epic.org | ELECTRONIC PRIVACY INFORMATION CENTER

Testimony of

Caitriona Fitzgerald, State Policy Coordinator

Electronic Privacy Information Center (EPIC)

Hearing on

Assembly Bill 303 relating to: prohibiting the Department of Workforce Development from requiring a job seeker to furnish his or her social security number to that department as a precondition to using the services of the job center network, including using the job center network Internet site.

Before the

Committee on Workforce Development

Wisconsin State Assembly

September 15, 2015

I. Introduction

My name is Caitriona Fitzgerald, and I am the State Policy Coordinator for the Electronic Privacy Information Center (EPIC). EPIC is a non-partisan research organization established in 1994 to focus public attention on emerging privacy and civil liberties issues.[1] We work with a distinguished panel of advisors in the fields of law, technology, and public policy.[2] EPIC is pleased to respond to Representative Loudenbeck's request for testimony on Assembly Bill 303 Relating to: *prohibiting the Department of Workforce Development from requiring a job seeker to furnish his or her social security number to that department as a precondition to using the services of the job center network, including using the job center network Internet site*.

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.[3] EPIC also maintains an archive of information about the SSN online.[4]

---

[1] About EPIC, EPIC, https://epic.org/epic/about.html.

[2] EPIC Advisory Board, EPIC, https://epic.org/epic/advisory_board.html.

[3] *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; Chris Jay Hoofnagle, Legislative Counsel, 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 & 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.

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

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.

This testimony will outline: the history of the SSN, the importance of limiting SSN collection, why DWD's collection of users' SSN is an unnecessary privacy risk, and other states' approaches to providing job search services without collecting SSN.

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

SSN is the classic example of "mission creep," where a program designed for a specific, limited purpose has been transformed for additional, unintended purposes, some times 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 bill being heard today.

The SSN was created in 1936 for the purpose of administering the Social Security laws. SSNs were intended solely to track workers' contributions to the Social Security fund.[5] Legislators and the public were immediately distrustful of such a tracking system, which can be used to index a vast amount of personal information and track the behavior of citizens. Public concern over the potential abuse of the SSN was so high that the first regulation issued by the new Social Security Board covered confidentiality and privacy.[6]

[5] U.S. Social Security Administration, *The Story of the Social Security Number*, http://www.ssa.gov/policy/docs/ssb/v69n2/v69n2p55.html.
[6] U.S. Social Security Administration, *Regulation No. 1*, http://www.ssa.gov/history/reg1.html.

Over time, however, legislation allowed the SSN to be used for purposes unrelated to the administration of the Social Security system. For example, in 1961 Congress authorized the Internal Revenue Service to use SSNs as taxpayer identification numbers.

A major government report on privacy in 1973 outlined many of the concerns with the use and misuse of the Social Security Number that show a striking resemblance to the problems we face today. Although the term "identify theft" was not yet in use, *Records Computers and the Rights of Citizens* described the risks of a "Standard Universal Identifier," how the number was promoting invasive profiling, and that many of the uses were clearly inconsistent with the original purpose of the 1936 Act. The report recommended several limitations on the use of the SSN and specifically said that legislation should be adopted "prohibiting use of an SSN, or any number represented as an SSN for promotional or commercial purposes."[7]

In enacting the landmark Privacy Act of 1974, Congress recognized the dangers of widespread use of SSNs as universal identifiers, and included provisions to limit the uses of the SSN. 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 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."[8] The Privacy Act makes clear Congress' recognition of the dangers of widespread use of SSNs as universal identifiers.

The Senate Committee report stated that the widespread use of SSNs as universal identifiers in the public and private sectors is "one of the most serious manifestations of privacy

[7] 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/.

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

concerns in the Nation." Short of prohibiting the use of the SSN outright, Section 7 of the Privacy Act provides that any agency requesting that an individual disclose his 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." This provision attempts to limit the use of the number to only those purposes where there is clear legal authority to collect the SSN. It was hoped that citizens, fully informed that the disclosure was not required by law and facing no loss of opportunity in failing to provide the SSN, would be unlikely to provide an SSN and institutions would not pursue the SSN as a form of identification.

But 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. According to a recent Pew Research Report, 90% of adults said that they were "very sensitive" about their social security number, the highest percentage of any set of personal information, including health data and content of their phone conversations.[9] This past June, the Office of Personnel Management was the target of one of the worst data breaches in US history. News reports suggest that the personal information, including SSNs, of more than 18 million government employees may have been breached.[10] Also this year, taxpayer data for over 610,000 Americans, including SSNs, was stolen from the Internal Revenue Service.[11] These breaches demonstrate why Section 7 of the Privacy Act is so important and why DWD should not be unnecessarily collecting Wisconsin job seekers' social security numbers.

---

[9] Mary Madden et al., *Public Perceptions of Privacy and Security in the Post-Snowden Era,* Pew Research Center, Washington D.C. (November 12, 2014). http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/, accessed on September 14, 2015.

