Social Security Numbers, Public Records, and Identity Theft

Just Say "NO" to Redaction

Dan Combs

Coalition for Sensible Public Records Access

CSPRA

Additional copies of *Social Security Numbers, Public Records, and Identity Theft – Just Say "NO" to Redaction* are available without charge from the

Coalition for Sensible Public Records (CSPRA)

www.cspra.org

or

CSPRA
620 42nd Street
Des Moines, Iowa 50312

About the Author

Dan Combs is a Senior Associate at Imadgen, LLC. Mr. Combs is a recognized expert on identity topics including identity policy, federation, and management. He has participated in multiple efforts to develop identity infrastructure and create identity management systems, identity federations, and credentialing systems. He has helped draft policy, rules, and standards; designed and managed identity, verification, and risk-decision systems; and has published numerous documents on identity topics. Previously, Mr. Combs served as the Director of Digital Government for the State of Iowa. There he was a key contributor to the creation and management of the Iowa Identity Security Program. Mr. Combs was also a consultant for the U.S. General Services Administration's E-Authentication Initiative.

Related Memberships and Activities:

- Harvard Policy Group for the "Leadership for a Networked World Executive Education Program"
  - Member of HPG working on IT related issues.
- EC3
  - At-large Board Member; Organizer, chair and participant in more than 15 workgroups and symposia. Papers can be found at eC3 Publications - General Information
- MIT Real ID Forum & MIT Real ID NPRM Forum
  - Helped to create and operate the MIT Real ID Forum serving as program director. Operates the two blogs for these topics.
- www.realidandrealids.org
  - Creator of web resource for identity information and co-founder of MIT/EC3 collaboration.
- Center for Democracy and Technology
  - Member Identity workgroup (formerly Authentication Privacy Principles workgroup)
- ANSI-BBB Identity Theft Prevention and Identity Management Standards Panel
  - Facilitated first meeting of panel and current participant
  - IDSP Report Summary
- Markle Foundation: Connecting for Health Workgroup on Consumer Authentication
  - Subject matter expert and participant
  - Consumer Authentication for Networked Personal Health Information
- Center for Ethical Identity Assurance
  - Founding Member
- Center for Strategic and International Studies Workgroup on Authentication and Identity on the Internet, Issues Paper, July 2002
  - Participated to help identify issues and create foundation for identity federation that became the E-Authentication Partnership
- E-Authentication Partnership
  - Original member; participated in development of policy documents; board liaison from EC3.
- Health IT Standards Panel, HITSP
  - Security and Privacy
  - Identity Credentials Management Working Group
- Homeland Security Standards Panel-HSSP
- Liberty Alliance
  - Member, Identity Assurance Expert Group

Social Security Numbers, Public Records, and Identity Theft

Just Say "NO" to Redaction

Dan Combs

Coalition for Sensible Public Records Access

CSPRA

Executive Summary—Identity Information Cannot Be both Public and Secret

There is a very important principle to understand that applies directly to the discussion of the use of Social Security Numbers (SSNs) and whether this information should be removed from public documents. This principle is neither controversial nor complicated and should be very easily grasped by almost anyone.

The principle is: Identity information cannot be both public and secret.

Names, by themselves, are not unique and are not a reliable identifier. Without pairing a name with secondary information such as a SSN many false positive and false negative conclusions and outcomes result. In the United States, much of this secondary information, used for the legitimate purposes of identification, comes from public records. The use of SSNs helps to properly identify people. To meet this need, the SSN has been treated as public information and used extensively to link people to their information to conduct legitimate societal functions. Without a clear and complete public record that includes identity information, there cannot be fairness for the blameless or consequences for the culpable.

There is a pervasive need throughout society to uniquely identify individuals to facilitate the conduct of business, government, and even social interactions. Without this ability, a government agency cannot ensure it is providing benefits to the proper citizens or that criminals are properly prosecuted. Similarly, financial institutions and employers may wrongly offer or deny credit or employment because of inaccurate credit and background histories.

