The Application of Digital Identity in the United States

Keith Duffy
Pasha Goudovitch
Pavel Fedorov

DRAFT

May 10, 2016

15.998 Independent Study on Blockchain Draft Report

Introduction

Identity theft affected nearly 18 million people in the United States in 2014[1] and resulted in billions of dollars of financial losses and other hardships for individuals, the government and businesses. With the increased prevalence of online financial transactions and other business interactions, there has not been a corresponding widespread adoption of a universally trusted and robust authentication mechanism online. We propose for the United States to adopt an Identity Management System ("IMS") similar to that of Estonia and Kazakhstan in order to combat the increasing occurrence of identity theft and to foster a higher level of online security.

The common causes of identity theft in the United States that facilitates credit and debit card fraud, tax refund fraud, and social welfare fraud is an IMS that relies on individuals providing a series of data points, the most important of which are a name and matching Social Security Number ("SSN"), that serve the dual role of an identifier and an authenticator of an individual. This method of online authentication requires the difficult task of both keeping your information secure while sharing it with a range of counterparties. With the prevalence of recent, large scale data breaches, the flaws with this method of digital authentication are causing increasing security risks across the system.

Several countries around the world have been attempting different approaches to a countrywide IMS that provided insights into benefits and risks of creating a new digital identity system. Estonia and Kazakstan have both created an identity card that implements a public-private key cryptographic system in a secure chip in the card. Using this identity mechanism, citizens of these countries are able to perform a range of secure activities online ranging from voting to online banking transactions with a substantially lower risk of fraud. India has created a new IMS which includes collecting biometric data for authentication. The Indian government's use of biometrics as a new form of authentication could add improved security, but it also introduces a range of privacy concerns and new identity theft risks that are not desirable in an IMS.

Finally, we believe there is a range of implications of a digital identity on the emerging blockchain-based services. A new IMS could add a new layer of security to emerging payment systems helping integrate them with existing laws and regulations. Aside from this, we believe there are exciting possibilities to utilize blockchain to securely manage various personal attributes in a distributed way that could mitigate personal privacy concerns with attribute pooling that we have seen with the Indian IMS.

There will be practical challenges to implementing countrywide IMS in the United States, but we believe that the risks inherent in our current system are substantial. By learning from the best practices in identity management around the world, the US government has a great opportunity to enhance security standard across the country while opening up room for new opportunities in digital commerce.

Case Study: Card Payments Fraud

Sizing the Problem

The single most common source of identity theft in the United States in 2014 was fraud related to credit and debit card accounts[2]. The total world-wide losses of card fraud was over $16 billlion in 2014, with nearly $8 billion in losses in US alone[3]. Due to the large growth in card payments globally, the Nilson's Report estimates that global card fraud losses could exceed $35 billion by 2020[4].

Identity Management Analysis

Identity authentication is an essential component at several stages of the card payment system, and how it is handled at each stage dictates the method of fraud. While financial criminals have found many ways to fraudulently use other people's credit and debit cards, these methods broadly fall under two categories:

- **Existing account fraud -** the most common form of card fraud, and it is frequently a result of physically stolen cards or the theft of key information such as the card number or magnetic strip information that allows the fraudster to make purchases. Thieves can skim the magnetic strip information off of cards using hand held devices in public which they can then use to replicate a magnetic strip on a counterfeit card. Other methods include classic phishing attacks where people are tricked into giving their credit card information to a bad source.
- **New account application fraud -** this kind of fraud, while less common, is where a more robust form of digital identity will be most useful. Most online credit card applications require very little identity authentication in order to open an account. With someone's name, SSN and date of birth, the fraudster could submit a credit card application on a person's behalf and have the card mailed to a fraudulent address. In addition to this, the person trying to perpetrate the fraud would have to provide a working email and phone number, but these pieces of information are not necessarily tied to the individual being impersonated and could be created separately.

Based on our research, the new account application process is where traditional identity verification takes place, and the physical or online payments can then happen with the card issued to the applicant without providing any additional identity authentication.

Creating a better system

Credit card companies try to balance the ease with which a new customer opens a credit card account with the risk that an application may be fraudulent. Their desire to remove friction from

the credit card application process unfortunately results in minimal requirements for an application to be submitted and approved making the process susceptible to fraud when a person's identity information is stolen. Improving this system would first require a widespread adoption of a more secure IMS within the market for credit cards enforced by either industry standard-setting agreements or regulatory mandates to ensure card issuers improve their authentication procedures.

An important impediment to the adoption of a more secure form of identity management is understanding where the liability for identity fraud is held. In nearly every from card related fraud, the customer is insulated from any financial losses. The financial losses from fraud relating to compromised existing accounts will almost always fall on either the card issuer or the merchant depending on the merchant's adherence to security standards at the time of sale. The customer can typically get any damage to their credit score caused by the fraudulent accounts reversed by credit agencies. Therefore, the parties in the current payment system with the greatest incentive to improve security are the merchants and the card issuers, not the customers themselves. But even at the merchant or card issuer level, liability can be further limited through insurance which spreads the risk but also adds an additional layer of cost to the system.

Ultimately, these parties will need to come together to create a better IMS with improved authentication standards. We believe that regulators are the best source of change in the industry because they are able to enforce better standards across all of the participants in the system. We are cognizant of the numerous bureaucratic and lobbying challenges that could deter regulatory progress but we strongly encourage the regulatory bodies to work on developing a better identity management framework for the banking industry.

Case Study: Identity Theft Tax Fraud

Sizing the Problem

In its 2015 report, the US Government Accountability Office ("GAO") published a special report on Identity Theft and Tax Fraud where it disclosed that the IRS paid nearly $6 billion in tax refunds that were later determined to be fraudulent[5]. This represents roughly 4% of the $147 billion in total refunds that IRS issued in 2014[6]. This figure includes confirmed fraudulent transfers and does not include any estimates for undetected fraud which will surely bring the figure higher. What is more staggering is that the GAO estimated that tax refund fraud would nearly quadruple to $21 billion by 2016[7] or to approximately 14% of total refund payments[8].

Identity Management Analysis

According to the GAO report, there are three key components to tax refund fraud:

1. Ease of obtaining sensitive and private information required to commit fraud – *"According to an official in IRS's Criminal Investigation division, the sources of stolen identities are limitless"[9]*.
2. Exploitation of IRS's current compliance model – "*Identity thieves are often able to exploit what IRS officials call a "look back" compliance model: rather than holding refunds until all compliance checks can be completed, IRS issues refunds after doing some selected, automated reviews of taxpayer-submitted information"[10]*. These automated reviews primarily include matching name and SSN and finding obvious mathematical errors[11].
3. The attractiveness of the tax refund fraud - "*refund fraud crimes often involve large criminal enterprises that exploit the speed and relative anonymity of preparing and filing tax returns. For this reason, they are difficult to prosecute, according to the Department of Justice"[12]*.

