PRESERVING IDENTITIES: PROTECTING PERSONAL IDENTIFYING INFORMATION THROUGH ENHANCED PRIVACY POLICIES AND LAWS

by

Robert Sprague* and Corey Ciocchetti**

The common law has always recognized a man’s house as his castle…. Shall the courts thus close the front entrance to constituted authority, and open wide the back door to idle or prurient curiosity?¹

The time will come when we are well known for our inclinations, our predilections, our proclivities, and our wants. We will be classified, profiled, categorized, and our every click will be watched.²

Introduction

The collection, storage, and sale of personal information is a legitimate hot-button topic for consumers, companies, and legislators as the twenty-first century bustles forward.³ As companies continue to collect personal data and sell it on the open market,⁴ Congress fails to stake out a position and various states attempt to pick up the slack.⁵ The topic of this national debate is Personal Identifying Information, or PII—essentially, data that identify a particular individual. Some pieces of PII—such as Social Security numbers—identify by themselves, while other pieces—such as a maiden name or employment address—only identify individuals when aggregated together into a digital profile.

Contemporary business requires the submission of a certain amount of PII to complete transactions (particularly on the Internet). In addition, this information is also being stored for future uses such as internal and external data mining.⁶ Individuals have little to no control over the collection and dissemination of their PII and, upon dissemination, the information is virtually irretrievable by the individual it identifies. Not only are individuals’ bank, credit, and financial account information being collected and stored, so too are the lives they lead online, from shopping habits, to social interactions, to Web sites visited. As one commentator noted, “Who controls our data controls our lives.”⁷

This paper explores the developing phenomenon of the ongoing collection and dissemination of personal identifying information. A significant amount of information, though not all, is collected via the Internet. Regardless of the manner in which the information is collected, it is stored and transferred electronically, making it vulnerable to unauthorized disclosure.

This paper begins by explaining the nature and form of personal identifying information, including the consequences of its collection. This paper then explores one of the greatest threats associated with data collection—unauthorized disclosure due to data breaches. The same section includes an overview of state and federal legislative reactions to the threats of data breaches and identity theft. Next, common law and constitutional privacy protections regarding the collection of personal information are discussed, revealing that United States privacy laws provide very little protection to individuals. This paper then discusses current practices by online commercial enterprises regarding privacy policy disclosure and conduct. This section reveals that there is almost no legal regulation of online privacy policies.

This paper concludes that new, stronger laws are required to protect individuals regarding the collection and dissemination of their PII. A model law is therefore proposed to address those areas where PII protection is lacking. As long as there are no requirements for companies to adopt and adhere to meaningful privacy policies and there is no liability for companies that allow unauthorized dissemination of PII, individuals will enjoy less privacy and continue to be at risk of identity theft.

Personal Identifying Information

Personal identifying information (PII) comes in various forms and data. While it may be as seemingly innocuous as a phone number or employment address, it is much more valuable than individuals might realize. From an e-commerce perspective, the collection of PII represents an efficient and important way for companies to provide goods and service transactions online.⁸ From a consumer perspective, the collection of PII allows Web surfers to customize their online

* J.D., M.B.A., Assistant Professor, Department of Management & Marketing, University of Wyoming College of Business. The authors would like to thank Stephen P. Smith, J.D. 2008, University of Wyoming College of Law, and Tigran Muradyan, J.D. 2008, University of Wyoming College of Law, for their excellent assistance in performing research for this paper.
** J.D., M.A., Assistant Professor, Department of Business Ethics and Legal Studies, University of Denver Daniels College of Business.
experience as websites store their information to facilitate navigation and purchases.\textsuperscript{5} From a more nefarious standpoint, the collection of PII represents a prime target for identity thieves and other bad actors interested in obtaining the information to benefit financially.\textsuperscript{10}

The amount of personal identifying information collected in modern life is vast: transactional data are tracked, cell phones are monitored, Web surfing is recorded, and our moves in public are recorded by surveillance cameras.\textsuperscript{11}“The small details that were once captured in dim memories or fading scraps of paper are now preserved forever in the digital minds of computers, vast databases with fertile fields of personal data.”\textsuperscript{12} Individually, each piece of personal information represents a mere pixel of someone’s life, but when pieced together, they present a rather detailed picture of that person’s identity.\textsuperscript{13} “The Internet’s greater targeting potential and the fierce competition for the consumer’s attention have given companies an unquenchable thirst for information about web users. This information is useful in developing more targeted advertising ….”\textsuperscript{14} Personal information is collected in cyberspace primarily through registration and transactional data—collected directly from users—and through clickstream data—surreptitious tracking of users as they navigate the Internet.\textsuperscript{15}

An individual’s “digital footprint” extends beyond transactional data.\textsuperscript{16} The digitization of public records, combined with the increasing accuracy of search engines, has made it easier for the general population to join creditors, law enforcement, and professional investigators to discover individuals’ personal information.\textsuperscript{17} As a result, it is far more likely that a stranger can learn a substantial amount of personal information about an individual—enough to even assume the identity of someone else.

Personal financial information, such as credit card numbers, while often collected in a face-to-face transaction, is transmitted and stored electronically, leaving it vulnerable to unauthorized access. In recent years, these so-called “data breaches” have grown in number and increased the risk of harm from credit card fraud and identity theft for a significant number of individuals.

**Risks Associated with Collecting PII: Data Breaches and Identity Theft**

One of the greatest risks posed by the collection of PII is its improper use as a result of data breaches. Weak data security ultimately results in the distribution of personal information beyond the bounds of consent and expectations.\textsuperscript{18} Data breaches can occur a number of ways, from unauthorized access of computer systems by outsiders (i.e., hacking) to the loss of portable computers or portable storage devices.\textsuperscript{19} Data breaches have been reported by businesses, financial concerns, educational institutions, government entities, and medical and healthcare concerns.\textsuperscript{20}

Exposure of PII through a breach of security can lead to identity theft and fraud. For example, in January 2007, TJX Companies, Inc., which operates the TJ Maxx and Marshalls stores in the United States (as well as additional stores in Canada and Puerto Rico), announced it had discovered that it had been the victim of a data breach.\textsuperscript{21} Initially, it was estimated that approximately 45 million records containing credit card information had been exposed to outsiders.\textsuperscript{22} Subsequently, that estimate was raised to over 94 million records.\textsuperscript{23}

The intruders were able to make fraudulent credit card purchases using the credit card account information of TJX customers.\textsuperscript{25} However, those losses were borne by the credit card companies rather than the customers.\textsuperscript{26} A bank and credit union that had issued credit cards that were subject to the TJX data breach filed suit, individually and on behalf of a class of similarly situated financial institutions, against Fifth Third Bancorp and Fifth Third Bank (“Fifth Third”) which acquires and processes Visa and MasterCard transactions for TJX as an “Acquiring Bank.”\textsuperscript{26} The financial institution plaintiffs alleged that TJX failed to safeguard sensitive data for its credit card transactions as required under the Payment Card Industry (PCI) Data Security Standard.\textsuperscript{27} The plaintiffs alleged, inter alia, that Fifth Third was liable for: (1) negligence for allowing TJX to not safeguard its credit card and personal information data in violation of industry standards;\textsuperscript{28} and (2) negligent misrepresentation based on implied representations that TJX and Fifth Third made to the issuing banks that they took the security measures required by industry practice to safeguard personal and financial information.\textsuperscript{29} The parties subsequently reached a tentative settlement, requiring TJX to pay nearly $41 million to Visa U.S.A., Inc. to compensate banks that issued Visa cards that were potentially affected by the breach.\textsuperscript{30}

Some of the data stored by TJX, though, also included customer PII, such as Social Security and driver’s license numbers, increasing the risk that up to 400,000 TJX customers could become the victims of identity theft.\textsuperscript{31} Unlike the fraudulent use of credit card accounts, individuals face greater risks of financial harm through identity theft, in which imposters use a victim’s PII to create new accounts for which the victim is potentially financially responsible.\textsuperscript{32}

The TJX data breach accounted for approximately 75% of the nearly 128 million records exposed in 2007 through data breaches,\textsuperscript{33} and nearly half the total since 2005.\textsuperscript{34} Even without the TJX data breach, millions of records, many potentially containing PII, are exposed each year through data breaches.\textsuperscript{35} The experience of LPL Financial of Boston, Massachusetts exemplifies some of the challenges faced by businesses regarding data breaches. On May 6, 2008, LPL sent a series of letters to the Maryland Office of the Attorney General, notifying the Office of data breaches that could potentially affect Maryland residents.\textsuperscript{36} On June 30, 2008, LPL learned that a current employee had compromised the personal information of one thousand customers, including names, addresses, account numbers, and Social Security numbers.\textsuperscript{37} The employee had access to the information due to an accounts system that did not properly secure data.\textsuperscript{38}

On September 12, 2007, a laptop computer was stolen from LPL’s San Diego, California office which contained PII (including fingerprints) of nearly 1,400 LPL registered representatives and employees.\textsuperscript{38} On December 11,
2007, five computers were stolen from LPL’s Diamond Bar, California office containing PII of 444 LPL customers. And on April 10, 2008, a car owned by an LPL employee was stolen, resulting in the loss of a laptop computer containing PII of approximately 2,800 LPL employees.