Poorly conceived and implemented identity practices have resulted in readily available personal information such as SSNs being inappropriately used as authenticators or "keys" to accounts and other valuable resources. These improper practices have made SSNs valuable to criminals. Current defense mechanisms, when deployed and properly used, competently defend against intrusions based on simple knowledge of SSNs and other personal information.

Information such as the SSN that has been public is all but impossible to make secret. Therefore, redacting SSNs and other personal information from public documents will provide virtually no benefit in reducing identity crimes and may hinder or damage current legitimate and successful efforts to do so. Society wide redaction of SSNs and other personal identifiers from public records will be very expensive and disruptive of beneficial processes but will not result in personal information being unavailable.

Resources can be more successfully employed to advance the implementation and use of better identity tools and practices and to educate individuals on how to protect themselves against identity crimes. Redaction cannot, and will not, stop identity theft. When redaction is proposed as the solution to the problem of identity theft, there is only one answer that makes sense: "Just say no."

Introduction

Identity theft has become a cause célèbre in the United States. During the current decade identity theft has been claimed to be the fastest growing category of crime. An online search produces over 20 million links related to the topic. Virtually every talk show, news show, newspaper and investigative journalist has addressed the issue, most of them doing so on multiple occasions. A survey sponsored by the Federal Trade Commission, conducted by Synovate in March and April of 2003, estimated that almost 10,000,000 people in the United States discovered they were victims of identity crimes in the preceding year at a cost to the victims and businesses affected of about $50 billion per year.

Reacting to constituents' fears many jurisdictions have enacted or are considering laws or rules intended to prevent identity related crimes or mitigate their effects. One currently popular reaction to citizens' fear of identity theft is requiring the removal of Social Security Numbers (SSNs) from public records and systems. However, this approach will produce virtually no positive result for reducing identity theft or limiting the availability of SSNs or other personal information. Indeed, removing SSNs from public documents and record systems will disrupt current means of battling identity criminals and prosecuting these crimes. Making decisions to require the removal of SSNs from public documents and systems will be costly and disruptive. It is critical to begin with some understanding of the function of SSNs in legitimate processes and in identity related crimes. It is essential to conduct a rational assessment of the effect and effectiveness of removing SSNs from public documents and systems.

This paper will provide an overview of several background topics important to understanding the role of the SSN, the effect of redaction, and the likelihood of reducing identity crimes through the mechanism of removing SSNs from public records. There is one very important principle to understand that applies directly to the discussion of the use of SSNs and whether this information should be removed from public documents. This principle is neither controversial nor complicated and should be very easily grasped by almost anyone. The principle is: Identity information cannot be both public and secret.

The topics of this paper are as follows:

- Identity Theft—information on who conducts these crimes and how
- Systems of Trust and Identity Functions—the role of identity functions in providing a foundation for interactions and transactions with an important principle for SSN use
- Social Security Number—the history of the SSN system and its role in society

This paper will conclude with evidence that redacting personal information from public records will fail to achieve the goal of reducing identity crimes. Further, it has been the poorly conceived and implemented identity practices that have resulted in the inappropriate use of readily available personal information as authenticators or "keys" to accounts and other valuable resources, and that it is these improper practices that have made SSNs valuable to criminals. Resources that might be dedicated to removing personal information from public records will be more effectively used to implement improved identity management technology and practices and to educate the public on self-protection measures against these crimes.

Identity Theft: Who, What, Why, and How

Who

Once upon a time, many hackers (used here to mean the people breaking into electronic systems) sought notoriety and renown from "hacking" or breaking into systems, often changing and defacing web pages or using other methods as proof of their exploits. They were largely young male computer "nerds," perhaps very bright and capable with electronic technology, but socially inept or outcast. Many of today's hackers, on the other hand, are identity criminals that come from around the world and many backgrounds. This criminal industry pairs together bored suburban teenagers with those supporting drug habits; traditional gangs with new specialized organizations; terrorists with various government organizations; and tight traditional gangs with loose associations of "providers." While nominally conducting the same activity as before, namely hacking, today's identity criminals use tremendously advanced techniques. However, due to developments in the methods used in these crimes some types of participation require little or no expertise with technology.

