.html.

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

[17] Diane Hembree, *Consumer Backlash Suprs Equifax to Drop 'Ripoff Clause' in Offer to Security Hack Victims*, Forbes, (Sep. 9, 2017), https://www.forbes.com/sites/dianahembree/2017/09/09/consumer-anger-over-equifaxs-ripoff-clause-in-offer-to-security-hack-victims-spurs-policy-change/.

[18] *Consumer Data Security and the Credit Bureaus*: *Hearing Before the S. Comm. on Baking, Housing, and Urban Affairs*, 115th Cong. (2017), (statement of Marc Rotenberg, Exec. Dir., Electronic Privacy Information Center), https://epic.org/privacy/testimony/EPIC-Testimony-SBC-10-17.pdf.

[19] Aaron Lorenzo, *IRS Reports Drop in Tax-related ID Theft for Second Straight Year*, PoliticoPro, (Feb. 8, 2018), https://www.politicopro.com/tax/whiteboard/2018/02/irs-reports-drop-in-tax-related-id-theft-for-second-straight-year-580230.

[20] Bannan, *supra*, at 4.

In a recent letter to the Senate, EPIC highlighted the fact that CFPB Acting Director Mick Mulvaney has apparently ended the investigation into Equifax.[21] According to reports, Mulvaney has ended plans to test Equifax's security systems, rejected offers from regulators to assist with the investigation, and declined to seek subpoenas or sworn testimony from Equifax executives.[22] This failure to pursue a thorough investigation of the Equifax matter verges on malfeasance.

A data breach at Uber was also the subject of a recent Senate hearing on "bug bounty" programs.[23] Uber's massive data breach in 2016 exposed the personal information of 57 million Uber customers and drivers, including their names, email addresses, phone numbers, and driver's license numbers.[24] Rather than disclose the data breach to the public, as required by law, Uber paid the hackers $100,000 to delete the information.[25] Uber did not disclose the data breach until a year later.[26] EPIC submitted a statement to the Senate in advance of the hearing, and warned that while bug bounties are sometimes legitimate, they do not excuse a company's legal obligation to notify the public of a data breach.[27] The risk that hackers will still user data and hold it for ransom will likely increase.[28]

C. Consumers lack control over their data

The Uber and Equifax breaches demonstrate why the current system is broken: consumers lack control over their own data. As the data broker industry proliferates, companies have enormous financial incentivizes to collect consumers' sensitive personal data.[29] Yet data brokers have little financial incentive to protect consumer data. There are between 2,500 and

---

[21] EPIC, *Letter to S. Comm. on Banking, Housing and Urban Affairs*, (Feb. 6, 2018), https://epic.org/EPIC-SBC-CFPBinvestigation-Feb2018.pdf.
[22] Patrick Rucker, *Exclusive: U.S. consumer protection official puts Equifax probe on ice – sources*, Reuters, (Feb. 5, 2018), https://www.reuters.com/article/us-usa-equifax-cfpb/exclusive-u-s-consumer-protection-official-puts-equifax-probe-on-ice-sources-idUSKBN1FP0IZ.
[23] *Data Security and Bug Bounty Programs: Lessons Learned from the Uber Breach and Security Researchers*, 115th Cong. (Feb. 6, 2018), S. Comm. on Commerce, Science, & Transportation, https://www.commerce.senate.gov/public/index.cfm/2018/2/data-security-and-bug-bounty-programs-lessons-learned-from-the-uber-breach-and-security-researchers.
[24] Eric Newcomer, *Uber Paid Hackers to Delete Stolen Data on 57 Million People*, Bloomberg, (Nov. 21, 2017), https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data.
[25] *Data security and Bug Bounty Programs*, *supra* at 24..
[26] *Id*.
[27] Letter from EPIC to S. Comm. on Commerce, Science & Transportation, *Data Security and Bug Bounty Programs: Lessons Learned from the Uber Breach and Security Researchers*, (Feb. 5, 2018), https://epic.org/EPIC-SCOM-UberBreach-Feb2018.pdf.
[28] There are other recent examples of hackers holding personal data for ransom. *See*, *e.g.* Phil Muncaster, *Over 19 Million California Voter Records Held for Ransom Again*, Info Security, (Feb. 9, 2018), https://www.infosecurity-magazine.com/news/over-19m-californian-voter-records/; Samm Quinn, *Hospital pays $55,000 ransom; no patient data stolen*, Greenfield Reporter (Jan. 15, 2018), http://www.greenfieldreporter.com/2018/01/16/01162018dr_hancock_health_pays_ransom/.
[29] Fed. Trade Comm'n, *Data Brokers: A Call for Transparency and Accountability*, (May 2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

