STATEMENT

of

Paul Rosenzweig
Senior Fellow, R Street Institute
Red Branch Consulting, PLLC
Professorial Lecturer in Law, George Washington University
Washington, D.C.

before the

Subcommittee on Social Security
Committee on Ways and Means
United States House of Representatives

May 17, 2018

The Future of the Social Security Number

Introduction

Chairman Johnson, Ranking Member Larson, and Members of the Subcommittee, I thank you for your invitation to appear today and present testimony on the question of data security and the use of Social Security Numbers (SSNs). My name is Paul Rosenzweig and I am a Senior Fellow at the R Street Institute.[1] I am also the Principal and founder of a small consulting company, Red Branch Consulting, PLLC, which specializes in, among other things, cybersecurity policy and legal advice; a Senior Advisor to The Chertoff Group and a Professorial Lecturer in Law at George Washington University, where I teach a course on Cybersecurity Law and Policy and another on Artificial Intelligence Law and Policy. From 2005 to 2009, I served as the Deputy Assistant Secretary for Policy in the Department of Homeland Security.

[1] The R Street Institute is a public policy, research, and educational organization recognized as exempt under section 501(c)(3) of the Internal Revenue Code. It is privately supported and receives no funds from any government at any level, nor does it perform any government or other contract work. Information about our funding is available at: http://www.rstreet.org/about-rstreet/funding-and-expenditures. My Truth in Testimony Disclosure accompanies this testimony.

Members of R Street testify as individuals discussing their own independent research. The views expressed are their own and do not reflect an institutional position for the R Street Institute or its board of trustees. I thank my colleagues at R Street for their research assistance and for helpful comments on an earlier draft of this testimony.

My testimony today is in my individual capacity and does not reflect the views of any institution with which I am affiliated or any of my various clients.

In my testimony today, I want to make a few points, which I can summarize as follows:

- The Social Security Number has a long history of utility as an identifier. Over time, however, the use case for SSNs has mutated so that now it is frequently used both as an identifier and as an authenticator.
- Authenticators of identity only have utility to the extent they rely on confidential, non-public information. This is classically defined as something you know, something you have or something you are. Initially SSNs appeared to be a suitable authenticator since they were non-public information that only a Social Security recipient would know.
- Today, however, SSNs are so deeply compromised and so widely available to the public (albeit, often through criminal settings) that they can no longer be used as an authenticator. This is because recent incidents, such as the Equifax breach (the anniversary of which occurs this week), have effectively disclosed the vast majority of previously confidential SSNs.
- As a result, any enterprise that continues to use an SSN as an authenticator is engaging in borderline cybersecurity malpractice. Yet, some do. Just the other day, for example, the last-four digits of my own SSN were used to verify my identity when I went to renew my Bar membership.
- In my view, Congress has the following three options for dealing with this problem. They range from worst to best.
    - Regulate or outlaw the use of SSNs. This is a plausible solution but one that comes with all of the usual disadvantages of government intervention: regulatory gridlock, administrative costs, and enforcement systems that necessitate procedural safeguards. In short, a regulatory response would come at great expense with a slow result, perhaps even no quicker than doing nothing.
    - Do nothing. The disutility of the SSN as an authenticator continues to become widely apparent. Eventually, the market will take care of the problem, but not before many more Americans suffer from data breach and identity theft.
    - Eliminate the utility of the SSN as an authenticator. Make it impossible, in practice, for anyone to continue to use it in this way. One simple, indeed quite elegant, solution (that I offer as both a thought experiment and as a possible practical answer) is to simply publish a phone book with the name and SSN of every citizen. In other words, make it clear that SSNs cannot be used as authenticators by making them radically publicly available.

A Short History of SSNs

Starting in 1936, most workers were required to participate in the Social Security program. As a result, the government needed a system to track all the participants. While the Social Security Act of 1935 did

not specifically call for a numbering system, it did require the federal government to create a tracking method for record purposes.[2]

Many ideas were considered, including the use of participants' names and addresses or a fingerprint system similar to what some federal agencies already had in place. Name identification proved unwieldy and ineffective.[3] And even though fingerprinting had a proven track record in the federal government, the public had an unfavorable view of the association between fingerprints and criminal activity. Fearing a backlash, the Social Security Administration (SSA) settled on the numbering system we use today.