While we agree with the GAO that the above elements are prominent features that facilitate tax refund fraud, we contend that these are merely symptoms of the underlying root cause issue that is IRS's current IMS. In order to issue a refund, the IRS matches the name on the return with the SSN provided and ensures that the basic math in the returns adds up in terms of allowable deductions and credits. In most cases, if these checks are satisfied, the return is accepted and the refund is issued[13]. Over the course of the year, IRS conducts additional due diligence such as matching third party data (ex. W2 submitted by employer) to the filed return and investigates any discrepancies[14]. While this method can be effective in retroactively identifying fraud, it is ineffective in the recovery of the fraudulent tax refund payments as the funds would have likely been moved.

Current Efforts to Mitigate Fraud

Following the GAO report, IRS has expanded its efforts to authenticate tax filers. In October 2015, IRS published a series of steps it is taking to detect fraud and authenticate users including[15]:

- Identifying and authenticating devices used to file tax returns
- Studying metadata in computer transactions to help capture related fraud
- Imposing stricter authentication procedures on tax software providers for password standards, timed lockout, security questions and two factor authentication

In addition to this, IRS is expanding its IP PIN program where it issues identity theft victims and opt-in filers from a few states a unique PIN annually that must be used to file the tax return[16].

Creating a Better System

We applaud any efforts that are being taken to improve the current system but we feel that the steps are a marginal improvement over status quo. For instance, we like the idea of tracking devices of tax filers using identifiers like the IP address but an identity thief could circumvent this by using commonly available technologies such as the VPN. While meta data can help detect some commonly used bank accounts for identity fraud, identity thieves can easily bypass this check by setting up a new account or requesting a check. Finally, while we think strengthening authentication of tax software providers is a good idea, we are afraid that with the abundance of tax software providers, it is fairly easy for identity thieves to set up new accounts whereby the authentication procedures have not been set up.

We would like to suggest that in order to reduce tax refund fraud, IRS needs to implement a better authentication system internally. We believe that matching a person's name to the SSN is an ineffective and a dangerous way to authenticate users and this makes tax refunds a very attractive target for fraudsters.

Case Study: Social Welfare and Benefit Fraud Related to Identity Theft

Sizing the Problem

According to Social Security Administration Supplemental Security Record, there are 65 million Americans receiving Social Security, Supplemental Security Income (SSI), or both, as of March 2016[17]. The groups receiving the social benefits include seniors, persons with disabilities, veterans and some other groups like recipients of SNAP program benefits. With addition of Medicare recipients, the total number of Americans receiving welfare payments is 121 million[18].

Overall, according to Federal Safety Net report, "*improper welfare payments, including fraud, are estimated to be about 9.0% of all federal welfare payments made*"[19]. Based on this, the estimated amount of improper payments is $38 billion for fiscal year 2014. This estimate is based on reports from the Office of Management and Budget(OMB)[20] and The General Accounting Office (GAO)[21].

Identity Management Analysis

Improper welfare payments are defined by OMB as cases when:

- Funds go to the wrong recipient
- The right recipient receives the incorrect amount of funds (including overpayments and underpayments)
- Documentation is not available to support a payment
- The recipient uses funds in an improper manner.

The most common methods used by fraudsters to receive welfare benefits can be separated into two big groups: intercepting physical checks and re-routing benefits using the victim's SSN and personal data obtained from various sources. One common example of hijacking social benefits is through phone services (for example, Medicare contact center). If the fraudsters possess victim's SSN, they can call Medicare, authenticate themselves as victim using SSN, date of birth and address information and then change the destination address of where the checks are submitted[22]. Another common method is to re-rout the payments to pre-paid debit cards using MySSN website, if the victim has an online account[23].

Despite the different methods of committing fraud, the root causes behind these types of fraud are similar. We believe that there are several reasons that play a significant role in the social welfare theft and/or misuse:

1. Low awareness of risks associated with identity theft among the target population (seniors, population with no income etc) allow fraudsters to access private information easily
2. Direct access to to the person's private information that fraudsters frequently have by virtue of being someone victim knows, for example, relatives or care providers[24]
3. Small number number of attributes required to authenticate the recipient of government welfare benefits – as it is seen from examples above, knowing victim's name, date of birth and SSN number is usually sufficient to re-route the benefits.
4. Inefficiencies SSA processes – reports indicate that SSA uses insufficient tracking mechanisms to distribute the social benefits, causing checks to be sent to non-existing or dead recipients[25].

All these drivers, together, create the favorable conditions for fraudsters to thrive in the social welfare space.

Creating a Better System

In order to reduce the frequency and magnitude of social benefit fraud that is due to identity theft, social benefit agencies need to increase the awareness about identity theft and to create a better IMS[26][27]. There have been efforts towards improving the benefit distribution system. As a senior adviser to SSA mentioned, "*Our focus right now is to make sure our data is as accurate and complete as it can be for our current program purpose. Right now, we're focused on making sure we're paying beneficiaries properly, and that's how we're investing our resources at this time.*"[28]