4,000 data brokers in the United States that collect and sell personal information without consumers' knowledge or consent.[30] For these companies, consumers are the product, not the customer.[31] Companies also maintain information about consumers that is often inaccurate, causing consumers to be wrongfully denied credit, housing, or even a job.[32] Furthermore, consumers face a "black box" of complex, secret algorithms that determine their creditworthiness.[33]

Under the current system, consumers bear the costs when companies fail to protect their personal information. Consumers must contact all three credit bureaus and pay a fee to each company each time they wish to freeze and unfreeze their credit.[34] Credit bureaus like Equifax do not make it easy for consumers to freeze their credit because they profit from selling access to consumer data. And consumers only learn of the breach once the company decides to notify the public.

II. Current law is inadequate to protect consumers

Consumers in the United States face a data protection crisis, and the current patchwork of state and federal laws are woefully inadequate to address the problem. Currently, no federal law requires credit reporting agencies to offer credit freezes. States have enacted their own credit freeze laws, but these laws permit companies to charge fees to consumers to freeze their credit. Fees are typically $10 per credit reporting agency but less in some states. Some states also mandate free credit freezes for protected categories of consumers, such as: spouses of identity theft victims, minors, consumers over 65 years of age, active duty military members, and victims of domestic violence.[35] Some states (Maine, South Carolina, Indiana, and North Carolina) have prohibited fees to both place and remove freezes for all of their citizens.[36] State laws also specify the length of the freeze: it can either be permanent (until lifted by the consumer) or it can expire after a certain period of time. In three states, a freeze will automatically expire after seven years.[37]

At the federal level, consumers have little protection over their credit reports. The Fair Credit Reporting Act (FCRA) entitles consumers to only one free credit report per year, and the

---

[30] *Id*.
[31] 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.
[32] Fed. Trade Comm'n., *Free Credit Reports*, March 2013, https://www.consumer.ftc.gov/articles/0155-free-credit-reports.
[33] Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 Wash. L. Rev. 1 (2014).
[34] Lisa Weintraub Schifferle, *Free credit freezes from Equifax*, Fed. Trade Comm'n., (Sep. 19, 2017), https://www.consumer.ftc.gov/blog/2017/09/free-credit-freezes-equifax.
[35] ConsumersUnion, *Consumers Union's Guide to Security Freeze Protection,* http://consumersunion.org/research/consumers-unions-guide-to-security-freeze-protection-2/.
[36] *Id.*
[37] *Id.*

process of obtaining one is cumbersome.[38] Additionally credit reporting agencies are only required to "maintain reasonable procedures designed" to prevent unauthorized release of consumer information under FCRA.[39] In practice, this means that credit reporting agencies must take some precaution to ensure that credit information will only be used for lawful purposes, but the Federal Trade Commission has specified that this standard can be met with a blanket certification from the purchaser of the credit report that the report will be used legally.[40]

The Federal Trade Commission has limited data protection authority under the "Safeguards Rule" of the Gramm-Leach-Bliley Act.[41] This rule only applies to financial institutions, however, and the Commission has also failed to make compliance with the rule mandatory.[42] Moreover, Gramm-Leach-Bliley disperses oversight of financial institutions across seven agencies and fails to cover credit reporting agencies.[43] 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.

