Social Insecurity: The End of Privacy

Ron Johnson
**Introduction**

We have lost all remnants of personal privacy as a result of the pervasive collection of personal information by for-profit data aggregators and voluntary sharing via social networks. The result of this loss has contributed to an epidemic of identity theft crimes; however, easy access to personal information is not the sole enabler of this phenomena. Instead, the identity theft crime wave is rooted in the use of a single, weak national identification number used by government and corporations to identify individuals providing opportunity for unprecedented levels of theft by amateur and professional alike.

The technological evolution of information collection and sharing has outpaced government's outdated single-factor personal identification system requiring the adoption of a system for multi-factor authentication of individual identity.
Chapter One

As a society we have permitted our privacy to erode to the point where we now have no protection against anyone acquiring our most personal information. The invasion of our privacy is not solely about government intrusion which we largely accept as a cost of protection but more by criminal elements determined to steal from us all they can. These criminal elements include organized groups of professional thieves as well as the amateur wanting to capitalize on the weaknesses in the system. As our privacy has been eroded we find ourselves now reeling from the reality that no one is safe from disclosure of the most private details of their lives. This new reality; this end of privacy, cannot be more clearly demonstrated than by the recent publication of personal information including Social Security numbers, dates of birth, even current credit reports of those whom we would all expect to be safe; such as, the FBI director, the Chief of the LA police department, the Attorney General of the U.S., and the Vice President of the U.S.

Roger Ehrenberg stated most succinctly: “I believe consumer privacy is largely dead...” (Lyster, 2013). Now in the postmortem examination we ask; who killed our privacy and do we bare any responsibility for its death?
Is there any remnant of privacy remaining in our lives? Furthermore, what does this new landscape mean for our expectations that our personal information is reasonably safe?

Naomi Troni suggests that we are complicit in the loss of our privacy: “Never in the course of human interaction have so many shared so much about themselves with so many others—and with so little apparent concern for their privacy.” (Troni, 2012) Our postings to social media sites, e-mails, web surfing habits, what we purchase, where we purchase it, everything we do feeds the system that invades our lives - there is no opt-out button. (Krishnamurthy & Wills, 2009) We are measured and weighed then categorized, analyzed, and collated; our online information is combined with other public data sources to create a virtual representation of each of us complete with details of every personal identifying bit of data to be used by anyone willing to pay for the privilege. The IT infrastructure constructed to violate us exists in an industry known as data aggregation; an industry which only recently has been placed in the spotlight due to several egregious data breaches.

The largest data aggregator, Acxiom, processes “more than 50 trillion data transactions per year” containing 1,500 data points per person for 500 million people.
globally and a majority of U.S. adults. (Singer, 2012) Companies in the data aggregation industry like Acxiom, Lexus-Nexis, and others comprise a multi-billion dollar industry collecting public information from a “variety of sources including: government census data, social network sites, personal web sites, directories, surveys, business lists and real estate data. All of this information is publicly available. Aggregators don’t create data, they mine it.” (Klingaman, 2010)

The concern about these vast stores of personal information is their security. When one of the largest data aggregators, ChoicePoint, was breached in 2005 145,000 individuals had their personal information stolen. “The identity thieves who obtained ChoicePoint accounts through the establishment of fake businesses had the information equivalent of the key to Fort Knox. With their online access to ChoicePoint’s data files, they were able to obtain all the personal information they needed – including Social Security number and date of birth – to successfully commit identity theft.” (Privacy Rights Clearinghouse, 2007) Commercial companies and government are equally guilty of failing to protect the information they store; for example, in South Carolina 3.8 million (81% of the state population) tax payer records including Social Security numbers were
negligently released by the state’s Department of Taxation. (McLeod, 2012) (Weisbaum, 2012)

The loss of privacy which has provided easy access to anyone’s personal information including Social Security number, address, date of birth, etc. has lead to the explosive growth of financial crimes targeting individuals, government, and commerce. With a target base of approximately 300 million in the U.S. alone criminals who are intent on stealing from us or in our names have limited obstacles while armed with the data that identifies us uniquely to commercial enterprises and to government. In possession of our most personal information a criminal can impersonate us, any one of us, collect his bounty moving on to the next victim without ever leaving her computer. Identity crimes are the fastest growing financial crimes in the U.S. with a 32% increase in 2012 with no sign of abatement due, in large part, to the ever increasing ease of obtaining personal identifying information. (Harper, 2010)

