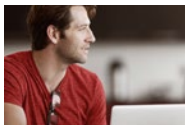
REPORT

McAfee
Together is power.

Modernizing the Social Security Number

A Foundation for Online Authentication of Identity

Table of Contents



Anonymity and lack of trust are among the internet's biggest problems. Securely establishing identity online has been difficult from the start.

This report was researched and written by:

James Andrew Lewis,
Senior Vice President, Center for Strategic and International Studies (CSIS)

Introduction

The Social Security Number (SSN) is the U.S. de facto national identifier, linking disparate records held by a wide range of public and private entities to a single individual. More than 453 million SSNs have been issued; they are unique to one individual, as SSNs are not reused.[1] This nine-digit number has become the core credential for government and commercial purposes—things for which it was never designed. Modernizing the SSN gives the U.S. an opportunity to fix one of the internet's most pressing problems: authentication.

Anonymity and lack of trust are among the internet's biggest problems. Securely establishing identity online has been difficult from the start. Traditional methods of identification using physical credentials, developed over decades of practice, are inadequate for the digital world. There have been many efforts to improve authentication of online identity, but authentication remains a problem. This is a particular challenge for the United States, given political sensitivities about the government' role and privacy. The solutions developed in many other countries for improved online identification—which usually involves a government-issued, national identity system or card—are not available here.

In the United States, the SSN is often the starting point for confirming an identity. Americans use the SSN to identify themselves in a broad range of transactions, but the SSN is easily stolen and misused. It is an appealing target for cybercriminals, who use stolen SSNs for a variety of fraudulent activities, or sell them in bulk on the cybercrime black market. Once stolen, it is difficult to reissue or replace the SSN, making it a weak foundation for online identity. Some estimates say that between 60 percent and 80 percent of all SSNs have been stolen. This means that the SSN as an identifier is compromised, given the scale of the data breaches of the last few years and the commercialization of stolen SSNs on cybercriminal markets.

But the SSN has been woven into the fabric of commerce, online and off, in ways that make it difficult to replace. Hundreds of millions of accounts—credit cards, banking, education, health, and perhaps most importantly, taxation—rely on the SSN. The SSN as an identifier needs to be fixed. Moving to a formal national identity system (the solution used by most other countries) faces both technical and political challenges in the United States that make it very difficult to even begin such an initiative. Given these constraints, this report looks at possible means to strengthen the SSN and build on its success. The goal should be to turn the SSN into the secure foundation for digital credentials, by moving the SSN to smart cards and by adopting best practices from commercial experience (especially in credit cards) so as to create the trusted foundation for innovation in improved authentication of identity.

The SSN's Potential Online Role

The United States never intended the SSN to serve as an identifier, but it has become firmly embedded into the fabric of U.S. commerce.[2] Internet commerce turned to the SSN from the start, since it is unique to single individuals, issued by a trusted source, and readily available at no cost. However, the SSN faces significant problems as an identifier, and after 80 years, it is time to modernize it. The goal for modernization should be to rebuild the SSN system as the foundation for online authentication of identity and to create a path for the private sector to develop authentication apps that are anchored in a modernized, digital SSN. The first step is to replace the paper social security card with a "smart card," a plastic card with an embedded chip, like the credit cards most of us carry.

Adopting a smart card for the SSN creates new opportunities to build a commercially driven authentication system while providing immediate security benefits to the Social Security Administration (SSA). We can identify four core principles to guide SSN modernization:

- It must preserve the SSN's ability to link multiple records to the same individual.
- It should allow for replacement when an SSN has been compromised.
- It should be a first step towards stronger online authentication in the United States and take advantage of advances in technologies for data storage, processing, and connectivity.
- It should be done in a way that minimizes costs (including transition costs) and complexity for taxpayers.

How Online Authentication Works

Authentication is the process of determining the trustworthiness of an assertion of identity. Online authentication is the process where an individual translates this assertion of identity into digital form and transfers it over a network to another party. In the United States, credentialing and identity documentation begin with a birth certificate and a Social Security Number (SSN). Neither was designed to work in a digital environment.

Online authentication is the process where an individual translates this assertion of identity into digital form and transfers it over a network to another party. In the United States, credentialing and identity documentation begin with a birth certificate and a Social Security Number (SSN). Neither was designed to work in a digital environment.

Authenticating an assertion of identity is based on relationships among four sets of actors: the disclosing party, the person (or device) that asserts its identity, the receiving party of that assertion, and the credential issuer (a credential is a document proving a person's identity). The credential links an individual to both a name and to the documentary record associated with the individual (e.g., school records, health records, and business accounts). The process of authentication begins with an assertion by the "disclosing party" to the "receiving party"; you assert "I am John Smith" and present various documents in support, which the receiving party can use to judge the validity of your assertion.

An easy way to think about this is going through Transportation Security Administration (TSA) checks at the airport. You present a credential, usually a driver's license that meets federal standards, to the TSA inspector, who reviews it to make sure it is not fraudulent. If the name and face on the license matches the name on the ticket and the face of the bearer, you are authorized to proceed.

In social situations, a verbal assertion of identity can be adequate, but most other transactions require some kind of documentary evidence to support the assertion. Instead of carrying around birth certificates or utility bills, the credential links an individual to both a name and to the documentary record associated with the individual.

There are many techniques that can be used for online authentication—passwords and other "shared secrets," biometrics, tokens, and smart cards. In all cases, the user must send data over a network. This means translating it into digital form. Each method has strengths and weaknesses. Passwords are the most common form of shared secrets and are the weakest, as they are ridiculously easy to guess or capture.

Enrollment is the process by which a person is issued a credential. Ideally, the credential issuer has done the work to verify an assertion of identity and provides some physical or software documentation as confirmation. This means that, whatever technology is used, a credential is only as good as the processes that lie behind its issuance.

The early internet, largely used by academic or research institutions, did not require strong authentication. Computers, of which there were relatively few in number, were usually located in some central facility where physical access could be controlled. Access to the internet and computers was often linked to a university or DOD-issued credential. Gaining access was akin in some ways to the processes used to access a safe deposit box. This early environment of assumed trust changed rapidly by the end of the 1990s, when tens of millions of new users adopted the internet and remote connections with strangers you had never met became the norm, yet the legacy of weak authentication lives on.