The Dodd-Frank Act transferred authority over certain privacy provisions of Gramm-Leach-Bliley to the Consumer Financial Protection Bureau, but Dodd-Frank did not give the CFPB authority to establish data security standards.[44] The CFPB, like the FTC, can only bring enforcement actions based on a company's affirmative misrepresentations about data security practices.[45]

III. Congress should enact comprehensive data protection legislation

There is widespread support for data protection legislation among Americans. According to the Pew Research Center, 91% of consumers say that they have lost control over how personal information is collected and used by companies.[46] The same study reported that 64% of Americans supported greater regulation over how advertisers handle their personal data. Even leading CEOs now support stronger privacy protections in the United States. Last fall, I had the

---

[38] 15 U.S.C. § 1681, *et seq*.
[39] EPIC, *Identity Theft*, https://www.epic.org/privacy/idtheft/.
[40] *Id*.
[41] *Standards for Safeguarding Customer Information*, 81 Fed. Reg. 61,632.
[42] *See*, Comments of EPIC to the Fed. Trade Comm'n, *Standards for Safeguarding Customer Information Request for Public Comment*, FTC Dkt. No. 2016-21231 (Nov. 7, 2016), https://epic.org/apa/comments/EPIC-FTC-Safeguards-Rule-Comments-11-07-2016.pdf.
[43] 15 U.S.C. § 6801; *see* 79 Fed. Reg. 37166 (2014) ("Section 501(b) of the Gramm-Leach-Bliley Act (GLB Act) 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.").
[44] *Id*.
[45] *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/.
[46] George Gao, Mary Madden, Privacy and Cybersecurity: Key Findings From Pew Research, Pew Research Center, (Jan. 16, 2015), http://www.pewresearch.org/fact-tank/2015/01/16/privacy/.

opportunity to speak with leading CEOs from across the country about the Equifax breach. After a brief exchange, the event moderator polled the CEOs and 95% "want stronger consumer privacy laws."

The basis of modern privacy law is "Fair Information Practices" – the rights and responsibilities associated with the collection and use of personal data.[47] These rights and responsibilities are necessarily asymmetric: the individuals that give up their personal data to others get the rights; the companies that collect the information take on the responsibilities. This is the approach that the United States, the European Union, and others have always taken to establish and update privacy laws concerning the collection and use of personal data.

In the section that follows I will outlines the most pressing Fair Information Practices that Congress that should enact.

A. Establish baseline standards for data security

Legislation should require companies to implement certain baseline data security processes, rather than give companies wide latitude to determine what constitutes reasonable security measures. For example, the Florida Information Protection Act requires that companies collecting consumer data "take reasonable measures to protect and 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]

EPIC supports a data minimization requirement. It has become clear that one of the best strategies to reduce the likelihood of an attack and to minimize the harm when such attacks do occur is to collect less sensitive personal information at the outset.[51] It is the credit card numbers, the bank account numbers, the government identification numbers, and the passwords that draw the attention of computer criminals. Reducing the target size reduces the vulnerability.

B. Require prompt breach notification

---

[47] EPIC, *Code of Fair Information Practices*, https://epic.org/privacy/consumer/code_fair_info.html; ALLEN & ROTENBERG, PRIVACY LAW AND SOCIETY 755-58, 760-64(WEST 2016)

[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] Data minimization obligations, and even data deletion provisions, can be found in many U.S. privacy laws. *See, e.g.,* Privacy Protection Act of 1987, 18 U.S.C. 2710(e):

> (e)Destruction of Old Records.—
> A person subject to this section shall destroy 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 and there are no pending requests or orders for access to such information under subsection (b)(2) or (c)(2) or pursuant to a court order.

Congress should mandate that companies notify consumers and law enforcement within 48 hours of a data breach. The only federal law with a breach notification rule is the Health Insurance Portability and Accountability Act, which only applies to protected health information.[52] Presently, companies often wait days, weeks, or even a year to notify consumers of a breach. When consumers are left in the dark, they cannot take measures to protect themselves, such as obtaining a credit freeze or monitoring their accounts. There is currently a patchwork of state laws mandating breach notification but no federal standard.[53] Florida 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.[54] A federal standard should go even further, but it should not preempt state law, giving states the flexibility to provide additional safeguards to consumers. A breach notification law should also require companies to notify consumers via automated texts, e-mail messages, and social media, as companies are increasingly communicating with consumers electronically.

