Understanding Amy Boyer's Law:

Social Security Numbers, Crime Control, and Privacy

A Special Report Issued by Privacilla.org
http://www.privacilla.org

December, 2000

Introduction

On October 15, 1999, 20-year-old Amy Lynn Boyer was gunned down in Nashua, New Hampshire by a deranged criminal. Liam Youens had become obsessed with Amy in school. He had watched her for years, and planned her murder. He revealed his twisted vision on an Internet Web site. And in the last days before he killed Amy Boyer, he had gotten information about her, including her Social Security Number, from an online investigation service.

Amy Boyer's death devastated her family. Their search for an answer prompted the introduction in Congress of a bill called "Amy Boyer's Law." That bill would prevent the use, display, and sale of Social Security Numbers. It awaits congressional action at any time.

Social Security Numbers have a strong connection to crimes like identity fraud, and some connection to certain invasions of privacy. Although Amy Boyer's Law and so many other proposals are nominally aimed at privacy, evidence of a large and growing crime problem is much stronger. Identity fraud — a crime — is increasing. Yet, federal law enforcers are unfocused on apprehending perpetrators.

Like some crime-control laws, and most privacy statutes, Amy Boyer's Law affects First Amendment free speech interests. This is a product of the fact that Social Security Numbers identify people; they are speech. The better way to address crimes like identity fraud, and threats to privacy, is to directly pursue the people who use Social Security Numbers to cause any kind of harm to American citizens.

Crime and privacy have become confused in public debate. This has distracted policy-makers from addressing real problems directly.

Crime and privacy have become confused in public debate. This has distracted policy-makers from addressing real problems directly, and it has caused Americans to distrust the delights promised by the Information Age. It is unfortunate that legislation introduced as a tribute to Amy Boyer should be bogged down in such a poorly articulated public debate. The result may be that neither crime nor privacy are properly addressed. Until the issues are sorted out, Americans will needlessly be victimized by crime and disproportionately anguished about their privacy.

A Depraved Criminal Act

If there ever was a homicidal maniac, it was Liam Youens.

Liam encountered Amy Lynn Boyer for the first time in the eighth grade. They had a class together in the tenth grade, but barely ever spoke. Yet somehow she became a target of the homicidal obsession that grew within him. In his warped mind, Liam concocted a relationship with Amy. He watched her from a distance at Nashua High School in Nashua, New Hampshire. He agonized over small events that he observed in her life. He manufactured stories about her actions and thoughts that appealed to his venal, self-absorbed existence.

After they both graduated, Liam stalked Amy. According to his own account of events, he took pictures of every house on her street, which he knew by where she had gotten off the bus. He eventually identified her house by spotting her car in the driveway. He wrote, "When I saw that car and looked at that house and realized Amy was asleep in there, Endorphines flew, it was like crack cocaine, I have never felt that kind of rush in my life, before or since."

Liam drove to her street at night and parked there, waiting for her to come or go. In his deluded and criminal mind, the placement of cars responded to his thoughts and plans to kill, as if he were playing a game of chess with her family and the local police.

"When I saw that car and looked at that house and realized Amy was asleep in there, Endorphines flew, it was like crack cocaine, I have never felt that kind of rush in my life, before or since."

Liam collected guns. He owned five rifles, two with scopes, and one handgun. He devised several different schemes for murder. He had a "Plan Owen," for a young man he imagined to be a rival. He had a "Plan: Mass Murder; Subplan: NHS," which he modeled on the massacre at Columbine High School in Colorado.

Liam Youens catalogued his thoughts, plans, and deeds on an Internet Web site, revealing to posterity how sick, demented, and bent-on-destruction he was. In the days leading up to the killing, Liam wrote daily about his movements, observations, criminal plans, and attempts to collect information. And on October 15, 1999, he unleashed his twisted vision on Amy Boyer's innocent young life, shooting her to death in the parking lot of the dentist's office where she worked. He then turned the gun on himself.

The sheer randomness of her killing — and the absence of a perpetrator created by Liam Youens' suicide — left Amy Boyer's family in a vacuum of pain, thirsting for justice. They began seeking an answer, some explanation, and some way to heal their broken hearts.

"How could somebody who was unstable and so clearly reaching out for help get a legal permit for this arsenal of guns?" Amy's stepfather asked a reporter for the Boston Globe. He suggested that Internet Web hosting companies should be required to report users who threaten criminal acts. He considered suing the companies that had hosted Liam Youens' Web sites.