Although the United States General Accounting Office has concluded that the extent to which data breaches result in identity theft is not well known, one survey conducted on behalf of the Federal Trade Commission estimates that 1.8 million American adults reported that in 2005 they had discovered that their personal information had been misused to open new accounts or to engage in other types of fraud, costing the victims an aggregate of $72 million in out-of-pocket costs. These costs do not include the hundreds of hours these victims spent resolving problems created by the identity theft, such as being harassed by credit collectors, correcting credit mistakes, being denied loans, having utilities cut off, and even being criminally investigated. Despite these direct and indirect costs, current law affords little to no remedy for a victim of a data breach or identity theft.

**Common Law Remedies For Victims Of Data Breaches**

For victims of identity theft, the principal obstacle for seeking damages through the courts has been the lack of actual damages suffered—the threat of harm resulting from identity theft is insufficient. For example, in *Pisciotta v. Old National Bancorp*, the plaintiffs (for themselves and on behalf of a putative class of customers and potential customers) sued after the defendant bank’s online banking system was breached by hackers, exposing “confidential information of tens of thousands” of customers. The plaintiffs sought compensation for all economic and emotional damages suffered as a result of the defendant’s acts which were negligent, in breach of implied contract or in breach of contract, plus credit monitoring services. Indiana’s security breach notification law took effect after the data breach in *Pisciotta* took place, but the Seventh Circuit Court of Appeals noted that Indiana’s law only requires disclosure of a data breach to potentially affected consumers; it does not require “any other affirmative act in the wake of a breach.” In particular, the law “imposes no duty to compensate affected individuals for inconvenience or potential harm to credit that may follow[,]” a data breach. Further, the plaintiffs were not able to show they were actual victims of identity theft as a result of the data breach. In dismissing their claims, the Seventh Circuit held that “[w]ithout more than allegations of increased risk of future identity theft, the plaintiffs have not suffered a harm that the law is prepared to remedy.”

On a different front, victims of identity theft have attempted to hold banks liable for issuing credit cards to imposters (using the victim’s identity) under a theory of negligent enablement of imposter fraud. For example, in *Polzer v. TRW, Inc.*, individuals in whose names an impostor had obtained credit cards sued the credit card issuers for negligent enablement of imposter fraud. A New York appellate division court upheld summary judgment against the plaintiffs because the defendant credit card issuers “had no relationship either with the impostor who stole the plaintiffs’ credit information and fraudulently obtained credit cards, or with plaintiffs, with whom they stood simply in a creditor/debtor relationship.” Similarly, the court in *Huggins v. Citibank, N.A.*, while “concerned about the rampant growth of identity theft and financial fraud in this country[,]” nevertheless agreed with *Polzer* and declined “to recognize a legal duty of care between credit card issuers and those individuals whose identities may be stolen.”

However, courts have recognized harm when highly personal information has been improperly disclosed. For example, in *Acosta v. Byrum*, the Court of Appeals of North Carolina reversed the lower court’s dismissal of the plaintiff’s complaint alleging breach of privacy and negligent infliction of emotional distress after a staff member of the defendant’s psychiatric office (of which the plaintiff was a former employee, as well as patient) allegedly gained access to the plaintiff’s medical file and shared private information with third parties. In particular, the plaintiff alleged the defendant knew of severe animus between the plaintiff and the staff member, yet the defendant gave the staff member his medical access code, allowing the staff member to show that code to access and obtain the plaintiff’s confidential medical records.

With no common law remedies available for identity theft, victims must turn to state or federal legislation for redress. As discussed below, current legislation provides very limited direct remedies to victims of identity theft.

**Legislative Responses to Data Breaches**

In early 2005, ChoicePoint, one of the three principal credit reporting agencies in the United States, discovered that it had been selling personal credit information to identity thieves posing as legitimate businesses. California residents who were victims of the ChoicePoint data breach were notified that their personal information may have been compromised as a result of California’s security breach notification law, which has since been used as a model by numerous states in response to the ChoicePoint data breach. California’s breach notification law requires businesses conducting business within the state to promptly notify individuals if their unencrypted personal information is acquired by an unauthorized individual. Personal information, under the California statute, includes “name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver’s license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information.”
All but seven states and the District of Columbia have since passed legislation requiring entities, particularly businesses, that maintain computerized PII of state residents to notify those residents if their PII has been disclosed through a data breach. For the most part, these statutes do not penalize businesses for allowing the data breach itself to occur, but only provide penalties if a business fails (or is too slow in taking steps) to notify affected individuals. For example, TJX’s wireless network, which was the point of penetration for its massive data breach, has been described as having “less security than many people have on their home networks.” The hackers had penetrated TJX’s computer system to the extent “[t]hey were so confident of being undetected that they left encrypted messages to each other on the company’s network, to tell one another which files had already been copied and avoid duplicating work.” Yet, under most of the laws passed in the wake of increasing data breaches, the onus is on TJX only to notify its customers, not to have implemented sufficient security to prevent the breach in the first place. Preventing data breaches is only indirectly encouraged, in that all but two of the data breach notification statutes provide an “encryption safe harbor,” making the notification requirements inapplicable if the breached data is encrypted.

And in the few states that do provide civil damages against a company that has had a data breach, victims will most likely encounter the same difficulties in succeeding as with common law actions. For example, in *Ponder v. Pfizer, Inc.*, Horne, an employee of Pfizer, sued after employee PII was exposed to outsiders. Horne alleged that Pfizer had violated Louisiana’s Security Breach Notification law because nine weeks elapsed between the data breach and the notification of the breach. The court did not directly address this issue, since it dismissed the complaint on the basis that Horne had failed to plead actual damages suffered. As with the common law remedies sought as a result of data breaches that were discussed above, the *Ponder* court concluded that “Horne’s complaint does not allege that he suffered any actual damages—that someone actually used the disclosed information to his detriment.”

While at least one commentator has argued that the cost and burden of providing notification of data breaches will be sufficient motivation for companies to avoid data breaches, the continuous number of data breaches indicates otherwise. With the emphasis of state data breach notification laws on notification, as opposed to prevention, and the limitation of damages to actual misuse by a third party, as opposed to the burden of monitoring credit after a data breach, victims have very limited state-based remedies.

**Current and Proposed Federal Legislation**

There are two current federal laws that do provide some protection against data breaches. The Gramm-Leach-Bliley Act requires financial institutions to insure the security and confidentiality of customer records and information. Since the Gramm-Leach-Bliley Act applies only to financial institutions, such as banks, credit unions, savings and loans, insurance companies and investment companies, its security requirements do not apply to merchants or other sources of data breaches, such as non-financial businesses or schools. Portions of the Fair and Accurate Credit Transactions (FACT) Act amends the Fair Credit Reporting Act to protect against identity theft. Specifically, the FACT Act requires that merchants providing an electronically printed credit card receipt truncate the card number so that no more than the last 5 digits are printed (and not print the expiration date of the credit card as well).

Although there have been over a dozen bills combating identity theft introduced in the 110th Congress, no legislation addressing data breaches by non-financial institutions has yet been enacted. The Identity Theft Enforcement and Restitution Act, which would allow victims of identity theft to be paid an amount equal to the value of the time reasonably spent by the victims in an attempt to remediate the harm incurred, has progressed the furthest, but has not yet passed both houses of Congress. The Personal Data Privacy and Security Act of 2007 takes a more comprehensive approach to data protection by requiring non-financial businesses to develop and implement administrative, technical, and physical safeguards (i.e., a security program) to protect the security of sensitive PII. Similar to the state data breach notification statutes, the Personal Data Privacy and Security Act of 2007 relies upon encryption (as well as redaction) to protect PII. The proposed legislation provides penalties of up to $5,000 per day a company is in violation of the security program requirements, up to a total of $500,000 per violation (doubled in cases of willful violations). State attorneys general are also provided the right to bring a civil action on behalf of affected state residents against any business in violation of the security program requirements for up to $5,000 per day a company is in violation, up to a total of $500,000 per violation.

As can be discerned from the previous discussion, individuals who have had their PII exposed have little legal recourse, other than expecting to receive notification of the breach that exposed the data. Unfortunately, current United States privacy laws do not provide an alternate path of protection.

**The Limited Role of Privacy Protection in the United States**

There are three primary sources of privacy law in the United States: a common law right to privacy; a constitutional right to privacy inferred from the Fourth Amendment; and specific federal privacy statutes. Although exposure of PII as a result of a private-entity data breach does not infringe constitutional rights, the constitutional right to privacy informs the overall approach to legal protections of privacy in the United States. As discussed below, the evolution of the right to privacy
in the United States does not incorporate PII, and the federal privacy laws so far enacted only address specific types of data and are often not applicable to exposures of PII.

The Common Law Right to Privacy

The origins of privacy protection in the United States hark back to 1890, when Samuel Warren and Louis Brandeis published their seminal work, The Right to Privacy, recognizing a “right to be let alone[,]” enforceable through legal protection from “injurious disclosures as to private matters.” Legend has it that the impetus for The Right to Privacy was Warren’s dismay from reading about his daughter’s wedding in the newspaper. In particular, Warren and Brandeis expressed concern not only over the aggressive activities of the press, but their accompanying technology as well. They argued for “a principle which may be invoked to protect the privacy of the individual from invasion either by the too enterprising press, the photographer, or the possessor of any other modern device for recording or reproducing scenes or sounds.” “Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that ‘what is whispered in the closet shall be proclaimed from the house-tops.’”

