

DAVID DENISON

717 17TH ST. APT. 9 • DES MOINES, IA 50314 • (319) 471-1176 • DAVID.DENISON@GMAIL.COM

WRITING SAMPLE

Privacy Protection on the Internet: a Proposal for a “Privacy Bill of Rights”

Privacy Protection on the Internet: a Proposal for a “Privacy Bill of Rights”

Steven Jobs, an average thirty-something businessman, was no stranger to the Internet. Over the years, he had used it for school projects, at work, and even from his cellphone. He had, however, never owned a computer at home, and decided it was time to purchase one. He spent hours unpacking it, sorting out the cables, getting everything connected, setting up his router that he picked up from his local Internet service provider (ISP), and finally, getting it online. Steven was not surprised by the complications of this process, he had known what to expect.

After logging onto the Internet for the first time from home with his new computer, Steven realized he forgot to buy a printer. He went to Google’s homepage, searched for printers, and found Amazon.com. He quickly decided on a cheap printer and set up an account with Amazon, giving them his name, address, email, phone, and credit card information. He then went to Gmail and emailed his friend telling him about this experience, and then turned off his computer for the night.

Even though Steven was done for the night, the story of his personal information had just begun. Google logged his search for printers and his computer’s IP address, and put it into a database that they use to track users. Google then sells this database to advertisers. Google also accidentally posted this database online a few weeks later. Amazon logged his name, address, email, and phone number and stored them in their unencrypted database, which a hacker breached that night and stole, and then sold to spammers within the United States for a sizeable profit. That same night one of Amazon’s employees took a laptop home that had the encrypted credit information of 100,000 customers who recently created accounts on Amazon. He lost this laptop, and because the password for the encrypted database was taped to the bottom of the computer, the entire list was distributed through underground chat rooms, and all 100,000

customers became the victims of identity theft. Meanwhile, the FBI had been investigating Steven's friend and had logged the email Steven sent in addition to installing a small file on Steven's computer called a tracker cookie, a file that can log each website visited and all information typed in and reports it back, when he installed the software bundle he obtained from his local ISP.

In the ensuing months, Steven's email inbox and his postal box were both stuffed full of unsolicited advertisements; advertisers wanting to sell him their products constantly called. In between the phone calls from advertisers, he received calls from debt collectors wanting to know how he was going to pay his maxed out credit cards. He explained to them about the identity theft, but they did not care, they only wanted their money. Steven also stumbled across all of his purchases on Amazon doing a random Google search right before his friend called him and told him that the FBI has been logging his email for the past several months.

Steven then reads in the newspaper how, in response to their use of personal information, Google and Amazon were both very sorry, but no one was fired, and no penalties were assigned. This was cold comfort for Steven who in less than a few hours online had his life ruined by the lack of protections for personal information and computer privacy in the United States.

Steven's story is fictional, but everything above could happen to anyone. In America, the possibilities for data exploitation are endless and there are no protections in place that adequately protect people from the above problems. A "Privacy Bill of Rights" is required to provide the protections that people need.

Congress' approach to the protection of personal information and computer privacy has been to wait until a company, newspaper, or person exploits a then unprotected specific privacy interest, and then, over the course of several years, hold hearings and ultimately pass a statute

that provides protections for only that limited area. For example, there is a right to financial privacy protected under the “Fair Credit Reporting Act,” the “Video Privacy Protection Act” regarding an individual’s video rentals, the “Driver’s Privacy Protection Act”, which protects drivers’ license and registration records from being shared with third parties, and the “Health Insurance Portability and Accountability Act” that protects medical records.¹

The problems with these statutes are that they took years to be enacted, do not always provide adequate protection, are often under-enforced or not enforced at all, and are more of a stopgap than a solution. What is needed is a comprehensive “Privacy Bill of Rights” creating rights protecting one’s private information. Information such as web pages visited, information entered, credit card information, contents of emails, and personal information such as a person’s address, phone number, and email address, in addition to other information that the average person would not want disclosed or sold to third parties, or permanently logged in a computer database.

This paper begins with a description of privacy protections that currently exist, and what problems they have. It then discusses non-legislative options for privacy protection, and their problems. It closes with proposals regarding a “Privacy Bill of Rights.”

I. Current Privacy Protections: What They Are and Why They Are Not Enough

A. Limited Protection of Privacy in the United States Constitution

Of all the provisions in the United States Constitution, none provides an explicit right to privacy. Over the years, the Court has inferred a right to privacy with regard to specific issues such as marriage, procreation, contraception, family relationships, child rearing and education.²

These rights, while important, do not provide general protection of one's privacy rights in cyberspace. Perhaps the only source for those rights is the Court's use of the Fourth Amendment in a variety of contexts.

The Fourth Amendment provides:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated...³

Like the rest of the Constitution, this amendment mentions no explicit right to privacy, but in the *Katz* case the court established a limited right to privacy.⁴ *Katz* was arrested under a federal statute criminalizing the transmission of wagering information by phone.⁵ *Katz* considered his privacy rights violated when the FBI sought to introduce into evidence the contents of *Katz*'s side of a phone conversation that they had obtained by attaching an electronic listening device to the outside of a public telephone.⁶ The Court stated that what one "knowingly exposes to the public...is not a subject of Fourth Amendment protection," but "what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."⁷ Because *Katz* closed the door to the phone booth to avoid being overheard, he had an expectation of privacy regarding the contents of his conversation.⁸ The Court stated that notwithstanding its language, the Fourth Amendment protects people, not places.⁹ In Justice Harlan's concurrence, he developed a two-part test for what constitutes a "search": something is a search if (1) the individual "has exhibited an actual...expectation of privacy," and (2) the expectation would be recognized as reasonable by the average person.¹⁰

Thirty-four years later in the *Kyllo* case, the Court updated its *Katz* opinion to take into account recent advances in technology.¹¹ The police suspected that *Kyllo* was engaged in the growing of marijuana.¹² Growing marijuana indoors requires the use of high-intensity lamps that

emit significant heat.¹³ The police made use of a thermal imager to take a thermal print of his home, which displays areas that might be emitting excessive heat.¹⁴ The police found that the roof over the garage was hotter than the rest of the house and got a warrant based upon this and some evidence of bills and informants.¹⁵ During his trial, Kyllo moved to suppress this information because it was obtained in violation of his Fourth Amendment right to privacy. In this case, the Court expands upon the developed idea that the home is supposed to be a sacred place and that any technological device that can register what is going on inside from the outside without entering the structure constitutes an impermissible search under the Fourth Amendment.¹⁶ The Court also says that there is no connection between the specificity at which a surveillance device can record activity within the home and permissibility of that device.¹⁷ If it invades an area where there would be an expectation of privacy, as established in *Katz*, the method of surveillance is not proper.¹⁸

When the Fourth Amendment was drafted the portion reading “persons, houses, papers, and effects” covered virtually all aspects of a person’s privacy. Any information a person wanted to keep private would be contained either on their person or in their house. Today, comparable protection would require that the Government obtain a warrant to log emails and search-engine use, install tracker cookies, or access an individual’s data held by data collection companies.