A compromised SSN is often a key part of successful online fraud. False SSN's are easily acquired, and there are websites that produce the entire package—false name, address, email address, date of birth, and SSN.[3] More sophisticated false identities include real SSNs that can be bought in cybercrime markets. SSN's can be used to create "synthetic identities," something that includes both false identities and identity theft. The constant breaches involving SSNs point to the need for a more secure and modernized system.

Most credentials we use today are ultimately based on a government document or record, like the SSN, and many credentialing processes use the SSN as the starting point to link a person to other records. New technologies can offer better approaches to authentication, but they still must be ultimately based on a trusted credential, which experience shows must be issued by the government. Ultimately, we may want to take advantage of the internet's ability to rapidly connect to other records, allowing a receiving party to verify an assertion of identity using multiple records rather than a credential, but even these records will require anchoring in something like the SSN.

The SSN, as a foundational document, can also be strengthened. New technologies and advances in cryptography offer the possibility to make the SSN more secure. A modernized, secure SSN can provide a foundation for better online authentication in the private sector. Such an SSN should be secure, private, and replaceable once compromised. Focusing on the SSN as a core component of online identity, rather than trying to build some new overarching system for identity management, can help avoid some of the problems that undercut previous federal attempts to improve online identity.

Efforts at Better Online Identity

The United States has tried many times in the last 20 years to improve digital authentication of identity, with key escrow in the 1990s, HSPD-12 in 2004, Real ID and the Electronic Authentication Partnership in 2004, and the National Strategy for Trusted Identities in Cyberspace (NSTIC) in 2012. None of these efforts have produced the desired outcome. One lesson we can draw from these experiences is that we should not use the government to create "the solution" to the authentication problem and instead use government to create the trusted foundation for markets and innovators to solve the authentication problem, the same way we lay the foundation of trust for financial transactions but let private institutions innovate and provide financial services.

In the 1990s, many governments including the United States focused their authentication efforts on creating public key infrastructures (PKI), building the legal framework for digital signatures where a digital signature would be treated the same as a paper and ink signature, or creating a key escrow system, where a "trusted third party" would hold encryption keys. Federal PKI and key escrow proposals ran into fierce opposition from privacy groups.

An early federal effort to adjust identification to the online environment was the Electronic Signatures in Global and National Commerce Act of 2000, which gave an electronic signature the same legal weight as those executed with paper and ink. However, e-signatures did not provide strong authentication for online transactions.

Other Federal efforts pursued Key Escrow solutions to authentication. Key Escrow was the culmination of several attempts that began with the Clipper Chip to develop a system of trusted third parties using sophisticated encryption to protect data and authenticate users. Key escrow solutions faced implementation and cost problems as well as strong opposition from privacy groups. More importantly, there was not a market for escrow services, in part because they could add expensive and technical complications at a time when users underestimated the cybersecurity threat. Key escrow depends on a trusted third party; interviews showed there was no such thing as a trusted third party in the absence of the experience and legal structures assigning cost and liability found in paper transactions.

PKI for corporate systems had greater success. Closed systems (such as internal company networks) are better able to manage the risks associated with enrollment, liability, or revocation of credentials that PKI can pose. But PKI was not as widely adopted as was expected. Unresolved risk and liability issues, privacy concerns, cost, and a lack of related applications limit their use.

The 2004 Homeland Security Presidential Directive-12 (HSPD-12) created a common identification standard for federal employees and contractors and instituted the use of personal identification cards for such employees. It remains in effect today, but hopes that HSPD-12 would become the foundation for secure commercial identifiers faced some of the same problems as key escrow in assigning liability for misuse, the lack of trusted third parties, and perhaps a fear in some agencies that commercial use could compromise government IDs.

The United States attempted to create a private-led system in 2004 with the Electronic Authentication Partnership (EAP), which developed consensus-based standards for federated identity by identifying criteria for interoperability and trust. A federated identity system allows the use of many different credentials issued by many different parties while meeting common security standards that ensure each credential can be trusted. Despite a promising start, EAP credentials did not gain traction, since there was not enough demand for interoperable credentials to support a market.

The 2005 Real ID Act set minimum standards for the issuance of driver's licenses—the most commonly held identity document—requiring a photo ID, a birth document, an SSN, and proof of address and citizenship for the establishment of identity.[4] More importantly, it requires the state to verify these documents before accepting them, including verification with the SSA that an SSN is valid and has not been used to issue another driver's license. This expansion of the enrollment process to include document verification is the most expensive element of the Real ID Act. Using state-issued driver's licenses as the basis for a digital identity proved to be difficult due to a lack of federal authority over state processes, an unwillingness on the part of Congress to commit the necessary resources, and privacy concerns.

An ambitious 2011 effort to create an "Identity Ecosystem" using the "National Strategy for Trusted Identities in Cyberspace" also did not lead to anything that was widely deployed. The biggest challenge NSTIC and its new National Program Office in the Department of Commerce faced was the lack of incentives for people to use online authentication. An appeal to adopt stronger authentication because of the unrealized potential benefits for e-commerce was not enough to swing the market.

Each of these efforts was dogged by a common set of problems involving interoperability, liability, and privacy. Interoperability means that a credential issued by one company to a consumer can be used and trusted by another company. While most companies want better online authentication, in the past some companies have

resisted any interoperable or federated system that would make it easier for a customer to switch accounts. Interoperability also requires decision making as to whom is responsible for fraudulent use—the issuer, the customer, or the company that relied on the credential. Unsurprisingly, companies believe they are better able to manage risk if they use their own credential rather than one issued by a third party.

Early generations of internet policy assumed that market forces would lead logically to the development of trustworthy public networks. Understanding why this did not occur is important for future efforts. There is too little demand for interoperable credentials for commercial services to flourish. In fact, there are disincentives, since proprietary credentials provide a way to lock in customers and their data to a sole source. Issues of liability, security, and privacy are also obstacles to third-party use.