Little more than a year later, the family's search for closure continues. On a Web site of their own (http://www.amyboyer.org), Amy Boyer's family has posted their thoughts, and they maintain an active discussion list. They have posted a copy of one of Liam Youens' Web sites — a site where he revealed his depraved plans for murder, and where he issued a silent, ignored cry for help. His dastardly crime caused a tragedy that strikes any heart with grief. Amy Lynn Boyer was innocent, full of life and hope, and loved by her family.

Heinous Crime Prompts . . . Privacy Law?

Seven months to the day after Amy Boyer's heinous murder by Liam Youens, U.S. Senator Judd Gregg (R-NH) introduced a bill inspired by the death of his young constituent. He called it "Amy Boyer's Law." A version of that bill, attached to the FY 2001 Commerce-Justice-State appropriations bill, awaits action by the Congress at any time.

Though the murder of Amy Boyer inspired Amy Boyer's Law, the law does not address murder, stalking, or gun control. Instead, the heart of the bill's original version is a section titled "Protecting Privacy by Prohibiting Display of the Social Security Number to the General Public for Commercial Purposes Without Consent."

In the last days before he murdered Amy Boyer, Liam Youens paid an online investigation service to find out her birth date, Social Security Number, address, and workplace, where he ultimately gunned her down. It would have been easy enough for him to murder Amy anywhere else or just follow her to work, but there is a slim chance that Liam would have abandoned his years-long murderous obsession if he had not been able to get Amy's information. This slender reed ties Amy Boyer's murder to the debate on Social Security Numbers and privacy.

Like violations of privacy, crimes affect people very personally. Whether they are crimes of violence, theft, or fraud, the victims suffer deeply from the pain, disruption, and sense of violation. For this

> It is understandable that some crimes may be discussed as offenses to "privacy," even if that is not the best term. This inaccuracy should be forgiven — until it misdirects policy-makers and advocates.

reason, it is understandable that some crimes may be discussed as offenses to "privacy," even if that is not the best term. This inaccuracy should be forgiven — until it misdirects policy-makers and advocates. Amy Boyer's Law appears to have done this.

Many people and institutions have adopted the idea that Amy Boyer's Law is a privacy bill. The Electronic Privacy Information Center maintains the legislation on its list of privacy, speech, and civil liberties legislation.[1] The Congressional Research Service listed it in a report called "Internet Privacy — Protecting Personal Information: Overview and Pending Legislation"[2]

Amy Boyer's Law has been amended as it has moved (too quickly) through the legislative process. Amendments to the bill would allow harmless uses of Social Security Numbers — economically beneficial ones, in fact — to continue. These changes, however, have caused the coterie of "privacy advocates" in Washington to jump into opposition. The Washington Post reported on this in an article headlined (uncritically of the "privacy" moniker) "Net Privacy Bill Called 'Trojan Horse.'"[3] The ACLU has issued an "Action Alert" on Amy Boyer's Law noting that every "privacy organization" has taken a position opposing the legislation.[4]

This has created a truly unusual circumstance: the world's finest civil liberties organization and its allies oppose a crime bill *because it does not go far enough*. Obviously, the issues need sorting out.

About Social Security Numbers

The Social Security Number is a nine-digit number assigned by the Social Security Administration to nearly every person in the United States. The first three numbers are an "area number." Issued before 1972, the area number indicates which local Social Security office issued the number; after 1972, it indicates where the social security card was mailed. The second two numbers are a "group number." Group numbers are issued within each area in a prescribed, non-consecutive order: odd numbers from 01 to 09, even numbers from 10 to 98, even numbers from 02 to 08, and odd numbers from 11 to 99. The last four numbers are a "serial number." These are issued consecutively within areas and groups, from 0001 to 9999.

The Social Security Number is, very simply, a form of identification. It attaches to a person the way a combination of words like "John Smith" does. Just like people use

[1] http://www.epic.org/privacy/bill_track.html
[2] http://www.cnie.org/nle/st-43.html
[3] *Net Privacy Bill Called 'Trojan Horse'*, by Robert O'Harrow, Washington Post (October 25, 2000) http://www.washingtonpost.com/wp-dyn/articles/A7249-2000Oct24.html
[4] http://www.aclu.org/action/infoprivacy106.html

combinations of given and family names to identify themselves in the social world, they use numbers — and most commonly Social Security Numbers — to identify themselves in the governmental and economic worlds.