SSNs were never designed for or intended to be national identification numbers (or cards) and were never supposed to be used to confirm a person's identity.[4] However, only a few years after the passing of the Social Security Act, President Roosevelt issued Executive Order 9397 that instructed federal agencies to use SSNs to identify individuals in any new system the agency was creating.[5] Few, if any, federal agencies complied with the new rule until 1961 when the Civil Service Commission adopted the practice. The Internal Revenue Service followed in 1962.[6] The trend only accelerated with the deployment of new electronic record keeping systems for which numerical identifiers were ideal, though the Privacy Act of 1974 did attempt to limit it somewhat.[7]

Once SSNs became universal identifiers, it was only a matter of time before they also became a universal authenticator.

Starting in the 1970's, Congress mandated the use of SSNs in any number of laws (for example, to combat welfare fraud and to stop undocumented workers from seeking employment). Over the next two decades, a series of laws required people to provide their SSNs to be verified with the government in order to receive benefits other than Social Security or to be hired. Today, SSNs are used in everything from banking to insurance to healthcare – often at the mandate of the federal government.

---

[2] Robert Pear, "The Nation; Not for Identification Purposes (Just Kidding)," *The New York Times*, July 26, 1998. https://www.nytimes.com/1998/07/26/weekinreview/the-nation-not-for-identification-purposes-just-kidding.html.

[3] This was the so-called "Fred Smith" problem: too many similar names existed for them to be used as a unique identifier. See Carolyn Puckett, "The Story of the Social Security Number," *Social Security Bulletin* 69:2 (2009). https://www.ssa.gov/policy/docs/ssb/v69n2/v69n2p55.html.

[4] Indeed, from 1946 until 1972, Social Security cards explicitly disclaimed that they were for "Social Security purposes—not for identification." See Adrianne Jeffries, "Identity Crisis: how Social Security numbers became our insecure national ID," *The Verge*, Sep. 26, 2012. https://www.theverge.com/2012/9/26/3384416/social-security-numbers-national-ID-identity-theft-nstic.

[5] "Executive Order 9397 Numbering System for Federal Accounts Relating to Individual Persons," The White House, Nov. 22, 1943. https://www.ssa.gov/foia/html/EO9397.htm.

[6] Pear. https://www.nytimes.com/1998/07/26/weekinreview/the-nation-not-for-identification-purposes-just-kidding.html.

[7] A good summary is provided in Flavio L. Komuves, "We've Got Your Number: An Overview of Legislation and Decisions to Control the Use of Social Security Numbers as Personal Identifiers," *The John Marshall Journal of Information Technology and Privacy Law* 16:3 (1997-1998), pp. 529-574.

Meanwhile, Congress has allowed private companies to use Social Security Numbers as both identifiers and authenticators without any restrictions. However, the private marketplace is neither specifically authorized nor restricted in asking for a person's SSN for record keeping purposes or authentication.[8]

Data Breach and the Loss of Confidentiality

Recent history is replete with examples of data breaches and the harm they cause. Especially relevant to this subcommittee is the Equifax breach that resulted from poor data security practices and compromised the sensitive, personal data of over 140 million Americans. Moreover, some of these data—like SSNs—cannot be changed, which means that individuals may face a long period of frustration and vulnerability to identity theft. This event was largely preventable had Equifax implemented reasonable security measures, such as encrypting relevant data.

The federal government itself has not been immune to cyber-attacks. A few years ago, for example, a breach at the Office of Personnel Management compromised the records of over 20 million people that also contained sensitive information, such as SSNs and fingerprints. Although it was made public in 2015, the attack occurred more than a year earlier and went unnoticed by the OPM. I, personally, was a victim of both of these breaches.

These attacks are emblematic of the fact that U.S. companies and the U.S. government have been and remain vulnerable to attacks, many of which are by actors linked to nation-states that are adversaries of the United States. Nor are these isolated incidents. As the most recent annual Verizon Data Breach Investigations Report notes, 2017 (the last year for which data is available) saw more than 53,000 incidents and over 2,200 confirmed breaches.[9] So, make no mistake, cyber threats are real, and recent experience has shown that neither the private nor public sectors are fully equipped to cope with them.

