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

March 14, 2019

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 are writing to you in response to your request for feedback on data privacy, protection, and collection. 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.[1] EPIC has previously testified before this Committee 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.[2]

1) What could be done through legislation, regulation, or by implementing best practices that would give consumers more control over and enhance the protection of consumer financial data, and ensure that consumers are notified of breaches in a timely and consistent manner?

Baseline federal legislation should be built on a familiar privacy framework, such as the original U.S. Code of Fair Information Practices and the widely followed OECD Privacy Guidelines. The rights and responsibilities set out in these frameworks 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. Core principles include:

- Transparency about business practices
- Data collection and use limitations
- Data minimization and deletion
- Purpose specification
- Access and correction rights
- Accountability
- Data accuracy
- Confidentiality/security[3]

[1] 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.
[2] *See, e.g.*, *Consumer Data Security and the Credit Bureaus: Hearing Before the Senate Comm. on Banking, Housing, and Urban Affairs*, 115th Cong. 6 (2017) (testimony of Marc Rotenberg, Exec. Dir., EPIC), https://www.banking.senate.gov/imo/media/doc/Rotenberg%20Testimony%2010-17-17.pdf; *Cybersecurity and Data Protection in the Financial Sector: Hearing Before the Senate Comm. on Banking, Housing, and Urban Affairs*, 112th Cong. (2011) (testimony of Marc Rotenberg, Exec. Dir., EPIC), https://epic.org/privacy/testimony/EPIC_Senate_Banking_Testimony%20_6_21_11.pdf.
[3] Privacy and Digital Rights for All, *The Time is Now: A Framework for Comprehensive Privacy Protection and Digital Rights in the United States* (2019), https://www.citizen.org/sites/default/files/privacy-and-digital-rights-for-all-framework.pdf.

Legislation or regulations should, at minimum:

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."[4] 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.[5] This is especially important because the Equifax hack and other major data breaches caused by known vulnerabilities are entirely preventable.[6]

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.[7] 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

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.[8] 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 are currently a patchwork of state laws mandating breach notification but no federal standard.[9] Florida has one of the most comprehensive data breach laws,

---

[4] Fla. Stat. § 501.171(2) (2017). See EPIC, State Data Breach Notification Policy (2017).
[5] 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.
[6] See Lily Hay Newman, Equifax Officially Has No Excuse, Wired (Sept. 14, 2017), https://www.wired.com/story/equifax-breach-no-excuse/.
[7] 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.
[8] 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).
[9] *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.

providing a mandatory 30-day notification rule, a broad scope, and proactive requirements for reasonable data protection measures.[10] 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. They were never meant to be used as an all-purpose identifier.[11] The unregulated use of the social security number in the private sector has contributed to record levels of identity theft and financial fraud.[12] 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.[13] 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).[14]

The solution is not, however, to replace the social security number with a national biometric identifier that raises serious privacy and security risks.[15] 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.[16] 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. 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.[17] 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.[18] The Federal Trade

---

[10] EPIC, *State Data Breach Notification Policy* (2017), https://epic.org/state-policy/data-breach/.
[11] Marc Rotenberg, The Use of the Social Security Number as a National Identifier, 22 Comp. & Soc'y nos. 2, 3, 4 (Oct.1991).
[12] 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.
[13] 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.
[14] Identity Theft Resource Center, ITRC Breach Statistics 2005-2016, https://www.idtheftcenter.org/images/breach/Overview2005to2016Finalv2.pdf.
[15] EPIC, *Identity Theft*, http://epic.org/privacy/idtheft/.
[16] *"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.
[17] *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.*
[18] 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).

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 arbitration clauses in consumer financial contracts, finding that class action waivers make it cost-prohibitive for consumers to obtain meaningful relief.[19] However, Congress recently voted to repeal that rule.[20] 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.[21] A private right of action that permits class actions is necessary to hold companies accountable for their data security failures.

E. Establish Federal Baseline 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.[22] They are updating privacy laws to address new challenges.[23] They are bringing enforcement actions to safeguard American consumers.[24] They are establishing the data protection standards that are safeguarding the personal data of Americans from attack by foreign adversaries.[25]

It is absolutely essential to the development of privacy safeguards that Congress establish 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.[26] This is all the more crucial in the rapidly evolving world of Internet services.

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.

---

[19] 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/.

[20] 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.

[21] 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.

[22] NCSL, *supra* at 57; EPIC, *State Policy Project*, https://www.epic.org/state-policy/.

[23] NCSL, *supra*, at 57.

[24] 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.

[25] EPIC, *State Consumer Data Security Policy*, https://epic.org/state-policy/consumer-data/.

[26] "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).

F. 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. 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.[27]

But today, Europe has surpassed the United States in protecting consumer data. The General Data Protection Regulation, which took effect last year, 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 data protection authority and only has jurisdiction over financial institutions. Neither of these agencies possess the resources needed to address data security.

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.

2) What could be done through legislation, regulation, or by implementing best practices to ensure that financial regulators and private financial companies (including third-parties that share information with financial regulators and private financial companies) provide adequate disclosure to citizens and consumers about the information that is being collected about them and for what purposes?