Building a more secure and trustworthy online environment faces several problems. First, the processes by which identity is established and credentials issued are weak or erratic. Second, meshing paper-based processes to a digital environment (and to digital credentials) has proven to be beyond the scope of private-sector activity and will not occur in the government absent legislative direction and funding. Finally, getting a digital credential to work smoothly across different networks is a major problem, not only because of the lack of technical interoperability but also because of the lack of a common framework of rules by which one network can decide whether to trust a credential issued by another network.

The political and commercial landscape for authentication efforts has not changed markedly since 2011. We can draw three lessons learned from the past efforts to improve authentication of identity and from the experience of online authentication since the internet was commercialized more than 20 years ago. First, complicated technologies that do not fit with commercial practices will not be adopted. Second, commercial credentials will only be trusted if they are firmly linked to a government-issued credential—a passport, a driver's license, or an SSN. Third, a small but influential segment of the population fears strong authentication and a national ID system, and their objections can result in gridlock.

To get around this, we need to find some way to link a trusted government identifier to innovation in private online authentication systems. Many companies already do this on an individual basis, driven by tax or credit card requirements, but these commercial identity systems are not interoperable. This means consumers need to identify themselves to every site where they want to do business; one product of this is the need for a plethora of passwords. Focusing on modernizing the SSN rather than a national ID or authentication system can start to allay these problems.

A modernized SSN needs to meet certain conditions. It must be secure, of course, but it also must be user-friendly. It needs to be scalable, to accommodate the millions of SSNs already issued—the SSA estimates they issue more than 5 million new SSNs every year. Whatever new system we adopt must be able to transition to a more secure format without affecting the hundreds of millions of records that already use the SSN as an identifier. This is a formidable list of tasks.

What Other Countries Do

Governments see the issuance of identity as one of their core functions, closely linked to security and social services. Providing digital credentials is a new public service. To help identify a way forward, we looked at the experience of other nations and at possible solutions. Strengthening the SSN faces technological and political issues. Fixing the first requires research into new technologies—by the National Institute of Standards and Technology (NIST) and the private sector—and the development of new and more secure credentials and authentication processes.

The second requires an open debate on how America adjusts to the digital age, something we are being forced to do as the original "internet compact" is eroded by concerns over social media, encryption, and the monopoly power of large service providers. For the discussion of a modernized SSN, the issue is whether the old view that having a national ID would create intolerable risks of government access to personal information, and whether it is possible to make progress without triggering these "antibodies."

Almost one hundred countries, including many in Europe, have compulsory national identity cards. Other developed countries, including the United States, Canada, New Zealand, Australia, and Ireland do not, but some of these countries have developed "workarounds" involving partnerships with the private sector to create a single identifier. Most industrial countries that do not have a national identity card have issued their residents health or social security card and the use of special-purpose cards for the provision of social services is common. The SSN is one such card, but its current paper format makes it one of the most primitive.

Other countries have opted to tackle the online identity problem by creating national credentials that serve as an identifier for online authentication of identity. For several reasons, this option is not open to the U.S., but we can draw some useful lessons from foreign experiences on how we might strengthen our identification system and its central component, the SSN.

Estonia

Estonia's approach to identity management has drawn considerable attention. Its electronic identification cards (eIDs) enabled a sweeping digitalization of public and private services. Estonian eIDs incorporate an embedded computer chip holding two unique digital certificates, allowing cardholders to authenticate their identities online and digitally sign electronic documents. Since the roll-out of Mobiil-ID in 2007 and SmartID in 2017, certificates have been available through mobile phones and smartphone apps.

The Estonian eID system uses a "public key infrastructure" (PKI) developed and overseen by the government, (although some services are outsourced to private partners). The digital certificates' keys are protected by unique user PIN. It also relies on "the X-Road," an interoperability platform that links databases of different organizations to facilitate sharing of citizens' data. X-Road allows the data of Estonian citizens to be widely dispersed among different agencies. Estonia uses a distributed ledger system to ensures the integrity of personal data that some have likened to blockchain (although Estonia developed its ID system before blockchain technologies were available). The ledger system overlays an oversight mechanism on top of the distributed databases used in X-Road. This ledger system does not directly hold citizens' data, but mediates access requests, verifies the integrity of data, and keeps a log of all those who accessed or modified it.

Estonia's welfare, law enforcement, and healthcare systems all use the eIDs, along with many private companies (such as banks). It might be difficult to scale an Estonia-style system to serve a population that is twenty times larger, but there are useful lessons on how to organize and structure national ID system in the PKI Estonia uses to support secure online authentication.

Germany

Germany e-IDs (called Personalauswis) are similar to the Estonian system on a much larger scale, with over 50 million identity cards in circulation. The card has an electronic chip that can store personal and biometric data. The system was built on the existing foundation of the national ID, and was driven by the government as part of its larger digital innovation strategy. It allows citizens to both authenticate themselves online and authorize their e-signature using a digital certificates system. Citizens can use the card to access a number of public services, register for universities, or file taxes.

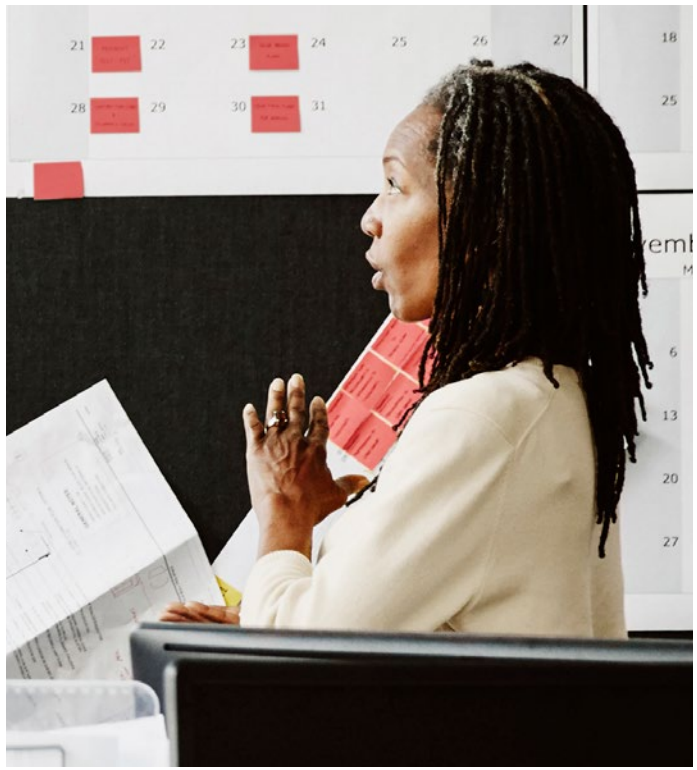
Germany highlights the cultural and societal issues related to a national ID. Germans already had a national ID system in place before moving to eIDs, but this followed a long debate in Germany on whether the cards were appropriate, given Germany's historical experience with the police states of the Third Reich and the Germany Democratic Republic (East Germany). We should expect a similar debate over the risks of a national ID in the United States.