C. Limit the use of the SSN in the private sector

Social security numbers have been asked to do too much. SSNs were never meant to be used as an all-purpose identifier.[55] The unregulated use of the social security number in the private sector has contributed to record levels of identity theft and financial fraud.[56] The Equifax breach illustrates this problem, as the social security numbers of nearly half of all Americans were stolen. Those whose SSNs have been breached suffer a rate of new account fraud more than six times higher than all consumers.[57] The more the SSN is used, the more insecure it becomes. Out of 1,091 total breaches in 2016, 568 exposed SSNs (52.1% of all breaches that year).[58]

The solution is not, however, to replace the social security number with a national biometric identifier that raises serious privacy and security risks.[59] Instead, we suggest that the best way to minimize the problem of identity theft is to reduce the industry's reliance on the

---

[52] 45 C.F.R. §§ 164.400–414. 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).
[53] *See* National Conference of State Legislatures, *Security Breach Notification Laws*, (Feb. 6, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.
[54] EPIC, *State Data Breach Notification Policy* (2017), https://epic.org/state-policy/data-breach/.
[55] Marc Rotenberg, *The Use of the Social Security Number as a National Identifier*, 22 Comp. & Soc'y nos. 2, 3, 4 (Oct.1991).
[56] Marc Rotenberg, Equifax, *The Credit Reporting Industry, And What Congress Should Do Next*, Harv. Bus. Rev., (Sep. 20, 2017), https://hbr.org/2017/09/equifax-the-credit-reporting-industry-and-what-congress-should-do-next.
[57] Identity Theft Resource Center, *New Account Fraud—A Growing Trend in Identity Theft* at 3 (November 2016), https://www.idtheftcenter.org/images/page-docs/NewAccountFraud.pdf.
[58] Identity Theft Resource Center, ITRC Breach Statistics 2005-2016, https://www.idtheftcenter.org/images/breach/Overview2005to2016Finalv2.pdf.
[59] EPIC, *Identity Theft*, http://epic.org/privacy/idtheft/.

social security number as a personal identifier.[60] Although the SSA and IRS are the only entities with clear statutory authority to use the number, use of the SSN in the private sector has become widespread. Congress should prohibit the use of the social security number in the private sector without explicit legal authorization.

D. Provide consumers with free credit freezes and thaws (change the defaults for report disclosures 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.[61] But only four states (Indiana, Maine, North Carolina, and South Carolina) mandate free consumer access to credit freezes and thaws, while four additional states "provide free freezes but charge for thaws."[62] This means that "[a]pproximately 158 million consumers between 18-65 in 42 states and DC must pay a fee to get credit freezes."[63]

E. Give consumers a private right of action and eliminate mandatory arbitration

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. U.S. privacy laws routinely provide statutory damages.[64] Many state data breach laws include private rights of action. California, Hawaii, Louisiana, and Washington include provisions in their laws that allow consumers to bring a civil action and recover damages.[65] The Federal Trade Commission and state attorneys general cannot pursue enforcement actions against every violation. A private right of action would empower consumers to enforce the law themselves and create a strong disincentive for the irresponsible handling of consumer data.

In addition, legislation should ban the use of arbitration clauses and class action waivers in consumer contracts. Consumers do not have the resources to pursue claims against powerful companies on their own. The Consumer Financial Protection Bureau ("CFPB") recently banned