But to create a legal protection from public invasions of privacy, Warren and Brandeis shifted the privacy argument in the United States from an already established body of law that protected privacy based on confidentiality. A confidential relationship requires just that—a relationship (either through contract, trust, or both). Warren and Brandeis noted, for example, that the photographic arts once required the subject to “sit” for a portrait; therefore the law of contract or trust would protect against improper circulation of the portrait. But by the late 1800’s, instantaneous photography allowed for surreptitious photographs, eliminating any sort of relationship between the photographer and the subject. Coupled with an expanding press, Warren and Brandeis were most concerned with a law that would prevent “injurious disclosures as to private matters” in circumstances where there was no relationship between the parties. For Warren and Brandeis, this type of privacy did not arise “from contract or from special trust, but are rights as against the world.”

By the mid-twentieth century, based in large part on Warren and Brandeis’ The Right to Privacy, the majority of states recognized a common law right to privacy. In 1960, Prosser identified four distinct types of invasion of privacy recognized by the courts: (1) intrusion upon seclusion; (2) public disclosure of embarrassing private facts; (3) publicity which places a person in a false light in the public eye; and (4) commercial appropriation of a person’s name or likeness. But an additional requirement had become ingrained in the first three types of invasion of privacy—highly offensive conduct.

Perhaps the tone was originally set in what is generally recognized as the first reported case recognizing a right to privacy. In De May v. Roberts, a doctor allowed an unmarried man with no medical training to be present when a woman gave birth. Given circumstances approximating an intrusion upon seclusion, the De May court acknowledged the woman’s right to privacy during “a most sacred” occasion, ruling “[i]t would be shocking to our sense of right, justice and propriety to doubt even but that for such an act the law would afford an ample remedy.” Or perhaps the tone was set by Warren and Brandeis when they limited protection to “those persons with whose affairs the community has no legitimate concern,” to prevent them “from being dragged into an undesirable and undesired publicity …”. This tone was reflected in the later case of Melvin v. Reid (involving public disclosure of private facts), in which a former prostitute and murder defendant who had abandoned her “life of shame,” married, and led a life in “respectable society” which was unaware of her past was facing the publication of these facts. Expressing a similar sentiment as the De May court, the California Court of Appeal held that the publication “of the unsavory incidents in the past life of [the woman] after she had reformed, coupled with her true name, was not justified by any standard of morals or ethics known to …” the court.

The modern application of intrusion upon seclusion occurs when someone “intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs …, if the intrusion would be highly offensive to a reasonable person.” Similarly, the publication of private facts is an invasion of privacy “if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.” This type of invasion recognizes the difference between a “shrinking soul who is abnormally sensitive about … publicity” and “details of sexual relations spread before the public gaze, …” or highly personal portrayals of intimate private conduct. Indeed, Prosser speculates that as this type of invasion has developed, Warren would not have had an actionable claim of invasion of privacy regarding the newspaper accounts which gave rise to his co-authoring The Right of Privacy. Finally, false light invasion of privacy is not actionable unless “the false light in which the other was placed would be highly offensive to a reasonable person.”

United States privacy law is based on a paradigm that understands privacy as protecting against highly offensive invasions into a person’s private world. As such, it does little to protect against the collection, use, and dissemination of PII. For example, in Dwyer v. American Express Company, the Appellate Court of Illinois ruled that renting transaction information based on credit card holders’ purchases was not an unauthorized intrusion or prying into the plaintiffs’ seclusion. The court stated that “[b]y using the [credit] card, a cardholder is voluntarily, and necessarily, giving information to defendants that, if analyzed, will reveal a cardholder’s spending habits and shopping preferences.” The Dwyer court refused to “hold that a defendant has committed an unauthorized intrusion by compiling the information voluntarily given to it and then renting its compilation.”
In addition, the collection of PII would not be considered a highly offensive intrusion upon seclusion because “[e]ach particular instance of collection is often small and innocuous.” Although “the danger is created by the aggregation of information, a state of affairs typically created by hundreds of actors over a long period of time,” Dwyer represents the courts’ approach in focusing on how the information is collected rather than how it is used. And when a court does examine sharing PII data, it trivializes the consequences. For example, in Shibley v. Time, Inc., the Court of Appeals of Ohio concluded “the right of privacy does not extend to the mailbox[,]” relying on a Federal District Court’s admonition: “The mailbox, however noxious its advertising contents often seem to judges as well as other people, is hardly the kind of enclave that requires constitutional defense to protect ‘the privacies of life.’”

Distribution of PII also does not fit within the parameters of invasion of privacy from the public exposure of embarrassing private facts. This type of invasion “appears designed to redress excesses of the press, and is accordingly focused on the widespread dissemination of personal information.” In addition, as noted above, this invasion of privacy is concerned with public disclosure of highly personal portrayals of intimate private conduct. Finally, invasion of privacy from public disclosure requires private facts. “Even if marketers disclosed information widely to the public, … some marketing data may be deemed public record, or a plaintiff, by furnishing data in the first place, may be deemed to have assented to its public dissemination.” “Certainly no one can complain when publicity is given to information about which he himself leaves open to the public eye.” For similar reasons, dissemination of PII would not constitute a “false light” invasion, as the disclosure would most likely not be considered highly offensive. “False light protect one’s reputation, but the type of information collected in databases often is not harmful to one’s reputation.”

The fourth type of invasion, commercial appropriation of a person’s name or likeness, “is designed to protect a person from having his name or image used for commercial purposes without consent.” But the value of individual transaction or demographic data is found in the aggregation of data, and that does not deprive an individual of any value his or her individual information may possess.

However, when the social networking Internet site Facebook implemented a new marketing technique in 2007 known as Beacon, it may have done so in a way that illegally appropriated the names and likenesses of its members. The key element of a social networking site (such as Facebook) is that individuals can share information with their friends (who are also members of the site). In late 2007, many Facebook members reportedly did not notice a small alert notifying them that their transactions on certain e-commerce sites would be broadcast to their Facebook friends (unless they selected on option preventing the broadcast). In addition, companies using this feature could also display the Facebook member’s photograph next to the purchase information. It is arguable that with an allegedly difficult to exercise “opt-out” feature (i.e., where members had to affirmatively select that information not be shared), Facebook and its e-commerce affiliates invaded Facebook members’ privacy by using their names and likenesses for commercial purposes.

The Constitutional Right to Privacy

While the focus of this paper is the collection, use, and dissemination of PII by private entities, restrictions on government access to information, via a constitutional right to privacy, inform the discussion. Although the U.S. Supreme Court had previously ruled that sealed letters and private papers were subject to Fourth Amendment warrant requirements, when it encountered its first electronic wiretapping case, it ruled telephone conversations were outside the Fourth Amendment’s warrant requirement. The Fourth Amendment’s language refers to seizing people or things, or searching places. Since there was no entry, no search, and no seizure, the Supreme Court initially ruled that telephone conversations were outside the Fourth Amendment’s warrant requirement.

Recognizing that one’s subjective expectation of privacy, reasonable under the circumstances, determines the extent of privacy protection, the Supreme Court reversed itself in Katz v. United States. In Katz, the Court held that the government’s activities in electronically listening to and recording an individual’s words violated the privacy upon which he justifiably relied while using a telephone booth, resulting in a “search and seizure” within the meaning of the Fourth Amendment. Foretelling its principal approach to United States privacy protection, the Katz Court stated that “[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection[,] … [b]ut what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.” Privacy in America is about reasonable expectations of keeping information secret.

This approach has been specifically applied, as to Fourth Amendment warrant requirements, to records maintained by third parties. For example, in Smith v. Maryland, the Supreme Court ruled that the state of Maryland did not need a warrant to install a pen register on a person’s home telephone line which recorded the phone numbers dialed from the telephone line, but not the actual conversations that took place. The Court concluded phone customers have no legitimate expectation of privacy in the phone numbers they dial because that information is transmitted to the phone company, which uses and records that information for a number of legitimate business purposes. And at least one court, following Smith v. Maryland, has ruled that using a “mirror port” (analogous to a pen register) to obtain from a criminal suspect’s Internet Service Provider account to/from addresses of e-mail messages, the Internet protocol (“IP”) addresses of websites visited, and the total volume of information transmitted to or from the account, is not a Fourth Amendment search.
The U.S. Supreme Court has also limited privacy rights in records maintained by third parties. In *United States v. Miller*, the subject of a tax evasion investigation (Miller) tried to prevent the government from using his bank records in the investigation. The Supreme Court concluded that Miller had no privacy interest in his bank records because they were not his personal papers which he did not own or possess—they were the business records of the bank. As a general matter, the U.S. Supreme Court has concluded “that when we convey information to a third party, we give up all constitutionally protected privacy in that information, for we assume the risk that the third party might relay it to others.” And following *United States v. Miller and Smith v. Maryland*, the federal courts have adopted the position that “subscriber information provided to an internet provider is not protected by the Fourth Amendment’s privacy expectation.”