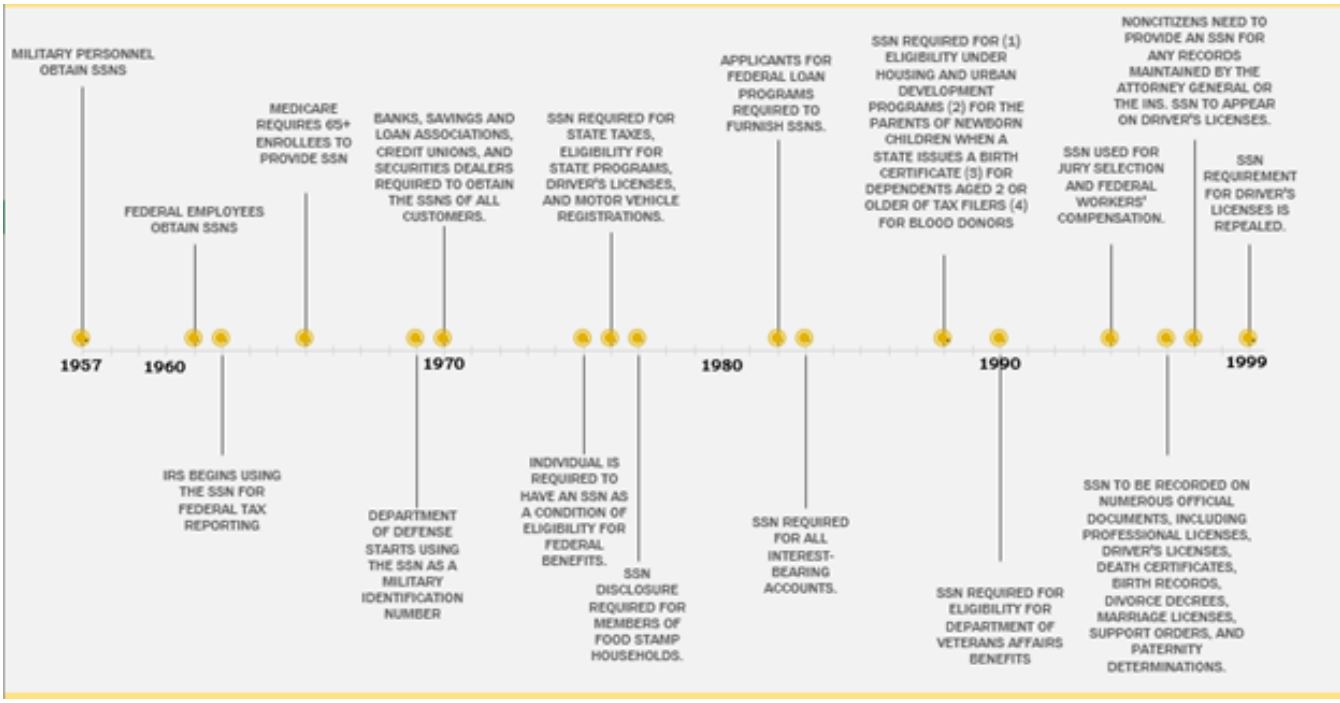
In order to make proper payments to beneficiaries, we advise for the social benefit agencies to improve its current authentication framework that would allow them to more accurately determine whether the person filing for benefits is really the applicant.

The Identity Dilemma in the US: Challenging SSN as a Form of Digital Identity

The most common identity management pitfall that is present across all three case studies that we covered is the use of the SSN to authenticate the person who is digitally submitting a form or an application. In this section, we will briefly explore the history of the SSN and its evolution as the de facto identifier in the US. We will also explain the important differences between an identifier and an authenticator within an IMS.

The SSN is a vital form of identity in the United States. The nine digit number must be submitted when applying for mortgages, opening bank accounts, filing taxes, obtaining benefits and getting a job among many other use-cases. It is currently the de facto identifier for people in the United States[29]. The below exhibit illustrates the widespread expansion in the use of the SSN since its inception[30].

Expansion of SSN use-cases over time

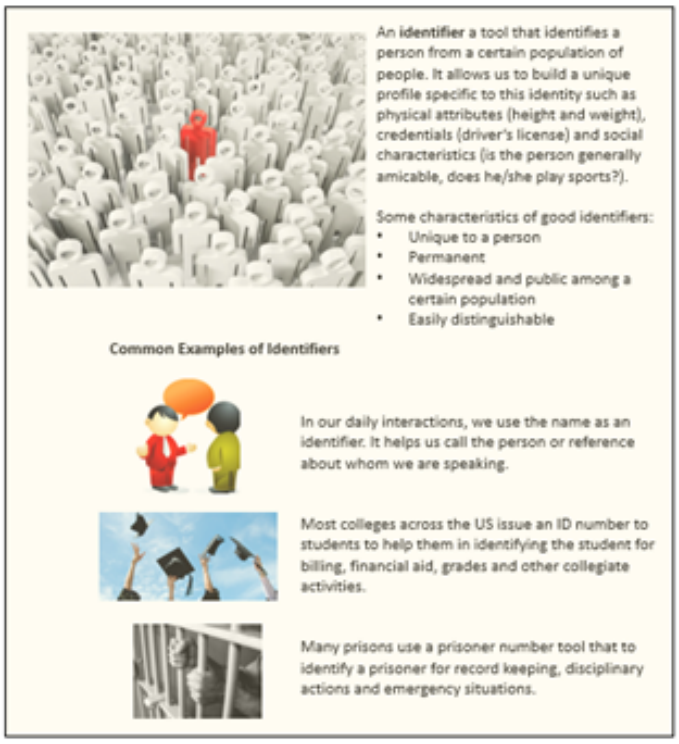


Despite its current use-cases, the SSN was established in 1936 to track earnings histories for the administration of social security entitlements and other benefits[31]. According to the Social Security Administration ("SSA"):

"The card was never intended to serve as a personal identification document—that is, it does not establish that the person presenting the card is actually the person whose name and SSN appear on the card. Although SSA has made the card counterfeit-resistant, the card does not contain information that would allow it to be used as proof of identity"[32].

SSA has publicly stated that the SSN card by itself can not provide proof of identity yet many private and public enterprises continue to use SSN as an authenticator; to verify the identity claimed by a person. While SSN number is a great identifier because it is unique for each person, permanent and widespread amongst the US population, the SSN is not a good authenticator of identity[33]. The exhibit below helps differentiate between an identifier and an authenticator.

Identifier versus Authenticator



According to a report published by a Task Force on Identity Fraud within FTC:

"…there is a broad consensus that the use of the SSN as an identifier is often beneficial, but that its use as an authenticator – as proof of identity – is problematic. Identifiers are effective only when they are widely shared. One's name, for example, is widely known and generally effective as an identifier, although in many cases its lack of permanence or uniqueness prevents it from being useful as an identifier. Authenticators, on the other hand, are effective only when they are secret and thus not widely known. According to commenters and workshop participants, SSNs do not function well as authenticators because they are used commonly as identifiers and thus are widely available"[34].

To better understand this issue, suppose an individual sets up an online bank account and a password. They will probably be comfortable if they knew that their password was private and known to very few parties such as a family member or the bank itself (so that it can facilitate a password reset if a password is forgotten). However, imagine if this password is now used and stored both in digital and paper formats by hundreds of different parties, many of whom the individual might not even know about and whose compliance and security procedures may be inadequate. One bad apple can leak your password to the world. This is unfortunately the reality with the SSN, only there is no password update feature that will allow an individual to change their SSN until their identity is compromised. According to SSA policy, one needs to obtain

proof that the SSN has been abused. In all of 2014, only 250 SSNs were replaced based on misuse[35].