Justice Harlan’s second prong for a “reasonable expectation of privacy” should encompass a user’s expectation that what goes on while using their computer at home stays on their computer, subject to a few necessary exceptions. Similar to the protection of *Katz*’s conversation in the phone booth he thought was private, the government should not be allowed to

monitor email as it comes out of a home computer or install tracker cookies on a computer when the end-user has a reasonable expectation of privacy.

Kyllo should also protect end-users' privacy when using their home computer. One view of how the Internet works is that the end-user initiates a communication, at which point a server responds and sends a communication back to the end-user. In this way, the computer is similar to the phone in the *Katz* case. If monitoring is done on the end-user's side, the Fourth Amendment should protect the contents of those communications. In addition, any software or computer used to intercept or collect an individual's searches, emails, and the like should be considered a technological device. Therefore, whenever the government logs this information it constitutes an impermissible search under the Fourth Amendment. It does not matter whether these end-user tracking devices limit themselves to only monitoring terrorist websites, or whether they monitor everything, they are still an impermissible search.

These principles would only provide people with protection from warrantless *government* monitoring. They would do nothing to protect individuals from private companies gathering information and using or selling it. Another concern is the limited privacy statutes already in place. Passing a "Privacy Bill of Rights" would necessarily affect how existing statutes function and in some cases, such as financial data, both statutes would have to be read together in order to figure out what protections are in place.

B. Health Insurance Portability Act (HIPAA)

HIPAA is an example of a privacy act that takes both computers and the protection of personal information into account. HIPAA expressly covers information stored in any form or media, whether it be electronic, paper, or orally.¹⁹ Even though HIPAA was enacted in 1996,

many government officials and healthcare institutions are still trying to figure out exactly how its provisions will be enforced because HIPAA's Privacy Rule did not go into effect until April 14, 2003.²⁰ In general, it protects patients' privacy interests in their medical records and insurance information.²¹ In order to advance this goal HIPAA limits the collection, use, and disclosure of patients' medical information.²²

HIPAA applies to nearly all healthcare providers and most medical data relating to patients.²³ In certain situations, HIPAA protections are not absolute; a complete restraint on the use and transfer of patients' private information would work to the patient's detriment. When there is an appropriate justification for doing so, HIPAA permits disclosure to third parties.²⁴

In order to protect patients' data after a healthcare provider has sold or disposed of a computer, HIPAA requires that the computer's hard drive be scrubbed.²⁵ Many computer users are not aware that when they delete a file that it is still there. When a user deletes a file, only the reference to the location of the data is removed. A subsequent buyer of the computer could easily restore most of the data from deleted references. Scrubbing rewrites gibberish data to the hard drive three or more times, completely filling and emptying the drive. This removes, or makes useless, all the underlying data. Requiring the hard drive to be scrubbed is a new idea, but with the ease at which an intermediate computer user can now recover data and the turnover rate of computer hardware, it has become a necessity for data protection.

HIPAA provides both criminal and civil penalties for violations.²⁶ The Office for Civil Rights (OCR), a division of the Department of Health and Human Services (HHS), is responsible for investigation and enforcement of violations of HIPAA Privacy Rules.²⁷ The Department of Justice (DOJ) oversees the procedures involved when there are criminal violations of the Privacy Rules.²⁸

The civil penalty section sets forth a \$100 fine for each violation; with total fines capped at \$25,000 per incident.²⁹ There are three exceptions for when fines are not applied: (1) if the violation is punishable under the criminal provisions, (2) if the person did not know, and by exercising reasonable diligence would not have known, that such person violated the provision, and (3) failure to comply was due to reasonable cause and not to willful neglect; and the failure to comply is corrected.³⁰ The civil penalties are aimed at providing incentives for companies to comply with these policies, but are not focused on punishing willful breaches of the HIPAA provisions. These exceptions only punish companies when there is something more than negligence, and still provide a reasonable opportunity for the violator to cure. The exceptions are important because a company who breaches is more likely to fix errant procedures or violations when they can escape liability for the violations.

The criminal provisions are aimed at punishing actions where a provider or employee takes the information and willfully sells or discloses it. The language used in the statute is “wrongful and knowing disclosure of individually identifiable health information.”³¹ Punishment for this type of violation can result in fines up to \$50,000 and up to one year in prison.³² The criminal provisions have the potential to make privacy violations serious enough to provide disincentives to employees and providers to willfully or intentionally release information.

Even though HIPAA provides important protections, its current application renders it a paper tiger. The OCR and the DOJ do not actively go out and look for violations, relying solely on complaints submitted for review.³³ The problem inherent with the complaint system is that patients often do not know their healthcare provider has disclosed their information. In addition,

even if a patient discovers his medical information has been breached it will be nearly impossible for him to trace the breach back to a particular provider.

Another weakness is that there is little incentive for an employee who learns of an accidental breach to notify his employer about the violation. If an employee reports a violation, the only result will be that his employer will be fined. This has the potential to create a hostile work environment for the employee and is a disincentive to disclose violations.