**Federal Privacy Laws**

Based on the fear of the growth of databases by the federal government in the 1960’s and 1970’s, Congress passed the Privacy Act, which regulates the collection and use of records by federal agencies. While the Privacy Act, on its face, appears to provide broad privacy protection—giving individuals the right to access and correct information about themselves held by federal agencies, and restricting the use of information by federal agencies only for relevant and necessary purposes—in reality, its exceptions provide minimal protections: it only applies to federal (not state or local) agencies; information can be disclosed to law enforcement entities and consumer reporting agencies; and information may be disclosed for any “routine use” that is “compatible” with the purpose for which the agency collected the information. The routine use exception is a significant loophole which has done little to bar external disclosure of personal information.

A principal method in which Web pages track user browsing is through cookies—files stored by Web sites on users’ computers. For example, DoubleClick, Inc., a company which specializes in collecting, compiling, and analyzing information about Internet users, uses cookies to create profiles of users in order to place customized advertisements in the Web pages they visit. In a class action lawsuit against DoubleClick alleging invasions of privacy through the use of cookies, the plaintiffs alleged DoubleClick was violating Title II of the Electronic Communications Privacy Act (ECPA). The ECPA creates both criminal sanctions and a civil right of action against persons who gain unauthorized access to communications facilities and thereby access electronic communications stored incident to their transmission. The plaintiffs alleged DoubleClick violated Title II because placing cookies on the plaintiffs’ computer hard drives constituted unauthorized access.

However, DoubleClick’s cookies only collect information concerning users’ activities on DoubleClick-affiliated Web sites. Therefore, the court’s focus was not on DoubleClick’s access of cookies on users’ computers, but whether the affiliated Web sites authorized DoubleClick to access those communications. And the court found it implausible that DoubleClick’s affiliated Web sites would not authorize DoubleClick to access information collected as a result of that affiliation.

Ultimately, though, the court determined that authorization was not even needed, as the communications at issue were outside the scope of Title II of the ECPA. Reviewing the legislative history of the Act, the court determined that Congress’ intent in passing Title II was “to protect communications held in interim storage by electronic communication service providers.” The court ruled that since DoubleClick’s cookies remained on users’ computers indefinitely, they “are never in ‘electronic storage’ under the ECPA, [and therefore] are not protected by Title II.”

There are a scattering of federal privacy laws that do provide some privacy protection related to data collection. However, these privacy laws miss a vast amount of data stored by merchants and various businesses, and, in particular, they often apply only to various types of information based on the particular types of third parties that possess them rather than on the types of information themselves.

As can be discerned from the above discussion, there is very little legal protection against the collection and dissemination of PII. Common and constitutional laws for the most part permit, rather than restrict, the collection and use of PII. The few privacy-related statutes are narrow in scope. In addition, state data breach notification laws do no more than require that victims of unauthorized disclosure of their personal information be notified of that disclosure. The next issue to be addressed is to what degree to collectors of PII, particularly on the Internet, agree to safeguard PII.

**Privacy Policies**

A privacy policy is a document in which a company discloses the manner in which it deals with the personal identifying information of its customers and other website visitors. Although brick and mortar establishments often draft privacy policies, the e-commerce world has made them famous. In today’s e-commerce arena, it is common for most legitimate e-commerce companies to post their privacy policies on their websites. Privacy policies are generally stand-alone documents but vary in their overall look and feel because there is no industry standard and no federal or state law requiring uniformity.

In theory, privacy policies should serve as a sustainable intermediary between a company and its visitors detailing the specifics of a particular e-commerce relationship. Through its policy, a company could accurately describe the
collection, storage and uses of PII. In addition, policies go a long way to prove to website visitors that the company takes their PII very seriously and that the company has taken the time to think through its personal information practices. Along those same lines, visitors could click on a privacy policy link, read these disclosures and surf the Web accordingly. This communication between company and customer was supposed to build trust and make individuals feel more comfortable when transacting business online. In reality, quite a different story emerged and the idealistic promise of privacy policies faded from memory.

Despite the ubiquity of privacy policies posted on e-commerce websites today, few Web surfers take them seriously; in fact, consumers rarely read or even look at the way particular companies handle PII. Exacerbating this problem is the fact that the vast majority of companies collect PII on their websites. Some of this information is collected actively through Web forms where visitors intentionally enter various pieces of PII such as names, addresses and credit card information. Other information is collected passively through technology such as cookies and Web beacons. These devices are able to collect information without notification to or knowledge of the person visiting the website. In addition, companies often reserve the right to amend their privacy policies at any time and have such amendment be binding on visitors who entered their PII under previous privacy terms. Other policies are unclear about whether privacy policy amendments are binding on visitors. Finally, many pieces of data collected online are at risk of being sold on the open market to one or more unrelated third parties—possibly including dangerous criminals. This section will next discuss each of these problems in more depth and then propose that privacy policies—if drafted differently and posted conspicuously—can reflect back to their idealistic promise and properly protect PII.

Privacy Policy Terms

Reading through many contemporary privacy policies leaves little doubt that lawyers skilled in drafting documents containing vague commitments, various loopholes, and versions of legalese were in charge of the creation process. A review of many of these documents reveals that too many of them obfuscate company privacy practices by: (1) containing boilerplate paragraphs; (2) using unnecessary legal words such as “herein” and “whereas;” (3) presenting rather simple PII concepts in a complicated manner; and (4) possessing other non-readability issues such as inconspicuous links and small font. With such a policy looming on the screen, it would take a brave consumer to delve into a company’s PII collection practices.

Encouragingly, some companies have begun to buck this trend and create more readable privacy policies—statements that use simple words and subheadings to guide the reader through each of the company’s practices. The most current trend in policy creation occurs in the form of a multi-layered privacy policy. Multi-layered policies come in at least two stages (layers), beginning with a summary of policy terms in the first layer and followed by the full privacy policy in the second layer. Some tri-layered policies begin with a one- or two-sentence policy statement intended for a small screen such as a cellular phone and are followed by the second, summary level, and the third, full policy level. The idea behind these types of statements is that readers will take the time to look at a clear and short summary concerning the way a company handles its PII and that a glance is better than no glance at all. Additionally, companies that choose to create a multi-layered policy—it is not currently required by any state or federal law—are dedicated to increasing the clarity and readability of their privacy statements, will take more time in the drafting process, and, in the end, create more visitor trust.

However, even though a few companies have committed to these simpler policies, studies continue to show that only the most diligent consumers actually understand the policy terms. At the same time, consumers continue to submit PII to websites in exchange for valuable products and services; in fact, most websites will not allow access to any product or service without the exchange of valuable PII. This situation results in a dilemma where a consumer does not want to/cannot understand the way that PII will be handled but, at the same time, strongly desires to use the website in the manner in which it was intended to be used. Companies understand this dilemma and, therefore, condition website participation on PII submission without fearing visitor defection. At the end of the day, the language and structure of privacy policies must improve before visitors will take them seriously and visitors must take them seriously because of the serious threats to their PII in cyberspace.

Privacy Policy Posting

Companies do not want to waste valuable homepage space on privacy policies themselves and so they generally place a link to their policy on the homepage. This is an acceptable compromise because homepages are valuable Web real estate and should be utilized in the most effective manner possible. However, some companies abandon this compromise and are reluctant to post a conspicuous link to their privacy policy on their homepages. Other companies force users to click on numerous links before they even arrive at the actual privacy policy statement. Evidence demonstrates that visitors—even if they want to be diligent in determining what will happen to their PII—will not take the time to scan a webpage over and over in search of privacy information that does not really interest them in the first place. Privacy policies should be
conspicuously-linked on a company’s homepage. This requires a link on a company’s homepage which is clearly labeled with the word “privacy” and which appears in a font no smaller than the average link size on the homepage.

Privacy Policy Amendments

Intelligent lawyers encourage clients to leave some wiggle room in company policies. This wiggle room allows the company to be flexible and implement policy changes without having to pay the expenses associated with notification and consent. Unfortunately, such flexibility comes with a cost to consumers in the form of decreased protection of their PII. In the case of information privacy, much wiggle room has been created and exploited in contemporary privacy policies. In such policies, companies generally reserve the right to amend the policy at any time and without much in the way of notice. These amendments are then made binding on all website visitors regardless of when they visited in the past and regardless of when they entered their PII.

For example, AT&T recently revised its privacy policy for its television and Internet services to state that PII collected by the company is now considered property of AT&T as part of its business records. The new policy terms also require visitors to agree to the revised policy before they proceed on the website or use AT&T services. Future amendments are always a possibility as the company continues to reserve the right to change its privacy terms without any prominent notice unless the new terms are material or involve using PII in a materially different manner than for which it was collected. If the change is material then the company promises to “attempt” to notify individuals within 30 days and provide a prominent notice on its website; if the notice is successful, individuals uninterested in having their PII utilized in the new manner will be given a choice as to whether to consent to the new PII use. On a more positive note, the new policy does state that the company does not “provide personal identifying information (other than information included in our directories and directory assistance service) to third parties for the marketing of their products and services without your consent.” Companies should be allowed to amend their privacy policies as times change but visitors should be notified via email and each amendment should be disclaimed prominently and its implications explained in plain English on a company’s privacy policy document.