---

[60] *"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.
[61] *See* U.S. PIRG, *Security Freeze and Identity Theft Tips*, http://uspirg.org/sites/pirg/files/resources/Security%20Freeze%20and%20Identity%20Theft%20Tips.pdf.
[62] 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.
[63] *Id.*
[64] *See*, The Privacy Act of 1974, 5 U.S.C. § 552a; Electronic Communications Privacy Act, 18 U.S.C § 2510 *et seq.*; Video Privacy Protection Act, 18 U.S.C. § 2710 *et seq.*; Telephone Consumer Protection Act, 47 U.S.C. § 227 *et seq*.
[65] Cal. Civ. Code 1798.82 (2011), Haw. Rev. Stat. § 487N-2 (2011), La. Rev. Stat. § 51:3071 *et seq*. (2011), Wash. Rev. Code § 19.255.010, 42, 56, 590 (2011).

arbitration clauses in consumer financial contracts, finding that class action waivers make it cost-prohibitive for consumers to obtain meaningful relief.[66] However, Congress recently voted to repeal that rule.[67] 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.[68] A private right of action that permits class actions is necessary to hold companies accountable for their data security failures.

F. Mandate algorithmic transparency

Consumers face the specter of a "scored society" where they do not have access to the most basic information about how they are evaluated.[69] 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.[70] 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.[71] Data brokers even scrape social media and score consumers based on factors such as their political activity on Twitter.[72] In one instance, a consumer found that his credit score suffered a forty-point hit simply because he requested accurate information about his mortgage.[73]

The use of algorithms can also have widespread discriminatory effects.[74] The Equal Credit Opportunity Act (ECOA) prohibits lenders from discriminating in credit decisions.[75] But studies have demonstrated that black and Latino communities have lower credit scores as a group than whites.[76] Current law does not allow consumers or regulators to evaluate these scores to determine whether they violate ECOA.[77] Although consumers have the right to request their credit scores, they do not have the right to know how this score is determined.[78]

---

[66] 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/.
[67] Donna Borak and Ted Barrett, *Senate Kills Rule That Made It Easier To Sue Banks*, CNN, (Oct. 25, 2017), https://www.cnn.com/2017/10/24/politics/senate-cfpb-arbitration-repeal/index.html.
[68] 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.
[69] Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 Wash. L. Rev. 1 (2014).
[70] *Id*.
[71] *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).
[72] *Id*.
[73] Barry Ritholtz, Where's the Note? *Leads BAC to Ding Credit Score*, THE BIG PICTURE (Dec. 14, 2010), http://www.ritholtz.com/blog/2010/12/note-bac-credit-score/.
[74] *See*, *e.g.* Cathy O'Neil, *Weapons of Math Destruction* (2016); Danielle Keats Citron & Frank Pasquale, *The Scored Scoiety: Due Process for Automated Predictions*, 89 Wash. L. Rev. 1 (2014).
[75] 15 U.S.C. § 1601 *et seq*.
[76] *See*, *e.g.* Consumer Fin. Prot. Bureau, *Analysis of Differences Between Consumer- and Creditor-Purchased Credit Scores*, (Sept. 18, 2012), http://files.consumerfinance.gov/f/201209_Analysis_Differences_Consumer_Credit.pdf.
[77] Citron & Pasquale, *supra*, note 72.
[78] 12 CFR Part 1002 ("Regulation B"); Citron & Pasquale, *supra*, note 54.

"Algorithmic transparency" is key to accountability.[79] Absent rules requiring the disclosure of these secret scores and the underlying data and algorithms upon which they are based, consumers will have no way to even know, let alone solve, these problems.

G. Provide Free Monitoring and Easy Access to Credit History

Current laws allow consumers to access 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, 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."[80] 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.[81] The other credit reporting agencies should do so as well.

H. Establish Federal Baselines Standards; Encourage States to Innovate as New Privacy Challenges Emerge

Today the states are on the front lines of consumer protection in the United States.[82] They are updating privacy laws to address new challenges.[83] They are bringing enforcement actions to safeguard American consumers.[84] They are establishing the data protection standards that are safeguarding the personal data of Americans from attack by foreign adversaries.[85]

It is absolutely essential to the development of privacy safeguards that Congress establishes baseline standards that all states must follow, but leave states with the freedom to adopt new protections. As Justice Brandeis once explained, the states are the laboratories of democracy.[86] This is all the more crucial in the rapidly evolving world of Internet services.