What

Identity theft has become the catch-all term for a number of crimes that rely upon compromising information personal to individuals. Only some of the most egregious of these can be considered outright theft of a person's identity. The victim's identity in these cases is assumed and in effect taken away from the victim by a criminal. In the worst cases, the victim can suffer long-term or even permanent consequences and have inadequate recourse to resolve the effects of the crime.

Importantly, the majority of the crimes in the identity theft category are actually credit card theft and fraud. These are more appropriately referred to as identity fraud or identity related crimes rather than actual theft of identity. Identity related crimes include a component in which personal information is used or compromised, but stop far short of stealing a victim's identity. These crimes are almost entirely crimes of opportunity. Seldom are individual victims targeted in order to inflict damage on a particular person. The perpetrator is often known to the victim, such as a relative, household member, or a co-worker. The criminal achieves access to a billfold or electronic information that is used to steal money from accounts, to fraudulently use a credit card, or to establish new accounts in the victim's name.

These types of crimes have existed in human societies since the beginning of trade and commerce and have been conducted on a "retail" basis, mostly one person victimizing one person or possibly a series of individuals. Even during the early decades of growth of computer use, a criminal determined to commit this type of crime would have to gain physical entry into a facility to access information contained in a system. Development of the Internet has opened virtual access to many physically inaccessible facilities. Implementation and use of the Internet does not cause these crimes. However, use of the Internet, while providing tremendous benefit to civil society, has enabled the transformation of identity crimes from "retail" to "wholesale."

The widespread implementation of the Internet has led to tremendous advances in our ability to conduct business, access information and services, and to become involved with people in ways never possible in the physical world. One of the major contributing characteristics to the growth in the use of the Internet and many of the related components is openness and relative ease of adoption. The Internet was designed and has been continually improved to facilitate the free flow of information and to make use easy and relatively inexpensive.

Just as the construction of the Interstate Highway System created the means for more rapid access to physical locations for beneficial and criminal uses (e.g. drug trafficking), construction of the Internet provided the means for instant virtual access for beneficial and criminal uses. Criminals have used this avenue to virtually enter our homes, businesses, and government offices, tricking us into divulging personal information. These attacks are often automated using vast networks of computers to perform the dirty work. While public information has become electronically available, use of publicly available information requires substantial additional work for criminals to capture and collate the information in order to collect a valuable return. It has become considerably more efficient and cost effective to use systems that take the information directly from individuals and data bases already sorted and collated, rather than to use public information sources requiring more work and producing smaller returns. Even though innovations such as the Internet and the Interstate Highway System facilitate new kinds of crimes, few would seriously advocate doing away with these innovations or the benefits, access, and related opportunities provided by them. Our country, communities, and citizens are working to get the balance right, create the right protections, and overcome the unintended consequences of these valuable innovations.

Why

The motivation for identity related crimes is primarily financial profit. It is a relatively low risk, high return criminal activity. Terrorists or governments also use these exploits to further their tactical or strategic interests, but by and large, those perpetrating these crimes are driven to derive financial gain.

These crimes tend to be very difficult to prosecute. The perpetrators can be anywhere, change tactics often, and disguise their activities. Tracking down these criminals or even deciphering an exploit can take months of dedicated work by teams of highly skilled law enforcement personnel. Many times the person who steals the victim's information is neither the person who runs the computers used in the crime nor the person who steals money from accounts or sets up fraudulent accounts in the victim's name. Many of the components required to carry out these crimes are offered as services or at commodity price levels requiring relatively little expertise for use. This makes the bar to entry into these crimes very low. High rates of return, low barriers to entry, and little fear of prosecution have drawn many new people to perpetrate these crimes.