Organized criminal enterprises specializing in identity theft operate on volume stealing from hundreds or thousands over a short period of time then moving on to avoid detection; therefore, gaining access to large stores of personal information is their goal. “Financial crime is a booming underworld industry in parts of the

Social Insecurity: The End of Privacy
Identity Theft Awareness and Prevention Organization (IDTAP.ORG)
former Soviet Union — so much so that local
governments are frequently willing to turn a blind eye.
Hackers can usually operate with impunity in areas
outside U.S. and Western European jurisdiction as long
as they observe three rules, said Lewis: buy off the local
cops, don’t hack the neighborhood bank and be
prepared to do favors for high-ranking state officials.”
(Otis, 2013)

The other class of identity thief is casual and
opportunistic often hoping for “one big score”. These
thieves are much less sophisticated but nonetheless
capable of stealing millions of dollars from government,
individuals, and corporations. Casual identity thieves
acquire personal information from any one of a number
of online data aggregators; such as:

- Intelius
- MyLife
- PeopleFinders
- PeopleSearch Pro
- Pipl
- Rapleaf
- Spokeo
- Zabasearch
Thieves may also acquire personal information from those who have direct access at hospitals, doctor’s offices, financial institutions, attorneys, police, Social Security Administration officials, etc. Commonly, the personal information about any individual may be purchased from a number of underground WWW sites for as little as $10. More exotically given an individual’s name, date of birth, and place of birth acquired from the myriad of publically accessible data aggregators the thieves follow a 5-step process for deriving the individual’s Social Security number. In any case, the identity thief’s goal is to use the personal information to drain bank accounts, open credit accounts, and defraud government services. The fastest growing and most profitable identity theft crime is IRS tax refund fraud which, by some estimates, exceeded $16 billion in 2011.

Faced with a multitude of threats on our privacy surprisingly few Americans take any action to protect themselves. According to a survey by The Ponemon Institute only 7 percent of Americans “change any behaviors in an effort to preserve their privacy.” (Sullivan, 2006) The result of this relaxed attitude has lead to increasing incidents of personal information being released in the public domain such as the recently reported publication of personal information for 17 people who we would assume based on their social
status have safeguards to protect against exactly what happened to them. “Among the specific details included in the data dump are the Social Security numbers and alleged home addresses and contact information for most of the celebrities, as well as their credit reports and other financial information.” (RT, 2013) “The full list of victims, according to the hacker’s Web site: Michelle Obama, Kim Kardashian, Joe Biden, Robert Mueller (FBI Director), Hillary Clinton, Eric Holder (U.S. Attorney General), Charlie Beck (LAPD Chief), Mel Gibson, Ashton Kutcher, Jay Z, Beyonce, Paris Hilton, Britney Spears, Sarah Palin, Hulk Hogan, Donald Trump, Arnold Schwarzenegger.” (Gupta, 2013) If thieves can access the personal data of these high-profile individuals how safe can the rest of us be?

Personal privacy no longer exists in our connected society whether through our own information sharing or via publication by data aggregators we have no security against identity theft. Current estimates suggest that some 30% of the U.S. population has suffered the compromise of their identity in the past 4 years. Those individuals whose identifying information has been used to defraud creditors, the IRS, Medicare, and others have little personal liability for the crimes; however, the process of recovery can be daunting. Only
recently have government agencies recognized the extent of the identity theft problem responding with regulations aimed at providing assistance to victims. Unfortunately, response is the only reaction to the growing identity theft industry because the only viable preventive solutions require fundamental and expensive modifications to the mechanisms used to establish and verify our identities.
Chapter Two