Enforcement has also been lackluster. The HHS has received approximately 20,000 privacy complaints since the rule went into effect in 2003, but as of 2006, they had yet to bring their first civil enforcement action.³⁴ Of these 20,000 complaints, 68% were closed and 231 were referred to the DOJ for criminal investigation.³⁵ The HHS is not the only one who is shirking its responsibility on punishing violators of HIPAA; the DOJ has followed up upon only a small handful of the 231 referrals sent to them.³⁶

A major blindspot in HIPAA is that it only applies to “covered entities.”³⁷ This allows employees to sell patients’ medical information without personal liability. In one case, however, the Court held an employee personally liable for selling patient information to third parties.³⁸ The DOJ did not agree with these cases and issued an opinion on June 1, 2005 stating that all cases of HIPAA violations must be analyzed starting with the covered entity.³⁹ This DOJ opinion makes little sense as it renders the one-year incarceration provision meaningless. A “covered entity” is never an individual and therefore cannot serve up to one year in prison. Seizing upon these inconsistencies, several federal prosecutors subsequently brought successful cases against individuals for disclosing protected patient medical information, rendering the final meaning of “covered entity” unclear.⁴⁰

C. Fair Credit Reporting Act (FCRA)

The FCRA was passed in 1970 and was significantly amended in 1996 and 2003 to deal with data privacy concerns.⁴¹ Because the FCRA is large and parts are irrelevant for the purpose of this paper, only sections addressing the privacy provisions relating to data privacy will be discussed.

In 2003, Congress enacted the Fair and Accurate Credit Transactions Act.⁴² This act significantly added and amended the FCRA in order to provide new protections for customers' private credit information. One such protection provides that if someone loses their card or suspects that they are the victim of identity theft they can notify one of the major three credit reporting agencies and have them put a "fraud alert" on all of their credit reports.⁴³ Similar to HIPAA, the FCRA requires an appropriate purpose for distributing protected credit report information to third parties. The FCRA also requires that computers that are disposed of or sold have their hard drives scrubbed.⁴⁴ The FCRA requires more security measures than just the hard drive scrubbing required in HIPAA. If a company gives computers to a third party for disposal the company must have a contract requiring the third party to utilize proper disposal techniques.⁴⁵ In addition to this requirement, the company must also provide some form of monitoring to make sure that the third party complies with its obligations.⁴⁶

These privacy protections are all adequate but, like HIPAA, are under-enforced.⁴⁷ Without proper enforcement, an unscrupulous company or employee can make a substantial profit by selling private credit information and customers' personal information with no adverse consequences. To give FACTA provisions bite, enforcement of its provisions must become a higher priority.

The FCRA requirement for companies to notify customers upon a breach of customer data also has problems. Creditors are doing everything they can to avoid notifying customers of breaches because they complain that it is costly and results in a negative image of the company.⁴⁸ While states such as California require and enforce breach notifications, enforcement under FACTA is almost nonexistent.⁴⁹

Finally, the “fraud alert” for possible identity theft problems is not helpful to customers. The only “protection” is that the credit reporting agencies are aware of the possibility that some transactions may be fraudulent. A victim of identity theft cannot freeze their credit and there is no protection from debt collectors trying to collect money the victim never charged. Without the ability for victims of identity theft to freeze their credit the fraud alert provides little actual protection.⁵⁰

D. California Data Privacy Protections

California has established itself as the leader in data privacy legislation in the United States. Unlike existing federal privacy statutes, California protects most forms of private information, and provides its citizens with the ability to enforce their rights.

California provides a right to privacy in its Constitution.⁵¹ The Constitution provides that people have a reasonable expectation of privacy.⁵² Subsequent interpretations have further divided privacy interests into two legally protected types: the interest in precluding the dissemination or misuse of sensitive and confidential information, and the interest in making intimate personal decisions or conducting personal activities without observation, intrusion, or interference.⁵³

The California statutes also include necessary limitations. The statutes only allow suits where a violation is “serious in its nature, scope, and actual or potential impact to constitute an egregious breach of the social norms underlying the privacy right.”⁵⁴ These qualifications act as a gatekeeper that will exclude common everyday perceived violations, and allows the courts to focus on violations committed by large companies engaged in widespread data gathering operations.

California builds upon the FCRA and HIPAA federal statutes. In addition to the normal HIPAA requirements, California imposes additional requirements on healthcare providers. When a provider shares medical information with a third party for a justifiable purpose, the provider must provide notice to the patient.⁵⁵ California also prohibits providers from using patient data for any marketing purposes unless the patient explicitly opts in to such a system.⁵⁶ Finally, California allows the recovery of punitive damages up to \$3,000, attorney’s fees up to \$1,000, and the costs of litigation in addition to the statutory damages allowed under HIPAA.⁵⁷

California’s version of the FCRA and FACTA provides stricter controls on creditors and puts more power into the consumer’s hands. The California Financial Information Privacy Act (FIPA) prohibits financial institutions from sharing consumer data with third parties unless the companies seek and acquire affirmative consent from the consumer prior to the sharing of the data.⁵⁸ Another provision requires that financial institutions provide yearly disclosures to consumers if they share consumer information with affiliates and give the consumer an opportunity to opt-out.⁵⁹

The California statutes remedy many of the weakness of the FCRA. They require that institutions notify customers of data breaches as well as prevent debt collectors from continuing collection activities once a police report alleging identity theft has been filed.⁶⁰ Businesses must

also take reasonable steps to identify the identity of any applicant for credit if the information provided by the applicant does not reasonably match the information in their credit report.⁶¹

California has also enacted protections to protect consumers from online data collection websites and other sales websites that also collect and sell consumer information. The statute requires that businesses take reasonable steps to destroy the records and information they have collected that contain personal information of consumers after the business is finished with a particular transaction.⁶² This protects consumers from companies who hold onto consumers' information indefinitely and sell it to third parties over time. California also has a requirement that online businesses post their privacy policies conspicuously on their website.⁶³ This statute applies to Californian companies and any non-Californian companies that collect private information from Californian citizens.⁶⁴ Another statute provides punishment for those who distribute spyware, utilize phishing, or hack into computer systems to alter, steal, or delete data.⁶⁵

The California statutes are some of the most comprehensive in force today. They provide many protections for private information that have become necessary as the Internet develops and expands. Delaware, New York, and New Jersey have all since enacted some level of privacy protections similar to those found in California.⁶⁶ In addition, as of June 2005, thirty-five states have already introduced legislation for privacy protection, and twenty-two have enacted laws requiring notifications to consumers of security breaches.⁶⁷

The problem with California's laws is limited jurisdiction. Many online businesses are not in California, and others are not even in the United States. While California requires websites to display prominently their privacy policies, these protections are meaningless unless actual enforcement is possible. Providing similar protections on a national level would remedy many of these jurisdictional problems.