How

Understanding the universe of identity crimes requires some grasp of how the various components or activities work together, resulting in stolen or compromised personal information and leading to theft, fraud, and other crimes based upon identity information. The

"The free market and the future of online crime
The shadow economy has all the attributes of a traditional economy – division of labor, price competition, marketing and so on – accelerated to Internet speed and carried out online. Adam Smith, the pioneering political economist, in his Wealth of Nations, foresaw that the division of labor could increase productivity and quality. Similarly, competition drives down prices and tends to drive innovation. While it is interesting to observe these classical economic principles at work, they hold a terrible warning: malware is going to get more common and more virulent.

There is a sophisticated online black market with tens of thousands of participants. Malware authors can produce new, unique malware every 45 seconds in order to keep it undetected."

The Online Shadow Economy-A Billion Dollar Market for Malware Authors by Maksym Schipka, Senior Architect of Development, MessageLabs

Figure 1

initial theft of information is rarely committed for the primary or sole purpose of compromising an identity. Taking that information by itself seldom provides value to the thief. In some aspects, this category of crime parallels that of art or jewelry theft. While some criminals may steal art or jewels because they desire those items, most do so as a step toward selling or monetizing those valuables. Similarly, with theft and misuse of identity information, almost all of these crimes are committed as a step toward some other crime. The identity information by itself has little or no value to a criminal. The information is only valuable when it can be monetized. While there are numerous ways in which monetization may occur, generally the information is used to access existing accounts or to establish new accounts to take assets through theft or fraud. This is possible because of weak or shoddy practices of identity verification used in establishing and controlling access to accounts and other assets, not because of the availability of stolen or compromised personal information. With improved systems of trust and identity verification, the easy link between personal information and fraud and theft would be broken, and these crimes would become substantially harder to commit. There will be more coverage of this in the section on identity practices.

One of the most dramatic developments facilitating the growth of identity crimes is the generation of an "identity black market." Creation of this market provides a means to rapidly monetize the results of an information theft (while at the same time driving down the value of the information), provides opportunities for specialization of labor in criminal activities, and brings to bear market forces on participants. As a result, this criminal market has spawned online "malls" facilitating the sale of products, services, and education; fostered development of business services such as maintenance and support agreements and escrow agents; and commoditized the raw materials of these crimes. The identity black market forces, such as commoditization of personal information, are driving down the value of the information and forcing participants to become ever more efficient in their criminal processes. These black market forces combined with improved trust and identity functions in legitimate markets will make publicly available personal information of low and diminishing value for identity criminals.

Systems of Trust and Identity Functions: An Effective Remedy

Trust

When one stops at the checkout counter at a local convenience store to purchase a loaf of bread with cash, there is no need to prove to the clerk one's identity. The person at the counter may mark the money with a particular marker or look for security features of the money with little care or interest as to the identity of the payer. The basis for "trust" in these transactions lies in the currency and the body of law, processes, and technology that combine to create a system through which a merchant and a customer can conduct trade. Parallel relationships and requirements exist between citizens and government, patients and doctors, clients and lawyers, and in many other situations. In general, for people to conduct meaningful interactions there is a requirement for a system of trust on which to base interactions. Without this foundation of trust some or all of society will collapse.

There are numerous times in our daily lives when we are asked or required to provide some "proof" of who we are. This could occur when cashing a check or using a credit card, when withdrawing money from an account, changing a delivery address, or many other common activities. This checking of identity is disruptive to conducting the related transaction, takes time, costs money, and may annoy the participants. So, why is it done?

Until recently, most of our commercial or societal interactions took place face to face. Our commercial transactions were based largely upon cash. Over a number of decades and increasingly rapidly in the recent past, these characteristics have changed. In a face-to-face, cash-based world, participants in interactions may often be unaware of the underlying trust mechanism or system and its implications. There are numerous cultural assumptions built into "doing business face to face" or looking someone "square in the eye" based upon unspoken and hidden presumptions about one's ability to ascertain the trustworthiness of another or to protect oneself from untrustworthy behavior. The face-to-face, cash-based environment provides substantial protections and stronger trust mechanisms for participants, whether or not they are known to the participants. The barriers imposed by physical distance to many would-be criminals in this environment are substantial. The trust in this environment is based upon a variety of factors, including, but not limited to, physical proximity, familiarity, and availability and support of local law enforcement. This face-to-face environment shields inhabitants from a lot of dangers we have come to learn are possible.

