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

May 22, 2017

The Honorable Sam Johnson, Chairman
The Honorable John Larson, Ranking Member
House Committee on Ways & Means
Social Security Subcommittee

The Honorable William Hurd, Chairman
The Honorable Robin Kelly, Ranking Member
House Committee on Oversight and Government Reform
Subcommittee on Information Technology

Dear Chairman Johnson, Chairman Hurd, Ranking Member Larson, and Ranking Member Kelly:

We write to you regarding the hearing "Joint Oversight Hearing on Protecting Americans' Identities: Examining Efforts to Limit the Use of Social Security Numbers."[1] EPIC is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC has participated in the leading cases involving the privacy of the Social Security Number ("SSN") and has frequently testified in Congress about the need to establish privacy safeguards for the SSN to prevent the misuse of personal information.[2] EPIC also maintains an archive of information about the SSN online.[3]

---

[1] *Joint Oversight Hearing on Protecting Americans' Identities: Examining Efforts to Limit the Use of Social Security Numbers*, 115th Cong. (2017), H. Comm. on Ways and Means, Subcomm. on Social Security and H. Comm. on Oversight and Gov't Reform, Subcomm. on Information Tech., https://waysandmeans.house.gov/event/joint-oversight-hearing-protecting-americans-identities-examining-efforts-limit-use-social-security-numbers/ (May 23, 2017).

[2] *See, e.g., Greidinger v. Davis*, 988 F.2d 1344 (4th Cir. 1993) ("Since the passage of the Privacy Act, an individual's concern over his SSN's confidentiality and misuse has become significantly more compelling"); *Beacon Journal v. Akron*, 70 Ohio St. 3d 605 (Ohio 1994) ("the high potential for fraud and victimization caused by the unchecked release of city employee SSNs outweighs the minimal information about governmental processes gained through the release of the SSNs"); Marc Rotenberg, EPIC, *Testimony at a Hearing on Protecting Seniors from Identity Theft: Is the Federal Government Doing Enough", Before the S. Special Comm. on Aging*, 114th Cong. (Oct. 7, 2015), *available at* https://epic.org/privacy/ssn/EPIC-SSN-Testimony-Senate-10-7-15.pdf; Marc Rotenberg, EPIC, *Testimony at a Hearing on Protecting the Privacy of the Social Security Number from Identity Theft, Before the H. Ways & Means Subcom. on Social Security*, 110th Cong. (June 21, 2007), *available at* https://epic.org/privacy/ssn/idtheft_test_062107.pdf; Marc Rotenberg, *Testimony at a Joint Hearing on Social Security Numbers & Identity Theft, Before the H. Fin. Serv. Subcom. on Oversight & Investigations and the H. Ways & Means Subcom. on Social Security*, 104th Cong. (Nov. 8, 2001), *available at* http://www.epic.org/privacy/ssn/testimony_11_08_2001.html; Chris Jay Hoofnagle, EPIC, *Testimony at a Joint Hearing on Preserving the Integrity of Social Security Numbers and Preventing Their Misuse by Terrorists and Identity Thieves Before the H. Ways & Means Subcom. on Social Security*

We appreciate your Subcommittees' interest in SSN privacy issues. It is important to emphasize the unique status of the SSN in the world of privacy. There is no other form of individual identification that plays a more significant role in record-linkage and no other form of personal identification that poses a greater risk to personal privacy. The use of the number for identification poses an ongoing risk of identity theft, financial fraud, and other forms of crime.

Social Security Number History and the Importance of Limiting SSN Collection

The Social Security Number is the classic example of "mission creep," a program designed for a specific, limited purpose has been transformed for additional, unintended purposes, often with disastrous results. The pervasiveness of the SSN and its use to both identify and authenticate individuals threatens privacy and financial security.

These risks associated with the expanded use of the SSN underscore the importance of the hearing today. But this problem has been well known to Congress for many years.