The key to any identity theft scheme is to compromise an individual's unique identification number. Not only is the idea of using a single number to identify an individual outdated, the weakness of the systems used to issue government identification numbers by countries from Albania to Vietnam has led to a growing global identity theft problem. India, Australia, China, Canada, and every country in the Euro-zone have reported significant increases in cases of identity theft; however, the United States leads the world with an estimated 32% of the population having suffered some form of identity theft. The cause of this scourge can be traced directly to the ease with which government-issued identification numbers can be accessed via the Internet as well as, although to a lesser degree, the antiquated process of assigning the identification numbers. A thief can, in most countries, acquire all of the personal information of an individual with access to that individual's unique government-issued identification number. While the thieves' continue to increase their technological sophistication governments have not reexamined the mechanisms used for authentication of identity.
In the United States we have accepted that the Social Security number, now assigned at birth, is our unique identifier for every record of our lives; education, credit, government benefits, health, employment, and every other personal record is tied to us using our assigned Social Security number. Unfortunately, the Social Security number was not intended for use as an identifier it was, instead, designed as an account number for the newly formed Social Security Administration as part of FDR's economic recovery plans. The well-documented algorithm for assignment of the number was developed in 1935 based on the postal service's zip codes allowing for nearly effortless derivation from basic personal information. “Information about an individual’s place and date of birth can be exploited to predict his or her Social Security number (SSN).” (Acquisti & Gross, 2009) As Frank Abagnale recently confirmed, "If you tell me your date of birth and where you're born [on Facebook] I'm 98% [of the way] to stealing your identity,..." Researchers were able to derive individual Social Security numbers "using only publicly available information". (Acquisti & Gross, 2009) Until recently the Social Security Administration used the 75 year-old algorithm for assignment of Social Security numbers finally bowing to overwhelming evidence of the
algorithm's weakness Social Security number assignment was randomized. Randomization will increase the difficulty of derivation which is good news for the new-born but does not address the tsunami of identity theft for the other 300 million of us at risk.

The Social Security number was designed without the foresight of the information age in a time when creating, cataloging, and tracing the account number was performed manually. The newly formed Social Security Administration needed a number that could be created and assigned locally without the possibility of repetition. The method of creating and assigning the Social Security account number is a marvel of the time; each state was assigned an Area number (XXX-) or range of numbers based on population. For example, the first three digits of a Social Security number for the states listed below are:

<table>
<thead>
<tr>
<th>State</th>
<th>Area Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alabama</td>
<td>416-424</td>
</tr>
<tr>
<td>Mississippi</td>
<td>425-428</td>
</tr>
<tr>
<td>Alaska</td>
<td>574</td>
</tr>
<tr>
<td>Vermont</td>
<td>008-009</td>
</tr>
<tr>
<td>Delaware</td>
<td>221-222</td>
</tr>
<tr>
<td>Wyoming</td>
<td>520</td>
</tr>
</tbody>
</table>

*Social Insecurity: The End of Privacy*
Identity Theft Awareness and Prevention Organization (IDTAP.ORG)
A states assigned number ranges are further subdivided within the state allowing for the mapping of a Social Security number's Area Number component to specific counties and / or postal zip codes within the state. In less populous states, as evidenced by the Area number assignment to Wyoming and Alaska, the assignment of Social Security numbers is based on a single Area number. The information mapping the Social Security Area numbers is widely available on the Internet including on the Social Security Administration's website.

The Group number (-XX-) component of the Social Security number is assigned algorithmically. The Group numbers range from 01-99 and are assigned within the state's Area number using odd numbers from 01 through 09 first. When the odd numbers are exhausted the even numbers from 10 through 98 are assigned, then the even numbers from 02 through 08, then the odd numbers from 11 through 99. The range of assignable Social Security numbers is based on the combination of the Area number and Group number (XXX-XX-). The Serial number, the last four digits (-XXXX) of the Social Security number, is assigned consecutively from values in the range of 0001 through 9999. Therefore, for each Area - Group number combination there are 10,000 assignable numbers. The
algorithm for Social Security number assignment may be stated in pseudo-code as:

1. For each Area number
2. For each Group number in the range of
   a) 01, 03, 05, 07, 09
   b) even numbers 10 to 98
   c) even numbers 02, 04, 06, 08
   d) odd numbers 11 to 99
3. Increment previous assigned Serial number by 1
   in the range of
   a. 0001 to 9999
4. Goto 2

The weakness inherent in the Social Security number assignment algorithm may not have been so exploitable were it not for data published by the Social Security Administration. Periodically the Social Security Administration publishes what it calls the Death Master File containing "over 85 million records of death reported since 1936". (Service, 2013) The purpose of the publication according to the Social Security Administration is "to verify death, as well as to prevent fraud". (Service, 2013) Ironically, it is the publication of the Death Master File that has enabled fraud on a massive scale.
Chapter Three

The Death Master File published by the National Technical Information Service from data provided by the Social Security Administration provides the name, date of birth, month and year of death, Social Security number, and zip code of every individual deceased in the U.S. since 1936. The Death Master File has legitimate uses in business and genealogical research; however, it has been demonstrated that the Death Master File contents combined with other public data is sufficient to derive the Social Security number of anyone born in the U.S. before 2012. The Death Master File has become another resource leveraged by those with criminal intent to use our universal identification number to steal in our names.

