epic.org | ELECTRONIC PRIVACY INFORMATION CENTER

Testimony and Statement for the Record of

Marc Rotenberg
President, EPIC
Adjunct Professor, Georgetown Law

Hearing on

"Protecting Seniors from Identity Theft: Is the Federal Government Doing Enough?"

Before the

U.S. Senate Special Committee on Aging

October 7, 2015
562 Dirksen Senate Office Building
Washington, DC

I. Introduction

Chairman Collins and Members of the Senate Committee, thank you for the opportunity to testify today regarding the use of SSNs on Medicare cards and the risks facing senior citizens in the United States. My name is Marc Rotenberg, and I am President of the Electronic Privacy Information Center ("EPIC"). I also teach Information Privacy Law at Georgetown Law. I am a former chair of the ABA Committee on Privacy and Information Security and the coauthor of a forthcoming casebook on privacy law.[1]

EPIC is a non-partisan research organization, 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]

We appreciate the Special Committee's 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

---

[1] ANITA L. ALLEN & MARC ROTENBERG, PRIVACY LAW AND SOCIETY (WEST 2016). *See also,* MARC ROTENBERG, JULIA HORWITZ, & JERAMIE SCOTT, EDS. PRIVACY IN THE MODERN AGE: THE SEARCH FOR SOLUTIONS (THE NEW PRESS 2015).

[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, Exec. Dir., 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, Exec. Dir., EPIC, *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.

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

privacy. The use of the number for identification poses an ongoing risk of identity theft, financial fraud, and other forms of crime.

II. Social Security Number History and the Importance of Limiting SSN Collection

The Social Security Number is the classic example of "mission creep," a particular 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 and identification cards 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 leading technical experts and legal scholars, made clear the risks from the expanded use of the Social Security Number.[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 the SSN as a universal identifier, and included provisions to limit its use. The Privacy 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

[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/

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 Social Security number 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.

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. We have urged the Congress to implement SSN privacy protections for over two decades, beginning in 1991 when I first testified before a House Committee at a hearing on the "Use of Social Security Number as a National Identifier."[7] The U.S. Government Accountability Office has urged Congress to remove SSNs from government documents since 2004.[8] In 2006, the growing misuse of the SSN and associated identity theft risks prompted President George W. Bush to establish an Identity Theft Taskforce. In a 2008 audit, the Inspector General for the Social Security

[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.
[7] Testimony of Marc Rotenberg, Computer Professionals for Social Responsibility, "Use of Social Security Number as a National Identifier," Before the Subcomm. on Social Security of the House Comm. on Ways and Means, 102d Cong., 1st Sess. 71 (February 27, 1991). republished Marc Rotenberg, "The Use of the Social Security Number as a National Identifier," *Computers & Society,* vol. 22, nos. 2, 3, 4 (October 1991).
[8] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-04-768T, SOCIAL SECURITY NUMBERS: USE IS WIDESPREAD AND PROTECTIONS VARY (2004).

Administration recommended swift removal of SSNs from Medicaid cards, supported by the following observation:

> Despite the increasing threat of identity theft, CMS continued to display SSNs on identification cards it issued to Medicare beneficiaries. Displaying such information on Medicare cards unnecessarily places millions of individuals at-risk for identity theft. This is particularly troubling because CMS instructs individuals, many of whom are elderly, to carry their Medicare card with them when away from home. We do not believe a Federal agency should place more value on convenience than the security of its beneficiaries' personal information.[9]

The SSN is central to identity theft in the United States. In 2014, 17.6 million U.S. residents experienced identity theft.[10] Elderly Americans are most at risk of identity theft and the problem is getting worse. According to the U.S. Department of Justice, "[m]ore persons age 65 or older were identity theft victims in 2014 (2.6 million) than in 2012 (2.1 million). The number of identity theft victims in all other age groups measured did not significantly change from 2012 to 2014."[11] According to the FTC's most recent Consumer Sentinel Network (CSN) Data Book, 39% of identity theft victims in 2014 were age 50 or older.[12]

Increasing data breaches in the healthcare industry compound the threat to seniors posed by the use of SSNs on Medicare cards. According to one 2015 study, 91 percent of healthcare organizations had experienced a data breach in the past twenty four months,

---

[9] U.S. SOC. SEC. ADMIN., OFFICE OF THE INSPECTOR GEN., A-08-08-18026, REMOVING SOCIAL SECURITY NUMBERS FROM MEDICARE CARDS (2008), http://oig.ssa.gov/sites/default/files/audit/full/html/A-08-08-18026.html.

[10] BUREAU OF JUSTICE STATISTICS, U.S. DEP'T OF JUSTICE, 17.6 MILLION U.S. RESIDENTS EXPERIENCED IDENTITY THEFT IN 2014 (Sept. 27, 2015), http://www.bjs.gov/content/pub/press/vit14pr.cfm.