We have created marvelous means to conduct virtually instantaneous interactions across the globe. It has become miraculously easy to purchase a product or to share thoughts with someone on the far side of the world. As users or consumers we want these interactions to be as simple, easy, and quick as the face-to-face, cash-based transactions. Implementation of the means to interact with anyone anywhere has bypassed various safeguards and undermined some of the systems and mechanisms upon which we often unknowingly relied. Unfortunately, the trust system that underlay that former environment is broken or circumvented by the ability to easily interact directly across the globe.

During the past decade there has been a tremendous amount of work and thought focused on replacing the mechanisms or system of trust. A lot of that work has addressed identity practices or processes that provide a foundation for trust. In very much the same way that identity information is of little direct interest to criminals, such information is seldom of direct interest to legitimate society. In this context of interactions or transactions, the knowledge of a person's (or organization's) identity is only interesting or valuable as it supports some other function. When, for instance, a bartender "checks an ID," it is not to verify the identity of a person ordering an alcoholic drink but to assure that the person is beyond a certain age. The ID, often a driver's license or other government credential, is issued according to certain processes. Those processes may include presentation of a birth certificate. These credentials often contain biometrics, such as photographs, that help to bind the credential to a particular person. The combination of these underlying issuance processes and the credential, the driver's license, allow people, such as the bartender, to trust the claimed age of the customer. The identity of the credential holder in this and many other instances is irrelevant to the transaction. The identity information is used to support another function (most often trust) among the participants. Parallel examples proliferate throughout the private and public sectors. Generally, for the purposes of interactions and transactions, it is important to know that the participants are old enough, deserve a privilege or benefit, own or control an account, are eligible or ineligible, and can be found later if necessary to enforce legal requirements. Very few common interactions and transactions require knowledge of the identity of the participants if other means are available to meet the necessary requirements of trust.

It is possible to imagine a future system that would provide these functions without exposing identity information to the participants. However, societies around the world and throughout history have employed a similar two-step or multi-step process. This process initially determines the identity of participants in interactions or transactions and then uses that information as a basis for obtaining

other pertinent information, determining the truth of that information, making decisions based upon that information, and trusting the results of the interaction or transaction.

The work to create identity-related standards, policies, processes, and technology has been undertaken for the purpose of replacing this trust and the underlying foundation for trust we had in the face-to-face, cash-based environment[1]. It is certain that the foundation upon which we formerly relied is no longer sufficient and that new foundations must be laid to support participants' trust in conducting interactions and transactions in this new, rapidly evolving electronic environment. Much progress has been made to understand the issues, conceptualize responses, and craft solutions to replace this foundation of trust and, much more is needed. This replacement effort is where policy makers should focus their efforts, resources, and support.

The Important Lesson: Identity Information Cannot Be both Public and Secret

There are many good resources to aid in understanding the standards, functions, and systems of identifying people, places, and things. This paper is not intended to provide more than a very general treatment of these topics. However, there is a very important principle to understand that applies directly to the discussion of the use of SSNs and whether this information should be removed from public documents. This principle is neither controversial nor complicated and should be very easily grasped by almost anyone.

The principle is: Identity information cannot be both public and secret.

Names, by themselves, are not unique and are not a reliable identifier. Without pairing a name with secondary information, such as a SSN, many false positive and false negative conclusions and outcomes result. In the United States, much of this secondary information, used for the legitimate purposes of identification, comes from public records. The use of SSNs helps to properly identify people. To meet this need, the SSN has been treated as public information and used extensively to link people to their information to conduct legitimate societal functions. Without a clear and complete public record that includes identity information, there cannot be fairness for the blameless or consequences for the culpable.

id Analytics
National Data Breach Analysis

STATISTICAL HIGHLIGHTS

ID Analytics studied the level of suspicious misuse of identity information across the approximately 500,000 identities in the breach files. Statistical highlights from the findings include:

- Sixty-eight percent of the publicly reported breaches during the study period were intentional breaches. Additionally, the vast majority of the identity-level breaches (38 out of 54) were intentional breaches.
- The calculated fraudulent misuse rate for consumer victims of the analyzed identity-level breach with the highest rate of misuse was 0.098 percent – less than one in 1,000 identities.