The process of derivation or reverse engineering the assignment of a Social Security number begins with a name - anyone's name. Searching on an individual's name in any Internet search engine yields that person's address and age, if not date of birth. This basic information augmented when necessary with data freely available from data aggregator websites is sufficient in combination with the information in the Death Master File to determine the Area and Group number of an individual's Social Security number. The
Serial number range for an individual's Social Security number can be reduced by comparison of the individual's date of birth with that of the deceased in the Death Master File born on or near the same date in the same area. With more than 2 million deaths per year recorded in the Death Master File the probability of finding information with close geographic and temporal proximity to a "target" individual is high. Experiments we conducted resulted in the reduction of the Serial number range to as few as 5 in the best case and within several hundred in the worst case.

The candidate Social Security numbers derived from the Death Master File can be verified using any one of a number of, mostly free, websites. Having deduced the Area and Group numbers with a corresponding list of possible Serial numbers all candidate Area, Group, and Serial numbers are "verified" to determine the Social Security number assigned to the individual. An individual's name and one of the candidate Social Security numbers is presented for verification resulting in either the confirmation or rejection of the Social Security number. The process is repeated with all candidate Social Security numbers until confirmation is received. Automating the process can yield thousands of names, addresses, dates of birth, and Social Security numbers in minutes.
The results of our experiments are consistent with the published results of research by Acquisti and Gross. (Acquisti & Gross, 2009) In the aforementioned research Acquisti and Gross relied solely on statistical analysis of the information in the Death Master File while, in contrast, we augmented our experiments by using additional publically available data. The additional data correlation resulted in our ability to derive Social Security numbers with nearly perfect results as compared to 30% claimed by Acquisti and Gross.

The Social Security Administration is not blind to this issue. In fact, were it not for a 1980 legal settlement the Death Master File would, most likely, never have been published. In the past 5 years significant evidence has been presented demonstrating the enabling nature of the data in the Death Master File resulting in the revision of the published data. As of late 2011 new releases of the Death Master File no longer contain last residence location or Social Security numbers of the deceased; additionally, legislation is pending to limit access to the data file to further thwart its illegitimate use. Unfortunately, the Death Master File releases prior to the 2011 revision remain available from third party vendors as well as from several private websites.
Chapter Four

Derivation of Social Security numbers may not be the primary method used by thieves to access our universal identification numbers. Instead, our personal information including Social Security numbers are commonly released by government agencies and commercial enterprises through negligence. Significant data breaches resulting in the release of personal identifiable information are regularly reported in the news media: *Laptop with NASA worker’s personal data is stolen, State now says 3.8 million tax records were hacked* and ‘Wall of Shame’ exposes 21M medical records. (McLeod, 2012) (Klotz, 2012) (Mearian, 2012) The headlining incidents are merely exemplars of a much broader issue which is now being brought to light as a result of data breach reporting requirements (for a comprehensive list of data breaches the reader is referred to: [The Privacy Rights Clearinghouse](https://www.privacyrights.org)). In addition to the headline-making incidents there are dozens more that do not garner such attention. Howard Schmidt, a recognized security expert, estimates there have been 564 million records released in data breaches in the U.S. (Weisbaum, 2012)

Regardless of the cause, a data breach is defined as “the intentional or unintentional release of secure
information to an untrusted environment.” (Wikipedia, 2012) The most damaging data breach involves the release of personal identifying information which is data that identifies a particular individual such as Social Security number that identifies by itself or bits of information such as maiden name, employment address, date-of-birth, place-of-birth, address, phone number, and other personal information that when aggregated together provide an individual’s identity. (Sprague & Ciocchetti, 2009) The preventable causes of data breaches include insecure systems, lost or stolen computers, and lost or stolen backup media and other storage devices; in short, negligence.