Norway

Norway's identity scheme is built off an existing national registry used to assign each citizen a unique identifying number. The provision of electronic identity credentials, however, is handled by the financial sector rather than the government. Since 2004, Norway's major banks have allowed citizens to come to them to receive a digital credential called a BankID after presenting identity documents to authenticate their identity. The BankID is a PKI-enabled identity system, and allows for users to digitally identify themselves online by entering their national ID, a BankID password, and a code provided by a hardware token or mobile app.

BankID allow users to authenticate themselves online and electronically sign documents. While originally only used for banking, the credential's use has been extended to include accessing health records, signing leases, submitting taxes, and voting electronically. BankID is interoperable among different companies and agencies and used by all the country's banks and public digital services and an increasing number of private firms.

Norwegian banks handle user registration, following standards set by the government, including the issuing of digital certificates and the verification of digital signatures. The BankID has gained widespread acceptance within Norway. A similar system also exists in neighboring Sweden. However, the success of BankID was also helped by timing. These credentials emerged just as an increasing number of services were migrating online, and subsequent developments, like Norway's Mobile BankID on cell phones, capitalized on the move to adopt mobile payments.



Follow

Share

Sweden

Sweden's system is significantly different from Estonia and Germany—but similar to Norway's—and consists of two identity services. First, the government entered into partnership with the private sector to issue eIDs that allow for secure online transactions, but that do not work as national identifier. The Swedish government also offers a national ID card that has a RFID chip that includes a digital key, but the role of the government is only to "support the use of e-legitimations, stimulate competition between providers…and remove obstacles related to infrastructure, market and competition."

The Swedish government regulates private-sector cards, using an "E-credential Board" that reviews applications for eIDs and evaluates them for security. A group of Swedish banks formed the first eID system, the BankID. A few more card issuers have emerged since the BankID debuted in 2003, three of which have been certified by the Swedish government for public use as both physical cards and mobile certificates.

The Swedish example provides useful precedents for how a public-private partnerhsip in the authentication of identity might work. Sweden is of course smaller than the United States and has a long tradition of state-private sector cooperation, but the mix of government regulation and financial institution implementation could be duplicated in the U.S.

India

Until recently, Indian citizens had no universal or unique national identifier. Linking individuals to government records or authorizing access to services was accomplished through a jumble of identity documents tied to passports, tax documents, ration cards, or voter ID documents. Only about 50 percent of Indians possessed any kind of identification document.

In 2009, the Indian government began building its Aadhaar identity scheme, which assigns Indian citizens a unique 12-digit ID number along with a card they can use to verify their identity when receiving welfare, accessing government services, and interacting with private actors like banks. To receive an ID number, Indian citizens must submit proof of identity (name, gender, date of birth), proof of address, and register their fingerprints and iris scans. After receiving their Aadhaar ID, citizens can use the credential to prove their identity by providing their ID card and authenticating through a fingerprint or iris scan. As of January 2017, 99 percent of Indian adults had enrolled in Aadhaar. Aadhaar provides a QR code—machine-readable information that can link to the Unique Identification Authority of India—which administers Aadhaar and allows the ID to be verified as genuine.

However, the implementation of Aadhaar has also given rise to fears over data protection and government surveillance. Multiple data breaches have shown the risk of centralizing a vast store of personal and

biometric information under the management of officials with a poor track record of information security. The government's desire to use Aadhaar to create a real-time database of citizens' spending to combat tax evasion has, in particular, raised protest. The Indian Supreme Court is currently hearing a case on the constitutionality of Aadhaar.

United Kingdom

In 2006, the UK considered issuing national electronic identity cards linked to a central register of biographical and biometric data. This proposal was dropped in the face of criticism over privacy and data protection. In its place, the government proposed a new digital identity assurance program IDAP, now known as Verify. Instead of a centrally-managed authentication scheme, Verify has been envisioned as a federated identity management system where instead of having only one single identity provider—the government—citizens are able to choose from multiple providers within a market of government-accredited identity services.

Under Verify, trusted third parties—like Barclays, Experian, and Royal Mail—offer identity authentication services to citizens, who can use one of these companies to obtain a secure digital credential, a single, trusted log-in that can be used across many different sites. This credential is intended to be interoperable within the wider Verify system, meaning that a credential issued by one company can be used with other companies who are part of the Verify system.

In practice, however, the UK has struggled to implement Verify at scale. Verify's federated identity system, which requires many companies to trust a credential issued by another, complicates the authentication process, leading to low success rates. Second, Verify does not provide a unique identifier. When a customer attempts to link a user to his or her records held by different companies or agencies, Verify does not link the different records or allow for access when data is stored in different formats. Finally, a lack of communication between government and industry about legal and technical aspects of Verify has slowed its adoption within the private sector.

The experience of these countries helps us identify the components needed for better authentication in the United States. Governments have to provide core credentials upon which trusted commercial authentication solutions can be built.

Better Credential or Better SSN?

In cryptography, there is something known as a shared secret, known only to the sender and recipient of a communication. A password is a shared secret.[5] A shared secret is intended to provide secure identification and authentication of the individuals involved in a transaction, creating the basis for secure communication. The SSN is often used as a shared secret, but millions of SSNs, thanks to cybercrime and espionage, have been "shared" are readily available on the internet and in cybercrime black markets. Even worse, shared secrets are used in internet commerce not only to authenticate the identity of an individual, but also to authorize the authenticated individual to conduct transactions. The SSN is no longer a secret, and this makes online fraud and impersonation easy.