E. Argentina and Habeas Data

Several years ago, the European Union (EU) put in place privacy requirements that were to be adopted and enforced by all of its member countries. The EU recognized that it needed to find a mechanism to balance the need of protecting its citizens' privacy interests and allow businesses from foreign countries access to the EU. The EU's mechanism is a requirement that for any country to do business in the EU, or with its citizens, that country must have in place privacy protection measures that the EU deems "adequate."

Argentina is one of the first of the Latin America countries who has met this requirement. Argentina and several other Latin American countries have a right they call habeas data.⁶⁸ The habeas data right puts the protection of peoples' privacy interests in their own hands, allowing them certain rights with respect to their own data. Habeas data creates an interest in personal information comparable to a property interest. Habeas data would lend another useful enforcement mechanism to a potential "Privacy Bill of Rights."

Habeas data gives a person the right to control his own personal information. Habeas data grants a person a cause of action against a holder of his personal private information allowing for injunctive relief in the form of destruction, correction, or updating of his private data.⁶⁹ Under this system, data is considered "personal" if it refers or relates to any physical or legal person, and is considered "private" if it reveals "racial or ethnic origin, religious, political, or philosophical beliefs, union membership, or info about health or sexual behavior."⁷⁰

Habeas data also includes a cause of action for a person to get access to all private data a public or private entity has concerning the person and check for inaccuracies.⁷¹ If they find that there is false or incorrect data about them in the file they have the right to change it, and, if

necessary, have the right to sue in order to enforce the change.⁷² Citizens also can sue a private entity for injunctive relief requiring the entity to freeze certain parts of the data, preventing transfer to third parties.⁷³

The Argentina statutes contain necessary penalties in order to give effect to the rights provided. Penalties include warnings, suspensions, fines, or the closing of the entire database of private information.⁷⁴ There are also additional criminal penalties for such things as knowingly inserting false information into a file or having it inserted into a file, and special penalties for hacking into private bank databases or otherwise getting unauthorized access to confidentially registered databases.⁷⁵ If a violation results in actual injury to a person, the punishment is increased by fifty percent.⁷⁶ There are also harsh penalties incorporated for public officials who violate these protections.⁷⁷ If a public official violates these provisions it results in the official automatically being disqualified from taking a public office for a specified period.⁷⁸

In order to oversee all of the aspects of habeas data, including enforcement, the Argentina legislature created a group called the National Directorate for Personal Data Protection (DNPDP).⁷⁹ The DNPDP's primary role is to aid individuals in their lawsuits to enforce their habeas data rights. The DNPDP will help individuals who file requests with it with the investigation of their cases prior to taking the individual's case to the courts.⁸⁰ The DNPDP will also be there to give an individual advice and assistance with their claim until its completion, in some cases even standing in place of the individual in the habeas data action.⁸¹

A significant problem with habeas data is that while it significantly empowers the individual, it takes too much responsibility away from the government and monitoring agencies, resulting in a significant burden on the individual. For example, when a person brings an action they must identify with as much precision as possible the name and domicile of the data file or

register, or attempt to identify the government body if a public entity holds the data.⁸² They must also identify, as clearly as possible, what information the data file contains and why that information is discriminatory, false, or inaccurate and must show that the data owner is required to follow the order under the habeas data provisions.⁸³

The concept of habeas data is a useful one, but standing alone it is not enough to protect the average person's privacy interest in their personal information. Part of the problem lies with putting the majority of the burden on the person. In America, the average person is not aware that data is being collected from them, and even if aware, they do not know who holds the data. This creates a problem in that it makes it extremely difficult to bring any kind of injunctive suit against the holder. Providing federal regulation standards for businesses coupled with adequate enforcement in addition to the habeas data protections would create a well-rounded system leaving regulation and enforcement primarily up to the government, but allowing individuals to sue on their own behalf if their rights are significantly violated or if they somehow fall through the cracks in the system.

II. A Description of Two Regulatory Schemes Not Involving Federal Legislation and Why Their Protections are Inadequate, Showing Why a Privacy Bill of Rights is Necessary

Market pressure and self-regulation are two ideas often used in lieu of formal statutes to control both public and private activities without the rigidity inherent in structured laws. Market pressure's premise is that in a well functioning market the consumer and the company will barter and reach a solution that is in the best interest of both parties. An example in the Internet context would be that in order to use a website at no charge the consumer would allow the website to collect any data the user created while using the website.

Self-regulation stands for the idea that companies will only infringe upon a consumer's privacy to the extent that the consumer will allow before he ceases using that company's products. For example, a person might use an operating system produced by Company A and allow them to know his name, address, and phone number, but when the person hears in the news that Company A sells this collected data to third parties for profit, the person would discontinue use of the operating system and find an alternative.

In the following two sections, this paper will discuss in more detail how each of these concepts work in the cyberspace privacy context and discuss why neither solution is effective, and shows no promise of becoming useful, requiring federal legislation to be enacted to protect consumers' privacy interest in their personal information.

A. The Inadequacies of Market Pressure as a Regulatory Scheme to Protect Private Information

The idea behind using market pressure as a regulatory scheme revolves around the assumption that the smart consumer has a dollar value attached to their personal information, and that they are willing to trade a certain level of their privacy interest in this information for a certain level of service.⁸⁴ In other contexts apart from privacy and personal information, this exchange system works well, but in the Internet context market pressure fails. An example of a way the market could work would be to give a consumer a choice before using a website. He could choose to use the website for free, but under the condition that everything he inputs or clicks on will be logged and sold to third parties or used for marketing purposes. Another option would be to pay a monthly fee, but have the company clear all information relating to the consumer at the end of each session.

This is currently not how the market is functioning. In most cases, consumers are not aware that their private data is being collected and used as currency.⁸⁵ In his article, *Shopping for Privacy Online*, James Neft cites the statistic obtained from several polls that less than one percent of consumers are aware that web pages have privacy policies.⁸⁶ In another survey where consumers were informed of certain provisions in a typical website's privacy policy, the average person was shocked and outraged at what the website could do with their personal information.⁸⁷ Most consumers are aware that companies collect certain data about them and use it for marketing purposes. Most assume, however, that companies are not using person-specific data. Consumers are not aware that companies are selling their person-specific data, and that other companies are compiling all of this data to create a complete profile of the person, and then selling the complete profile to the government, marketing companies, or anyone else interested.⁸⁸

Market pressures will not work unless consumers are made aware that this market for their personal information exists and that their private data is an item to be bartered.⁸⁹ Further, consumers are also under-informed when data breaches result in the disclosure of their private information.⁹⁰ Keeping the consumer in the dark regarding privacy policies and data breaches works to companies' advantage. As long as consumers remain unaware of the situation, companies can amass as much private data as they want and sell it to whomever.