External Sharing of PII

PII is a valuable commodity. Companies collect such information at a very low cost in terms of time and money and can sell the information with the same efficiency. In fact, an entire data brokerage industry has sprung up around such data sales. External PII transfers raise some very serious threats. First, once data is disseminated outside of the possession of the individual it identifies and its collector it becomes virtually irretrievable. Once released into cyberspace, PII can be used to commit cybercrimes from across the globe. Second, it is very difficult for sellers to properly identify buyers and the intentions of such buyers. This difficulty makes it very likely that data may fall into the hands of bad actors with merely the click of a mouse. This situation was exemplified when ChoicePoint—one of the country’s largest data brokers—discovered that it had sold over 165,000 pieces of PII to criminals posing as legitimate businesses. Finally, PII sharing can be done at a very low cost in terms of time and money. This removes one incentive for businesses to actively monitor their data transactions. In fact, companies are incentivized to sell PII on the open market to generate additional low-cost revenue streams.

Companies should disclosure their external PII sharing practices in a privacy policy. This will allow visitors to properly undertake an analysis of whether it is wise to submit various pieces of PII.

A Proposal for a Model Personal Identifying Information Statute

Unfortunately for privacy advocates and consumers in general, it is much easier to identify the serious threats associated with the collection, storage, use and dissemination of PII than it is to motivate Congress to target these threats via specific PII legislation. This final section proposes a model federal law dealing specifically with personal identifying information (Model Law) and presents a useful start in the Congressional-encouragement process. At its core, the Model Law is designed to prevent the major threats identified throughout this article and, at the same time, increase consumer confidence in the security and privacy of the PII they increasingly submit online.

Companies Must Be Forced to Draft Privacy Policies Designed To Protect PII

Despite their well-deserved bad rap, privacy policies can be effective tools in the quest to protect PII. Recall that the purpose behind the first e-commerce privacy policies was to inform consumers about a company’s practices regarding personal identifying information. However, because companies have not been legally required to draft policies in a manner that serves this purpose, contemporary policies began to obfuscate privacy practices, proliferate with legalese and, at the end of the day, cause consumers to dread even the thought of skimming through this important information.
The Model Law can claim a poll position in protecting PII by targeting privacy policies for regulation because companies have become accustomed to drafting and posting privacy policies, and because consumers have become accustomed to, at the least, seeing a link to such policies. The idea is that, once privacy policies come into compliance with the Model Law and begin to accurately and clearly describe a company’s PII practices, consumers will be encouraged to read the information and take more responsibility before submitting their information online. With this in mind, any law targeting personal information online should utilize the potential of privacy policies as a threat-reducing tool. To accomplish this mission, the Model Law requires companies to adhere to the following guidelines to create compliant privacy policies:

1. **DRAFTING**—Plain English is a must;
2. **POSTING**—a conspicuously-linked privacy policy is key;
3. **AMENDMENTS**—companies must adequately disclose all material privacy policy changes; and
4. **DESCRIBE KEY PRIVACY PRACTICES**—full and accurate disclosure must be made in the areas of PII collection, protection/storage, use, and sharing.

An important caveat is that this Model Law does not require companies to adopt specific privacy practices or to place specific language in the privacy policies it regulates (Covered Policies). Instead, the Model Law only requires that companies cover two bases in their privacy policies: (1) Covered Policies must clearly discuss particular areas especially relevant to PII protection (drafting, posting, amendments and key privacy practices); and (2) Covered Policies must disclose all privacy practices clearly and accurately.

Other than these requirements, companies will remain free to experiment with the most effective manner of collecting, utilizing and sharing PII for their e-commerce environment. For example, visitors in the online arena surf the World Wide Web for vastly different purposes and engage in many different types of transactions. A law that requires specific and standardized policy terms will be unable to cover each of these unique needs and will take away a company’s freedom to experiment with efficient and effective forms of e-commerce. More specifically, the reason content regulations are omitted from the Model Law is that a particular requirement stating, for example, that a company can only collect certain types of PII from certain types of people or forbidding a company from selling PII externally would excessively burden e-commerce efficiency without providing significant additional benefits as those found in a less-restrictive regulation.

Instead of over-regulating in this area, companies forced by law to comply with each of the four requirements listed above will now be required to clearly and accurately inform consumers of each of their privacy practices. In turn, these newly informed consumers will begin to be able to read privacy policies and decipher whether their PII will be properly cared for and protected by specific websites. In the process, because companies remain relatively free to determine the specific content of their policy, consumers are forced to take some form of personal responsibility for their actions online and must examine such policies and then choose whether a website is worthy to receive their PII. In the end, the Model Law presents the proper balance between e-commerce efficiency and an individual’s personal information privacy. The following sections discuss the required privacy policy elements of the Model Law in more detail.

**Drafting**

The Model Law requires that covered policies be drafted in Plain English. The Plain English concept has found its niche in the world of securities regulation and requires clarity in prose and content in written materials disclosing securities information to the general public. It is important to understand that compliant Plain English documents submitted to the Securities and Exchange Commission are neither dumbed-down versions of what a company intends to disclose nor are they missing complex policy terms important to a transaction. Instead, the concept of Plain English means analyzing and deciding what information investors need to make informed decisions, before words, sentences, or paragraphs are considered. A plain English document uses words economically and at a level the audience can understand. Its sentence structure is tight. Its tone is welcoming and direct. Its design is visually appealing. A plain English document is easy to read and looks like it’s meant to be read.

The provisions in this section of the Model Law require covered companies to make a deliberate attempt to draft their privacy policies to avoid:

1. Long sentences;
2. Passive voice;
3. Weak verbs;
4. Superfluous words;
5. Legal and financial jargon;
6. Numerous defined terms;
7. Abstract words;
8. Unnecessary details; and
9. Unreadable design and layout.
Although many of these requirements are subjective, it will be easy for a court or the Federal Trade Commission to analyze a company’s intent in the drafting process by merely reading the policy itself and seeking a basic understanding of privacy practices.

Posting

Second, the Model Law requires Covered Policies to be: (1) posted conspicuously in a full-text version somewhere on a company’s website; AND (2) conspicuously linked from a company’s homepage. As discussed previously, a company’s homepage is valuable real estate and not meant to contain the entire text of a privacy policy. Any legal requirement that a homepage must contain the full text of a privacy policy is too restrictive. However, this space is not too valuable to allow a company to neglect the posting of a conspicuous link to its privacy policy.

The most important aspect of this part of the Model Law is the requirement that a company place a conspicuous link to its privacy policy on its homepage. A link is conspicuous if it is located anywhere on a company’s homepage and posted in at least the same font style and size as any surrounding links. This requirement will stop companies from the common practice of omitting such a link from the homepage altogether or locating a policy link at the very bottom of a homepage in a font size smaller than anything important that is posted nearby. Website visitors will soon become accustomed to the fact that a privacy policy exists, understand that it will be linked somewhere on the homepage, and, because of the other requirements of the Model Law, begin to feel comfortable reading through the policy itself.

Amendments

Third, the Model Law requires all Covered Policies to properly notify consumers about any material privacy policy amendment. Too often, companies reserve the right to amend their privacy policies either without notifying existing customers at all or via notification occurring only through the amended policy itself. Neither of these options is acceptable in an e-commerce environment where people do not read privacy policies in the first place and where these same people are extremely unlikely to look at privacy policies for any amendments. Making matters worse, companies often claim that policy amendments are binding on all users—past and present—when posted and regardless of the fact that no notice has been provided.

Proper notification is the key to this part of the Model Law. Too often companies only post changes in the revised privacy policy itself and expect consumers to look often for any changes that affect their PII. The requirements of the Model Law are more stringent and require a company to make a serious attempt to notify anyone who has submitted PII electronically of material policy changes via e-mail. For those people who cannot be notified via email (i.e., because of an invalid e-mail address) the company must include a prominent statement that its privacy policy has been modified on its homepage. Regardless of how notice is communicated, the modified privacy policy itself must show exactly where the amendments have been made and then explain what the material changes mean. This homepage notice and explanatory information must remain in place for six consecutive months after each material policy amendment.

Key Privacy Practices

Fourth, the Model Law requires that Covered Policies include information about a company’s key PII practices in the areas of: (1) collection; (2) storage/protection; (3) use; and (4) dissemination. As stated previously, it is excessively burdensome for the law to require specific PII practices from companies offering products and services in multifarious arenas. Consumers should possess at least some of the responsibility for learning as much as they can about any website that requires their PII submissions. This knowledge cannot occur, however, unless companies are required to provide information regarding crucial privacy practices in crucial areas.

Therefore, as an initial matter, a company’s privacy policy must discuss how PII is collected. In this section, a company must disclose whether it collects information passively—via cookies or web beacons—and/or actively—via web forms. Policies must briefly describe what it means by passive and active collection and detail which types of information are collected by each method. If a company does not collect PII passively, for instance, then its privacy policy must disclose this fact.