There have been several efforts to improve the security of the SSN, but most have focused on preventing the counterfeiting of the SSN itself. A number of states have restrictions on SSN use, but these limit sharing or public revelation rather than curtail its use as an identifier.[6] In 2011, in an effort to improve security, SSN numbers were randomized (previously they used the "Soundex" system, which linked an account holder's name to the account number). Randomization does not, however, deal with the problem of account compromise, where an SSN assigned to one person is used by another.

One problem with these efforts to create a national system for the authentication of identity is that they tried to solve the authentication problem with immature technologies. As better technologies become available, they will create the possibility for strong credentials and a stronger credentialing process. This will likely involve some combination of biometric identifiers and personal mobile devices, creating a scalable replacement for the vulnerable and outdated password as the means to authenticate our identity. However, there will still be a need for a unique identifier that links a citizen or consumer to records stored in multiple databases. In the United States, this means the SSN. The SSN is unique to each individual, issued by a trusted source, and is used to link records held in different private and government databases back to the same person. This makes the SSN indispensable.

However, if we make the SSN too secure and secret, it will harm commerce by making it difficult to link consumers to their financial records. If we accept the status quo, the static SSN will remain a potent source of fraud and we will miss the opportunity to improve authentication. We really confront two problems: how to make the SSN harder to compromise and what do to do once it has been compromised.

Options for a More Secure SSN

These are problems for policy. They are also problems that the market will not solve by itself, at least not in a timely fashion. The authentication problem goes beyond what the private sector can do alone. Regulation is also not the answer. The adoption of new network technologies and new policies anchored on a smart SSN can make the SSN the basis of more secure authentication.

There are many authentication systems emerging in both the public and private sectors. No single system will work for all transactions, nor will U.S. consumers want such an identity system. Individuals, agencies, and companies will want to be able to use multiple credentials that provide different degrees of liability and trust. Participation will be mandatory in some systems and voluntary in others.

The goal for any SSN modernization effort should be to make the SSN less vulnerable to misuse. There are basically two approaches to reducing the risk of using the SSN as an identifier. The first is to strengthen the SSN to make it harder to steal or use fraudulently. This most likely will require some way to encrypt the SSN. The second approach is to reduce or eliminate the SSN's value as a credential. Possible solutions involve new technologies, based on PKI or other forms of encryption (but not yet blockchain), and new processes.

One option we did not consider is a national ID. While a national ID is the preferred solution of almost all other countries for online digital authentication of identity, we have discounted it for the United States given the vociferous opposition from privacy groups that has greeted this idea in the past. Many of the objections raised about a national ID are frivolous, with some privacy groups fearing that it would create "a database of all Americans," forgetting that the SSN is already a database of all Americans, or become an "internal passport" (a concern heightened by recent efforts to control illegal immigration). But the fundamental objection is that a national ID leads to the "slippery slope of surveillance."

Many of these concerns arise from a misunderstanding of the rules that govern the access of different agencies to information on U.S. persons, especially when held by a different agency. There is no single Federal database that holds all information associated with all U.S. persons (although these exist in the commercial world); no agency has access to all the various databases; and there is no system that allows any agency to correlate data scattered across dozens of federal databases. However, whatever the merits of the privacy arguments, they are strongly held and may resurface in any effort to modernize the SSN, especially if this effort is linked to a national ID program.

An improved SSN can be a first step towards improving our ability to authenticate identity online, but our immediate goal should be simply a better SSN, not an online identity system. A modernized SSN is a good first step towards improving online identity in the U.S., and we can describe the attributes of a modernized SSN. It should be dynamic, able to respond to compromise and draw on the connectivity the internet provides. It should use encryption to make fraudulent use more difficult. It should retain the SSN's ability to provide a unique identifier from a trusted source that allows for the linkage of records in disparate databases. A modernized SSN can draw on the best practices of other countries. The following section examines some possible new approaches to the SSN.

Blockchain

One alternative would be to anchor the SSN in a blockchain-like ledger. Blockchain is kind of software that creates an encrypted public ledger, where stored data that cannot be erased or modified without leaving a record. In theory, this makes blockchain-based records difficult to steal or alter. Some have called for basing a modernized SSN on blockchain technology.

The issue with blockchain, however, is that it has been slow to gain traction in large scale implementations other than cryptocurrencies. With innovations in policy and practice, this could change. Blockchain's use of distributed and decentralized public ledgers is a promising technology, but other than digital currencies, there are still few implementations. This will eventually change, but making the SSN the testbed for a deployment involving hundreds of millions of individuals would create the risk of turmoil in the U.S. economy. It takes time to build scale and gain adoption. In the future, a blockchain-based approach might be feasible, as the technology matures and as the needed legal and regulatory infrastructure is developed, and modernization must be designed to accommodate this and other new technologies.

Mobile Apps

Most people interact online using applications (apps) on their mobile device. This will become even more pronounced as 5G wireless technologies are deployed, enabling high-speed data transfers across a broad range of devices. Mobile devices have the advantage of carrying numerous sensors (such as cameras and fingerprint scanners) that can be used for biometric identification while possessing the ability to connect to databases held somewhere in the "cloud" to provide verification. Right now, mobile authentication apps are not interoperable, and the enrollment processes are not uniformly strong. This can and will likely change; in the future, developing mobile authentication apps that use strong encryption and allow a person to verify identity and create and exchange credentials will change the authentication landscape, but these are not yet available.

Public Key Infrastructure (PKI)

Public key infrastructures (PKIs) are based on public key cryptography – an encryption method that allows strangers to exchange keys for the coding and decoding of secret messages. A modernized SSN that used PKI would be more secure, but this approach faces significant difficulties relating to scale and trust.

In the 1990s, the U.S. assumed that the PKI process would be managed by 'trusted third parties' from the private sector that would provide digital certificates which could be used both to encrypt and decrypt messages and to confirm identity. Certificate authorities would provide the digital credential as a commercial service.