In controlled situations where consumers were given clear and easy to understand website privacy policies and then permitted to go through and simulate online activity, they were able to make rational decisions regarding what amount of data they were willing to give up in exchange for service.⁹¹ This experiment shows that in a well functioning market the market pressure approach can work. One method of informing consumers is to start a marketing campaign informing consumers about this market, their rights, and giving them options on what they can

do with their private data.⁹² In reality, such a marketing campaign is not likely to succeed. The average person will probably not listen, and in addition, many news corporations are also engaged in the same practices and have no reason to stop the collection of data.

Even the Federal Trade Commission (FTC) has given up on using market pressure as a control mechanism. In the late 1990s, the FTC decided that self-regulation was no longer working and started making proposals and recommendations that Congress enact protective legislation.⁹³ This was all curbed after September 11. The FTC backed off their proposals in order to let the government have room to fight against terrorism and went back to recommending that the market be controlled by market pressure.⁹⁴ Recently, the FTC has come back from that position and is now using existing statutes, like HIPAA and the FCRA, in a more aggressive way.⁹⁵ The FCC has recently come to settlements in three cases where violations of some of the privacy statutes occurred under this new approach.⁹⁶ These enforcements are merely a start. If a “Privacy Bill of Rights” were enacted the same results could be obtained much more efficiently, by allowing control agencies to go after violators without the legal maneuvering currently required.

B. Self-Regulation Will Not Work Because Companies Have No Reason to Regulate Themselves

Theoretically, online companies should be thinking about what level of privacy they should provide to consumers in order to keep consumers using their products. If a company was to take every bit of private information from a consumer and sell it and the consumer found out, the consumer would probably cease using that product, and eventually many others would follow as word was spread. With respect to the Internet, in a well functioning market companies would

want to put proper privacy policies in place in order to appeal to consumers. The market is currently not functioning well, however, and companies have little limit on what they can collect and subsequently use private personal information for.

Privacy policies did not always exist, and in comparison to the rest of the Internet were slow to develop. Around the year 2000, larger websites started putting up privacy policies in order to inform consumers of their practices. At the time, it was perceived that it was of interest to consumers to see what protections were in place by companies and what was happening to their data. In order to promote the posting of privacy policies many larger online companies would only allow advertisements from and link to websites that had privacy policies posted on their front page.⁹⁷ In this way, larger companies forced smaller companies to write privacy policies and post them for consumers to read.

Shortly after posting privacy policies became widespread, online companies realized that no one was reading them. Companies then began expanding the policies to unwieldy sizes and burying them so deeply in the site that finding them became nearly impossible, all in an effort to further deter consumers from reading the policies. For example, Google's privacy policy does not actually appear on their front page. Two clicks down there is a summary of the privacy policy that leaves out all of the details that would cause concern to a consumer.⁹⁸ Another click from their discloses the full privacy policy, which states that Google is collecting all the data consumers enter and all the links clicked and can use this data for any purpose.⁹⁹

Similar to the faults of market pressure factors, online companies have no incentive to make protective privacy policies. Most consumers have never read a privacy policy and are never informed of misuses of their information. Another practice that further cuts into the usefulness of privacy policies is cookies. Many online companies attach a cookie to a users'

computer that tracks all of his movements through their website, and sometimes beyond, as soon as the user loads their front page.¹⁰⁰ This practice invades a user's privacy before there is even a chance to read the privacy policy and assent to it by continuing to use the page, or reject it by navigating away from the page, rendering any decision based upon reading the privacy policy moot.

For all of the reasons discussed in this section, the market has failed and is showing no signs of improvement. The only option left to protect consumers is to enact national legislation that provides guidelines for online companies who if left unchecked may result to even more sinister behavior as long as a profit can be derived from it. In the next section, this paper discusses what provisions should be included in a "Privacy Bill of Rights".

III. In Order for a Privacy Bill of Rights to be Effective It Must Contain Provisions That Actually Address Privacy Problems in a Thorough and Restrictive Way

Protection of peoples' privacy interests has become a hot topic of late. In the last few years, there were federal bill proposals by Arlen Specter of Pennsylvania, Dianne Feinstein of California, and Hillary Clinton of New York.¹⁰¹ The bills have their plus and minus points, but none of them adequately address the relevant issues. Specter's is thorough, but is difficult for the average person to understand. The bill's principle problem is that it is difficult for companies to read and understand the requirements placed upon them, creating compliance problems. In addition, the average person reading the bill would also not understand what rights they have or how to enforce them. Feinstein's bill is written to be easier to understand, but lacks key protections such as protections for victims of identity theft.¹⁰² Clinton seems to be the most in

touch with the current issues, but her bill puts too much emphasis on regulation and does not give enough power to the consumer to enforce their rights.¹⁰³

Due to the changing and evolving nature of the Internet, no “Privacy Bill of Rights” can provide complete protection. Even though no bill can be perfect, there are varying levels of protection. For the consumer, more is always going to be better than less. On the other hand, businesses will balk if restrictions on them are too severe, especially considering the last twenty years of unenforced legislation and lack of regulation. A “Privacy Bill of Rights” containing the provisions outlined in the proceeding will be a significant step in the right direction and will provide protections for many problems currently left unresolved.

A. A Privacy Bill of Rights Must be Federal to be Effective

State’s each passing their own bills will not adequately protect peoples’ privacy interests because of the nature of the Internet. Jurisdictional issues would be so prevalent that a state statute would not be effective; courts have not even come to a consensus yet as to where subject matter jurisdiction or personal jurisdiction applies in the Internet context. Second, if each state passes their own legislation it will be difficult for companies to conform to the standards set out. Uniformity is necessary in order to provide an effective solution.

Making the bill federal will not be enough to provide complete protection because many of the data gathering and exploiting companies are not located in the United States. Even though companies could still be found to violate rules, enforcement of judgments would be difficult. Even though these foreign companies are out there, many of the largest online companies with advanced data collection and organization software used on American citizens are located in the United States. Therefore, a federal bill would still provide significant protections.