Second, a company’s privacy policy must discuss how PII is stored upon collection. An important part of these storage disclosures is how a company protects the information from bad actors and data theft. Here, the Model Law requires companies to disclose the type of storage device on which PII is stored as well as the electronic protections governing these devices. The next major section in this part will discuss further the detailed protections of the Model Law regarding the protection of PII against data theft.

Third, a company’s privacy policy must disclose how the company will use the PII—both internally and externally. Under the Model Law, companies are allowed to use PII for any legal purpose but must disclose these purposes clearly and accurately.
Finally, Covered Policies must disclose how a company disseminates PII: (1) internally; (2) among company affiliates; and (3) to unrelated third parties. Dissemination of PII is a process whereby collected information leaves the hands of its initial collector and enters the vast realm of cyberspace. Purchasers of such information can be individuals or corporations and can theoretically come from any corner of the globe that has an Internet connection. The largest threat looming with dissemination is that, once PII is disseminated, it is extremely difficult—if not impossible—to control. Therefore, the Model Law requires that companies: (1) detail the types of PII it sells (i.e., phone numbers, addresses, etc.); and (2) disclose the types of parties to whom the information is sold (i.e., only to companies that promise to protect it or to anyone interested in such a purchase). Through this disclosure, Website visitors will be able to determine where their PII might be headed and choose whether the risk of submission is worth the benefit that the Website provides.

Disclosing how PII is collected, for what purpose, and how it may be disseminated is only one aspect of protection. As noted above, equally important is how PII is protected once it is collected.

Data Breaches: Notification and Prevention

For non-financial Web-based activities and transactions there are no direct legal restrictions on what companies can do with the PII they collect—particularly the manner in which PII is stored. Though nearly all the states have enacted data breach notification laws which promote data encryption, companies are only obligated to notify individuals if their unencrypted PII has been the subject of an unauthorized disclosure. Otherwise, there are minimal requirements that businesses protect PII.

In the meantime, however, it is clear more comprehensive legislation needs to be adopted to encourage companies to provide and follow consistent, meaningful privacy policies, as well as provide stronger protection to consumers when their unencrypted PII is exposed through data breaches. Considering that notification need only be provided when PII is unencrypted, given the number of data breaches that are being disclosed, at a minimum, on a weekly basis, entities that collect PII are not extensively using encryption.

A data protection program that effectively protects PII from unauthorized disclosure must include:
1. A design that protects against anticipated threats of unauthorized disclosure;
2. Continual risk assessment and control;
3. Vulnerability testing and modernization; and

This is the approach the federal government is beginning to pursue, through proposed legislation and enforcement actions by the Federal Trade Commission (FTC).

Senate Bill 495, the Personal Data Privacy and Security Act of 2007, adopts the above-described approach. While S. 495 has yet to be passed by Congress, the FTC has adopted a similar approach in actions against companies that have been the subject of data breaches. For example, in the matter of Life is good, Inc., the FTC brought a complaint against the company alleging it failed to provide reasonable and appropriate security for the consumer information stored on its network, including credit card numbers, expiration dates, and security codes. In particular, the Life is good privacy policy stated PII was stored in a secure file when, in fact, it was stored in clear, readable text.

In a consent agreement, Life is good, Inc. agreed to establish, implement, and maintain a fully documented comprehensive information security program reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about its consumers. Implementation and maintenance of the security program requires Life is good to: (1) designate an employee or employees to coordinate the information security program; (2) identify internal and external risks to the security and confidentiality of personal information and assess the safeguards already in place; (3) design and implement safeguards to control the risks identified in the risk assessment and monitor their effectiveness; (4) develop reasonable steps to select and oversee service providers that handle the personal information of Life is good customers; and (5) evaluate and adjust its information-security program to reflect the results of monitoring, any material changes to the company’s operations, or other circumstances that may impact the effectiveness of its security program.

The FTC has brought similar actions, and reached similar agreements, with three additional businesses, Goal Financial, LLP, Reed Elsevier, Inc., and TJX. These actions by the FTC and the proposed Personal Data Privacy and Security Act of 2007 provide a blueprint for the type of security programs companies need to implement to protect PII.

The one element missing in the FTC complaints and agreements, but included in the Personal Data Privacy and Security Act of 2007, are penalties for non-compliance. The FTC’s approach to ensuring ongoing compliance with the security program requirements is to require biennial assessment by a third-party professional for 20 years. In contrast, the Personal Data Privacy and Security Act of 2007 imposes a fine of up to $500,000 for failure to comply with the Act’s security program requirements, as well as allowing state attorneys general to bring civil suits on behalf affected citizens, up to a maximum of $500,000.

While a $500,000 fine could arguably be a significant incentive for smaller companies to implement adequate security measures to protect PII, recent evidence suggests that it may be somewhat insignificant for larger companies. For example, TJX initially set aside nearly $200 million for the costs associated with what it termed the “Computer Intrusion.”
And that is the estimated approximate cost required to settle the incident with the various parties involved.\textsuperscript{221} TJX’s data breach appears to have been a financial non-event; its sales remained strong and its stock price remained steady despite the data breach, implying that its costs associated with the breach will not be a significant drag on its earnings.\textsuperscript{222} TJX may stand for the proposition that maximum fines should be structured to take into account not only the size of the data breach but also the relative financial strength of the company in violation of the security program requirements.

**Conclusion**

Current laws do not favor consumers who are trying to limit the collection, use, dissemination, and misuse of their PII. Victims of data breaches have no cause of action unless they can show direct losses as a result of unauthorized use of their PII, while data breach notification laws only indirectly encourage encryption of data. Privacy laws are also not well-suited to PII.

Better privacy policies can lead to more visitor awareness of PII-handling practices. Better awareness of PII-handling practices can lead to visitors being more careful before submitting PII to websites that may not protect it adequately or that may sell it on the open market. This type of privacy-protective behavior could give companies more of an incentive to protect PII in order to maintain business that would be lost under their current privacy regimes.

Ultimately, companies must design, implement, and maintain adequate security programs to protect PII. Based on the continuous reports of data breaches, companies have yet to be properly “incentivized” to implement such programs. The FTC has made a start with its recent agreements with companies that have had data breaches. Eventually, Congress must pass legislation at least based on the approaches found in the Personal Data Privacy and Security Act of 2007. This Act would not only continue the data breach notification requirements already in place in most states, but also mandate adequate security programs—and include the fines necessary to give companies the proper incentive to put those program in place.

**Footnotes**

4. See, e.g., Edmund L. Andrews, *U.S.-European Union Talks on Privacy are Sputtering*, N.Y. TIMES, May 27, 1999, at C6 (stating that “European authorities continue to insist that the United States fails to provide enough consumer protection from companies that collect and often re-sell personal information.”); and Saul Hansell, *Big Web Sites To Track Steps of Their Users*, N.Y. TIMES, Aug. 16, 1998, at A1 (stating that it “is not illegal for Internet services to sell personal information about their customers and there are few laws protecting consumers’ privacy in cyberspace.”).
5. See infra notes 57-90 and accompanying text, for a discussion of state security breach notification laws and proposed federal identity theft legislation.
6. See, e.g., Dan Mitchell, *Online Ads vs. Privacy*, N.Y. TIMES, May 12, 2007, at C5 (discussing the collection of PII as it relates to online advertising and stating, “To approach individuals with customized advertising, you have to know who they are. Or at least, you have to gather enough personal information about them that their identity could be easily figured out.”).
Cookies are pieces of information generated by a Web server and stored in the user’s computer, ready for future access. … Cookies were implemented to allow user-side customization of Web information. For example, cookies are used to personalize Web search engines, to allow users to participate in WWW-wide contests … and to store shopping lists of items a user has selected while browsing through a virtual shopping mall.

10 See, e.g., ABOUT IDENTITY THEFT, FED. TRADE COMM’N, at http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html (last visited May 19, 2008) (discussing identity theft and stating, “Identity theft occurs when someone uses your personally identifying information, like your name, Social Security number, or credit card number, without your permission, to commit fraud or other crimes.”). The Federal Trade Commission estimates that “as many as 9 million Americans have their identities stolen each year.” Id.


12 Solove, supra note 2, at 1394.


14 Solove, supra note 2, at 1410.

15 See id. at 1411.

16 Mary Madden et al., Digital Footprints: Online Identity Management and Search in the Age of Transparency, Pwinternet & American Life Project 2, Dec. 16, 2007, at http://www.pewinternet.org/pdfs/PIP_Digital_Footprints.pdf (describing the persistence of personal data trails online). Some digital footprints are “active,” traces of data contributed voluntarily, “often in specific contexts with specific audiences in mind[,]” id. at 4, while other digital footprints are “passive,” referring to “[P]ersonal data made accessible online with no deliberate intervention from an individual[,]” id. at 3.

17 See id. at 3. See also Ciocchetti, supra note 13, at 55 (describing how, for $29.95, he was able to obtain via e-mail in fifteen minutes a fairly comprehensive dossier on himself, including an extensive address history, past and present property ownership records, political party affiliation, and various information concerning his current neighbors and past relatives).


24 See Jaikumar Vijayan, Data Breach at TJX Leads to Fraudulent Card Use, COMPUTERWORLD, Jan. 25, 2007, at http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9009158 (reporting credit and debit cards compromised in the TJX security breach were being fraudulently used in several states in the U.S. and even overseas).