---

[79] EPIC, *Algorithmic Transparency,* https://epic.org/algorithmic-transparency/.
[80] 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/.
[81] *See, e.g.*, Discover, *Social Security Alerts* (2017), https://www.discover.com/credit-cards/member-benefits/security/ssn-newaccount-alerts/.
[82] NCSL, *supra* at 57; EPIC, *State Policy Project*, https://www.epic.org/state-policy/.
[83] NCSL, *supra*, at 57.
[84] Fla. Att'y Gen., *Settlement Reached With Target Regarding Data Breach,* Press Release, (May 23, 2017), http://myfloridalegal.com/__852562220065EE67.nsf/0/267E8BE9BB21436C85258129005E37B8?Open&Highlight=0,data,breach; Reuters, *Washington state attorney general sues Uber after data breach*, (Nov. 28, 2017), https://www.reuters.com/article/us-uber-cyberattack/washington-state-attorney-general-sues-uber-after-data-breach-idUSKBN1DS2UF; N.Y. Att'y Gen., *A.G. Schneiderman Launches Formal Investigation Into Equifax Breach, Issues Consumer Alert,* Press Release, (Sep. 8, 2017), https://ag.ny.gov/press-release/ag-schneiderman-launches-formal-investigation-equifax-breach-issues-consumer-alert.
[85] EPIC, *State Consumer Data Security Policy*, https://epic.org/state-policy/consumer-data/.
[86] "It is one of the happy incidents of the federal system that a single courageous state may, if its citizens choose, serve as a laboratory[.]" *New State Ice Co. v. Liebmann*, 285 U.S. 262, 311 (Brandeis, J. dissenting).

If Congress chooses to preempt the states in this crucial area of national security, it could leave Americans more vulnerable to attack from foreign adversaries.

IV. Congress should establish a data protection agency in the United States

The United States is one of the few democracies in the world that does not have a federal data protection agency, even though the original proposal for such an institution emerged from the U.S. in the 1970s.[87] The United States was once a global leader on privacy. The Fair Credit Reporting Act, passed in 1970, was viewed at the time as the first modern privacy law—a response to the growing automation of personal data in the United States.[88] The Privacy Act of 1974 was based on the Code of Fair Information Practices, which have served as the foundation for international privacy laws and frameworks, such as the Organization for Economic Cooperation and Development ("OECD") Privacy Guidelines[89] and the European Commission's Data Protection Regulation.[90] This common approach to data protection helps facilitate international data transfer and trade.[91]

But today, Europe has surpassed the United States in protecting consumer data. The General Data Protection Regulation, which is set to take effect on May 25, 2018, strengthens the fundamental rights of individuals and puts consumers back in control of their personal data. It gives European data subjects rights to breach notification (within 72 hours of breach), right to access (whether or not personal data concerning them is being processed, where and for what purpose), right to be forgotten (to have the data controller erase his/her personal data, and data portability (the right for a data subject to receive the personal data concerning them and to transmit that data to another controller). American data subjects have none of these rights. American companies will be required to provide these protections to Europeans but not to Americans, creating a digital lower class. U.S. companies are leaders in technology, and the U.S. government should be a leader in technology policy.

There is an urgent need for leadership from the United States on data protection. Virtually every other advanced economy has recognized the need for an independent agency to address the challenges of the digital age. Current law and regulatory oversight in the United States is woefully inadequate to meet the challenges. The Federal Trade Commission is fundamentally not a data security agency. The FTC only has authority to bring enforcement actions against unfair and deceptive practices in the marketplace, and it lacks the ability to create prospective rules for data security. The Consumer Financial Protection Bureau similarly lacks

---

[87] See, EPIC, The Privacy Act of 1974, https://epic.org/privacy/1974act/#history.
[88] EPIC, *The Fair Credit Reporting Act*, https://www.epic.org/privacy/fcra/.
[89] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.
[90] Proposal for a Regulation of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and the free movement of such data (General Data Protection Regulation), E.C. COM (2012) final, (Jan. 25, 2012), available at http://ex.europa/eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.
[91] Marc Rotenberg, *In Support of a Data Protection Board in the United States, Government Information Quarterly*, vol. 8, no. 1, 79-94 (Spring 1991)

data protection authority and only has jurisdiction over financial institutions. Neither of these agencies possesses the expertise and resources needed to address data security across the country. And the Privacy and Civil Liberties Oversight Board, another agency that could help safeguard Americans and their data, lies dormant.