The advantage that Social Security Numbers have over names is that one Social Security Number will never be issued to the same person. In the absence of fraud or error, Social Security Numbers accurately identify individuals, preventing mistaken identity and allowing people to enjoy the benefits of a "good name" without having to develop a personal reputation of honesty and trustworthiness each time they do business with someone new. Social Security Numbers have come to be used for a wide variety of purposes because of this extraordinary benefit. They should be replaced — and most likely will be, in time — by identifiers that are just as unique, that have more advantages, and that are not issued by the government.

For good or bad, forms of identification like names and Social Security Numbers are tools for social and business interaction. They link people to information about themselves. Individuals, businesses, and governments use these tools in a variety of combinations to create relatively easy access to an astounding array of products, services, and benefits. Social Security Numbers can give people access to medical information they need for treatment while traveling, and they can give government investigators and criminals access to information that can be used to cause harm. Amy Boyer's Law, and many other recent proposals, would limit the uses that could be made of these tools.

What Amy Boyer's Law Would Do

Amy Boyer's Law would amend the Social Security Act to prohibit the display or sale to the general public of any individual's Social Security Number without the consent of the individual. To display or sell a Social Security Number, one would have to inform the individual of what the number will be used for and to whom it may be made available, then get "affirmatively expressed" consent. The law would also prohibit obtaining an individual's Social Security Number with the intent to injure, harm, or use the identity of the individual for illegal purposes.

Amy Boyer's Law has many exceptions. It allows the display, sale, or use of Social Security Numbers:

- if it is permitted, required, or excepted by various federal laws;
- by a professional or commercial user who "appropriately" uses Social Security Numbers and who does not display or sell Social Security Numbers to the public;
- for purposes of law enforcement, including investigation of fraud; or
- if the Social Security Number may appear in a public record.

A violator of Amy Boyer's Law could be sued civilly by the individual whose Social Security Number was improperly used. The damage awards possible are the higher of a) actual damages; b) $2,500; or, c) $10,000, if the violation resulted in monetary gain. In addition the Commissioner of Social Security could issue fines for violations of Amy Boyer's Law of up to $5,000 per violation — up to $50,000 if the violation was a general business practice. On top of that, violating Amy Boyer's Law would be a federal felony, punishable by fines and up to five years in prison.

As a crime-control measure, Amy Boyer's Law addresses a real and growing problem, though perhaps not in the best way. Amy Boyer's Law also addresses privacy, but — surprisingly — the evidence of a problem in that area is not as clear. Like many crime-control measures, and almost all privacy laws, Amy Boyer's Law would affect First Amendment free speech interests.

Social Security Numbers and Crime

It is unfortunate, though unsurprising, that information-related crimes should grow in the Information Age. Social Security Numbers and other forms of personal information are increasingly becoming instruments of crime. The premier example of this is identity fraud.

Identity fraud — often confusingly referred to as identity "theft" — takes a number of different forms. Most commonly, criminals use information about people, including their Social Security Numbers, to fraudulently apply for credit cards. They charge goods and services on those fraudulently gotten cards, making off with the goods or services charged to the card. Credit card companies shoulder most of the financial loss. Individual consumers suffer emotional loss, and the loss of money and time as they struggle to salvage their credit histories.

The U.S. House of Representatives Committee on Banking and Financial Services has done extensive study on the issue of identity fraud. According to a September 18, 2000 letter written by Chairman James A. Leach (R-IA) to Attorney General Janet Reno, 500,000 people are victimized by identity fraud each year. Fraudulent charges in the average identity fraud case are $18,000, and $3 out of every $4 lost by community banks to credit fraud is due to some form of identity fraud. Chairman Leach summarized the problem by noting that identity fraud is robbing the banking system on a far grander scale than John Dillinger and Jesse James could ever have envisioned.

Far less common — and much more tenuously linked to Social Security Numbers — is the crime that Liam Youens committed against Amy Boyer. He did obtain information about Amy Lynn Boyer in the days leading up to her death, but he obsessed over her and stalked her for years. It is hard to say that learning her Social Security Number or using it to find her workplace allowed Liam Youens to kill Amy Boyer. Criminologists would probably find a remote link between the availability of Social Security Numbers and premeditated murder.

In identity fraud, however, it is clear that information like the Social Security Number is an "instrument of crime." But instruments of crime must be distinguished from contraband. The former have legal and beneficial uses. The latter do not.

In identity fraud, it is clear that information like the Social Security Number is an "instrument of crime." But instruments of crime must be distinguished from contraband.

