epic.org | ELECTRONIC PRIVACY INFORMATION CENTER

Testimony and Statement for the Record of

Sam Lester, EPIC Consumer Privacy Counsel
Electronic Privacy Information Center

Hearing on "Securing Americans' Identities: The Future of the Social Security Number"

Before the

House Committee on Ways and Means
Subcommittee on Social Security

May 17, 2018
1100 Longworth House Office Building
Washington, DC, 20002

Mister Chairman and Members of the Committee, thank you for the opportunity to testify today on securing Americans' identities: the future of the Social Security Number ("SSN"). My name is Sam Lester. I am the Consumer Privacy Counsel at 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. EPIC has urged Congress to establish privacy safeguards for the SSN for two decades.[1] EPIC has also participated in leading cases involving the privacy of the SSN and maintains an archive of information about the SSN online.[2]

It is important to emphasize the unique status of the SSN in the world of privacy. There is no other form of personal identification that poses a greater risk to privacy. The recent Equifax data breach exposed the SSNs of almost half of the U.S. population. The SSN was never meant to be an all-purpose identifier. The fact that the SSN is now so pervasive as both an identifier and an authenticator in both the public and private sector has undoubtedly contributed to the alarming rise in data breaches, identity theft, and financial fraud.

In my testimony today, I will outline the steps Congress can take to protect the privacy of the SSN. Congress should (1) prohibit the use of the SSN in the private sector without explicit legal authorization; (2) prohibit companies from compelling consumers to disclose their SSN as a condition of service or sale unless there is a statutory basis for the request; and (3) promote technological innovations that enable the development of context specific identifiers. Congress should *not*, however, replace the SSN with a national biometric identifier, which would raise serious privacy and security risks.

I. Original purpose of the SSN and the dangers of a national identification number

A. The SSN was never meant to be an all-purpose identifier or to be used in the private sector

Social Security Numbers are a classic example of "mission creep," where a program with a specific, limited purpose is transformed for additional, unintended purposes, often with disastrous results. When the SSN was first introduced in 1936, it was to be used only as a means

---

[1] *See, e.g.*, *Protecting Seniors from Identity Theft: Is the Federal Government Doing Enough*: *Hearing Before the S. Special Comm. on Aging*, 114th Cong. (Oct. 7, 2015) (statement of Marc Rotenberg, Exec. Dir., EPIC), https://epic.org/privacy/ssn/EPIC-SSN-Testimony-Senate-10-7-15.pdf; *Protecting the Privacy of the Social Security Number from Identity Theft*: *Hearing Before the H. Ways & Means Subcom. on Social Security*, 110th Cong. (Jun. 21, 2007) (statement of Marc Rotenberg), https://epic.org/privacy/ssn/idtheft_test_062107.pdf; *Social Security Numbers & Identity Theft*: *Joint Hearing Before the H. Fin. Serv. Subcom. on Oversight & Investigations and the H. Ways & Means Subcom. on Social Security*, 104th Cong. (Nov. 8, 2001) (statement of Marc Rotenberg), http://www.epic.org/privacy/ssn/testimony_11_08_2001.html; *Preserving the Integrity of Social Security Numbers and Preventing Their Misuse by Terrorists and Identity Thieves*: *Joint Hearing Before the H. Ways & Means Subcom. on Social Security & the H. Judiciary Subcom. on Immigration, Border Sec. & Claims*, 105th Cong. (Sept. 19, 2002) (statement of Chris Jay Hoofnagle, EPIC), http://www.epic.org/privacy/ssn/ssntestimony9.19.02.html.