Figure 2

Social Security Number: the Address to Your House, Not the Key to Your Front Door

Conducting the operations of government and private organizations requires the collection, collation, and coordination of information about people, places, and things. The "market," both government and private sectors, recognizes implicitly and explicitly the need for a way to uniquely

identify entities, businesses, organizations, people, places, and things. The evidence for this lies in the adoption of various ways of uniquely identifying objects, locations, organizations, and individuals. Take, for example, the system for unique addresses used by the United States Postal Service. Address information is provided by jurisdictions across the country. That information is collected, standardized, and added to a database of addresses. Many public and private sector operations rely upon and use this system of unique location addresses. Correct delivery of a package, for instance, requires a unique physical address. Without a unique addressing system, it would be impossible for the USPS or others to determine where to deliver packages. Further evidence can be found in the success and explosion in use of Global Positioning Systems (GPS), Geographic Information Systems (GIS), and in-car navigation. The explosion in use is based on a need for improved address functions and the connecting of unique latitude and longitude coordinates with other data about physical places. Additionally, people are often connected with physical addresses in order to associate and conduct physical location functions with individuals such as E911 and property ownership. If the current address system ceased to exist, then the needs of those that depend on that system would force the replacement of the vanished system by another. The replacement system might look very different, but there is no doubt that one is required and would be re-created if the current system was eliminated.

Similarly, there is often a need to associate information with a person. This requirement is a parallel function to physical addresses--an "information address." This address allows for correct "delivery" of information and association to the proper person. The SSN resulted in large proportion from the need for this information address function. Today, as was the case seventy years ago, there is a requirement to associate information such as Social Security tax, payment, and benefit information with individual workers. The Social Security Administration (SSA) created the SSN to meet this need. The SSA highlights legislative and other changes to the policies and procedures affecting SSNs in its Social Security Number Chronology. A large proportion of the entries in the seventy year span of the chronology relates to the expansion of required or allowed use of the SSN to meet this requirement. A number of the entries display requirements for disclosure of the SSN for various types of "information address" functions. A few of the entries relate to improving security of the system and its components in support of that role. A small fraction of the entries, mostly those from the last decade, relate to privacy of the SSN, but none mention secrecy of the number. Paralleling the government expansion of SSN use has been a growth of SSN use, often government required or sanctioned, as an identifier in the private sector.

The effect of this market requirement for an information address and the seventy year trend of expanding SSN use is that SSN information has become readily available and relatively public. SSNs have been adopted to fill the need for an information address and, as a result, are captured and stored in hundreds of thousands of physical and electronic repositories. The SSN has come to serve a very valuable role as an information address through which both public and private entities coordinate numerous societal functions including identity verification. Among the many benefits it serves, the SSN facilitates better legitimate identity functions.

Referring back to the principle that identity information cannot be both public and secret, the SSN cannot effectively serve both an address function (public) and a "key to the door" function (secret). Few people would accept the notion that knowledge of the address of their home should confer a right to someone to enter or move in. The same concept should apply to the use of the SSN. Knowledge of the SSN or information address for a person should not confer upon anyone any rights to access accounts or perform any other functions. It cannot be both public and secret and it is

inappropriate to use knowledge of SSNs for both address and access control functions. The SSN has a long and successful history serving as a public information address. Repurposing the SSN to serve a "key" function would require a comprehensive reengineering of the SSN system and society wide changes in its use. It will also require the replacement of the SSN with another unique identifier to meet the lost functional requirements currently provided by the SSN.