The impulse to restrict information like Social Security Numbers is a natural response to information-based crimes, but it may not be ideal because of the attendant costs. The Federal Trade Commission reported to Congress about information brokerage in 1997:

> Convenient access to so much information about individuals through individual reference services confers myriad benefits on users of these services and on society. The look-up services enable law enforcement agencies to carry out their missions, public interest groups to find missing children, banks and corporations to prevent fraud, journalists to report the news, lawyers to locate witnesses, and consumers to find lost relatives.

A more appropriate response to information-based crime is to go directly after criminals. This is not being done. As Chairman Leach wrote to the Attorney General: "Despite [the] profusion of Federal and State statutory authority and the exponential increase in reported cases of identity [fraud], there is little evidence that law enforcement agencies have made combating this crime a priority. . . . [T]he lack of meaningful enforcement efforts currently being directed at identity [fraud] has helped foster a climate of lawlessness . . . ."

Social Security Numbers and Privacy

Amy Boyer's Law is widely believed by many to be privacy protection legislation and, to some extent, it is. The link between Social Security Numbers and violations of privacy is similar to the link between Social Security Numbers and crime. Surprisingly, however, there appears to be scant evidence that Social Security Numbers are being used

to violate privacy. To assess the relationship between Social Security Numbers and privacy, though, we must first address what we mean by "privacy," a poorly understood concept compared to crime.

There are two separate and very different privacy regimes in American law, though the distinction is poorly recognized. One is privacy from government. The founders of our country established constitutional privacy rights to protect citizens from government out of just suspicion for the powers that governments alone exercise. Amy Boyer's Law allows almost any display, sale, or use of Social Security Numbers by governments, so we need not compare it to privacy as a concept relative to governments.

The other privacy regime deals with non-governmental actors. When dealing with individuals and businesses, Americans protect their privacy using a combination of self-help, contracts, and torts. The most direct privacy protection law in the United States is the set of common law torts inspired by an article called *The Right to Privacy* in the 1890 Harvard Law Review. Written by Samuel D. Warren and Louis D. Brandeis, the article discussed the specter of newspapers, photography, and other technologies that could expose people's images and personal information to the public. Their key concern was with publicity given to sensitive personal information — undesirable and embarrassing scrutiny of private life by the press and public.

In 1960, eminent legal scholar William L. Prosser documented how privacy as a legal concept had come to constitute four distinct torts. That is, a person whose privacy has been invaded could sue the privacy invader for damages. These torts still exist today, and are contoured as four separate branches:

1. Intrusion upon seclusion or solitude, or into private affairs;
2. Public disclosure of embarrassing private facts;
3. Publicity which places a person in a false light in the public eye; and
4. Appropriation of name or likeness.

Illustrating the centrality of the privacy torts to privacy protection in the United States, the U.S. Department of Commerce wrote in a July, 2000 memorandum to the European Commission: "The right to recover damages for invasion of personal privacy is well established under U.S. common law." Given this brief outline of the United States' comprehensive privacy law, we can assess the effect of Social Security Numbers.

"The right to recover damages for invasion of personal privacy is well established under U.S. common law."

Social Security Numbers have almost no relation to the third and fourth branches of the privacy torts. The Social Security Number neither helps nor hinders someone who would make false statements about another, or appropriate another's image.

For the first and second branches, however, Social Security Numbers stand in about the same position as they do to crime. Someone seeking to invade the privacy of another may use Social Security Numbers to intrude into their private affairs or to collect embarrassing private information and disclose it. Social Security Numbers are very clearly a tool that can be used to invade privacy.

Surprisingly, however — and contrary to received knowledge — evidence of a privacy problem growing out of Social Security Numbers is scarce. Statistics about information *crimes* like identity fraud are available, and the amount of information is growing, but very little information about invasions of privacy as defined by our nation's comprehensive law can be found.

Contrary to received knowledge, evidence of a privacy problem growing out of Social Security Numbers is scarce.

Polls suggest widespread concern, and congressional committees — knowing the power of imagery — are assuredly scouring the country for victims, but the victims of privacy violations are not coming forward. The uses of Social Security Numbers in privacy invasions have not been documented. Information about the number of cases filed in the states' common law courts has not been collected, and the failure of those courts to redress harm to their citizens has not been suggested, discussed, or explained.

Social Security Numbers and Speech

Congress can, of course, enact laws to regulate Social Security Numbers without having to answer for its factual judgments. This is not the case if it enacts laws that violate the First Amendment. The conflict between Amy Boyer's Law and First Amendment speech interests illustrates that going after criminals and privacy violators directly may work better than limiting uses of Social Security Numbers.