Indeed, it does not matter if your personal data is held by a private business or the government, as both have lost millions of SSNs to hackers. Indeed, even before the Equifax breach, experts hypothesized that between 60 - 80% of all Americans have had their SSNS stolen.[10] After Equifax, that number is surely a low estimate.

Given the prevalence of data breaches, it is no surprise that SSNs are not expensive on the Dark Web. Indeed, the SSNs of newborns, which are highly coveted by bad actors because, in essence, they are

[8] "The Expansion of the SSN as an Identifier," U.S. Social Security Administration. https://www.ssa.gov/history/reports/ssnreportc2.html.

[9] "2018 Data Breach Investigations Report," Verizon, 2018. https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf.

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

clean slates, only cost around $300.[11] By contrast, an adult's Social Security Number can sell for as little as $1 each.

In short, the modern rule of thumb is simple: assume your SSN is insecure.

The SSN Authenticator Nightmare

The idea of an SSN as an identifier is not terribly problematic. Everyone in America has a half dozen identifiers that are ways of uniquely denoting their identities to other people. I, for example, am Paul Samuel Rosenzweig. That's my primary identifier.

But I am also a number of other identities. For example, I am my email address: prosenzweig@rstreet.org. That identifier changes more often than my name, but it is, nonetheless, a unique way of pointing to me. A much more permanent identifier that most Americans have today is their mobile phone number. Ever since Congress made sure that we could transfer our number when we changed mobile carriers (thank you!), it has become a commonplace for people to keep their cell phone number, even if they move across country. I took my (202) number with me when I went on sabbatical to Chicago, and most people today anticipate never giving up the number they started with. That unique ten-digit string of numbers is me and only me.

In much the same way, my 9-digit SSN is also a unique string of numbers that is tied inextricably to me, and only to me. The problem is not, however, that the SSN identifies me. I need an identifier for the purposes of accessing my government social security account and, in this way, the SSN is really no different than my account number at the bank where I keep my checking account. It is merely a number linked to my name. But that numerical symbol is as much me as my name or my SSN is.

Nor is the problem that, 20 years ago, some enterprises started to use the SSN as an authenticator. After all, at the time they did so, the SSN was a confidential number known only to the issuer (the federal government) and to the beneficiary. If I, as the beneficiary, shared that SSN with an enterprise to use as my password for an account, I did decrease its confidentiality. But as an approximation of a confidential random password, the SSN was accurate. More importantly, at least at the outset it was efficient. Almost everyone has an SSN and almost everyone could remember it, which created a ready-made password authentication system.

The problem is that our initial assumptions about the confidentiality of the SSN (and thus about its utility as an authenticator) have, over time, proven not to be robust. As the SSN became more and more widely used for authentication, it became more and more widely known. Indeed, the concern about widespread use of a password/authenticator is why one of the cardinal rules today in password management is to try to avoid reusing the same password in multiple settings. This is, of course, because, when compromised, reused password/authenticators become a ready pathway to widespread access.

[11] Emma Z., "Excuse Me, Are You Using That Child Tax Credit?," *Terbium Labs*, January 18, 2018. https://terbiumlabs.com/2018/01/18/excuse-me-are-you-using-that-child-tax-credit.html.

And, with widespread use comes widespread vulnerability. A reused password is only as secure as the least-secure place that it is stored. As we have already discussed, it turns out that almost no storage location is secure enough – and even those like Equifax in whom we might repose greater confidence prove quite vulnerable.

Despite this, for reasons that surpass comprehension, some enterprises still use the SSN to authenticate my identity and prove that I am who I say I am. In fact, every Member of this subcommittee has, I am certain, been asked to provide the last-four digits of his or her SSN not to denote an identity but rather to prove it conclusively.

But, in a post-Equifax world, SSNs are so widely known and so readily available on the Deep Web or Black Market that they effectively provide no security at all. It would almost be as if my User Name for a login were my email address and the website allowed me to use the last-four letters of my last name as my password. That would be ludicrous, but the last-four digits of my SSN are as widely known and as readily available publicly as the last-four letters of my last name.