Social Security Numbers and Identity Theft

It is important to understand the role SSNs play in identity crimes and how it came to be. SSNs have no inherent value for criminals. Knowledge of an SSN offers little opportunity for direct monetization. Defrauding the Social Security Administration through SSN-related exploits is a relatively low return crime requiring a disproportionately large amount of work over a long period of time.

SSNs, for a range of reasons, have been imbued with value for identity criminals. SSNs came to be inappropriately used for "key" functions. It became common practice in the context of numerous types of interactions or transactions to ask a customer or applicant for his or her SSN. It was presumed that knowledge of the SSN provided proof that the person was who he or she claimed to be. Organizations, over time, made many decisions to use the SSN to help in identity verification, thus escalating the level of trust based on knowledge of the SSN. SSNs have come to be used to control access to accounts, as passwords, and as verifications of identity. These uses all require secret information. All of these uses are inappropriate for public or easily available information such as the SSN. These inappropriate uses of SSNs increased their value to identity criminals.

Even in this case, monetization of SSN information by criminals is a multi-step undertaking. For example, the SSN information must first be stolen or compromised, it must be connected to an account, and access must be gained. SSN information in these circumstances is still not inherently valuable but is one factor facilitating criminal gains. As identity practices improve through replacement of knowledge of SSN with other means of identity verification or authentication, the value of SSNs diminishes. The instant an organization changes its practice of inappropriate use of the SSN, the SSN becomes worthless to criminals in the environment of that organization. When all organizations discontinue these improper practices, SSNs lose all value for identity criminals.

Even before much of the work to improve identity practices had been implemented, the conversion rate of information theft, including SSN, was low and declining. Figure 3 contains excerpts from a 2005 idAnalytics study that show that the highest rate of conversion is less than one-tenth of one percent. Additionally, changes to improved identity management systems and practices, including better identity verification, authentication, policies, practices, and technology are underway. The evidence shows these efforts are reducing identity crimes and forcing changes in the nature of identity crimes.

While identity crimes are still a tremendous issue, the work that has been undertaken to fight these crimes is well underway and is becoming effective. There is still much to be done, but the strategy and tactics being implemented are successfully reducing identity crimes.

Statement of Chris Swecker
Assistant Director, Criminal Investigative Division
Federal Bureau of Investigation
Before the
Senate Judiciary Committee
April 13, 2005

To assist in the development of the types of cases that necessitate federal treatment, the FBI is developing financial crimes intelligence related to identity theft. The FBI utilizes analysts to review information contained in suspicious activity reports, the Federal Trade Commission's Identity Theft Clearinghouse, fraud reporting to the Internet Crime Complaint Center and other sources of data to identify and target criminal organizations engaged in identity theft.

Choicepoint, like LexisNexis and the other available data resources, has become an invaluable research tool for the FBI's analytical cadre in a number of ways. Choicepoint consolidates a large number of public information sources in a single, online location for quick retrieval. Much of the information provided by Choicepoint could only be obtained historically by making direct and sometimes in-person contact with the originating Agency. Information from Choicepoint is used to provide useful leads for analysts and investigators to follow through on and can be integral in helping to draw connections between previously segregated pieces of data. The Choicepoint information is used regularly by investigators in contributing to probable cause for search warrants, court orders and other legal documents that are executed every day by FBI Agents.

An example of how Choicepoint can and has been used in analytical research can be seen in several of its search parameters. When the FBI has initiated an investigation, Choicepoint, through name and address information, can provide social security information on search projects. Once a social security number is available, analysts can enter this information into a new search parameter. These searches will produce all names that have ever been associated with the number. Many times, the production of these aliases can be used to run additional searches, providing even more potential leads for investigators to pursue. The automation of this multiple-source data, as with similar analytical engines, has dramatically reduced the amount of time and effort needed to include or exclude information.

Congressional Testimony on Federal Bureau of Investigation efforts to combat Identity Theft.