A reliance on private sector initiatives slowed adoption, given public attitudes about who can be trusted to confirm identity. This is usually a government function and depends on government processes. Most users assign a high degree of trust to government credentials. Credentials issued by private vendors using processes that are opaque to the users were not accorded the same level of trust. Financial institutions are perhaps the only place in the private sector where trust matches that given to government credentials, given their emphasis on building, and preserving trust and their acceptance of financial liability.

Interoperability is another dilemma for PKI. A private sector approach means that there will be multiple credential issued by different vendors. Interoperability, the problem that a federated identity system attempts to solve, has been a major difficulty for private credential systems. Interoperability requires that the vendors use the same rules, standards, and policies to let each other (and their customers) trust different credentials. Countries with smaller populations face a lesser burden, but the United Kingdom, with a population of 65 million, found it difficult to implement a federated, private sector authentication system, as did the U.S. in the early-2000s.

Privacy concerns, legal uncertainty, and lack of interoperable applications have been obstacles to the adoption of PKI. These problems are commercial and legal, not technical, and they suggest that PKI is not a good option for SSN modernization.

Federated Identity

Federated authentication systems allow users to engage in transactions using a single credential for transactions with many different companies, the same way that a driver's license from one state can be reliably used—after the Real ID Act—in other states. There are two examples of partially "federated" systems that have worked. The first is mobile telephony, which allows a phone from one service provider use another service provider's network. The companies have created technical standards that allow this and contractual arrangements to ensure payment across networks. The second model is the credit card, where a single card can be used at multiple establishments, supported by sophisticated "backroom" processes that verify both the use and the ability to engage in the transaction.

Federation requires cooperation among independent systems so that a digital identifier issued by another system can be reliably used by another. A federated approach needs common rules that allow identities issued by different processes and places to be recognized and treated equally. The root of the problem is the absence of trust. Companies do not want to trust a credential issued by another private entity for high-value transactions. While consumers can use Facebook or Google accounts to sign into low-value activities, higher-value transactions still rely on their own credentials. Changing this will require the development of a legal framework covering liability for fraudulent transactions and errors, standards for credentialing, and contractual obligations for the use of federated services. Consumers, if assured about liability and privacy protections, might want interoperable services and be willing to pay for them. Governments should consider ways to incentivize interoperable credentials, but this has been a challenge for the United States in the past. Sweden and the United Kingdom have also found it difficult to get widespread adoption of federated systems.

Biometric Identifiers

Biometrics measure some personal feature – voice, iris, fingerprint, hand motions - one system under development even uses the pattern of your brain waves when you think of a particular word - and use that to identify you. People are unique, down to the way they type, and some unique identifying feature can be converted by the smartphone into a unique code and then used to identify the individual. Many phones offer this, with the built-in camera "recognizing" your face and using the image to unlock the device. Several companies are developing technologies that let you authenticate yourself to your phone, and then use your phone as a token or credential to authenticate yourself to other websites.

People forget their password all the time, but they are much less likely to forget their phone, and since you control your phone, the risks to privacy are manageable. Used with other techniques, like two-factor authentication (a technique that banks have adopted), biometrics can create the complexity that makes life harder for cyber criminals. Authentication of identity on the internet has been a problem from the start. Until now, there has been no real solution for identifying yourself other than a password. The combination of biometric identifiers and mobile devices loaded with sensors gives us a way to change this.

However, moving to the use of biometric technologies to modernize the SSN would be expensive, since SSA might need to collect and store biometric data for every card holder. The use of biometrics is certain to raise privacy concerns that would complicate and perhaps block any effort to modernize the SSN. Most American do not now have biometric identifiers (like fingerprints) in government databases and public acceptance could be difficult. As the use of biometric identifiers on telephones becomes commonplace, using biometrics to verify an SSN will become easier, but currently the administrative and legal framework need to support this does not exist.

Ending the SSN's Role as a Credential

One problem with the SSN as a commercial credential is that it is used to both authenticate identity and to authorize transactions. This means that comprising the SSN can enable fraud and identity theft. One suggestion for dealing with the is to publish the SSN, which would lower or eliminate their value to criminals.

Another approach would be to ban the use of the SSN as a commercial credential. This would force companies to find an alternative solution and, judging from the Swedish and Norwegian experiences, could incentivize a market for private credentials. Private credential issuers could be required to meet identification standards such as HSPD-12 or NIST's SP 800-63 Digital Identity Guidelines. Putting aside the difficulties of enforcing this ban, the same problems of trust and interoperability that have hampered other commercial identity services would work against this approach. A ban on the SSN as a commercial credential would, however, impose higher costs on citizens and the private sector. A ban on SSN use would require a long lead time, to allow commercial providers to develop alternatives and for "relying parties" to replace the SSN associated with their accounts.

Simple publication of SSNs is the least expensive option for the federal government and for the private sector and would create incentives for companies to use something other than the SSN as an identifier. Judging from the Swedish and Norwegian experience, publication could incentivize a market for private credentials. Congress would need to identify a transition period for the SSA's move to a smart-card based system, and it would have to create incentives for companies and individuals to move the SSN to the proxy number. While publication would lower the SSN's black-market value, doing this alone would be insufficient and represent a squandered opportunity to bring the SSN into the twenty-first century.

When your credit card is stolen, your financial institution cancels the old one and issues you a new card number. You are still linked to your account, but not to the old credit card number. The SSA could also adopt a similar approach, which would provide a way to replace an SSN when it is compromised, since compromise is unavoidable.

The Credit Card Model

When credit cards were first introduced, a customer presented their card to the merchant, who recorded the account number and the transaction's value and then sent that information to the card issuer for payment. As fraud increased, merchants might ask to see a driver's license. As transactions moved online, when you swiped your card on a device, it would connect to a credit card company's records, showing whether you had sufficient funds and, later, if the transaction was in some way unusual (from a strange location or for an unusual amount). The addition of a chip to the card makes them more difficult to counterfeit and can allow companies to require that you also enter a pin number as a second layer of confirmation.

The simplest approach to modernization would be for the U.S. to transform the venerable Social Security Card into a "smart card." Instead of receiving the printed paper card, new enrollees would get a plastic smart card, and existing account holders would receive a replacement smart card.