Current Risk with the SSN

There is a wealth of evidence to suggest that the current security of most Americans' SSN is very poor. While the SSA and FTC do not have any reliable information on how many SSNs have been compromised to date, Jay Jacobs, an expert on data breaches and former data scientist at Verizon, estimates that 60-80% of all SSNs have been stolen by hackers already[36]. This is a startling estimate, but it does not appear unreasonable given instances like the Anthem data breach in February 2015 that resulted in up to 80 million compromised accounts[37]. This represents 18% of all SSNs ever issued by the SSA[38]. Verizon's latest data breach investigations report estimates that 285 million records have been compromised to date (though the extent of the information acquired is not known)[39]. In our view, it is very possible that the majority of SSNs have been compromised and are therefore available to identity thieves.

If you have not yet experienced any incidents of identity theft, it is likely due to good fortune as opposed to secure storage of your private details by your service providers. There were nearly 18 million identity theft victims in 2015 according to a Bureau of Justice Statistics Report[40]. This represents 7% of the entire adult working population in the US[41]. At this pace, every member of the working population will experience identity theft approximately every 15 years which is a conservative estimate based on an assumption of no growth in the total number of identity theft victims every year. With the increasing availability of sensitive information online, worldwide internet adoption trends, and the growing sophistication of fraudsters online, it seems likely that the occurrence of identity theft will only grow with time without the adoption of new security standards. In our opinion, with the current IMS in place, it seems inevitable that identity theft will continue to be pervasive.

Fortunately, this trend can be contained and even reversed with a better IMS. In the remainder of the paper, we will cover several case studies of government identity systems and we will discuss the benefits and pitfalls of each. We will also lay out the framework for a better identity management system. We believe that steps must be taken today to address the growing concern of identity theft and to combat identity thieves who are finding US citizens and residents to be easy targets.

Estonia, Kazakhstan and India: Three Approaches to National Identity Management

Case Study: Estonia

History of the Identity Management System

The Estonian identity system and public IT infrastructure developed over the past decade and a half is at the forefront of what most governments are able to provide to their citizens. People are able to securely identify themselves both with computers and through their phones so they can do things such as vote or set up a company online. The push to build this infrastructure started shortly after the gained independence from the Soviet Union in 1991, and this makes them an excellent example of how a country might best design an IMS from scratch in the age of the internet. While the public-private key cryptography underlying the Estonian IMS has been known and implemented in other contexts for decades, the country's success in implementing the solution in coordination with the legislative process and the private sector has made it truly exciting.

Components of the Identity Management System

In 2002, Estonia introduced an identity card for its citizens with a secure chip that holds a range of key data. This data includes the person's name, national ID number, and gender, but perhaps most importantly it includes a public/private key pair and public key certificate.[42] Using this public key certificate, a counterparty is be able to go to check with the government that the public key is owned by the individual and that the ID has been issued by the government. This is the same basic security protocol widely used online, and Estonia has made their IDs compatible with current online standards so it had wide operability.

The applications of a digital version of key attributes pertaining to an individual such as national ID number are readily apparent in digital world, but the public-private key pair adds two important pieces of functionality for identity verification. First, this allows you to send and receive encrypted messages from verifiable sources. Second, you are able to digitally sign documents, and these signatures are legally binding in the country. These digital signatures have proven to be the most popular new feature in Estonia, while very few people have taken advantage of the secure messaging.[43] Nevertheless, these new features represent a great advance in universal adoption of a public-private key infrastructure.

A key component to making this identity truly digital is Estonia's push to have operability with people's computers through the use of a card reader dongle and the availability of the ID on your phone, a feature that was recently introduced. The functionality of the ID would be limited without this additional support, and this highlights the importance of building features around

this new identity system in order to make it relevant. As technology advances and people start to adopt new patterns of behavior, it takes coordination with government and private sector to develop and implement technology.

Creating a Working Identity Management System

One important feature in Estonia's IMS is the reliance on the government as a trusted authority. There is no decentralized nature to the way these identities are originated or verified, and this is common to all current forms of identity management in other countries. However, since the government is already involved in comprehensive identity management for its citizens, it is well placed to be this authority as a type of public utility. Also, since the issuance of this ID is based on a physical authentication, which is considered to be the highest level of identity verification, the ID should provide a high standard of security. There are certainly potential risks with the administration of such a program, but they are most likely lower than the risks that exist with current systems in the United States and other developed countries.

Case Study: Kazakhstan

History of the Identity Management System

Kazakhstan has a population of approximately 17 million people and ranks 28th worldwide in UUN open government rating (jumped from 83th spot in 2003) and is first in Central Asia region[44]. The concept of Kazakhstani e-government system including digital identity and digital signature was approved in 2004[45] to minimize physical interactions of citizens and corporations with the government bodies and to deliver government services online through a single point. Much like Estonia, Kazakhstan gained independence from Soviet Union only in the 1991 so the country did not have a well established identity system in place. In the beginning, the national identity system in Kazakhstan was fragmented. Citizens used various means to identify themselves for different purposes:

- TRN (Taxpayer Registration Number) for paying taxes
- SIC (Social Individual Code) for pension savings
- ID number for banking accounts, property rights and other purposes

Eventually, Kazakhstan developed an IMS that used several important tools and concepts to identify and authenticate citizens in both the digital and the physical spaces.

Components of the Identity Management System

The Individual Identification Number ("IIN") became a key identifier for any person or legal entity. Each Kazakhstani resident has an identification number, which is unique, public (person

can search for another person's IIN online by name and/or date of birth on the designated government website[46]) and the only single number used to identify the person. The IIN is assigned to a person once he/she obtains the ID document or passport and is permanent throughout the person's life. The number needs to be provided to fulfill essential chores such as:

- Paying taxes
- Open bank accounts
- Receiving medical services

While the IIN is widely used as an identifier, it is not an authenticator. Residents of Kazakhstan obtain a digital signature, which is a pair of private and public keys, that identify and authenticate the person. In fact, each person is authenticated either in-person using a picture or other physical attributes or digitally using the person's digital signature. In order to obtain the digital signature, a person would need to be physically authenticated by the National Certification Center, which issues the digital signature. The digital signature is then stored on a number of devices including:

- In a file format on person's computer
- On mobile phone SIM-card
- On a microchip embedded inside each resident's ID card[47].

By signing the request with the valid digital signature, the person can make payments, register companies, pay fines/taxes and apply for marriage among many other use-cases[48].