Figure 3

Redacting Social Security Numbers

A well-known issue or phenomenon for military strategists is that of "fighting the last war." There is a tendency in preparing for future military operations to focus on the previous war fought. This phenomenon leads to improperly focused efforts based on outdated expectations of attack and response methods rather than likely future adaptations. Succumbing to this phenomenon will leave a military force woefully unprepared to face new adversaries employing new and different tactics and technology.

The current efforts to remove SSNs from public records falls victim to the phenomenon of "fighting the last war." The current perpetrators of identity crimes rapidly evolve their tactics and technologies in order to adapt to attempts to thwart the criminal exploits. Due to this increasingly rapid evolution of methods and technology the removal of SSNs from public records as a response to identity crimes suffers not just from "fighting the last war," but from fighting a war from several generations past.

The expenditure of significant taxpayer resources in pursuit of ineffective and disruptive responses to real needs should be in and of itself of great concern to government decision makers. Of potentially more importance would be if these expenditures worsened the very problem they are intended to address. Figure 4 contains an excerpt from the testimony presented to Congress on the FBI's use of publicly record information, including SSN information, to fight identity theft. This is one of many examples of how public record information is used to improve identity functions and to fight identity crimes. Removing SSNs from public records will halt these beneficial uses of the information and damage current methods implemented to fight identity crimes.

Conclusion

Redacting Social Security Numbers and other personal information from public documents will provide virtually no benefit in reducing identity crimes and may hinder or damage current legitimate and successful efforts to do so. Society wide redaction of SSNs and other personal information from public records will be very expensive and disruptive of beneficial processes but will not result in personal information being unavailable. Such an effort will require years of work and billions of taxpayer dollars and be inconsequential in reducing identity crimes.

Identity crimes are a major concern to U.S. citizens and have been the most prevalent type of complaint to the Federal Trade Commission for many years. Poorly conceived and implemented identity practices have resulted in readily available personal information such as SSNs being inappropriately used as authenticators or "keys" to accounts and other valuable resources. These improper practices have made SSNs valuable to criminals. When improper SSN use is discontinued, SSNs become worthless to identity criminals. The "weapons" of the identity criminal have evolved many generations beyond the "last-war" tool of the SSN. Current defense mechanisms, when deployed and properly used, competently defend against intrusions based on simple knowledge of SSNs and other personal information.

Resources can be more successfully employed to advance the implementation and use of better identity tools and practices and to educate individuals on how to protect themselves against identity crimes. Redaction cannot and will not stop identity theft. When redaction is proposed as the solution to the problem of identity theft, there is only one answer that makes sense: "Just say no.

---

[1] ***Many organizations in recent years have undertaken efforts and collaborated to create a body best practices and standards for the policies, processes and technology of identification and credentialing systems.***

The U.S. Federal Government has provided significant leadership in improving identity policy, practices and technology. The information contained in the National Institute of Standards (NIST) documents such as Special Publication 800-63, "Electronic Authentication Guideline" and related documents has become nationally and internationally influential on these topics. The following programs and projects have produced tremendous advances in identity verification and authentication: the General Services Administration's E-Authentication Identity Federation and E-Authentication Partnership (now part of the Liberty Alliance), the Federal Government's Personal Identity Verification (PIV) system, created in response to Homeland Security Presidential Directive-12 (HSPD-12), the Federation for Identity Cross-Credentialing System (FIXs), the U.S. Department of Defense Common Access Card (CAC) and Defense Cross Credentialing Identification System (DCCIS)

Following are several notable collaborations of government and private sector organizations in whole or in part working to improve identity functions through development of standards and best practices.

- Liberty Alliance
- The Health Information Technology Standards Panel (HITSP)
- Homeland Security Standards Panel (HSSP)
- Identity Theft Prevention and Identity Management Standards Panel (IDSP)

The Coalition for Sensible Public Records Access (CSPRA) is a not-for-profit organization dedicated to preserving responsible access to public record information. CSPRA sponsors research and publications, legislative briefings, and other activities designed to foster a more thoughtful debate about how such access should be balanced with privacy concerns. Additional information about CSPRA is available at www.cspra.org