B. Private Data Must be Encrypted on Servers and Hard Drives

Companies should be required to provide adequate encryption on their servers in addition to any personal computer that contains consumers' private information. The encryption level should also be regulated. There are different levels of encryption, with the lower levels being easier to crack by hackers and the higher ones being nearly impossible to crack. In order to provide adequate protection of personal information encryption should be of a high enough level to act as a significant deterrent to hackers. Encryption alone, however, is not going to be enough. Encryption policies will need to be supported by mandatory employee training informing employees on how they are to handle protected data.

Recently, many legislatures have discussed "encryption" as though it were a magic talisman that would solve all issues relating to data breaches. This is overstating the effectiveness of encryption. Encryption is only as good as the person using it. It is possible to crack any encryption with enough time and computing power. The time might be decades, but it can be done. In addition, to decrypt data employees will often have to use a password, and employees are notorious for keeping passwords on their computers, under their keyboards, or using common words as passwords. The employer could address all of these employee-related issues with mandatory training.

C. Companies Must Use Reasonable Efforts to Install Tracking Technology on Hardware Containing Private Data

There have been several reports of lost data tapes or laptops full of private information in the news of late. The companies responsible do nothing more than throw their hands up and say,

“there’s nothing we can do.” That may have been the case ten years ago, but tracking technology is now cheaper than ever. Not only that, but many laptops now come with tracking technology already installed in order to track down the laptop if it is stolen.

Using the term “reasonable efforts” should be enough of a burden on companies to implement some cheaper tracking technologies, but not be so costly as to be of significant financial detriment to a company. Currently, computers can be bought with Global Positioning System (GPS) dots installed in them in order to track them with a GPS device. In addition, every computer has a built in network card identifier address that can be tracked whenever a computer is plugged into the Internet. Either of these mechanisms could be easily implemented by companies.

D. Consumers Must be Notified upon a Data Breach of Unencrypted Data, or Before Their Private Information is Sent Abroad

In the last five years, many large companies have contracted out their data processing to companies operating in other countries, primarily India. The protections provided by a “Privacy Bill of Rights” mean little if they cannot be applied. Companies should be required to notify their customers before sending data overseas for processing, and give them an opportunity to opt out.

Requiring notification to consumers of data breaches will help consumers enforce their rights. Notifying consumers of breaches will make them more aware of who has their private information and allow them to make intelligent decisions regarding who should be holding their data based on the number of breaches that have occurred. It also gives consumers the ability to start monitoring their records for themselves, giving them responsibility over their own data. If a

consumer finds suspicious activity, he can then file an identity theft report. Filing a report will enable him to be protected from debt collection and potentially allowing a freeze on his accounts until the situation can be resolved.

If too many notices are sent, consumers will stop reading them. For this reason, data breach notifications should be limited to unencrypted data. Even with a smaller number of notices, it is still likely that over time consumers will begin ignoring the notifications. A “Privacy Bill of Rights” cannot force the media to publicize data breaches, but media cooperation would help bring large breaches to consumers’ attention.

E. When a Data Breach Has Occurred, Fraud Protection Must be Enacted for Consumers Wronged

In the last few years, companies have already started to provide some form of fraud protection. A fraud protection provision would apply to those who hold private financial information. If information were to be disseminated because of a breach, the company responsible for that data would be required to provide some limited fraud protections for a limited time.

F. Opt-In Requirements Should be Used over Opt-Out for Data Collection and Retention

This statute would require that any information sharing agreements sent to consumers would be in the form of opt-in rather than opt-out. While this places a heavy burden on companies, it provides more protection to consumers. In one study, it was found that if an informed person could vote between opt-out and opt-in, he would choose an opt-in system because of the greater protection provided.¹⁰⁴

Many companies are already required to give opt-out forms to consumers when they want to use consumer information for marketing or sell it to a third party. These opt-out forms usually are hidden amongst the mountain of advertisements included in credit card statements, or buried so deep in a contract and worded so incomprehensibly that the average person would have no chance of finding it. Enacting opt-out requirements forces companies to be more responsible and allows consumers more control over the use of their private information.

G. Companies Must Have Data Protection Policies in Place and Provide Employees

Training

Many of the provisions proposed are useless unless companies provide their employees with training. Simply telling an employee that he should use encryption is not useful if he has no idea how to.

Typical policies would include provisions requiring employees to carry and use locking cables for laptops, implementing a system where old computer hard drives are scrubbed thoroughly before they are resold or scrapped, and setting password policies requiring employees to use stronger passwords. Companies should also be required to dispose of private information when the use for it has ended, similar to what California has in their statute. Finally, social security numbers should never be used as a consumer identification method.

H. Consumer's Shall Have a Right Similar to Habeas Data

Habeas data would empower consumers with rights concerning their data similar to the bundle of rights given in the property context. Giving consumers power over their own data provides a failsafe for instances when they fall through the system and any of the other

protections do not help them protect their privacy interests. Giving consumers habeas data rights also provides a low-cost means of enforcement. The government will not have to launch as many investigations as consumers are held responsible for their own data and will be notified when a data breach has occurred so they can work to vindicate their own rights. Habeas data rights would provide consumers the right to sue for injunctive relief order to see, update, freeze, or remove their data from the company's database.

I. Willful and Intentional Violations of these Provisions Will Incur Criminal Liability

Willful and intentional breaches of data are more serious than accidental or negligent releases of private information because it often results in an improper use of the information to the detriment of the consumer and causes actual injury. Because these violations are intentional and they often lead to more identity theft related crimes, they should be treated as more serious by imposing fines and sentencing similar to those found in HIPAA. Unlike HIPAA, however, there should be provisions explicitly holding employees liable for data breaches. Applying the "Privacy Bill of Rights" requirements to companies and their employees individually would avoid the problems and inconsistencies of HIPAA discussed in the HIPAA section above.

J. Grossly Negligent, Negligent, and Reckless Violations will Incur Civil Liability

For grossly negligent, negligent, and reckless violations, civil fines should be the main form of punishment. The method used in HIPAA is relevant not only in the context of private medical data, but would work well if implemented in a "Privacy Bill of Rights." Under HIPAA, there is a list of factors to be weighed when assessing the fines for violations.¹⁰⁵ These factors consist of the nature of the violation, the circumstances and consequences of the violations, the

degree of culpability, the financial conditions of the corporation, and any history of prior violations, specifically: how the company responded, to what extent they remedied the violation since, and the similarity of the current violation to past violations.¹⁰⁶

IV. Passing This Bill of Rights and Imposing These Standards on Companies Will Work to Further Consumers' Interests

A "Privacy Bill of Rights" is necessary because other non-legislation systems have failed. Self-regulation and market pressure have proven to be ineffective to protect peoples' rights. Most consumers are not aware that a market for their data exists and businesses have no incentive to scale back their uses of private information because there is little chance of retribution by consumers for exploitation. In other contexts similar to this, such as in the Anti-Trust context, statutes were passed to protect consumers when the market failed.