The pervasive occurrences of unauthorized releases of personal identifying information from government agencies and commercial enterprises exposed more than 232 million individuals' to identity theft in a single year - 2011. (Symantec, 2012) Software, information technology, and healthcare companies are regular offenders accounting for 93 percent of the total number of stolen identities in 2011. (Symantec, 2012) According to a recent study most data breaches are easily avoidable; the targets were most often not "pre-identified for attack; 79 percent of victims were targets of opportunity, and 96 percent of attacks were not highly difficult." (Verizon Business, 2012) The apparent
negligence in the storage of our personal identifying information exposing us to theft could be easily avoided if these companies took the simplest approach to thwart potential breaches. Increasing the opportunity cost by introducing technical barriers would significantly reduce the incidents of data breach.

The easiest and least costly approach for protecting the personal identifying information of individuals is to encrypt the data when it is stored. The arguments against encryption are feeble given the technology available in current data storage systems. In one popular data storage system, SQL Server, the process of encryption may be accomplished in as little as three steps. (Johnson, 2013) Unfortunately, only 30 percent of systems storing personal identifying information use encryption. It is widely argued that enforcement of any requirement to protect personal identifying information must be accompanied by fines and more stringent civil penalties. Recently, the California Attorney General, Kamala Harris, has become an advocate of data encryption “threatening greater scrutiny of companies that suffer data breaches but don’t use encryption, Harris recommended that the California Legislature should consider enacting a law requiring organizations to use encryption to protect personal information.” (Samson, 2013)

*Social Insecurity: The End of Privacy*

Identity Theft Awareness and Prevention Organization (IDTAP.ORG)
Data breaches involving personal identifying information are the single most prevalent cause of fraud. Data breaches are commonly caused by weak password protection and lack of data encryption resulting in the mass release of personal information, including Social Security numbers. "These breaches are driving fraud." (Carrns, 2013) In one such data breach by the Department of Homeland Security that went undetected from 2009 to 2013 the Social Security numbers, dates of birth, names, and other personal information of every employee of the department were released. (Miller, 2013) According to a recent study those whose personal information has been released as a result of a data breach have a one in four chance of becoming a victim of fraud. (Carrns, 2013)

The South Carolina Department of Revenue only recently discovered the importance of encryption. According to a spokesperson, “The state agency is now working to encrypt taxpayers’ Social Security numbers” (McLeod, 2012). Too late for the 3.8 million South Carolina taxpayers (81% of the 4.7 million total residents) who have had their Social Security Numbers and other personal identifying information released. According to a government report South Carolina is not alone in its negligence, government agencies were responsible for over 15,000 data breaches in 2012.

*Social Insecurity: The End of Privacy*
Identity Theft Awareness and Prevention Organization (IDTAP.ORG)
(Office, 2012) However, as those involved in the data security community from government officials, data scientists, and hackers know all too well releases of the kind suffered in South Carolina represent one of many opportunities to steal our most private information. For thieves; in fact, the personal identifying information of any individual may be purchased from nefarious Eastern European and Chinese websites, derived from publically available information, or purchased from data aggregators.
Chapter Five

Data aggregators "collect, manage, buy, and sell personal information they collect from public records, credit applications, and other sources of information." (Committee, 2005) There are a number of data aggregators including ChoicePoint, LexisNexis, Axciom, and Experian that possess information on every individual in the U.S. The unregulated data aggregation industry has been the source of significant data breaches providing access to personal identifying information to anyone willing to pay for the privilege.

These data aggregators collect and sell personal information such as Social Security numbers, dates of birth, addresses, property records, criminal records, and DNA information. The industry circumvents the reporting and compliance requirements of credit reporting agencies by limiting the use of its data; i.e. the data should not be used for evaluation of credit worthiness. Needless to say, the data is used, legitimately, by prospective employers, landlords, marketers, and various government agencies, in fact, when the government needed information following the September 11, 2001 attacks that information was provided for 11 of the hijackers by a data aggregator. The information collected and sold by the data

*Social Insecurity: The End of Privacy*

Identity Theft Awareness and Prevention Organization (IDTAP.ORG)
aggregators "peers deeper into American life than the F.B.I. or the I.R.S., or those prying digital eyes at Facebook and Google." (Singer, 2012)

There are no boundaries to the data collection. Although cell phone data has long been used to track individuals' locations, new uses allow data aggregators to identify individuals; where they go, who they meet, etc. (Gallagher, 2013) From cell phones, Internet usage, email, shopping habits, and other sources comes a new data aggregation company. The company, Vigilant Video, is constructing a repository "containing hundreds of millions of data points showing the travel patterns of millions of people in this country." (Lennard, 2013) The company plans to combine the travel data with data from other aggregators including facial recognition technology to create a collection of data that will enable tracking and identification of anyone in the U.S.