Individuals cannot have meaningful control of their personal data if the terms of service require them to waive their privacy rights. Furthermore, requiring individuals to pay more or receive lower quality goods or services if they do not waive their privacy rights is unfair and discriminates against those with less means. Federal law should require that consent, where appropriate, is

[27] EPIC, *The Fair Credit Reporting Act*, https://www.epic.org/privacy/fcra/.

meaningful, informed, and revocable, and should prohibit "pay-for-privacy provisions" or "take-it-or leave it" terms of service.

3***) What could be done through legislation, regulation, or by implementing best practices to give citizens and consumers control over how financial regulators and private financial companies (including third-parties that share information with financial regulators and private financial companies) use consumer data?***

The above mentioned U.S. Code of Fair Information Practices and the widely followed OECD Privacy Guidelines also give guidance here. Legislation or regulations should put the following obligations on data collectors:

1. Transparency about business practices
    - Openness about developments, practices, and policies
    - Existence of data systems
    - Purpose of use of data
    - Identity and location of data controller
2. Data collection limitations
    - Limits on collection
    - Lawful collection
    - Fair collection
    - Knowledge or consent where appropriate
3. Use Limitations
    - Presumption against disclosure inconsistent with purpose specification
    - Narrow exception for consent of data subject
    - Narrow exception for legal authority
4. Purpose specification
    - Purpose stated
    - Purpose specified at time of collection
    - Subsequent use consistent with purpose
    - New purpose specified for new use
5. Accountability
    - Data controller is specified
    - Compliance is required
    - Accountability mechanisms are established
6. Confidentiality/Security
    - Protection against loss
    - Protection against unauthorized access
    - Protection against unauthorized destruction
    - Protection against unauthorized use
    - Protection against unauthorized modification
    - Protection against unauthorized disclosure
7. Data accuracy
    - Data is relevant for purpose
    - Data is necessary for purpose
    - Data is accurate
    - Date is complete
    - Data is up-to-date

And consumers whose data is collected must have access and correction rights, such as:

1. Confirmation of whether personal data is collected
2. Obtain data about her in possession of controller
3. Challenge to denial of access
4. Ability to have personal data: erased, corrected, completed, and/or amended.

4) What could be done through legislation, regulation, or by implementing best practices by credit bureaus to protect consumer data and to make sure that information contained in a credit file is accurate?

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 in 2017 after finding that the companies "lured consumers into costly recurring payments for credit-related products with false promises."[28] 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.[29] The credit other reporting agencies should do so as well.

5) What could be done through legislation, regulation, or by implementing best practices so a consumer can easily identify and exercise control of data that is being (a) collected and shared by data brokers and other firms and (b) used as a factor in establishing a consumer's eligibility for credit, insurance, employment, or other purposes.

Consumers face the specter of a "scored society" where they do not have access to the most basic information about how they are evaluated.[30] 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.[31] 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.[32] Data brokers even scrape social media and score consumers based on factors such as their political activity on Twitter.[33] In one instance, a consumer found that his credit score suffered a forty-point hit simply because he requested accurate information about his mortgage.[34]

---

[28] 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/.

[29] *See, e.g.*, Discover, *Social Security Alerts* (2017), https://www.discover.com/credit-cards/member-benefits/security/ssn-newaccount-alerts/.

[30] Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 Wash. L. Rev. 1 (2014).

[31] *Id*.

[32] *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).

[33] *Id*.

[34] 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/.

The use of algorithms can also have widespread discriminatory effects.[35] The Equal Credit Opportunity Act (ECOA) prohibits lenders from discriminating in credit decisions.[36] But studies have demonstrated that black and Latino communities have lower credit scores as a group than whites.[37] Current law does not allow consumers or regulators to evaluate these scores to determine whether they violate ECOA.[38] Although consumers have the right to request their credit scores, they do not have the right to know how this score is determined.[39]

"Algorithmic transparency" is key to accountability.[40] 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.

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 current privacy laws are woefully out of date and fail to provide the necessary protections for our modern age. We also now face threats from foreign adversaries that target the personal data stored in U.S. companies and U.S. government agencies. The longer Congress delays, the greater the risks will increase.

Sincerely,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

/s/ *Caitriona Fitzgerald*
Caitriona Fitzgerald
EPIC Policy Director

Enclosures:
Privacy and Digital Rights for All, *The Time is Now: A Framework for Comprehensive Privacy Protection and Digital Rights in the United States* (2019)

Marc Rotenberg, *America Needs a Privacy Law*, New York Times (December 25, 2018)

Marc Rotenberg, *Congress can follow the EU's lead and update US privacy laws,* Financial Times (June 1, 2018)

Marc Rotenberg, *The Facebook-WhatsApp Lesson: Privacy Protection Necessary for Innovation*, Techonomy (May 4, 2018)

Marc Rotenberg, *Promoting Inovation, Protecting Privacy,* OECD Observer (June 2016)

Marc Rotenberg*, On International Privacy: A Path Forward for the US and Europe,* Harvard International Review (June 1, 2014)

---

[35] *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).
[36] 15 U.S.C. § 1601 *et seq*.
[37] *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.
[38] Citron & Pasquale, *supra*, note 72.
[39] 12 CFR Part 1002 ("Regulation B"); Citron & Pasquale, *supra*, note 54.
[40] EPIC, *Algorithmic Transparency,* https://epic.org/algorithmic-transparency/.