Ending the Nightmare

So, what then, should be done? If SSNs are valueless as authenticators, why do we continue to use them this way? The answer seems relatively clear – momentum or, if you prefer, legacy costs. Having built systems that rely on the SSN, too many users have sunk costs in their security architecture. Changing how identities are verified is costly. It may require significant expenditures of time and money. New systems may not be backward compatible with older ones, which necessitates wholesale re-architecture. In short, it is sometimes easier to do nothing than to change.

Of course, that is not the whole story. Increasingly, companies in America are beginning to bear the costs of their security failures. Data-breach insurance is now becoming commonplace and it comes at a real cost to those who purchase it. As time passes, we can anticipate that insurers will come to more closely grade the security of the enterprises to whom they issue insurance and charge differential rates based on that assessment.

Thus, over time, the market will come to value greater security against identity theft through insurance pricing. One perfectly plausible solution, then, to the SSN problem is simply to do nothing and over time, the insecurity of SSNs as authenticators will come to be so great a cost that enterprises will migrate away from them. Though I have not seen any data on the subject, it does seem anecdotally that this is already happening. Fewer enterprises today are using SSNs than were doing so ten years ago. And that is a good thing.

But waiting for the market to fix the problem has a cost. As I have already noted, the market is “sticky.” With sunk costs and barriers to change, many enterprises will be slow to modify their practices. The question then, is whether or not Congress has a role in moving this process forward more rapidly in the interest of avoiding continued harm to social security registrants.

To this end, one can envision two possible ways forward.

The first, more typical one would be for Congress to directly regulate the matter in the form of a law that directs companies to stop using the SSN as an authenticator. Such legislation would necessarily come with all of the regulatory baggage that attends all such laws. For example, there would be notice-and-comment rulemaking, followed by some form of audit and ultimately regulatory enforcement. If the task were given to the Social Security Administration (a natural choice since they "own" the SSNs), this would become an administrative requirement that would likely distract the SSA from its current duties. The SSA is not set up to handle most issues outside their core mission of helping seniors and disabled Americans. Indeed, while the Social Security Trust Fund is funded by dedicated taxes, administration money is appropriated. Any additional regulatory requirement would flounder unless Congress were to accompany it with additional funding; a problematic thought in these times of deficit spending.

Thus, I offer you a second possibility derived from the groundbreaking work of Nobel prize winning economist Richard Thaler:[12] Simply publish the Social Security Numbers. In other words, instead of continuing to treat them as confidential numbers that are "secret" when they manifestly no longer are, instead change the paradigm. Make them public numbers that are identifiers in the same way that my telephone number is an identifier published in the phone book. Doing so would demonstrate, in a definitive way, that SSNs are not suitable for identify verification or authentication (any more than my phone number is).

Admittedly, this idea may seem a bit outside the box at first. However, if the goal is to move the markets to more quickly discontinue use of the SSN as an authenticator, we need to make its disutility even more clear than it is now. This would raise the costs of maintaining it to a point where the incentive to stop using it is greater. Such a method simply helps to push the markets in the wiser policy direction without being overly directive in a regulatory way.

Of course, some individuals might object. I suppose we could add an opt-out provision that came with personal liability for identity theft. But my preference would be to see the publication of SSNs as a public good—much like vaccination—that the government could undertake on its own initiative.

I feel confident in predicting that within three to five years of publication in a public SSN log, their use as an identity authenticator would be a thing of the past. And that would be a good thing.

One final thought: As the brief history we recounted at the beginning of this testimony reflects, Congress itself bears much of the blame for the use of SSNs as identifiers and authenticators. We have legislated uses for SSNs that range from welfare fraud and bank identification to certifications of healthcare insurance compliance. In many ways, then, Congressional concern over SSN usage has an air of unreality given this history – and so another first step or nudge would be to systematically reduce and ultimately eliminate all use of SSNs as authenticators within government programs. As in the case of most federal programs, U.S. government leadership could also drive private sector change.

[12] These are summarized for popular consumption in Richard H. Thaler and Cass R. Sunstein, *Nudge: Improving Decisions about Health, Wealth, and Happiness* (Penguin Books, 2009).

Conclusion

In any event, the bottom line is simple. SSNs should no longer be used as a method of authenticating identity. The sooner we get to a place where this is universally true, the more secure our systems will be. While I have offered one creative way forward, others can also be imagined. The singular key is for Congress to take the initiative and lead the charge. Exactly how we get there in the end matters far less than the fact that we start down the road.