A primary source for the personal identifying information collected by aggregators comes from public records, credit files, our responses to surveys, and tracked online behavior; therefore, there is no opt-out from these massive collections of our personal information. The surrender of our privacy to the data aggregators for legitimate use may be acceptable because of the perceived benefit of directed marketing;

*Social Insecurity: The End of Privacy*

Identity Theft Awareness and Prevention Organization (IDTAP.ORG)
however, the unregulated and insecure nature of the industry has enabled large-scale theft of personal identifying information. Each of the data aggregators has a history of data breaches and; unfortunately, the breaches routinely involve hundreds of thousands of records. (American Civil Liberties Union, 2005) The ease with which the detailed personal data can be accessed is disturbing.

Thieves often mask themselves as legitimate businesses to gain access to the personal identifying information available from data aggregators. Establishing a company in most states requires no legal expertise, in fact, in Delaware and Nevada a company can be created in minutes anonymously for less than $200. For an additional fee the legitimacy of the company may be enhanced by its registration with the Internal Revenue Service resulting in the issuance of an Employer Identification Number (EIN). Armed with a "legitimate" company thieves purchase personal identifying information for a specific demographic group marketed by the data aggregators; i.e. physicians, homeowners, high net worth, etc. With the purchase the thieves gain possession of data that will allow them to drain bank accounts, open credit lines, apply for mortgages, and perpetuate fraud using the targeted individuals' personal identifying information.

*Social Insecurity: The End of Privacy*

Identity Theft Awareness and Prevention Organization (IDTAP.ORG)
Unfortunately, a victim of identity theft has no recourse against the data aggregators because the source of information enabling identity theft cannot be definitively trace back to the data provided by the data aggregators. However, there is growing concern that the data aggregation industry is a root cause of the identity theft crisis which has garnered the attention of the legislature. As with most technological issues involving commercial industries, especially those whose lobbyists are active campaign donors, legislative inertia has shielded the data aggregation industry from new regulations. In the current environment "data brokers have almost no accountability for how they collect the information and to whom they sell it because there are currently no Federal standards regulating the commercial data broker industry." (Committee, 2005)
Chapter Six

There is a one-in-three chance that one of us has been a victim of identity theft or that we know someone who has been. (Harper, 2010) Opportunistic identity theft results in fraudulent financial transactions with, in most cases, little impact on the individual. A victim need only execute an affidavit of fraud with the appropriate financial and credit reporting companies, or government agencies in order to "clear" their records (an identity theft resource kit is available at IDTAP.org). In general, the recovery from low-level identity theft involving fraudulent account activity is quick and relatively painless; however, there are exceptions as demonstrated in published research that suggests the time and effort to "recover" from identity theft may require as long as six months.

Opportunistic, low-level identity theft is "manageable" in the sense that there is typically clear evidence of fraud with many private and government resources available to assist the victim. The average financial loss associated with opportunistic, low-level identity theft is $3,000; certainly not significant to the victim who has no financial responsibility for the fraud. (Finklea, 2012) However, the enormity of the identity theft crisis is costing companies billions of dollars in losses which has
lead to the implementation of proactive fraud detection tools. In most identity theft cases the financial fraud occurs over a very brief period of time - a flash of fraudulent financial activity which many companies can now detect with the use of behavioral analysis allowing the company to terminate the fraud before significant financial losses are incurred.

A greater concern is identity theft that is not motivated by the opportunity for fast cash but instead for other nefarious purposes. Large-scale criminal enterprises are using fraudulent identities to commit financial fraud not for thousands of dollars but for millions; one such criminal enterprise used fraudulent identities in a scheme that resulted in $200 million in losses. (Cooney, 2013) Additionally, the national security implications associated with the wide-spread availability of fraudulent identification documents undermines our physical security. (Committee, 2005) While the often disregarded issue of high school and college students using fraudulent identities to circumvent age restrictions in pursuit of a "good time" places us all at risk during our daily travels. Obtaining fraudulent identification documents is enabled by many factors including the availability of production equipment but is facilitated by the availability of personal identifying information for authenticity.