[11] BUREAU OF JUSTICE STATISTICS, U.S. DEP'T OF JUSTICE, NCJ 248991, VICTIMS OF IDENTITY THEFT, 2014 3 (2014), http://www.bjs.gov/content/pub/pdf/vit14.pdf.

[12] FED. TRADE COMM'N, CONSUMER SENTINEL NETWORK DATA BOOK FOR JANUARY – DECEMBER 2014 14 (2015), https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2014/sentinel-cy2014-1.pdf.

and 40 percent has more than five data breaches during that time period.[13] Another study found that 42.5% of all data breaches in 2014 occurred in this field, outpacing breaches in all other sectors. A third study warns of the persistent and growing threat of healthcare breaches.[14]

Given the rising frequency of healthcare data breaches, the use of SSNs on Medicare cards places an already vulnerable population at even greater risk for identity theft. In addition, the crime of medical identity theft – when someone uses another individual's identity to obtain medical goods and services – can cause significant harm to victims.[15]

The need to find a solution to the problem of the widespread use of the SSN is critical.

III. Solutions to Prevent the Misuse of SSNs and Identity Theft Risks

Fortunately, CMS does not need to look far to find a model for removing and replacing SSNs on Medicare cards. The U.S. Department of Defense has engaged in similar efforts over the past several years. According to DOD's published materials on the SSN Reduction Plan,

> In response to an increasing awareness of the growing need to protect the safety of Service members and their families' identity information, the Department of Defense (DoD) has begun to eliminate the Social Security Numbers (SSN) from DoD identification (ID) cards. In support of this

[13] The Ponemon Institute, *Fifth Annual Benchmark Study on Privacy and Security of Healthcare Data* (May 2015), https://www2.idexpertscorp.com/fifth-annual-ponemon-study-on-privacy-security-incidents-of-healthcare-data.
[14] Experian, *2015 Second Annual Data Breach Industry Forecast* 2 (2015), https://www.experian.com/assets/data-breach/white-papers/2015-industry-forecast-experian.pdf?_ga=1.172114915.1943093614.1418003182
[15] *Medical Identity Theft*, WORLD PRIVACY FORUM, https://www.worldprivacyforum.org/category/med-id-theft/ (last visited Oct. 5, 2015).

initiative, a three-phased plan for the removal of the SSN on all DoD ID cards was announced.[16]

The DoD stopped printing SSNs on all DoD ID cards as of June 2011. SSNs are being replaced with DoD ID Numbers on all ID cards, and DoD Benefits Numbers on cards that provide healthcare benefits. The U.S. Department of Veterans Affairs also introduced new Veterans Health Identification Cards in 2014 that removed SSNs from the cards' magnetic strips and barcodes.[17]

Recognizing the huge risk of printing SSNs on identification cards, numerous states have already required private insurers to eliminate the practice. Arizona,[18] Colorado,[19] Georgia,[20] Hawaii,[21] Illinois,[22] New Jersey,[23] North Carolina,[24] Texas,[25] Utah,[26] Virginia,[27] and Washington[28] all have laws prohibiting the printing of an individual's SSN on his or her insurance card. Other state laws limit the use of SSNs in higher education,[29] by private businesses,[30] by state agencies,[31] and financial

[16] Def. Human Res. Activity, Dep't of Def., *Removal of the Social Security Number (SSN) From DoD ID Cards*, http://www.cac.mil/docs/SSNReductionUpdate_201409.pdf (last visited Oct. 5, 2015).
[17] Hans Petersen, *New ID Cards for Vets Enrolled in VA Health Care*, U.S. DEP'T OF VETERANS AFFAIRS (Feb. 24, 2014) http://www.va.gov/health/newsfeatures/2014/february/new-id-cards-for-vets-enrolled-in-va-health-care.asp.
[18] Ariz. Rev. Stat. § sec. 44-1373.
[19] Colo. Rev. Stat. § 10-3-129.
[20] Ga. Code Ann. § 33-24-57.1.
[21] Haw. Rev. Stat. § 487J-2.
[22] 815 Ill. Comp. Stat. § 505/2QQ.
[23] N.J. Stat. Ann. C.56:8-164.
[24] N.C. Gen. Stat. sec 75-62.
[25] Tex. Bus. & Com. Code § 35.58.
[26] Utah Code § 31A 21-110.
[27] Va. Code sec 59.1-443.2.
[28] Wash. Rev. Code Ann. sec 48.43.022.
[29] *See e.g.* N.Y. Educ. Code sec. 2-b; W. Va. Code Ann. sec. 18-2-5f; Ariz. Rev. Stat. Sec. 15-1823.
[30] *See e.g.* R.I. Gen. Laws 6-13-17.
[31] *See e.g.* Ala. Code sec. 41-13-6; Cal. Civ. Code sec. 1798.85.

institutions.[32] In 2004, Congress passed legislation prohibiting the display of SSNs on state drivers' licenses.[33]