What makes the cards "smart" is that the chip they carry can be "read," and if the reader connects to a network, the information carried on the smart card can be checked and verified against a remote database. Smart cards were adopted by credit card companies some time ago as a way to reduce fraud. Most people are familiar with smart cards, which would ease the burden of both acceptance and transition for SSN holders. Even if nothing else was changed, a smart card would be an improvement over the current paper card. One benefit is that smart cards allows us to end the use of the SSN itself as a credential. A smart card provides the foundation—for use now or for later—to build a more secure system.

For a modernized SSN, this means the number on your SSA-issued smart card will not be your SSN account number. Instead, it will be a proxy number that links to your SSN account. In this approach, citizens would get two numbers from the SSA. The first would be the traditional SSN; the second would be a proxy number linked to the SSN. If this proxy number was compromised, a new proxy number could be generated. The SSN itself could be kept secret and encrypted, and any replacement number could be controlled by the SSA. The SSN itself would not be used in commercial transactions—use of the SSN for commercial purposes could even be forbidden by law once the proxy number system became available.

People are familiar with this credit card model. Your credit card has a number used to authorize transactions. It is linked to an account at a financial institution that has its own account number. When your credit card is stolen or compromised, you notify the card company, which generates a new credit card with a new number for you that is linked to your account, whose number does not change. Having two separate numbers solves an essential problem. The account number is used to identify, but it cannot be used to authorize transactions.

For this to work, merchants, banks, and others who now use the SSN will need some way to verify that the proxy number links to a real SSN account. This means the SSA will need some sort of verification process similar to that used by credit card companies. When you insert a credit card into a card reading device, that device connects to the credit card company's database where the information stored on the chip is verified. You present your credit card, then the number is automatically checked to see if the card has been reported stolen or if there are indications of fraud. The credit card company then authorizes the transaction. The entire process usually takes a few seconds.

Credit card companies already make use of this approach to reduce fraud. They have developed sophisticated algorithms to spot fraudulent charges. These algorithms compare a transaction to a pattern based on previous transactions to determine if it is legitimate or not. The appearance in the last decade of major information brokers, who have amassed collections of records on millions of individuals, simplifies this transactional approach to authentication. High-speed digital networks allow for rapid checking against these databases. While the SSA would not need to duplicate these high-end anti-fraud systems, they could be precedential for improved efforts to identify fraud in the application for a card. An SSN verification system could build off existing verification systems already in use by the SSA where an employer submits an SSN to see if it is a real number, except now these systems would need to be expanded to confirm that the proxy number is linked to a real account. At some point in the future, the SSA could even develop a mobile app for the verification process.

The SSA currently operates two verification services to confirm the SSN and name of an individual for wage reporting purposes. One verification process requires registration and the other charges a fee.[7] These are useful, but could be modernized and improved by creating a searchable database, perhaps cross-linked to the SSA's Death Index.[8] Other data could also be appended depending on the degree of privacy sensitivity, allowing an assertion of identity based on an SSN to be verified.

If the United States was to move to a smart card system similar to that used by credit card companies, it would need to adapt the existing verification system to allow companies to check if the proxy SSN was still valid. The SSA could adopt additional measures similar to those used by financial institutions to identify possible fraudulent use. The SSA would also need some system for citizens to report when their number has been compromised and needs to be replaced.While creating a searchable database has associated costs for the SSA, it would be cheaper than the annual cost of fraud and identity theft (an estimate in the Economist pegs this at $16 billion).[9]

Replacing a Compromised SSN

Currently, it is very difficult to replace a compromised SSN. If the SSA moved to a proxy system, this difficulty could be reduced. Exchanging a compromised proxy number would require a citizen going to SSA and requesting a replacement number. Before issuing a replacement, SSA would need to verify that the request was legitimate. Banks and online merchants use multifactor authentication to verify such requests. This uses a shared secret, usually a password, and then some other some other secret to verify identity. The SSA could do the same. The transition burden would be reduced as many citizens are already familiar with these systems.

The SSA could, for example, issue its customers a PIN for use with their smart card, and the PIN would be needed to request a new number. The SSA would need the ability to receive a request, verify the password, and have on file an email address or phone number to which an authorizing code could be sent. Citizens would receive a new smart card with a new proxy number.

This sounds complicated, but hundreds of millions of commercial transactions are carried out every day using this approach. There are costs, however. Non-recurring costs include replacing paper cards with plastic smart cards, building an online account verification system at the SSA, and the cost to firms and agencies of changing numbers used in existing accounts from the real SSNs to the proxies. Recurring costs would include providing the verification service and the cost of regenerating a new proxy number. The United States could consider user fees (something almost certain to be unpopular, although we charge for passports and driver's licenses), or a modernized SSN could be funded from general revenues. No modern system comes without cost.

Given the immense experience of the private sector, the United States could choose to rely on private-sector service providers to supply the smart card and the proxy number. The SSA would still need to create and hold the actual account number. Commercial venders already have the "backroom" processes needed for a smart card. The SSA could subcontract the card issuance process to the private sector since this would reduce the burden on the SSA. The United States would need to develop privacy rules that restrict the ability of a private-sector provider to "harvest" data for commercial purposes.

One consideration to bear in mind is the transition cost of moving to any new system. Countries with smaller populations face a lesser burden as they have fewer people and fewer companies involved. The complexity of improving online authentication for a massive economy like the United States argues for an iterative approach and for using technologies that are already familiar to people.

Moving Ahead

The internet has been reshaped by the use of mobile apps, small specialized programs designed for mobile devices. This is how most people connect and it is likely to become the way that people will authenticate themselves. The combination of apps and fast mobile connectivity will provide new means to authenticate identity. Apps by themselves are not a solution. The primary problem for authentication is trust, not technology, and making authentication using apps on a mobile device trustworthy will require a reliable foundation. A digital SSN is the best way to provide this foundation.

The United States needs to move the Social Security card into the twenty-first century. The SSN has become crucial for U.S. commerce. Modernization must safeguard this. It is the central identifier for the U.S. economy, linking disparate records held by a wide range of organizations to a single individual. Modernization should change the SSN from its current form and replace it with a dynamic credential that relies on online processes for confirmation and provides a path forward for the adoption of new technologies developed in the private sector, such as mobile authentication apps or blockchain.