Amy Boyer's Law anticipated First Amendment problems. It contains congressional "findings" that include the following:

> A Social Security Number is simply a sequence of numbers. In no meaningful sense can the number itself impart knowledge or ideas. Persons do not sell or transfer such numbers in order to convey any particularized message, nor to express to the purchaser any ideas, knowledge, or thoughts.

Even if it were true, this statement would not help a court resolve a First Amendment challenge. Though it may give some deference to legislative findings that certain activities are harmful, a court could not defer to legislative findings as to what constitutes speech without abandoning the First Amendment.

A court analyzing the constitutionality of Amy Boyer's Law would easily conclude that Social Security Numbers are speech. Each Social Security Number identifies an individual. The Social Security Number is a type of name — just as "table" means table, and "John Smith" refers to John Smith.

The question is whether Amy Boyer's Law is a content-based regulation of speech — constitutional only if it is the least restrictive means of serving a compelling state interest[5] — or a content-neutral time, place, and manner restriction — permissible so long as it is narrowly tailored to serve a rational state interest.[6] One might argue that the law is content-based because it bans a particular type of content, like a ban on poetry or weather reports would. Arguably, the law is similar to restrictions on "fighting words," addressed to what old-fashioned jurists would call a "breach of the peace" — the risk of crime. Alternately, one might argue that the law is content-neutral, because it does not discriminate against any particular viewpoint.

Under the lower standard for content-neutral restrictions, a law must be narrowly tailored to further a significant governmental interest and leave open ample alternative channels for communication. Amy Boyer's Law is not narrowly tailored. It not only bars the sale of Social Security Numbers by criminals in furtherance of fraud or murder, but covers sale and display of Social Security Numbers for any purpose, including legitimate or harmless ones.

One especially relevant example illustrates this point. On the Web site maintained by Amy Boyer's family, there is an active discussion list. The following post appears on the list:

> Hi, my name is Andrew Nelson. I live at 120 Greenway Terrance [sic] in Jupiter, FL. My phone number is (312) 437-8754. My SS# is 143-98-2721
>
> I also think Internet privacy is an important issue, but this information is already out there anyways, so what does it matter? The government keeps huge databases

---

[5] Content-based restrictions of speech are permitted only if narrowly tailored to serve a compelling state interest, and do not "'unnecessarily interfere with First Amendment freedoms.'" *See, e.g.*, Schaumburg v. Citizens for a Better Environment, 444 U.S. 620, 637 (1980).

[6] Time, place, and manner regulations must be narrowly tailored to further a significant government interest and leave open adequate alternative channels of communication. *See, e.g.*, Clark v. Community For Creative Non-Violence, 468 U.S. 288 (1984).

> on all of us, most of the information needed to stalk someone is a matter of public record. What good will legislation do? None. . . .[7]

The writer is stating his opinion — and illustrating in a forceful way — that exposure of contact and identification information does not harm people. This is speech, protected by the First Amendment, but if Amy Boyer's Law were enacted, her family would be breaking the law by leaving this post on their Web site.

> Amy Boyer's family is probably in violation of the law proposed in their lost daughter's honor.

Unless they have informed Andrew Nelson of the general purposes for which his Social Security Number will be used and to whom it will be made available, then obtained his "affirmatively expressed" consent, Amy Boyer's family is probably in violation of the law proposed in their lost daughter's honor. It is very unlikely that they have, and it would be prohibitively impractical for the thousands of very active bulletin boards worldwide to police the law. If Amy Boyer's Law were already enacted, postings on their own Web bulletin board would expose Amy Boyer's family to federal civil lawsuits, administrative penalties, criminal fines, and imprisonment.

One might argue around the First Amendment and defend Amy Boyer's Law by saying that the federal government can specially control Social Security Numbers because it created the numbers in the first place. This argument seems appealing at first, but makes little sense in light of the vast arrays of information that governments create, such as addresses, names of towns and cities, names of buildings, and so on. Allowing governments to control information that they create would have bizarre and unwanted consequences. Other than in compelling circumstances like threats to national security, governments may not control widely disseminated information consistent with the First Amendment.

Conclusion

At times, "privacy" seems to be a label put on just about every threat caused by the modern world, and there are many legitimate concerns. Information practices that have been evolving for years are being newly analyzed in the great civic discussion that is underway. Solutions to legitimate Information-Age concerns will be found more readily if we categorize the problems correctly, distinguishing between crime-control and privacy protection.