As the data breach epidemic reaches unprecedented levels, the need for an effective, independent data protection agency has never been greater. An independent agency can more effectively utilize its resources to police the current widespread exploitation of consumers' personal information. An independent agency would also be staffed with personnel who possess the requisite expertise to regulate the field of data security.

V. Current Legislative Proposals

There are bills in both the House and Senate that move in the right direction, but none are comprehensive data protection legislation. Data breaches affect all industries; therefore legislation that only applies to the credit bureaus will only address a small fraction of the problem. The Consumer Privacy Protection Act of 2017 (S. 2124), sponsored by Senator Patrick Leahy, is the most comprehensive proposal. It incorporates many of our suggestions including free credit freezes, objective data security standards, and a federal baseline.

The Comprehensive Consumer Credit Reporting Reform Act of 2017, (H.R. 3755), sponsored by Representative Maxine Waters, also includes several proposals we support. It expands consumers' access to free credit reports and limits the circumstances in which a credit reporting agency may furnish a consumer report for employment purposes. The bill also provides free credit freezes and credit monitoring for victims of identity theft, and caps the cost to place or lift a credit freeze at $3 for all other consumers.

Several bills propose amendments to FCRA. The PROTECT Act of 2017 (H.R. 4028 and S. 1982), sponsored by Representative Patrick McHenry and Senator David Purdue respectively, provides for federal supervision and examinations of the cybersecurity standards of large consumer reporting agencies. The bill also prohibits the use of SSNs by credit bureaus, and while this would be an improvement on the status quo, it would only limit the collection and use of the SSN by a few companies.

The Free Credit Freeze Act (H.R. 3878) prohibits bureaus from charging for placing, thawing, or lifting a credit freeze. But some proposals still allow bureaus to charge (e.g., H.R. 3755) and none require default freezes The Credit Information Protection Act of 2017 (H.R. 3766) only requires bureaus to provide free freezes after a breach has occurred. These bills contain some good measures, but they only marginally improve the regulatory landscape.

Some bills—including the Personal Data Notification and Protection Act of 2017 (H.R. 3806)—preempt state law. Data security is a dynamic field, so it is critical to ensure that the states are able to protect consumers. These bills should be modified to establish a federal baseline and allow states to regulate upwards, providing more protection than federal law if their legislatures so decide.

The Data Breach Prevention and Compensation Act of 2018 (S. 2289), sponsored by Senator Elizabeth Warren, comes close to creating a data protection authority by giving the FTC rulemaking authority. This would allow the agency to promulgate regulations setting standards for cybersecurity, setting clear standards that companies must meet.

The Data Broker Accountability and Transparency Act (S. 1815), sponsored by Senator Edward Markey, would address data protection beyond the credit reporting industry. S. 1815 applies to data brokers, including but not limited to credit bureaus, that collect and sell personal information to third parties. There are thousands of data brokers that make dossiers on individuals but are not regulated under FCRA because they do not create credit reports.

It is worth noting that members of both parties have introduced significant privacy bills in the House and the Senate. To be sure there is a lot of disagreement in Washington today. But on the issue of protecting the personal data of Americans, there is little reason for partisan disagreement. Privacy is an American value, and privacy protection is a fundamental American right.

Conclusion

EPIC believes it is time to enact comprehensive data protection legislation in the United States to and to establish a data protection agency. Our privacy laws are out of date and fail to provide the necessary protections for our modern age. We also face threats from foreign adversaries that target the personal data stored in U.S. companies and government agencies. The longer Congress delays, the greater the risks will be. Now is the time to act.

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