Companies will try to fight a "Privacy Bill of Rights" to the end. It is to their advantage to keep people in the dark because they continue to make profit from an unlimited source of essentially free information. This bill does not attempt to provide complete protection for consumers, but aspires to provide reasonably sufficient protection.

The protections provided in this "Privacy Bill of Rights" will empower consumers to be responsible for their own private information. One of the underlying ideas of this bill is that a consumer's private information is either a part of them or is similar to their own property and that they are essentially leasing it or entrusting it to corporations, and that if there is a breach of trust, they can then pursue a remedy appropriate for their situation. The addition of breach notifications will further empower people to enforce their rights by making them more aware of potential violations.

A “Privacy Bill of Rights” will necessarily have many provisions that require corporations to implement burdensome procedures. It would be best to implement the various provisions of the bill on staggered dates over a period of years. This will give corporations time to phase in new requirements gradually, lowering the cost to them, and allowing the courts to make sense of specific provisions over time.

Privacy has been an issue on everyone’s mind lately. News organizations are more frequently releasing stories discussing large data breaches, legislatures are proposing bills, speakers are addressing the issue, and many other countries have already passed legislation protecting their citizens’ interests. It is time the legislature stepped up and passed a “Privacy Bill of Rights” in the United States to protect Americans from a real-life disaster similar to the story of Steven Jobs.

Endnotes

- ¹ See Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, 92 Stat. 3641 (1978) (codified as amended at 12 U.S.C. § 3402); Video Privacy Protection Act of 1988, Pub. L. No. 100-618, 102 Stat. 3195 (1988); Driver's Privacy Protection Act of 1994, Pub. L. No. 103-322, 108 Stat. 2099 (1994) (codified as amended at 18 U.S.C. 2721); and Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 100 Stat. 1936 (1996).
- ² See, e.g., *Griswold v. Connecticut*, 381 U.S. 479 (1965); *Whalen v. Roe*, 429 U.S. 589 (1977); *Paul v. Davis*, 424 U.S. 714 (1976).
- ³ U.S. CONST. amend. IV.
- ⁴ *Katz v. U.S.*, 389 U.S. 347 (1967).
- ⁵ *Id.* at 348.
- ⁶ *Id.*
- ⁷ *Id.* at 351-352.
- ⁸ *Id.* at 352.
- ⁹ *Id.* at 351.
- ¹⁰ *Id.* at 361.
- ¹¹ *Kyllo v. U.S.*, 533 U.S. 27 (2001).
- ¹² *Id.* at 29.
- ¹³ *Id.*
- ¹⁴ *Id.*
- ¹⁵ *Id.* at 30.
- ¹⁶ *Id.* at 37-38.
- ¹⁷ *Id.* at 38.
- ¹⁸ *Id.*
- ¹⁹ Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, § 3486(a)(1)(A), 100 Stat. 1936 (1996).
- ²⁰ Berrie Rebecca Goldman, *Pharmacogenomics: Privacy in the Era of Personalized Medicine*, 4 N.W. J. TECH. & INTELL. PROP. 83, 93 (2005).
- ²¹ See Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 100 Stat. 1936 (1996).
- ²² *Id.*
- ²³ § 1171(3).
- ²⁴ § 2713.
- ²⁵ Nusrat N. Rahman, *Reflections on Privacy: Recent Developments in HIPAA Privacy Rule*, 2 ISJLP 685, 696 (2006).
- ²⁶ Health Insurance Portability and Accountability Act §§ 1176, 1177.
- ²⁷ Rahman, *Reflections*, *supra* note 25, at 688 (2006).
- ²⁸ *Id.*
- ²⁹ Health Insurance Portability and Accountability Act § 1176(a)(1).
- ³⁰ § 1176(b).
- ³¹ § 1177.
- ³² § 1177(b)(1).
- ³³ Rahman, *Reflections*, *supra* note 25, at 696 (2006).
- ³⁴ Peter P. Swire, *2005-2006 Privacy Year in Review Annual Update: Introductory Essay for "Privacy Law Year in Review, 2005-2006"*, 2 ISJLP 475, 480 (2006).
- ³⁵ Rahman, *Reflections*, *supra* note 25, at 691.
- ³⁶ Swire, *2005-2006 Privacy*, *supra* note 34, at 480.
- ³⁷ *Id.*
- ³⁸ See Plea Agreement, *U.S. v. Gibson*, No. CR04-0374RSM, 2004 WL 2237585 (W.D. Wash. 2004).
- ³⁹ David V. Marshall, *Justice Department Limits Prosecution Under HIPAA*, DAVIS WRIGHT TREMAINE LLP, June 2005, http://www.dwt.com/practc/hc_ecom/bulletins/06-29-05_ProsecutionLimits.htm.
- ⁴⁰ *U.S. v. Ramirez*, No. 7:05CR00708 (S.D. Tex. 2005); *U.S. v. Ferrer*, No. 06-60261 CR-COHN (S.D. Fla. 2006).
- ⁴¹ Fair Credit Reporting Act, Pub. L. 91-508, 84 Stat. 1128 (1970) (codified as amended at 15 U.S.C. 1681 et seq.).