26 In re TJX Companies Retail Security Breach Litigation (Financial Institutions Track), Amended Consolidated Class Action Complaint, Master Docket No. 07-10162-WGY, filed Sept. 26, 2007. In a payment card transaction, an Acquiring Bank, such as Fifth Third, takes credit card transactions from the merchant (in this case TJX) and transmits them to the financial institution issuing the card (the “Issuing Bank”), such as Plaintiffs. Once the Issuing Bank authorizes payment, the Acquiring Bank credits the merchant’s account with the purchase price minus transaction fees. Id. at 5.

27 The PCI Data Security Standard is promulgated by the Security Standards Council to enhance payment account data security. See https://www.pcisecuritystandards.org/.
3.3 million American adults reported discovering the misuse of one or more of their existing store credit card approval process.

The survey also revealed that, in 2005, an additional 4.9 million Americans reported the misuse of their information limited to the misuse of one or more of their existing accounts were allegedly compromised during the in-store credit card approval process. See Clarke Canfield, *Supermarket Data Breach Still Unsolved*, MSNBC, March 18, 2008, at http://www.msnbc.msn.com/id/23698169/.


Id. at 639. See also Key v. DSW, Inc., 454 F. Supp. 2d 684, 689 (S.D. Ohio 2006) (summarizing cases that have held, in the identity theft context, that an alleged increase in risk of future injury is not an "actual or imminent" injury); Kahle v. Liton Loan Servicing, LP, 486 F. Supp. 2d 705, 710 (S.D. Ohio 2007) (holding same); Randolph v. ING Life Ins. & Annuity Co., 486 F. Supp. 2d 1, 7-8 (D. D.C. 2007) (dismissing plaintiffs’ complaint with prejudice; holding plaintiffs’ claim of having been placed at a substantial risk of harm in the form of identity theft due to defendant’s loss of computer containing plaintiff’s PII is only hypothetical or speculative harm and therefore not actionable); Middleton v. Kelly, ---F. Supp. 2d ---, 2008 U.S. Dist. LEXIS 25563, *2 (D. D.C. 2008) (holding same).


Id. at 195.

585 S.E.2d 275, 277 (S.C. 2003). But see Wolfe v. MBNA America Bank, 485 F. Supp. 2d 874, 882 (W.D. Tenn. 2007) (holding that under Tennessee negligence law, the defendant bank had a duty to verify the authenticity and accuracy of a credit account application before issuing a credit card in plaintiff’s name, where plaintiff was a customer of the defendant). See also generally Danielle Keats Citron, Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age, 80 S. CAL. L. REV. 241 (2007) (arguing for a strict-liability model to address the risks of data breaches); Michael L. Rustad & Thomas H. Koenig, The Tort of Negligent Enablement of Cybercrime, 20 BERKELEY TECH. L. J. 1553 (2005) (arguing for a tort of negligent enablement as a remedy for computer intrusions due to defective software).

568 S.E.2d 246 (N.C. App. 2006).

See id. at 251-52. See also Randi A.J. v. Long Island Surgi-Center, 842 N.Y.S.2d 558 (N.Y. App. Div. 2007) (holding medical center’s wrongfully disclosing confidential medical information to patient’s parents was sufficient to conclude center’s conduct amounted to recklessness, gross negligence and callousness, supporting punitive damages award).

See PRIVACY RIGHTS CLEARINGHOUSE at http://www.privacyrights.org/ar/CPResponse.htm. It is estimated that approximately 165,000 records were exposed in this particular data breach. See A Chronology of Data Breaches, supra note 19.

58 CAL. CIV. CODE §§ 1798.80—97 (West 2007).


59 CAL. CIV. CODE § 1798.80(b). Section 1798.80 was repealed and replaced by 2007 Cal. Legis. Serv. Ch. 699 (A.B. 1298) (West) on October 14, 2007, which expanded the law to include medical and health insurance information, at http://www.dhs.ca.gov/privacyoffice/LegUpdate/default.htm.

60 CAL. CIV. CODE § 1798.80(e).

61 Alabama, Alaska, Kentucky, Mississippi, Missouri, New Mexico, and South Dakota.

governmental and private data breaches have been numerous.

For example, LPL Financial, a Boston, Massachusetts-based company notified the Maryland Office of Attorney General of data breaches because some of the breached data concerned Maryland residents. See supra, notes 36-40 and accompanying text.

See, e.g., CAL. CIV. CODE § 1798.84(b) (providing a cause of action for damages for customers injured by a violation of the disclosure requirements of the statute).

Id.

District of Columbia and Wyoming.

Encryption is a method of scrambling data, which then requires a “key” to unscramble the data. See What is Encryption?, SEARCHSECURITY.COM DEFINITIONS, at http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci212062,00.html (last visiting May 21, 2008).


Or, as so eloquently phrased by the court, “Sometime before June 2007, private data on approximately 17,000 former and current Pfizer employees left the confines of a Pfizer hard drive and ventured into an unauthorized domain.” Id. at 794. Ponder was the original named plaintiff of a putative class of similarly situated plaintiffs; Terry Horne was subsequently substituted as the named plaintiff. See id. at 794, n.1.

See A Chronology of Data Breaches, supra note 19.


See supra note 1.

See also James H. Barron, Warren and Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193 (1890); Demystifying a Landmark Citation, 13 SUFFOLK U. L. REV. 875, 877 (1979) (noting near unanimity among courts and commentators that The Right to Privacy created the structural and jurisprudential foundation of the tort of invasion of privacy).

Warren & Brandeis, supra note 1, at 204.

See William L. Prosser, Privacy, 48 CAL. L. REV. 383, 383 (1960) (reporting that in a city and an era “in which a lady and a gentleman kept their names and their personal affairs out of the papers[,]” Warren became annoyed “when the newspapers had a field day on the occasion of the wedding of a daughter…”). But see Barron, supra note 91, at 893 (noting that Warren’s first daughter was only six years old in 1890, and speculating the newspaper story in question may have covered the wedding of one of Mrs. Warren’s cousins); Daniel J. Solove, The Future of Reputation 109 (2007) (discussing same).

Warren & Brandeis, supra note 1, at 206.

Id. at 195.

See id. at 132.

See Warren & Brandeis, supra note 1, at 211.

See id.

See id. at 204.

Id. at 213. See also Richards & Solove, supra note 96, at 132.

See Prosser, supra note 93, at 386-89.

See id. at 389.

9 N.W. 146 (1881).

Id. at 148-49.

Warren & Brandeis, supra note 1, at 214.

297 P. 91 (1931).

Id. at 93.


Prosser, supra note 93, at 397.

See id.

RESTATEMENT (SECOND) OF TORTS § 652E (1977). The fourth type of invasion, the commercial appropriation of a person’s name or likeness, applies when “one … appropriates to his own use or benefit the name or likeness of another ….” RESTATEMENT (SECOND) OF TORTS § 652C (1977).

See Solove, supra note 2, at 1431.


Id.

Id.

Solove, supra note 2, at 1432.

Id.

341 N.E.2d 337, 339 (1975) (holding the sale of “personality profiles” based on subscription lists is not an invasion of privacy).

Lamont v. Comm’r of Motor Vehicles, 269 F. Supp. 880, 883 (D.C.N.Y. 1967) (upholding the constitutionality of N.Y. VEH & TRAF LAW § 202(4) (McKinney 2008), authorizing the sale of copies of motor vehicle registration records by the Commissioner of Motor Vehicles). But see the Driver’s Privacy Protection Act of 1994, 18 U.S.C. §§ 2721-25 (2007), which prohibits states from selling driver’s license information without prior consent. However, prior consent actually means electing to “opt-out.” See, e.g., N.Y. VEH & TRAF LAW § 202(4)(b) (McKinney 2008) (allowing the sale of information unless a registrant requests the deletion of his or her information from the records to be sold).

See supra, notes 110-111 and accompanying text.

Solove, supra note 2, at 1433.

See supra, note 111 and accompanying text.

See supra, note 110 and accompanying text.

Solove, supra note 2, at 1433.

Prosser, supra note 93, at 394.

Solove, supra note 2, at 1433.

See supra, note 113.


See id. at 1356. See also Shibley v. Time, Inc., 341 N.E.2d 337, 339 (1975) (denying plaintiffs’ invasion of privacy claim arising from defendants’ alleged unjust enrichment by selling “personality profiles” based on plaintiffs’ data).


See Jesdanun, supra note 132.

Ex parte Jackson, 96 U.S. 727 (1877).


See id. at 464-65.


Id. at 353.

Id. at 351 (citations omitted).

Best Buy is changing its online privacy policy, allowing the company to combine customer information from its Web site with that collected in its stores.

... Best Buy spokeswoman Joy Harris said that combining online and offline data will help the company serve customers better. Already 40 percent of the company’s in-store customers research products through the BestBuy.com Web site, she said.

See, e.g., TRUSTe Online Privacy, supra note 162, at 6 ( “Posting a privacy statement online is the industry standard. Most Web sites now post an online privacy statement.”).