Creating a Working Identity Management System

Another unique element of the Kazakhstani identity management system is the role of the centralized certification authority. The Government Certification Center has the authority to delegate the issuance and validation of digital signatures to third parties after they pass the required certification procedures. Therefore, there can be several independent government-approved identity providers in the country. In fact, there are currently two such providers in addition to the National Certification Center[49][50].The Kazakhstani government's vision is to rollout identity management to the private sector under the government's supervision.

There are, several drawbacks with country's current IMS. The methods for storing the digital signature are not equally safe or convenient. There are known cases when digital signature files were sent to the customer via email by the government representatives, which can pose serious information security risks. Having the certificates stored on a piece of hardware (ID document, USB dongle) is more secure but it is also more cumbersome for the end users. Also, storage on the SIM-card raises questions about risks of losing the phone and the level of access that the mobile operators providing the SIM-cards will have to users' keys.

It is also important to mention that engagement level from the private sector outside of the financial system is still relatively low. One possible reason for this is the necessity to deal with government to access existing APIs or to request new ones. User adoption of digital signatures is also relatively low currently, especially in more rural areas. Current number of active digital signatures is approximately 4 million[51], which is represents 21% of the country's population.

Despite the difficulties, Kazakhstan's IMS is considered successful by state authorities whose main goal was to reduce the bureaucracy in the provision of the government services to its citizens. Currently, 522 out of 730 services are available online and are facilitated by the IMS. Kazahkstan's government plans to rollout all of remaining government services online by 2018[52].

Case Study: India

History of Aadhaar and motivation to create the Identity Management system

In 2009, the Indian government launched the Aadhaar, a 12 digit unique identifier, with the goal of creating a national standard of identification. Prior to this program there were several identification schemes throughout India, and the government believed that instituting a national unique identifying code for each person along with a national identification card would allow better tracking of the distribution of government benefits to its citizens, similar to the role of SSN in the United States. Unlike in the US, the Indian government's effort included collecting biometric attributes such as fingerprints and iris scans during the onboarding process and linking them to the identification number along with other data on the individual. While the program is not mandatory, the government has successfully signed up over 950 million people in the country and expects to reach 1 billion in 2016[53].

The creation of a unique identifier is an essential piece of government infrastructure for many administrative functions of the government including the prevention of fraud within the distribution of rations or welfare benefits. The Indian government was also well aware of many of other important non-government benefits their citizens would receive from having a widely accepted method of identification. For instance, this ID would allow many more citizens to open bank accounts and be included in the financial system. Given India's size and the it's goal of essential benefit distribution, the IMS that it chose was not a fully digital one like the one in Estonia or Kazakhstan.

It is interesting to note that despite the lack of sophistication relative to the IMS in Estonia or Kazakhstan, India's IMS has still build a necessary authentication layer that the US currently lacks. While the unique identifier will help to create a more accurate record of the population, the

biometric data that the government is collecting will help the people authenticate themselves when they receive necessary benefits or apply for a bank account.

Criticism of the Identity Management System

The identity project in India has met resistance from some members of the country who have concerns about the government's mass collection and pooling of personal data. A Supreme Court ruling[54] on the privacy concerns related to Aadhaar has determined that the card is legal because it is not mandatory, implying that government does not have the constitutional authority to mandate the collection of biometric data from its citizens. Many countries may have similar protections for their citizens against this kind of data collection, and there are reasons people would want to prevent the expansion of the government's access to personal information beyond what is necessary. In India, there have been cases of law enforcement agencies attempting to access the fingerprint data collected for Aadhaar for their trials[55]. The Aadhaar system has been testing the boundaries of violating personal privacy, and this will continue to be an issue as other countries consider updating their IMS.

Another concern with the Aadhaar system is the security risk of having a centralized store of biometric information. Unlike the national identification number, people's biometric information cannot be replaced if stolen, which makes the safety with which the government stores this data essential. The hack of the Office of Personnel Management in the United States resulted in the loss of over 5 million fingerprints of government employees[56], and one can imagine the impact of an attack like this being magnified many times over in the case of India where nearly 1 billion fingerprints and iris scans are stored in government databases. Since central governments are already targets of many of the most sophisticated hacks, trusting them with more sensitive information is not desirable.

The Aadhaar project highlights some of the risks of setting up a IMS. While having a trusted standard of identification and authentication is a powerful way to enable commerce and government activity, storing the attributes of that individual introduces security risk and privacy concerns that are undesirable.

Framework for the US Digital Identity System

We believe that the three cases on the IMS implemented in Estonia, Kazakhstan and India highlight how far behind US is in implementing an IMS that is effective the digital world. In the following section, we will address the lessons we learned from the three countries and we will propose a framework for a better IMS. We will also discuss the potential role of blockchain technology in creating a more secure identity.

Lessons Learned from Estonia, Kazakhstan and India

An element that all three countries have in common with the US is the existence of a unique identifier for all citizens of the country:

- Estonia = National Identification Number
- Kazakhstan = Individual Identification Number
- India = Aadhaar
- US = Social Security Number

The overarching difference between US and the other three countries is that only in the US is the unique identifier a secret piece of information that is used to authenticate users. Estonia and Kazakhstan both utilize public and private key encryption as well as certificates to authenticate devices as well as users. This means that in order for citizens to be authenticated, they would need to know the private key (or password) related to their public key and they would need to have a cryptographic certificate that is issued by an approved authority. In India, a user can be authenticated using biometrics that are associated with their Aadhaar number.

We believe that adding the public and private key infrastructure as well as cryptographic certificates is a proven way to improve the IMS in the US. The technology is well studied and is already widely implemented across enterprises that store sensitive and private information. Estonia and Kazakhstan also offer useful pilots for US to use in attempting a similar system.

Just to clarify, our proposition is not far from efforts that some US agencies have been experimenting with. For instance, IRS is experimenting with rolling out an IP PIN for users to use in conjunction with the SSN when filing taxes[57]. The IP PIN is similar to a private key while the SSN resembles the public key associated with the identity. We would recommend a much wider rollout of this feature with use-cases outside of filing taxes. For instance, we recommend for the same private key to be used when applying for benefits or filling out a credit card or a bank account application. We also recommend to complement the widespread rollout of a private key with the issuance of certificates to approved devices which adds another layer of authentication for those users that are filling out forms and applications digitally.