*Social Insecurity: The End of Privacy*

Identity Theft Awareness and Prevention Organization (IDTAP.ORG)
Access to false identification documents has never been easier whether purchased from a foreign website or from forgers on the streets of any city. In a 2012 New York Post investigative report a reporter was able to purchase "frighteningly real" fraudulent identification documents on a street in Queens for $260. (Giove, 2012) According to law enforcement investigators as many as ten fraudulent identification production facilities are operating on Roosevelt Avenue between 103rd and 76th streets. (Giove, 2012) This issue is not isolated to the U.S., fraudulent identification documents are easily obtained on the streets of Thailand, New Delhi, Beijing, and elsewhere across Asia. (Divya Shah, 2008) (Ehrlich, 2009) The producers of the fraudulent documents are equipped with the same technology used by legitimate issuers of government identification cards allowing them to produce nearly-perfect fraudulent documents including drivers' licenses, green cards, birth certificates, and even passports.

A simple Internet search will yield a listing of dozens of websites offering fraudulent identification documents. Again, most of the websites operate outside the U.S. legal system in Asia or Eastern Europe offering nearly perfect fraudulent identification documents conveniently delivered to you. Enabling this vast, profitable enterprise is the ability to obtain legitimate

*Social Insecurity: The End of Privacy*

Identity Theft Awareness and Prevention Organization (IDTAP.ORG)
names, dates of birth, and Social Security numbers for use on the documents. A purchaser either provides the name, date of birth, and Social Security number or the falsified information is included in the "package". The legitimate names, dates of birth, and Social Security numbers used to produce the fraudulent identification documents are culled from records of personal identity information released via data breaches, derived from personal identifying information garnered from the Internet, purchased from data aggregators, or acquired from insiders.

Definitive identification of individuals is in the collective interest of society to ensure the enforcement of law, assignment of benefits, and protection of life and property. Government agencies recognized the weakness of the U.S. individual identification system over forty years ago yet have not acted to correct the deficiencies in the system. Repeated attempts to augment the Social Security number with a more secure system have failed as have attempts to discontinue the use of birth certificates as identification documents. A variety of government and private agencies have demonstrated that with over 10,000 agencies in the U.S. issuing birth certificates fraud detection is nearly impossible. (Brown, 2000) Additionally, thirteen states do not restrict access to birth certificates allowing
anyone to purchase a copy of any birth certificate on file in that state. Purchasing or, with rudimentary skills, creating a fraudulent birth certificate allows its use as a source document for the issuance of other legitimate identification documents. The combination of the weak Social Security numbering scheme and the ease with which a birth certificate can be obtained are driving enablers of identity theft.

False identification is a significantly more disturbing aspect of identity theft than thieves stealing a few thousand dollars. Possessing identification documents with someone else's personal identification information allows for the assumption of the identity of that person. There are many cases of "total identity theft" with perhaps the most well documented being that of Michelle Brown whose story was adapted as a movie. Ms. Brown testifying before the U.S. Senate recounted being arrested for drug trafficking, spending days incarcerated, and subsequently spending months "clearing her name" after someone assumed her identity. (Judiciary, 2000) In the current geopolitical environment our society faces danger from within its borders as well as from external elements either of which can easily circumvent deterrent efforts by law enforcement by using false identification. For example, on an average day Customs and Border Patrol agents...
intercept 75,000 false identification documents presented by individuals seeking entry into the U.S. Yet, for over forty years the government has failed to act to strengthen the identification system with the Federal Advisory Committee on False Identification concluding in 1976, "that any attempt to improve on or replace the highly unreliable SSN scheme would not be worth the money."
Bibliography


*Social Insecurity: The End of Privacy*

Identity Theft Awareness and Prevention Organization (IDTAP.ORG)
Social Insecurity: The End of Privacy

Identity Theft Awareness and Prevention Organization (IDTAP.ORG)


*Social Insecurity: The End of Privacy*

Identity Theft Awareness and Prevention Organization (IDTAP.ORG)

McLeod, H. (2012, November 8). State now says 3.8 million tax records were hacked. Retrieved November 8, 2012, from NBC News - Technology: state-now-says-3-8-million-tax-records-were-hacked-1C6891691


Social Insecurity: The End of Privacy
Identity Theft Awareness and Prevention Organization (IDTAP.ORG)


*Social Insecurity: The End of Privacy*

Identity Theft Awareness and Prevention Organization (IDTAP.ORG)