A major government report on privacy in 1973 outlined many of the concerns with the use and misuse of the SSN that show a striking resemblance to the problems we face today. Although the term "identify theft" was not yet in use, a detailed report, prepared by Willis Ware and technical experts and legal scholars, made clear the risks from the expanded use of the SSN.[4]

The Report of the Ware Commission provided the cornerstone of the landmark Privacy Act of 1974. In enacting the Privacy Act, Congress recognized the dangers of widespread use of SSNs as universal identifiers, and included provisions to limit the uses of the SSN. The Act makes it unlawful for a government agency to deny a right, benefit or privilege because an individual refuses to disclose his or her SSN. Section 7 of the Privacy Act specifically provides that any agency requesting that an individual disclose his or her SSN must "inform that individual whether that disclosure is mandatory or voluntary, by what statutory authority such number is solicited, and what uses will be made of it."[5] This section reflects a presumption that the SSN should not be used for recordkeeping purposes unrelated to Social Security and taxation. In its report supporting adoption of Section 7, the Senate Committee stated that the widespread use of the SSN as a universal identifier in the public and private sectors is "one of the most serious manifestations of privacy concerns in the Nation."[6]

Since passage of the Privacy Act, concern about SSN confidentiality and misuse has become even more compelling. The SSN is central to identity theft in the United States. In 2016,

---

& the H. Judiciary Subcom. on Immigration, Border Sec. & Claims, 105th Cong. (Sept. 19, 2002), *available at* http://www.epic.org/privacy/ssn/ssntestimony9.19.02.html.

[3] Social Security Numbers, EPIC, https://epic.org/privacy/ssn/.

[4] Department of Health, Education, and Welfare (HEW), *Records Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems* (1973) (Ware Commission report), available at https://www.epic.org/privacy/hew1973report/.

[5] Privacy Act of 1974, 5 U.S.C. § 552 (a) (2006).

[6] S.Rep. No. 1183, 93d Cong., 2d Sess., reprinted in 1974 U.S. Code Cong. & Admin. News 6916, 6943.

almost 30% of identity theft complaints received by the FTC were incidents of tax fraud.[7] In 2015, it was announced that the Office of Personnel Management was the target of one of the worst data breaches in US history. The breach compromised the personal information of over 21.5 million individuals, including social security numbers and fingerprints.[8] Also in 2015, taxpayer data for over 610,000 Americans, including SSNs, was stolen from the Internal Revenue Service.[9]

Solutions to Prevent the Misuse of SSNs and Identity Theft Risks

EPIC favors technological innovation that enables the development of context-dependent identifiers. Such a decentralized approach to identification 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. If you are enrolled in a university, you should have a student ID number. Utility bills, telephone bills, insurance, the list goes on. These context-dependent usernames and passwords enable authentication without the risk of a universal identification system. That way, if one number gets compromised, all the numbers are not spoiled and identity thieves cannot access all your accounts. All your accounts can become compartmentalized, enhancing their security.

Conclusion

The reality is that today the SSN is the key to some of our most sensitive and personal information, and it is more vulnerable than ever. Given the growing risk of identity theft coupled to the SSN and the ease of alternative systems, there is simply no excuse for the use of SSNs in either the public or private sector. *The need to find a solution to the problem of the widespread use of the SSN is critical.*

We ask that this statement be entered in the hearing record. EPIC looks forward to working with the Subcommittees on these issues of vital importance to the American public.

Sincerely,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

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

---

[7] FED. TRADE COMM'N, CONSUMER SENTINEL NETWORK DATA BOOK FOR JANUARY – DECEMBER 2016 12 (2017), https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2016/csn_cy-2016_data_book.pdf.

[8] Julie Hirschfeld Davis, "Hacking of Government Computers Exposed 21.5 Million People," NY Times (July 9, 2015), https://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html.

[9] Lisa Rein, "IRS says breach of taxpayer data far more widespread than it first thought: 610,000 taxpayers at risk," Wash. Post (August 17, 2015), http://www.washingtonpost.com/blogs/federal-eye/wp/2015/08/17/irs-says-breach-of-taxpayer-data-far-more-widespread-than-it-first-thought-610000-taxpayers-at-risk/.