We recommend smart cards as the best path for modernization for several reasons. First, there is already extensive experience with smart cards on a mass scale. This can minimize implementation problems and maximize public acceptance. Second, smart cards allow an incremental approach to SSN modernization which, given political sensitives over privacy, can avoid some of the pitfalls that have hampered previous U.S. efforts on authentication of identity. Third, SSN databases that could support a smart card already exist, the SSA already has some (limited) verification processes, and the SSA is a trusted issuer. This would ease the transition to a new card and help address concerns. Alternative approaches are less attractive. A national identity program is politically unfeasible, and there is no broad market for private-sector authentication solutions.

The advantage in credentialing lies with federal and state government agencies. They have public trust. They began issuing credentials to provide access to some service, (e.g., social insurance, driving, and crossing borders). These credentials were not designed for online use, but they are cheap and reliable, and the SSN has become a core element of online commerce. Essentially, identity and credentials have become a new government service paid for by general revenues and available to all citizens that companies can use, the way they use highways.

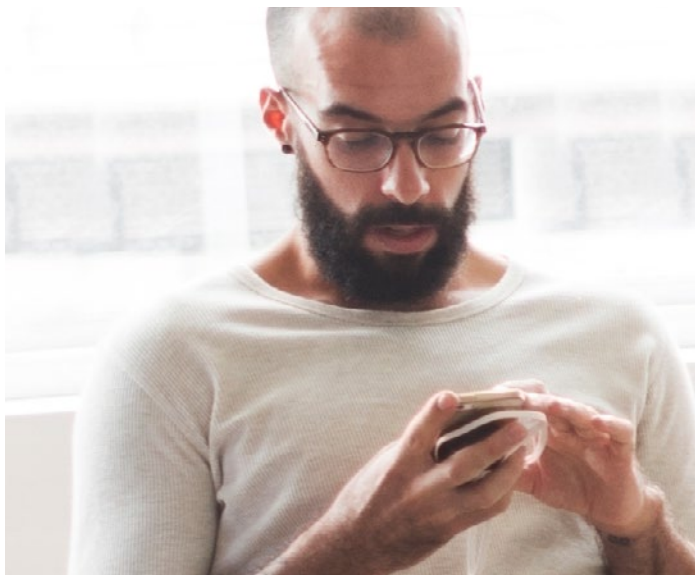
There is not going to be some grand scheme for national authentication that will work. U.S. politics are too convoluted for that, the country is too big, and the commercial incentives are not there. The European experience suggests that governments can mandate the use of secure credentials for accessing government services, but commercial applications are best left to the market to develop. A smart card SSN with the necessary “backroom” support would lay the foundation for private-sector innovation in identity and, with

experience and legal modernization, could lead to a more secure and interoperable online authentication system. There are new opportunities that could arise from ubiquitous smart phones and credit cards and new forms of encryption and verification, such as blockchain, but experimentation and development will need to be based on a secure foundation. This experimentation is best left to private-sector entrepreneurs and innovators, working off a secure foundation of a modernized SSN.

In this political and commercial environment, an incremental approach will work best. The first step is to move the SSN from paper to plastic and build the infrastructure needed to make it a verifiable base for online credentialing (and there are plenty of example on how to do this, as all the major internet companies run their own proprietary credential services). Our ultimate goals should be to make accessing government services as easy as accessing Amazon or Google and to build the online infrastructure to support a credentialing system that will allow companies to build and create commercial opportunities.

Moving to a more secure and modern SSN will be a complex transition, but we can take advantage of the experience of many companies in going online and the growth in internet connectivity that has occurred in the last decade to create a modernized SSN that can sustain both the delivery of government benefits and improvements in online authentication well into the twenty-first century. Authentication of identity will now occur in an environment of ubiquitous networks and internet access best supported by smart cards. Smart SSN cards can enable online authentication by providing a digital credential and by allowing for confirmation of the credential's validity. For optics alone, it would be nice to move from a printed paper card largely unchanged since the 1930s.

This is not the job that the SSA was created to do, but given the centrality of the SSN in the online environment, the SSA, with increased resources, is best placed to do it. Using the SSA will reduce some of the governance problems an online authentication system would face and the SSA's credibility and existing programs create opportunities to take another step. Modernizing the SSN may require new legislation and funding, but it is the step towards better authentication most likely to succeed.



About McAfee

McAfee is the device-to-cloud cybersecurity company. Inspired by the power of working together, McAfee creates business and consumer solutions that make our world a safer place. By building solutions that work with other companies' products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection, and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all.

www.mcafee.com.

1. U.S. Government Accountability Office, Government and Commercial use of Social Security Number Is Widespread, GAO/HEHS-99-28, (Washington, D.C., February 16, 1999), https://www.gao.gov/assets/230/226868.pdf.
2. CarolynPuckett, "The Storyof the Social Security Number," Social Security Office of Retirement and Disability Policy, Social Security Administration, July1,2009, www.ssa.gov/policy/docs/ssb/v69n2/v69n2p55.html.
3. The justification for these sites is that false credentials can be used for protecting privacy and preventing identity theft.
4. The license is required to show name, date of birth, gender, address, and signature; incorporate tamper proof features; and use common, machine readable technology using common data elements.
5. The most commonly used passwords are "password" or "12345." It doesn't take a criminal mastermind to guess this.
6. Gail Hillebrand, "State laws restricting private use of Social Security Numbers," San Francisco: Consumers Union, 2008, http://consumersunion.org/news/state-laws-restricting-private-use-of-social-security-numbers/.
7. "Verifying Social Security Numbers," Social Security Administration, https://www.ssa.gov/employer/verifySSN.htm.
8. "U.S., Social Security Death Index, 1935-2014," Ancestry.com, https://search.ancestry.com/search/db.aspx?dbid=3693.
9. "America should borrow from Europe's data privacy law," The Economist, April 5, 2018, https://www.economist.com/news/leaders/21739961-gdprs-premise-consumers-should-be-charge-their-own-personal-data-right.

McAfee™
Together is power.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com