Many private organizations that provide comprehensive health services do not use the SSN as a patient identifier. For example, the Harvard Community Health Plan, with over half a million subscribers, uses a separate number for patient identification in its automated records system. The SSN is collected for administrative use but is not publicly disclosed. Nearly a decade ago, the Blue Cross Blue Shield Association mandated that its members replace SSNs with Subscriber ID numbers by January 1, 2006.[34] Today, most private health insurance companies have abandoned the use of SSNs as patient identifiers in light of identity theft concerns.[35]

To safeguard against privacy threats that SSNs present, universities have routinely adopted policies prohibiting the use of SSNs for student ID numbers and cards. For example, Georgetown University's "Policy on the Use, Collection, and Retention of Social Security Numbers by Georgetown University" states:

> The University will take steps necessary and appropriate to guard the confidentiality of SSNs and to eliminate or minimize its exposure to liability and other harms arising from unauthorized access to, or data breaches involving, SSNs. No use of the SSN, or any part of the SSN, is permitted except as authorized under this Policy. SSNs are highly confidential information and must be handled in accordance with applicable law pursuant to this policy.[36]

---

[32] *See e.g.* Fla. Stat. Ann. sec 659.062; Mass. Gen. Laws. Ann. ch. 167B, sec. 14.
[33] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458 § 7214, 118 Stat. 3638, 3832 (codified at 42 U.S.C. § 405(c)(2)(C)(vi)(II) (2012).
[34] *Empire Physician Sourcebook*, EMPIRE BLUE CROSS BLUE SHIELD, https://www.empireblue.com/provider/noapplication/f4/s2/t0/pw_e209016.pdf?refer=ehpprovider (last visited Oct. 5, 2015).
[35] Robert Pear, *New Cards for Medicare Recipients Will Omit Social Security Numbers*, N.Y. TIMES (Apr. 20, 2015), http://www.nytimes.com/2015/04/21/us/new-law-to-strip-social-security-numbers-from-medicare-cards.html?_r=0.
[36] Georgetown University Information Security Office, *Policy on the Use, Collection, and Retention of Social Security Numbers by Georgetown University*, https://security.georgetown.edu/technology-policies/use-collection-retention-policy.

The policy holds:

> **SSNs, or any part of the SSN, are NOT permitted:**
> 1. As the primary record key, or sort key, in any University database or other business system or operation
> 2. As an identifier among University departments or with external University affiliates
> 3. To be transferred by the University to external entities (i.e. benefits providers)[37]

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, [which] may be used to identify, track, and provide services to individuals for all University electronic and paper data systems and processes."[38]

Georgetown's policy is partially adapted from Northwestern's SSNs policy, which states in relevant part:

> 1. [T]he University does not permit the use of a SSN as the primary identifier for any person or entity in any system, except where the SSN is required or permitted by law, and permitted by University policy. . . .
>
> 4. Except where the SSN is required by law, the University ID (EMPLID) replaces use of the SSN and will be used in all future electronic and paper data systems and processes to identify, track, and service individuals associated with the University. The University ID will be permanently and uniquely associated with the individual to whom it is originally assigned.[39]

---

[37] *Id*.
[38] *Id*.
[39] Northwestern University Information Technology, *Information Security Policy and Standards: Secure Handling of Social Security Numbers*, http://www.it.northwestern.edu/policies/SSN_policy.html. *See also* Virginia Tech Office of the University Registrar, *Student Identification Numbers*, https://www.registrar.vt.edu/faculty/privacy/student-numbers.html; University of Pittsburgh, *Use and Management of Social Security Numbers and University Primary ID ("UPI") Numbers*, https://www.cfo.pitt.edu/policies/policy/10/10-02-08.html; University of New Mexico, *The Pathfinder – UNM Student Handbook*, "Student ID Number and Social Security Numbers," https://pathfinder.unm.edu/common/policies/student-id-number-policy.html.

EPIC favors technological innovation that enables the development of context-dependent identifiers. For the purpose of Medicare cards, a context-dependent identifier would be a specific number assigned to an individual for the specific purpose of Medicare patient identification. An example of this is the Medical Identification Number used in Canada. This would be conceptually similar to a student ID number, driver's license number, bank account number, utility bill number, the list goes on.[40] Rather than using the SSN to identify and authenticate an individual across these various contexts, individuals would be assigned separate numbers depending on the context. These context-dependent usernames and passwords enable authentication without the risk of a universal identification system. That way, if one number gets compromised, all of the numbers are not spoiled and identity thieves cannot access all of your accounts. All of your accounts can become compartmentalized, enhancing their security.

IV. Conclusion

Given the growing risk of identity theft coupled to the SSN and the fact that other federal agencies have already removed the SSN from identity cards, there is simply no excuse for further delay by CMS. We urge the committee to ensure that the problem is addressed before the elderly in America face the ever-greater risk of financial fraud and medical fraud.

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

[40] Testimony of Marc Rotenberg, Computer Professionals for Social Responsibility, "Use of Social Security Number as a National Identifier," Before the Subcomm. on Social Security of the House Comm. on Ways and Means, 102d Cong., 1st Sess. 71 (February 27, 1991).