[2] *See, e.g.*, *Greidinger v. Davis*, 988 F.2d 1344 (4th Cir. 1993); *Beacon Journal v. Akron*, 70 Ohio St. 3d 605 (Ohio 1994); EPIC, Social Security Numbers, https://epic.org/privacy/ssn/.

of tracking earnings to determine the amount of social security taxes to credit each worker's account. At the time, public concern over potential abuse of the SSN was so high that the Social Security board had to reassure Americans that it was for the exclusive use of the Social Security system. Over time, however, Congress allowed SSNs to be used for purposes unrelated to the administration of the Social Security system. In 1961, Congress authorized the IRS to use SSNs as taxpayer identification numbers.[3] In the 1980s, Congress passed a series of bills authorizing the SSN for purposes such as opening an interest-bearing account, cash transactions over $10,000, and applying for numerous types of federal benefits.[4]

Congress attempted to rein in the widespread use of the SSN with the Privacy Act of 1974. A landmark 1973 report on privacy prepared by Willis Ware and the Department of Health, Education and Welfare ("HEW") described how the increasing use of the SSN in the private sector was promoting invasive profiling, and recommended legislation "prohibiting use of an SSN, or any number represented as an SSN for promotional or commercial purposes."

The HEW report laid the groundwork for the Privacy Act.[5] Specifically, Section 7 of the Privacy Act provides:

> (a)(1) It shall be unlawful for any Federal, State or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his social security account number
>
> (b) Any Federal, State, or local government agency which requests an individual to disclose his social security account number shall inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it. [6]

This provision is critical to keep in mind today, because consumers are so often compelled to disclose their SSN to obtain a product or service.

As originally conceived, the Privacy Act would have applied to both the public and private sector. However, negotiations with the White House led to the removal of provisions that

---

[3] Pub. L. No. 87-397, 75 Stat. 828 (codified as amended at 26 U.S.C. §§ 6113, 6676).
[4] *See*, Carolyn Puckett, *The Story of the Social Security Number*, Soc. Sec. Bulletin, Vol. 69, No. 2, Soc. Sec. Admin., (2009), https://www.ssa.gov/policy/docs/ssb/v69n2/v69n2p55.html.
[5] Dep't of Health, Educ. & Welfare, Secretary's Advisory Comm. on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens* 125-35 (MIT 1973), *available at* http://www.epic.org/privacy/hew1973report/.
[6] Pub. L. No. 93-579, 7. This provision of the Privacy Act was never codified, but is instead set out as a historical note to 5 U.S.C.A § 552(a) (2016).

covered the private sector.[7] As a consequence, the SSN has been allowed to proliferate as an all-purpose identifier in the private sector.

B. EPIC has repeatedly urged Congress to restrict the use of the SSN in the private sector

In 2007, EPIC testified before this Committee on how the proliferation of the SSN in the private sector has exposed consumers to unprecedented risks. We said:

> [T]he reality is that today the SSN is the key to some of our most sensitive and personal information. The financial services sector, for instance, has created a system of files, keyed to individuals' SSNs, containing personal and financial information on nearly 90 percent of the American adult population. This information is sold and traded freely, with virtually no legal limitations. In addition, credit grantors rely upon the SSN to authenticate a credit applicant's identity.[8]

In October 2017, EPIC testified before the Senate Banking Committee following the Equifax breach. We again emphasized how "the unregulated use of the social security number in the private sector has contributed to record levels of identity theft and fraud" and again urged Congress to restrict its use.[9] Earlier this year, EPIC reinforced the urgency of legislation to limit the use of the SSN in testimony before the House Financial Services Committee, explaining, "the more the SSN is used, the more insecure it becomes."[10]

II. Consumers face an epidemic of data breach, identity theft and financial fraud as a result of the pervasive use of the SSN in the private sector

The ubiquity of the SSN in the private sector has created unprecedented risks for consumers. Incidents of data breach continue to rise in the United States, and the prevalence of the SSN in consumer databases undoubtedly contributes to this alarming epidemic. Last year was again the worst year ever for data breaches, as the number of breaches almost doubled from

---

[7] EPIC, *The Privacy Act of 1974*, https://epic.org/privacy/1974act/; Robert Ellis Smith, *Gerald Ford: Privacy's Godfather*, Forbes (Jan. 5, 2017), https://www.forbes.com/2007/01/04/privacy-protection-ford-oped-cx_res_0105privacy.html.