With that said said, there are several limitations when using Estonia and Kazakhstan as pilots demonstrating the successful implementation of an IMS in the digital world. There are several significant differences that exist between those two countries and the US, such as:

- Both Estonia and Kazakhstan had the benefit of building a new IMS without the need to replace an established legacy infrastructure. The US has SSN as the de facto identifier. Any IMS would need to include the SSN as a key component

- The population size in Kazakhstan and Estonia is much smaller (17 million and 1.3 million people respectively) compared to US resulting in a lot of additional complexity and cost when getting users to adopt and understand the new system
- US economy and regulations are much more complex and serve to accommodate a much larger number of companies and industries. New IMS will have to involve getting these players on board to implement the necessary changes

While recognizing that there are quite a few differences between US and Estonia/Kazakhstan, we still believe that the long term benefits of the new system in terms of added security and reduced cost related to various types of identity fraud far outweighs the cost of implementing the system throughout the country, although more quantitative analysis needs to be done to explore the benefits and costs of this IMS. With that said, we also considered an alternative technology, the blockchain, when weighing potential solutions for identity management.

Digital Identity and the Blockchain

While we think that the blockchain offers several attractive characteristics, especially when serving as a decentralized and distributed ledger for transactions, we believe that blockchain at this point in time is not a practical solution for advancing a national IMS with respect to issuing a form of identity that can later be authenticated when transacting with third parties. However, we do see a lot of potential complementary benefits that a blockchain can add to a working IMS that can help reduce fraud and/or comply with existing regulations. In addition to this, blockchain does have some significant applications for managing the attributes associated with a digital identity in a distributed way allowing one to transact personally sensitive information about themselves through the use of permissions. A truly digital IMS similar to that of Estonia of Kazakhstan could enable these applications of the blockchain in a secure way that reduces the utility of governments to pool data about individuals.

Need for Centralization

Having a digital ID that allows you to be easily identified online. The public-private key pair along with a certificate used in Estonia is a very effective system, but it requires a robust method of authentication, such as in person authentication at the time of issuance for the system to be reliable and trustworthy. This is why having an authority that is widely trusted acting as the issuer of these identities is essential to the system. This identity authority does not need to be a government body, and there could be several authorities so long as they all can be trusted to follow a similar authentication procedure in order to issue the identity. However, in the case of a county like the United States, it is most practical for the government to be the single trusted authority and a shared utility. As we see in Estonia, the integration of the digital identity system into the law and public services such as tax collection and voting are key functionalities that the government is best suited to implement.

Applications of a Digital Identity on Current Applications of Blockchain

Creating a IMS in the United States would have broad benefits across the various forms of identity theft that we have explored in this paper, and would potentially enable many other activities online, including blockchain applications. In fact, many of the current financial applications using bitcoin and blockchain may ultimately have to be reconciled with the fraud, anti money laundering and sanctioning regulations that have resulted in high cost structures in the current banking system. Transactions on the blockchain are immutable which makes the liability for any fraudulent transaction fall on sender of the payment. Short of adding a broader consumer protection scheme to a blockchain payment scheme, incorporating a robust IMS with participants in blockchain transactions will be essential to preventing fraud. Also, if the identity of a counterparty in a blockchain transaction could be verified through a trusted IMS, it would enable people to confirm that whether the person they are attempting to transact with is on a sanctioned list or is at a high risk of being part of a money laundering operation.

Blockchain Applications for Identity Attribute Management

Blockchain can be used as a public registry of permissions that allows holders of a digital identity to publicly permission counterparties to access different pieces of information about them. We envision this system as being similar to one proposed by MedRec[58], a project created in the MIT Media Lab to facilitate the sharing of medical records across different medical providers. In this example, medical records generated from a visit with a physician are stored on a database within that medical institution and a pointer to that information is stored onto the Ethereum Blockchain along with a smart contract that stores the counterparties who are permissioned to access that file. During a visit with a separate physician, the patient could use MedRec to permission the new doctor to view the medical record and the file could be automatically transferred to the new doctor. What this system allows for is a distributed record of where official information is stored along with a trusted method for the patient to control access to that information. There is no need for any central body to maintain a list of medical documents associated with an individual, and it potentially helps cut the administrative burden of handling sensitive data.

With a secure digital identity, we believe there is an opportunity to implement a similar distributed registry and permissions system for a range of potentially sensitive and official attributes associated with an individual. For instance, one could use such a blockchain to associate a person with their college degree and transcript, driver's license, birth certificate, or insurance documents when these documents are created or issued. These documents could be associated with an account that requires a digital ID in order to permission other people to view that information. This would give the user easy access to their private information, and does not require any central source to act as an intermediary. The current process of sharing this sort of

information is cumbersome and often times very costly. Many people moving to a new country have difficulty asserting their job qualifications acquired in their home country, and it may even be burdensome to verify attributes such as marital status. In many job applications, applicants are asked to provide their educational history which is only verified after a decision has been made through more extensive background checks. A digital identity could be used in conjunction with something similar to MedRec to provide easy way of sharing sensitive information digitally.

Conclusion

In this report, we discussed prevalence of identity fraud in credit card applications, issuance of tax refunds and distribution of social welfare benefits. In each of the cases, we raised concerns about the current IMS in the US and the systematic dependence on the SSN as an identifier and an authenticator. We then examined several existing models of an IMS in Estonia, Kazakhstan and India attempting to draw meaningful lessons from these implementations for a specific use case in the US. Finally, we drew several preliminary recommendations for a better IMS in the US encouraging the adoption of a private-public key infrastructure and certificate framework similar to Estonia and complementing the system with a new distributed permissions ledger made possible by blockchain technology.

Given our research to-date and conclusions that we drew from our examples in Estonia and Kazakhstan, we recommend further evaluation of the benefits, costs, risks and opportunities of implementing a public-private key infrastructure and certificate system in the US. The areas of focus that interest us most include:

- Practical implementation - assessing and quantifying the scope, resource requirements and budget needed for reorganizing US IMS
- Data security and privacy - as seen in the example of Aadhaar in India, personal information storage is an important part of the design of the successful identity management system. Projects like Enigma[59] and Vanish[60] can serve as a starting point for further research in this field
- User experience and adoption - while physical token is the most secure way for storing the private key, users usually find it less convenient than files stored on their devices or in the cloud. There needs to be experimental testing to strike a balance between convenience to the user and the robustness of security

We hope that this report elevates concerns regarding identity theft and prioritizes the need for a new IMS in the US. Our goal is to start a conversation and to encourage others to explore the many questions and concerns that still need to be addressed in an effort to build an identity system that works.