[7] http://www.amyboyer.org/_reqdis/00000031.htm

Crimes like identity fraud appear to be growing as a result of the increasing availability of information like Social Security Numbers on electronic media. Identification of this crime problem as a "privacy" problem has limited the ability of policy-makers to attack it directly. While the nation's law enforcers sit on the sidelines, the crime of identity fraud has become far too common. Americans are worried, and they feel threatened by what they hear. By controlling crimes like identity fraud, our national leaders could go a long way to assure Americans that the future holds far more promise than danger.

Because of First Amendment problems, and because of its indirect approach to solving the identity fraud problem, Amy Boyer's Law would likely be ineffectual. Its failure, in fact, could fuel calls for even more laws that attack an ambiguous "privacy" problem even more fiercely, without ever actually identifying the culprits or the harms they are causing. Attacking identity fraud as a threat to "privacy" is misleading.

In summary, political leaders should:

- recognize that identity fraud is a serious and growing crime problem;
- ensure that proper law enforcement resources are dedicated to combating identity fraud;
- resist the impulse to confuse the public by attaching the word "privacy" to problems not recognized as such in American law.

Unfortunately, and unintentionally, Amy Boyer's Law has done a disservice to our nation's struggle to come to terms with these issues. Though it grew out of a tragic and horrible crime, the law has metamorphosed, and it has confused public debate. As either a crime-control measure or a privacy measure, it would be ineffective, and it is thwarting progress on these serious issues. This leaves it a poor tribute to the lost life of Amy Lynn Boyer.

APPENDIX
Amy Boyer's Law
Section-by-Section Summary

Sec. (a). Short Title
Names the Act "Amy Boyer's Law."

Sec. (b). Findings

Sec. (c). Amendments to Social Security Act

Subsec. (1). Amends the Social Security Act (42 U.S.C. 1301 et seq.) to add a new section 1150A.

New Subsec. 1150A(a) Limitation on Display or Sale
Subject to exceptions, prohibits display to the public of any Social Security Number or derivative thereof without consent.

New Subsec. 1150A(b) Prohibition of Wrongful Use as Personal Identification Number
Prohibits obtaining any Social Security Number or derivative thereof with intent to harm or use the identity of the person for illegal purposes.

New Subsec. 1150A(c) Prerequisites for Consent
Requires person seeking consent under subsection (a) to —

- inform the individual of the general purposes for which number will be used and to whom it will be made available; and
- obtain "affirmatively expressed" consent.

New Subsec. 1150A(d) Exceptions
Allows display, sale, or use of Social Security Numbers —

- permitted, required, or excepted by various federal laws;
- by a professional or commercial user who "appropriately" uses Social Security Numbers and who does not display or sell Social Security Numbers to the public;
- for purposes of law enforcement, including investigation of fraud; or
- that may appear in a public record.

New Subsec. 1150A(e) Civil Action Created
Allows victim of a violation of this section to bring a civil action to recover —

- equitable relief; and

- the greater of actual damages, $2,500, or, in the case of a willful violation, $10,000 and attorney's fees and costs;

subject to a 3-year statute of limitations.

New Subsec. 1150A(f) Enforcement by Commissioner of Social Security Administration
Allows Commissioner of Social Security to determine violations and levy civil money penalties of up to $5,000 per violation, or up to $50,000 if violation constituted a general business practice.

New Subsec. 1150A(g) Definition of "Display or Sell to the General Public"
Defines "display or sell to the general public" to mean "the intentional placing of an individual's Social Security Number, or identifying portion thereof, in a viewable manner on a web site that makes such information available to the general public, or otherwise intentionally communicating an individual's Social Security Number, or an identifying portion thereof, to the general public."

New Subsec. 1150A(h) Exceptions
Limits construction of section so that governmental purposes are preserved, including national security, law enforcement, public health, federal or federally-funded research; and entitlement programs.

Subsec. (2) Creation of Felony Offenses
Makes it a felony, punishable by fines and imprisonment of up to five years, to sell or display to the general public any Social Security Number or derivative thereof or to obtain any Social Security Number or derivative thereof with intent to harm or use the identity of the person for illegal purposes.

Subsec. (3) Date of Applicability
Makes subsection (a) applicable two years after date of enactment.

Sec. (d). Study by Comptroller General
Requires General Accounting Office to study and report within one year on feasibility and advisability of imposing additional limitations or prohibitions on use of Social Security Numbers in public records.