[8] *Id*.

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

[10] *Examining the Current Data Security and Breach Notification Regulatory Regime: Hearing Before the S. Comm. on Financial Services*, 115th Cong. (Feb. 14, 2018) (statement of Marc Rotenberg, EPIC), https://epic.org/testimony/congress/EPIC-Testimony-HFS-2-14-18.pdf.

2016.[11] 73% of all U.S. companies have now been breached.[12] As a consequence, identity fraud reached an all-time high in 2017, with 16.7 million victims and a total of $16.8 billion stolen.[13]

A. SSNs are the most valuable piece of personal data for identity thieves

SSNs are the "keys to the kingdom" for identity thieves.[14] The SSN is so valuable because it can be used to open new accounts without any other identifying information. Many retailers and banks will extend offers of credit to individuals with an SSN attached to a good credit score, even if the names do not match.[15] Those whose SSNs have been breached are more than six times as likely to suffer new account fraud.[16]

This is particularly important in light of the Equifax breach, in which almost half of all Americans had their SSN stolen. In a recent SEC filing, Equifax provided the most detailed analysis to date of the information that was stolen.[17] Of the 146.6 million victims, 145.5 million had their SSN stolen.[18] Compare that with only 20.3 million who had their phone number stolen, 17.6 million who had their driver's license number stolen, and 1.8 million who had their email address stolen.[19]

Criminals in possession of SSNs can completely derail a person's financial future. The Bureau of Justice Statistics reported that "[v]ictims experiencing the opening of a new account or the misuse of personal information had greater [out-of-pocket] loss than those experiencing misuse of an existing credit card or bank account."[20] The IRS estimates that it paid out $3.1 billion in fraudulent tax refunds for the 2014 filing season.[21] A criminal in possession of your stolen SSN can:

---

[11] 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.
[12] *Id.*
[13] Javelin, *Identity Fraud Hits All Time High With 16.7 Million U.S. Victims in 2017, According to New Javelin Strategy & Research Study*, (Feb. 6, 2018), https://www.javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-us-victims-2017-according-new-javelin.
[14] Fed. Trade Comm'n., *Security in Numbers: SSNs and ID Theft* 2 (Dec. 2008), https://www.ftc.gov/sites/default/files/documents/reports/security-numbers-social-security-numbers-and-identity-theft-federal-trade-commission-report/p075414ssnreport.pdf.
[15] Bob Sullivan, *Your Social Security Number Isn't a Secret*, N.Y. Times (Sept. 13, 2017), https://www.nytimes.com/2017/09/13/opinion/your-social-security-number-isnt-a-secret.htm.
[16] 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.
[17] Brian Fung, *145 Million Social Security numbers, 99 million addresses and more: Every type of personal data Equifax lost to hackers, by the numbers*, Washington Post, (May 8, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/05/08/every-type-of-personal-data-equifax-lost-to-hackers-by-the-numbers/.
[18] *Id.*
[19] *Id.*
[20] Erika Harrell, *Victims of Identity Theft, 2014*, Bureau of Justice Statistics, (revised Nov. 14, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf.
[21] U.S. Gov't Accountability Office, GAO-16-589T, *IRS Needs to Further Improve Controls Over Taxpayer Data and Continue to Combat Identity Theft Refund Fraud* 1–2 (2016), https://www.gao.gov/assets/680/676493.pdf.