Endnotes

1. Harrell, Erika. Victims of Identity Theft, 2014. Rep. U.S. Department of Justice, Sept. 2015. Web. 10 May 2016.
2. Harrell, Erika. Victims of Identity Theft, 2014. Rep. U.S. Department of Justice, Sept. 2015. Web. 10 May 2016.
3. "The Nilson Report | News and Statistics for Card and Mobile Payment Executives." The Nilson Report | News and Statistics for Card and Mobile Payment Executives. The Nilson Report, 10 May 2016. Web. 10 May 2016.
4. "The Nilson Report | News and Statistics for Card and Mobile Payment Executives." The Nilson Report | News and Statistics for Card and Mobile Payment Executives. The Nilson Report, 10 May 2016. Web. 10 May 2016.
5. Identity Theft and Tax Fraud. Rep. no. GAO-15-119. US Government Accountability Office, Jan. 2015. Web. <http://www.gao.gov/assets/670/667965.pdf>.
6. “2014 Refunds Ahead of Last Year." 2014 Refunds Ahead of Last Year. IRS, 3 Mar. 2014. Web. 9 May 2016. <https://www.irs.gov/uac/Newsroom/2014-Refunds-Ahead-of-Last-Year>.
7. Hunter, Matt. "Tax-refund Fraud to Hit $21B." CNBC. CNBC, 11 Feb. 2015. Web. 09 May 2016. <http://www.cnbc.com/2015/02/11/tax-refund-fraud-to-hit-21-billion-and-theres-little-the-irs-can-do.html>.
8. Assuming no change in total tax refund payments from the year 2013. Latest IRS publishing shows total tax refund payments decrease to $125 billion during the year 2015.
9. Identity Theft and Tax Fraud. Rep. no. GAO-15-119. US Government Accountability Office, Jan. 2015. Web. <http://www.gao.gov/assets/670/667965.pdf>.
10. Identity Theft and Tax Fraud. Rep. no. GAO-15-119. US Government Accountability Office, Jan. 2015. Web. <http://www.gao.gov/assets/670/667965.pdf>.
11. Identity Theft and Tax Fraud. Rep. no. GAO-15-119. US Government Accountability Office, Jan. 2015. Web. <http://www.gao.gov/assets/670/667965.pdf>.
12. Identity Theft and Tax Fraud. Rep. no. GAO-15-119. US Government Accountability Office, Jan. 2015. Web. <http://www.gao.gov/assets/670/667965.pdf>.
13. Identity Theft and Tax Fraud. Rep. no. GAO-15-119. US Government Accountability Office, Jan. 2015. Web. <http://www.gao.gov/assets/670/667965.pdf>.
14. Identity Theft and Tax Fraud. Rep. no. GAO-15-119. US Government Accountability Office, Jan. 2015. Web. <http://www.gao.gov/assets/670/667965.pdf>.
15. "IRS, States and Tax Industry Combat Identity Theft and Refund Fraud on Many Fronts." IRS, States and Tax Industry Combat Identity Theft and Refund Fraud on Many Fronts. IRS, 1 Jan. 2016. Web. 09 May 2016. <https://www.irs.gov/uac/Newsroom/IRS,-States-and-Tax-Industry-Combat-Identity-Theft-and-Refund-Fraud-on-Many-Fronts>.
16. Identity Theft and Tax Fraud. Rep. no. GAO-15-119. US Government Accountability Office, Jan. 2015. Web. <http://www.gao.gov/assets/670/667965.pdf>.
17. Number of People Receiving Social Security, Supplemental Security Income (SSI), or Both, March 2016 (in Thousands) (n.d.): n. pag. Web. https://www.ssa.gov/policy/docs/quickfacts/stat_snapshot/2016-03.pdf

18. Total Number of Medicare Beneficiaries. N.p., n.d. Web. 09 May 2016. http://kff.org/medicare/state-indicator/total-medicare-beneficiaries/
19. "Welfare Fraud." Federal Safety Net. N.p., n.d. Web. 09 May 2016. http://federalsafetynet.com/welfare-fraud.html
20. Improper payments, a joint federal government website from the U.S. Department of the Treasury, in coordination with the U.S. Department of Justice and Office of Management and Budget (OMB). https://paymentaccuracy.gov/content/faq
21. General Accounting Office. Testimony Before the Committee on Homeland Security and Governmental Affairs, U.S. Senate. Improper Payments. March 16, 2015 http://www.gao.gov/assets/670/669026.pdf
22. "Identity theft: the fastest growing crime in America", TrustedID inc, June 2009 https://www.scranton.edu/alumni/pdf/TrustedID_Complete%20Insight%20into%20Identity%20Theft%20in%20America-1.pdf
23. Melanie Payne, The (Fort Myers, Fla.) News-Press. "Online Scam Hijacks Social Security Benefits." USA Today. Gannett, 28 July 2013. Web. 09 May 2016. http://www.usatoday.com/story/news/nation/2013/07/28/social-security-benefits-scam/2594675
24. "Identity theft: the fastest growing crime in America", TrustedID inc, June 2009 https://www.scranton.edu/alumni/pdf/TrustedID_Complete%20Insight%20into%20Identity%20Theft%20in%20America-1.pdf
25. "Report: Social Security Numbers Active for 6.5 Million People Aged 112." PBS. PBS, n.d. Web. 09 May 2016. - http://www.pbs.org/newshour/rundown/death-stop-social-security-payments/
26. "May Is Public Assistance Fraud Awareness Month - Record Herald - Recordherald.com." Record Herald. N.p., n.d. Web. 09 May 2016. http://recordherald.com/news/6229/may-is-public-assistance-fraud-awareness-month
27. "FTC to Host Tax Identity Theft Awareness Week Jan. 25-29." Federal Trade Commission. N.p., n.d. Web. 09 May 2016. –https://www.ftc.gov/news-events/press-releases/2016/01/ftc-host-tax-identity-theft-awareness-week-jan-25-29
28. "Report: Social Security Numbers Active for 6.5 Million People Aged 112." PBS. PBS, n.d. Web. 09 May 2016. - http://www.pbs.org/newshour/rundown/death-stop-social-security-payments/
29. Kouri, Jim (March 9, 2005). "Social Security Cards: De Facto National Identification". American Chronicle
30. Puckett, Carolyn. The Story of the Social Security Number. Rep. Social Security Bulletin, Vol. 69, No. 2, 2009. Web. 09 May 2016. <https://www.ssa.gov/policy/docs/ssb/v69n2/v69n2p55.html>.
31. Puckett, Carolyn. The Story of the Social Security Number. Rep. Social Security Bulletin, Vol. 69, No. 2, 2009. Web. 09 May 2016. <https://www.ssa.gov/policy/docs/ssb/v69n2/v69n2p55.html>.
32. Puckett, Carolyn. The Story of the Social Security Number. Rep. Social Security Bulletin, Vol. 69, No. 2, 2009. Web. 09 May 2016. <https://www.ssa.gov/policy/docs/ssb/v69n2/v69n2p55.html>.
33. Security in Numbers: SSN's and ID Theft. Rep. Federal Trade Commission, Dec. 2008.