[10] Evan Perez and Shimon Prokupecz, "U.S. data hack may be 4 times larger than the government originally said." (June 24, 2015) http://edition.cnn.com/2015/06/22/politics/opm-hack-18-milliion/index.html

[11] Lisa Rein, "IRS says breach of taxpayer data far more widespread than it first thought: 610,000 taxpayers at risk." (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/

III. The Wisconsin Dept. of Workforce Development's SSN Requirement to Use the Job Center Network is an Unnecessary Privacy Risk

The Wisconsin Department of Workforce Development ("DWD") requires a user to enter their SSN to use most of the job search tools on the Job Center of Wisconsin website.[12] The website gives the user the option to decline to provide SSN, but doing so basically strips all functionality from the site. The legislation under consideration, AB303, prohibits the DWD from requiring a job seeker to furnish his or her SSN as a precondition to using the services of the Job Center website.

DWD has indicated that the U.S. Department of Labor ("DOL") requires the agency to report self-service participants and the Department was required by DOL to change its online registration in 2011 after a comprehensive review. DOL referenced the Wagner-Peyser Act and "DOL's Training and Employment Notice (TEN) 08-10 reporting recommendations" as the basis of their finding.

TEN 08-10 states:

> While individual state online systems will vary, in general, only those individuals who complete a registration process and engage in self-directed or informational activities, such as posting a resume or application, searching for job opening, or requesting a referral to a job listing are to be counted as self-service Wagner-Peyser and [Workforce Investment Act] Adult program participants. All anonymous individuals are excluded as are individuals that do not provide a social security number (or alternative unique identification number).[13]

Further, a 2008 Guidance Letter from the Department of Labor's Employment and Training Administration Advisory System entitled "Policy for Collection and Use of Workforce System Participants' Social Security Numbers" states:

---

[12] *See* https://jobcenterofwisconsin.com

[13] Department of Labor, Training and Employment Notice No. 08-10, *available at* http://wdr.doleta.gov/directives/attach/TEN/ten2010/ten08-10.pdf (2010).

> This guidance does not imply or require that a participant provide a social security number to the state to receive services through [the Workforce Investment Act] or any other workforce investment program, with the exception of a participant filing a claim for unemployment compensation. In instances where a participant does not provide a social security number, states should exclude the outcomes of this individual from performance measures, unless supplemental information is available to verify the performance outcomes for non-wage based measures, which is consistent with established policy.[14]

Thus, it is clear that states can develop alternate techniques for unique identification of program participants. The Guidance Letter goes on to state that states must "[keep] in mind that the state must not deny access to any participant who refuses to provide a social security number," citing Section 7 of the Privacy Act.[15]

IV. Other States Do Not Require SSN Collection for Job Seekers

Other states have managed to implement the Workforce Investment Act and offer their residents online job seeker tools without requiring the collection of the SSN. For example, Michigan[16] and New York[17] require a unique email address, but not SSN. Minnesota's job search website states:

> You are encouraged, but not required, to provide your Social Security Number (SSN). We use your SSN to improve our service. Every precaution is taken to safeguard your private data, including encryption and secure databases. If you choose not to share your SSN, please enter a unique nine-digit number beginning with the number 9.[18]

In Illinois, a user can simply decline to provide their SSN, but can still use the job seeker tools.[19]

---

[14] U.S. Department of Labor, Employment and Training Administration Advisory System: "Policy for Collection and Use of Workforce System Participants' Social Security Numbers," *available at* http://wdr.doleta.gov/directives/attach/TEGL/TEGL05-08.pdf (2008).
[15] *Id.*
[16] Pure Michigan Talent Connect, https://jobs.mitalent.org/job-seeker-create-account/ (last visited Sept. 14, 2015).
[17] New York State Career Services, https://labor.ny.gov/careerservices/careerservicesindex.shtm (last visited Sept. 14, 2015).
[18] MinnesotaWorks.Net, https://www.minnesotaworks.net/Registration/SeekerRegistration.aspx (last visited Sept. 14, 2015).
[19] Illinois Job Link, https://illinoisjoblink.illinois.gov/ada/mn_jsreg_dsp.cfm (last visited Sept. 14, 2015).

In Florida, a 2007 memorandum[20] from the state's Director for Workforce Services specified how to create a pseudo social security number specifically for individuals who cannot, or refuse to, provide their social security number but who are requesting Wagner-Peyser services. It directs career center staff to construct a number as follows:

> *1. Enter "9" as the first digit.*
> *2. Enter the last two digits of the jobseeker's birth year as the next two digits.*
> *3. Enter zeros as the two middle digits, and*
> *4. The last four digits will be sequentially the month and day of birth.*

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're renting videos from a video rental store, you should have a video rental store card number. Utility bills, telephone bills, insurance, the list goes on.[21] 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. Wisconsin's DWD could develop such an approach for its Job Center website.

V. Conclusion

There is little dispute that identity theft is one of the greatest problems facing consumers in the United States today. There are many factors that have contributed to this crime, but there is

[20] http://www.floridajobs.org/PDG/Memos/pdf/general/PseudoSSNs062907.pdf

[21] 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).

no doubt that the misuse of the Social Security and the failure to establish privacy safeguards are key parts of the problem.

It is simply inconsistent with Section 7 of the Privacy Act to require a Wisconsin resident to surrender their social security number in order to perform the simple task of searching for a job. DWD can choose to develop a different technique for authenticating users or it can alter its approach as to which users are reported to DOL as self-service participants. No matter the solution, Wisconsin job seekers should not be denied access to useful information provided by the state because they do not want to disclose their SSNs.