- File fraudulent tax returns in your name
- Open new accounts in your name
- Take out lines of credit in your name
- Receive unemployment, food stamps and Social Security benefits in your name
- Apply for student loans, obtain driver's licenses and passports in your name

For example, a retired certified public accountant in Colorado received a Form SSA-1099 for $19,236 in Social Security benefits earlier this year, even though he had never applied for benefits.[22] A home buyer can experience their worst nightmare when a lender pulls their credit to discover that their FICO score is too low to qualify for a loan because someone has fraudulently run up debt in their name.[23] It can take years for individuals who have experienced new account fraud to recover financially.[24]

SSNs are routinely bought and sold on the black market. These illicit marketplaces are "growing in size and complexity" and are now dominated by "financially driven, highly organized and sophisticated groups."[25] Complete dossiers of personal data that contain SSNs—referred to as "fullz"—are sold in bulk for as little as $15 per victim, demonstrating how inexpensive it can be to commit identity theft, yet how lucrative it can be for a hacker who has stolen data on millions of individuals.[26]

Children in particular are targets for identity theft and fraud using their SSN because they do not have a credit history. Among the notified breach victims in 2017, 39 percent of minors were victims of fraud compared with 19 percent of adults.[27] Earlier this year, employees at the cybersecurity firm Terbium Labs spotted a set of stolen data—titled "infant fullz"—that contained a baby's full name, SSN, date of birth and mother's maiden name. The listing price was $312—significantly more than the $5 requested for similar bundles of information for adults.[28]

---

[22] Susan Tompor, *Social Security Benefits Stolen By Hackers, Leaving Families With Bill*, Detroit Free Press (Feb. 28, 2018), https://www.freep.com/story/money/personal-finance/susan-tompor/2018/02/28/identity-theft-crooks-steal-social-security-benefits/354307002/.
[23] Kenneth R. Harney, *Theft of Equifax data could lead to years of grief for home buyers and mortgage applicants*, Washington Post, (Sept. 13, 2017), https://www.washingtonpost.com/realestate/theft-of-data-could-lead-to-years-of-grief-for-home-buyers-and-mortgage-applicants/2017/09/12/ed0f66fc-971a-11e7-82e4-f1076f6d6152_story.html.
[24] *Id*.
[25] Lillian Ablon, Martin C. Libicki, & Andrea A. Golayix, RAND Corp., *Markets for Cybercrime Tools and Stolen Data*, at ix (2014), https://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf.
[26] Dell SecureWorks, *Underground Hacker Markets* 14 (2016), https://www.secureworks.com/resources/rp-2016-underground-hacker-.
[27] Kelli B. Grant, *Identity theft isn't just an adult problem. Kids are victims, too*, CNBC, (Apr. 24, 2018), https://www.cnbc.com/2018/04/24/child-identity-theft-is-a-growing-and-expensive-problem.html.
[28] Bree Fowler, *Why Child Identity Theft Is a Growing Concern During Tax Season*, Consumer Reports, (Apr. 12, 2018), https://www.consumerreports.org/identity-theft/why-child-identity-theft-is-a-growing-concern-during-tax-season/.

B. Consumers cannot protect themselves from the misuse of their SSN

The SSN is so coveted by identity thieves because, unlike a credit card number, it is almost impossible to change. In 2014, the Social Security Administration replaced only 250 SSNs due to identity theft or misuse.[29] The SSA will only replace an individual's SSN in the most extreme circumstances, such as "harassment, abuse, or life endangerment."[30] Even then, the SSA will only assign you a new number if "you've done all you can to fix the problems resulting from misuse of your SSN, and someone is still using your number."[31]

The credit reporting industry also makes it difficult for consumers to protect themselves. Credit freezes are burdensome and costly. Consumers wishing to freeze their credit must contact all three credit bureaus and pay a fee to each company every time they freeze and unfreeze their credit. Credit monitoring and fraud alerts are far less effective, and do not prevent thieves from accessing credit files or opening new accounts. The CEO of LifeLock had his identity stolen 13 times after he displayed his real SSN in a commercial that was supposed to demonstrate how effective his product was at preventing identity theft.[32]