Web. 9 May 2016. <https://www.ftc.gov/sites/default/files/documents/reports/security-numbers-social-security-numbers-and-identity-theft-federal-trade-commission-report/p075414ssnreport.pdf>.
34. Security in Numbers: SSN's and ID Theft. Rep. Federal Trade Commission, Dec. 2008. Web. 9 May 2016. <https://www.ftc.gov/sites/default/files/documents/reports/security-numbers-social-security-numbers-and-identity-theft-federal-trade-commission-report/p075414ssnreport.pdf>.
35. Shahani, Aarti. "Theft Of Social Security Numbers Is Broader Than You Might Think." NPR. NPR, 15 June 2015. Web. 09 May 2016. <http://www.npr.org/sections/alltechconsidered/2015/06/15/414618292/theft-of-social-security-numbers-is-broader-than-you-might-think>.
36. Shahani, Aarti. "Theft Of Social Security Numbers Is Broader Than You Might Think." NPR. NPR, 15 June 2015. Web. 09 May 2016. <http://www.npr.org/sections/alltechconsidered/2015/06/15/414618292/theft-of-social-security-numbers-is-broader-than-you-might-think>.
37. "Anthem." Privacy Rights Clearinghouse. Privacy Rights Clearinghouse, 5 Feb. 2015. Web. 09 May 2016. <https://www.privacyrights.org/content/anthem>.
38. Based on 450 million issued SSNs according to Puckett, Carolyn. The Story of the Social Security Number. Rep. Social Security Bulletin, Vol. 69, No. 2, 2009. Web. 09 May 2016. <https://www.ssa.gov/policy/docs/ssb/v69n2/v69n2p55.html>.
39. "Evolution of the Verizon Data Breach Investigations Report (2008-2016)."Evolution of the Verizon Data Breach Investigations Report (2008-2016). Verizon, 25 Apr. 2016. Web. 09 May 2016. <http://www.slideshare.net/VerizonEnterpriseSolutions/evolution-of-the-verizon-data-breach-investigations-report-20082016>.
40. Victims of Identity Theft, 2014. Rep. no. NCJ 248991. Bureau of Justice Statistics, Sept. 2015. Web. 9 May 2016. <http://www.bjs.gov/content/pub/pdf/vit14_sum.pdf>.
41. Victims of Identity Theft, 2014. Rep. no. NCJ 248991. Bureau of Justice Statistics, Sept. 2015. Web. 9 May 2016. <http://www.bjs.gov/content/pub/pdf/vit14_sum.pdf>.
42. "Electronic ID Card." - E-Estonia. E-estonia.com, 10 May 2016. Web. 10 May 2016.
43. "Avaleht ID.ee." Avaleht ID.ee. Http://www.id.ee/, 10 May 2016. Web. 10 May 2016.
44. "EGOVKB | United Nations Home." EGOVKB | United Nations Home. N.p., n.d. Web. 09 May 2016. https://publicadministration.un.org/egovkb/Data-Center
45. On state program of e-government creation in Kazakhstan in 2005-2007, Decree of President of Kazakhstan, 10 November 2004, "О Государственной программе формирования "электронного правительства" в Республике Казахстан на 2005-2007 годы." - ИПС "Әділет" N.p., n.d. Web. 09 May 2016.http://adilet.zan.kz/rus/docs/U040001471_
46. Taxpayer search, "Поиск налогоплательщиков | Комитет государственных доходов Министерства финансов Республики Казахстан." Поиск налогоплательщиков | Комитет государственных доходов Министерства финансов Республики Казахстан. N.p., n.d. Web. 09 May 2016. http://www.kgd.gov.kz/ru/services/taxpayer_search
47. "National Certification Authority." Национальный удостоверяющий центр РК. N.p., n.d. Web. 09 May 2016.http://pki.gov.kz/index.php/en/fizicheskie-litsa
48. "List of Online Services for Citizenry." Electronic Government of the Republic of

Kazakhstan. N.p., n.d. Web. 09 May 2016. http://egov.kz/cms/en/online-services/for_citizen
49. "KISC Certification Authority." KISC Certification Authority. N.p., n.d. Web. 09 May 2016. http://www.kisc.kz/english/ca/general.html
50. Gamma Technologies DS Certificate, Gamma Technologies - https://ca.gamma.kz/en
51. "National Certification Authority." Национальный удостоверяющий центр РК. N.p., n.d. Web. 09 May 2016. http://pki.gov.kz/index.php/en/
52. 9.7bn Rubles spent in Kazakhstan for e-government "9,7 млрд рублей потратили в Казахстане на электронное правительство - ИА REGNUM." ИА REGNUM. N.p., n.d. Web. 09 May 2016., – http://regnum.ru/news/polit/2116603.html
53. "DASHBOARD SUMMARY." UIDAI. Unique Identification Authority of India, 10 May 2016. Web. 10 May 2016.
54. "Aadhaar Purely Voluntary, Says Supreme Court; but Extends Its Use to More Schemes." The Hindu. The Hindu, 15 Oct. 2015. Web. 10 May 2016.
55. "Stop Aadhaar Data Use to Probe Crime: UIDAI to SC." The Indian Express. The Indian Express, 19 Mar. 2014. Web. 10 May 2016.
56. KOREN, MARINA. "About Those Fingerprints Stolen in the OPM Hack." The Atlantic. Atlantic Media Company, 23 Sept. 2015. Web. 10 May 2016.
57. "IRS, States and Tax Industry Combat Identity Theft and Refund Fraud on Many Fronts." IRS, States and Tax Industry Combat Identity Theft and Refund Fraud on Many Fronts. IRS, 1 Jan. 2016. Web. 09 May 2016.
58. Ekblaw, Ariel, Asaf Azaria, Thiago Vieira, and Andrew Lippman. "MedRec."PubPub. PubPub, 02 May 2016. Web. 10 May 2016.
59. "Want to Dive in the Technical Details? See Our Whitepaper!" Enigma. N.p., n.d. Web. 09 May 2016.http://enigma.media.mit.edu
60. "Vanish: Enhancing the Privacy of the Web with Self-Destructing Data." Vanish: Enhancing the Privacy of the Web with Self-Destructing Data. N.p., n.d. Web. 09 May 2016. http://vanish.cs.washington.edu