-
- ⁴² Fair and Accurate Credit Transactions Act, Pub. L. No. 108-159, 117 Stat. 1952 (2003) (codified as amended at 15 U.S.C. 1681 et seq.)
- ⁴³ Fair and Accurate Credit Transactions Act § 112(a).
- ⁴⁴ 16 C.F.R § 682.1(c)(2) (2005).
- ⁴⁵ Fair and Accurate Credit Transactions Act § 628(a)(2).
- ⁴⁶ *Id.*
- ⁴⁷ Gary M. Victor, *Identity Theft, Its Environment and Proposals for Change*, 18 LOY. CONSUMER L. REV. 273, 289 (2006).
- ⁴⁸ *Id.* at 287.
- ⁴⁹ CAL. CIV. CODE § 1798.29(a) (LexisNexis 2007).
- ⁵⁰ Hillary Rodham Clinton, Senator, New York, Remarks of Senator Hillary Rodham Clinton on Privacy to the American Constitution Society (June 16, 2006) *available at* <http://www.senate.gov/~clinton/news/statements/details.cfm?id=257288>.
- ⁵¹ C.A. Const. art. I, § 1 (LexisNexis 2007).
- ⁵² *Id.*
- ⁵³ Hill v. Nat'l Coolegiate Athletic Ass'n, 7 Cal. 4th 1 (Cal. 4th 1994).
- ⁵⁴ *Id.* at 37.
- ⁵⁵ CAL. CIV. PROC. CODE. § 1985.3 (LexisNexis 2007).
- ⁵⁶ CAL. CIV. CODE § 56.10(d) (LexisNexis 2007).
- ⁵⁷ CAL. CIV. CODE § 56.35 (LexisNexis 2007).
- ⁵⁸ Cal. Fin. Code § 4051.5(b)(1) (LexisNexis 2007).
- ⁵⁹ *Id.* at 4053(b)(1).
- ⁶⁰ CAL. CIV. CODE § 1798.29(a) (LexisNexis 2007); CAL. CIV. CODE § 1788.18 (LexisNexis 2007); CAL. CIV. CODE § 1785.20.3 (LexisNexis 2007).
- ⁶¹ *Id.*
- ⁶² CAL. CIV. CODE § 1798.81 (LexisNexis 2007).
- ⁶³ Margaret Betzel, *2005-2006 Privacy Year in Review Special Topic: Privacy Law Developments in California*, 2 ISJLP 831, 866 (2006).
- ⁶⁴ *Id.*
- ⁶⁵ See CAL. BUS. & PROF. CODE §§ 22947.3 and 22948 (LexisNexis 2007); CAL. PENAL CODE §§ 630-637.9, 530.5, 502, and 530.9 (LexisNexis 2007).
- ⁶⁶ Milton C. Sutton, *2005-2006 Privacy Year in Review Special Topic: State Laws, Federal Proposals, and Recommendations*, 2 ISJLP 927, 931-935 (2006).
- ⁶⁷ *Id.*
- ⁶⁸ CONST. ARG. § 43(3) *available at* <http://www.servat.unibe.ch/law/icl/ar00000.html>.
- ⁶⁹ *Id.*
- ⁷⁰ Personal Data Protection Act, Law No. 25326 § 2, Oct. 4, 2000 *available at* <http://www.privacyinternational.org/countries/argentina/argentine-dpa.html>.
- ⁷¹ CONST. ARG. § 43(3).
- ⁷² *Id.*
- ⁷³ *Id.*
- ⁷⁴ Personal Data Protection Act, Law No. 25326 §§ 31-32, Oct. 4, 2000 *available at* <http://www.privacyinternational.org/countries/argentina/argentine-dpa.html>.
- ⁷⁵ Law No. 25326 § 32(1)(1).
- ⁷⁶ Law No. 25326 § 32(1)(3).
- ⁷⁷ Law No. 25326 § 32(1)(4).
- ⁷⁸ *Id.*
- ⁷⁹ Law No. 25326 § 29.
- ⁸⁰ Law No. 25326 § 29(1)(a).
- ⁸¹ Law No. 25326 § 29(1)(a) and (g).
- ⁸² Law No. 25326 § 38(1).

-
- ⁸³ Law No. 25326 § 38(2).
- ⁸⁴ James P. Nehf, *Shopping for Privacy Online: Consumer Decision-Making Strategies and the Emerging Market for Information Privacy*, 2005 U. ILL. J.L. TECH. & POL'Y 1, 1 (2005).
- ⁸⁵ Nathaniel Good et al., *User Choices and Regret: Understanding Users' Decision Process about Consensually Acquired Spyware*, 2 ISJLP 283, 293 (2006).
- ⁸⁶ Nehf, *Shopping*, *supra* note 78, at 11.
- ⁸⁷ Good, *User*, *supra* note 79, at 293.
- ⁸⁸ *Id.*
- ⁸⁹ Nehf, *Shopping*, *supra* note 78, at 12.
- ⁹⁰ *Id.* at 36.
- ⁹¹ *Id.* at 15.
- ⁹² *Id.* at 6.
- ⁹³ *Id.* at 2.
- ⁹⁴ *Id.*
- ⁹⁵ See Federal Trade Commission, Eli Lilly Settles FTC Charges Concerning Security Breach, Jan. 18, 2002, <http://www.ftc.gov/opa/2002/01/elililly.htm>; Federal Trade Commission, Microsoft Settles FTC Charges Alleging False Security and Privacy Promises, Aug. 8, 2002, <http://www.ftc.gov/opa/2002/08/microsoft.htm>; and Federal Trade Commission, High School Student Survey Companies Settle FTC Charges, Oct. 2, 2002, <http://www.ftc.gov/opa/2002/10/student1r.htm>.
- ⁹⁶ *Id.*
- ⁹⁷ Nehf, *Shopping*, *supra* note 78, at 3.
- ⁹⁸ Google Privacy Policy Highlights, <http://www.google.com/intl/en/privacy.html> (last visited Mar. 29, 2007).
- ⁹⁹ Google Privacy Policy, <http://www.google.com/intl/en/privacypolicy.html> (last visited Mar. 29, 2007).
- ¹⁰⁰ Matthew C. Keck, *Cookies, the Constitution, and the Common Law: A Framework for the Right of Privacy on the Internet*, 13 ALB. L.J. SCI. & TECH. 83, 109 (2002).
- ¹⁰¹ Milton C. Sutton, *2005-2006 Privacy Year in Review Special Topic: State Laws, Federal Proposals, and Recommendations*, 2 ISJLP 927, 935-939 (2006).
- ¹⁰² *Id.* at 939.
- ¹⁰³ Hillary Rodham Clinton, Senator, New York, Remarks of Senator Hillary Rodham Clinton on Privacy to the American Constitution Society (June 16, 2006) available at <http://www.senate.gov/~clinton/news/statements/details.cfm?id=257288>.
- ¹⁰⁴ Gary M. Victor, *Identity Theft, Its Environment and Proposals for Change*, 18 LOY. CONSUMER L. REV. 273, 301 (2006).
- ¹⁰⁵ Rahman, *Reflections*, *supra* note 25, at 698-699.
- ¹⁰⁶ *Id.*