III. There have been recent efforts to limit the use of the SSN, but much more needs to be done

In 2015, we explained to the Senate Special Committee on Aging that identity theft disproportionately targets seniors.[33] In 2017, Medicare finally announced that it would remove SSNs from Medicare benefits cards, the result of an effort led by Senators Susan Collins and Claire McCaskill.[34] And the Social Security Number Fraud Prevention Act of 2017, sponsored by Representative David Valadao of this Committee, prohibits federal agencies from including anyone's SSN on any document sent by mail unless authorized by law.[35]

---

[29] Aarti Shahani, *Theft of Social Security Numbers is Broader Than You Might Think*, NPR, (Jun. 15, 2015), https://www.npr.org/sections/alltechconsidered/2015/06/15/414618292/theft-of-social-security-numbers-is-broader-than-you-might-think.

[30] Soc. Sec. Admin., *Can I Change My Social Security Number?* (Mar. 11, 2016), https://faq.ssa.gov/link/portal/34011/34019/Article/3789/Can-I-change-my-.

[31] Soc. Sec. Admin., *Identity Theft and Your Social Security Number* 6 (Feb. 2016), https://www.ssa.gov/pubs/EN-05-10064.pdf.

[32] Kim Zetter, *LifeLock CEO's Identity Stolen 13 Times*, Wired (May 18, 2010), https://www.wired.com/2010/05/lifelock-identity-theft/.

[33] *Protecting Seniors from Identity Theft: Is the Federal Government Doing Enough*: *Hearing Before the S. Special Comm. on Aging*, 114th Cong. (Oct. 7, 2015) (statement of Marc Rotenberg, EPIC), https://epic.org/privacy/ssn/EPIC-SSN-Testimony-Senate-10-7-15.pdf.

[34] EPIC, *Medicare to Remove SSN from ID Cards*, (Sep. 5, 2017), https://epic.org/2017/09/medicare-to-remove-ssn-from-id.html.

[35] Pub. L. No. 115-59, 131 Stat. 1152 (2017).

In addition, a number of state laws limit the use of the SSN in higher education,[36] by private businesses,[37] by state agencies,[38] and financial institutions.[39] For example, Arizona prohibits state universities and community colleges from using the SSN as an ID number.[40] Rhode Island prohibits businesses from requiring consumers to disclose all or part of their SSN to purchase most goods or services.[41] A number of states prohibit private insurers from printing SSNs on identification cards.

Many private organizations have also curtailed or eliminated the use of the SSN. Georgetown University prohibits use of the SSN "as the primary record key, or sort key, in any University database or other business system or operation."[42] In lieu of SSNs, Georgetown uses the "Georgetown University ID," a "nine digit number beginning with the numeral 8" listed on each person's GU identification card.[43] And nearly a decade ago, the Blue Cross Blue Shield Association mandated that its members replace SSNs with Subscriber ID numbers.[44]

IV. Solutions to prevent misuse of SSNs and protect consumers

There is widespread support for legislation limiting the use of the SSN. According to a Pew Research Report, 90% of adults said they were "very sensitive" about their SSN, the highest percentage for any form of personal data.[45] Pew Research Center also found that 91% of consumers say they have lost control over how their personal information is collected, and 64% support greater regulation over how companies handle their personal information.[46] Even leading CEOs now support stronger privacy protections in the United States. Congress should adopt the following measures to limit the use of the SSN and protect consumers from identity theft and financial fraud:

- **Prohibit the use of the SSN in the private sector without explicit legal authorization**. While an employer should be permitted to ask an employee for an SSN for tax-reporting purposes, a health club should not be permitted to ask a customer for an SSN as a condition of membership. Even if a service is not conditional on someone providing their

---

[36] *See e.g.* N.Y. Educ. Code sec. 2-b; W. Va. Code Ann. sec. 18-2-5f; Ariz. Rev. Stat. Sec. 15-1823.
[37] *See e.g.* R.I. Gen. Laws 6-13-17; Vt. Stat. Ann. tit. 9, § 2440; N.C. Gen. Stat. § 75-62.
[38] *See e.g.* Ala. Code sec. 41-13-6; Cal. Civ. Code sec. 1798.85.
[39] *See e.g.* Mass. Gen. Laws. Ann. ch. 167B, sec. 14.
[40] Ariz. Rev. Stat. Sec. 15-1823.
[41] R.I. Gen. Laws 6-13-17.
[42] Georgetown University Information Security Office, *Policy on the Use, Collection, and Retention of Social Security Numbers by Georgetown University*, https://security.georgetown.edu/it-policies-procedures/use-collection-retention-policy#.
[43] *Id.*
[44] *Empire Physician Sourcebook*, EMPIRE BLUE CROSS BLUE SHIELD, https://www11.empireblue.com/provider/noapplication/f4/s2/t0/.
[45] Mary Madden, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, Pew Research Center (Nov. 14, 2014), http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/.
[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/.

SSN, having that field on a form causes many people to provide it anyway, assuming it is required.

- **Prohibit companies from compelling consumers to disclose their SSN as a condition of service or sale unless there is a statutory basis for the request**. Representative Patrick McHenry has proposed the PROTECT Act of 2017, which would prohibit consumer reporting agencies from using a consumer's SSN as a method to identify the consumer.[47] Congress should go much further, however, and prohibit its use for all commercial transactions unless the use is explicitly authorized by statute.

- **Promote technological innovations that enable development of context-specific identifiers**. A system of decentralized identification reduces the risks associated with data breaches and the misuse of personal information. Such a decentralized approach is consistent with our commonsense understanding of identification. If you're going to do banking, you should have a bank account number. If you're going to the library, you should have a library card number. Utility bills, telephone bills, insurance, the list goes on. An example of this approach is the Medical Identification Number used in Canada. These context-dependent usernames and passwords enable authentication without the risks of a universal identification system. That way, if one number gets compromised, all your other numbers are not spoiled, and identity thieves cannot access all your accounts. All of your accounts become compartmentalized, enhancing their security.

- **Do not replace the SSN with a national biometric identifier**. There have been proposals recently to replace the SSN with a national biometric "identity framework," with fingerprints and facial recognition.[48] This is the wrong solution and would raise serious privacy and security risks. In passing the Privacy Act of 1974, Congress was specifically reacting to and rejecting calls for the creation of a single entity for the reference and storage of personal information. There are also significant problems that would arise with the breach of a biometric identifier. In fact, in the massive OPM data breach, foreign hackers targeted the digitized fingerprints stored in federal databases.[49] That risk would be compounded if the US were to move to a national biometric identification system.

Conclusion

There is little dispute that identity theft is one of the greatest concerns for consumers in the United States today. There are many factors that have contributed to this problem, but the

---

[47] H.R. 4028, 115th Cong. (2017).

[48] *See, e.g.*, *Protecting Consumers in the Era of Major Data Breaches*: *Hearing Before the S. Comm. on Commerce, Science and Transportation*, 115th Cong. (Nov. 8, 2017), (statement of Todd Wilkinson, President and CEO, Entrust Datacard), https://www.commerce.senate.gov/public/_cache/files/9348f11b-49a4-4c47-922e-f5cc98d61b54/469C33D81041FAB151DC6B1E6608A18B.11.08.2017---wilkinson-testimony.pdf.

[49] David E. Sanger, *Hackers Took Fingerprints of 5.6 Million U.S. Workers, Government Says*, N.Y. Times, (Sept. 23, 2015), https://www.nytimes.com/2015/09/24/world/asia/hackers-took-fingerprints-of-5-6-million-us-workers-government-says.html.

widespread use of the SSN in the private sector and the failure to establish privacy safeguards are key parts of the problem. It is time that Congress passed strong and effective legislation that will limit the use of the SSN, encourage the development of more robust systems for identification that safeguard privacy and security, and not limit the ability of states to develop better safeguards. Congress must not, however, replace the SSN with a new national identification system.

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