Privacy statements come in many shapes and sizes. There is no current industry standard in the online community about what privacy statements should look like. Some take the form of lengthy, downloadable
PDFs while others are simple disclaimers presented in a one-paragraph pop-up window. Every Web site is unique and a privacy statement must reflect a site’s unique data-handling and collection practices.

Id. at 3.

166 See, e.g., Hunton & Williams, Multi-Layered Notices Explained, CENTER FOR INFORMATION POLICY LEADERSHIP 2 [hereinafter Multi-Layered Notices] (discussing the importance of clarity in this e-commerce relationship and stating that the effect of today’s difficult-to-understand policies “has been to obscure the content that individuals need to know when making judgments about whom they will do business. This has been an impediment to on-line commerce.”).

167 If there is ever a place for such disclosure it is in a company’s self-titled privacy policy. See id. (stating that “[p]rivacy notices are the windows to how organizations collect, use, share, and protect the information that pertains to individuals.”).

168 See, e.g., TRUSTe Online Privacy, supra note 162, at 4 (“Privacy statements build consumer confidence. A privacy statement signals to consumers that a site respects their privacy concerns and has taken the time to evaluate its privacy practices and institute procedures to protect personal information.”).

169 See, e.g., Major R. Ken Pippin, Consumer Privacy on the Internet: It’s “Surfer Beware,” 47 A.F.L. REV. 125, 160 (1999) (providing advice to Web surfers on protecting their personal information online and stating that “consumers should read and understand a company’s privacy policy. If the web site fails to provide a privacy policy, consumers should be sensitive to the increased risks associated with transacting business on that site.”).

170 Consumer attitudes toward privacy issues have become tougher in recent years. Studies reveal that fewer people trust businesses to handle consumers’ personal information in an acceptable way. At the same time, fewer people put faith in existing laws to provide reasonable levels of privacy protection. Privacy statements help to allay consumer anxieties significantly.

TRUSTe Online Privacy, supra note 162, at 4 (internal citations omitted).

171 See, e.g., Ciocchetti, supra note 13, at 68-71 (discussing how contemporary privacy policies have failed to live up to their expectations).

172 See, e.g., Data Privacy: CDT’s 1997 Privacy Survey Results, CENTER FOR DEMOCRACY AND TECHNOLOGY, at http://www.cdt.org/privacy/survey/findings/results.shtml (last visited May 21, 2008) (providing a consumer survey dealing with online privacy). The survey included the question: “Did you check into your online service providers’ terms of service before signing up to see if they had rules to protect your privacy?” Based on this question, the survey revealed that less than one-half of the people surveyed responded that they did check into (i.e., look for and/or read) a privacy policy from their online service provider. Id. at http://www.cdt.org/privacy/survey/findings/graph2.html (last visited May 21, 2008).

173 See, e.g., Steelcase Privacy Policy: Active Information Collection, STEELCASE.COM, at http://www.steelcase.com/na/privacy_policy_cnav.aspx?f=10033 (last visited May 21, 2008). The Steelcase privacy policy displays a subheading titled “Active Information Collection” and describes the practice as follows:

At various points on this Site, you might choose to actively provide certain kinds of information, including personally identifiable information, such as full name, address, phone number, e-mail address, etc. The Site typically will indicate which information is required and which information is optional at the information collection point in question. In any case, by submitting information via an active information collection point at this Site, you specifically consent to the collection, use, and dissemination of such information in accordance with this Privacy Policy.

Id.

174 See, e.g., Apartments.com Privacy Statement, APARTMENTS.COM, http://www.apartments.com/privacy.htm (last visited May 21, 2008). The Apartments.com privacy policy displays a subheading titled “Passive Information Collection” and describes the practice as follows:

The Site automatically collects information and may also customize your visit through technical means, including the following:

- **Cookies:** Cookies are small text files that are placed on your computer’s hard drive by computers (or servers) to identify your computer.
- **Web Beacons:** Web beacons (also known as pixel tags, Internet tags, clear GIFs, or single-pixel GIFs) are electronic images embedded into a Web page.
- **IP Address Logs:** Apartments.com also logs Internet Protocol (IP) addresses—the location of your computer on the Internet.

Id. (emphasis in original).

175 See, e.g., Brian Quinton, Study: Users Don’t Understand, Can’t Delete Cookies, SEARCHONLINEINFO.COM, May 18, 2005, at http://searchlineinfo.com/InsightExpress_cookie_study/ (discussing various studies regarding how website visitors interact with and understand cookies and stating that “another study . . . finds . . . that consumers not only don’t get what cookies can do and how they work, but that many of the people who say they’re getting rid of cookies are not in fact successful at doing so.”).
If we decide to change our Privacy Policy, we will post those changes here so that you will always know what information we gather, how we might use that information and whether we will disclose it to anyone. All changes to this policy will be posted on our Web site prior to the time they take effect. **In the event that we make material changes to the way we use personally identifiable information, affected consumers will be notified via e-mail and will be given the opportunity to opt-out.**

(emphasis added). An opt-out choice would not be necessary if such amendments were not binding.

**See, e.g., Privacy Policy: Amendments, BUSINESSWORLD ONLINE, at http://www.businessworldonline.com/assets/main.php?id=privacypolicy (last visited May 21, 2008)** (discussing amendments to its privacy policy in the following, rather unclear, manner: “As changing circumstances may require the revision of this Privacy Policy, we encourage our users to check our Privacy Policy from time to time.”).

**See, e.g., Jonathan Krin, Online Data Gets Personal: Cell Phone Records for Sale, WASH. POST, June 8, 2005, at D1 (discussing the sale of personal identifying information):**

A tool long used by law enforcement and private investigators to help locate criminals or debt-skippers, phone records are a part of the sea of personal data routinely bought and sold online in an Internet-driven, I-can-find-out-anything-about-you world. Legal experts say many of the methods for acquiring such information are illegal, but they receive scant attention from authorities.

In addition, “[s]uch records could be used by criminals, such as stalkers or abusive spouses trying to find victims.” *Id.*

**See, e.g., Lost in the Fine Print: Readability of Financial Privacy Notices, PRIVACY RIGHTS CLEARINGHOUSE, July 1, 2001, at http://www.privacyrights.org/arb/GBL-Reading.htm [hereinafter Lost in the Fine Print] (discussing a study of the readability of 60 financial privacy notices and finding they were written at a third- to fourth-year college reading level “instead of the junior high school level that is recommended for materials written for the general public.”).**

An interesting study is posted on the Privacy Rights Clearinghouse website demonstrating that privacy policies drafted by financial institutions are often very difficult to read. **See, e.g., Take the Cloze Test: Readability of a Financial Privacy Policy, PRIVACY RIGHTS CLEARINGHOUSE, at http://www.privacyrights.org/fs/fs24b-ClozeFinancial.htm (last visited May 21, 2008) (providing readers an opportunity to actually read a sample privacy disclosure from a financial institution and gauge the readability themselves). See also Lost in the Fine Print, supra note 179 (concluding that “[c]onsumers will have a hard time understanding the notices because the writing style uses too many complicated sentences and too many uncommon words.”).**

**See, e.g., Privacy: IBM Privacy Practices on the Web, IBM, at http://www.ibm.com/privacy/us/en/ (last visited May 21, 2008) (demonstrating the clarity and readability of a more recent privacy policy trend called a multi-layered privacy policy—multi-layered policies contain a summary of the policy terms that appears as a separate statement apart from the full privacy policy).**

**See, e.g., Ten Steps To Create a Multilayered Privacy Notice, CENTER FOR INFORMATION PRIVACY LEADERSHIP 1-2, at http://www.hunton.com/files/tbl_s47Details/FileUpload265/1405/Ten_Steps_whitepaper.pdf (last visited May 21, 2008) (discussing the idea of a multi-layered privacy policy and providing businesses with an approach to drafting such statements).**

**See id. at 2-3 (describing the content of each of the different levels in a multi-layered privacy policy).**

**See id.**

**See id.**

**Companies win because multilayered notices easily build consumer trust. Research conducted in Hong Kong, Germany, the United Kingdom, and the United States shows that consumers prefer the template-based condensed notice to longer text-based notices.** The US Postal Service changed its notice when the template-based notice scored highest in a survey of public trust. Consumers like multilayered notices because they like information that is clear, graphically appealing, and easy to compare.

**Id. at 3.**


Though Web sites regularly collect information on visitors, many Americans—even those who claim to understand Web site privacy policies—erroneously believe that sites with privacy policies will not share that information with other sites or companies, according to a new study by the Annenberg Public Policy Center of the University of Pennsylvania.


---


_The Weather Channel reserves the right to alter our Privacy Policy as business needs require._ If we decide to change our Privacy Policy, we will post those changes here so that you will always know what information we gather, how we might use that information and whether we will disclose it to anyone. All changes to this policy will be posted on our Web site prior to the time they take effect. _In the event that we make material changes to the way we use personally identifiable information, affected consumers will be notified via e-mail and will be given the opportunity to opt-out._

177 See, e.g., Privacy Policy: Amendments, BUSINESSWORLD ONLINE, at http://www.businessworldonline.com/assets/main.php?id=privacypolicy (last visited May 21, 2008) (discussing amendments to its privacy policy in the following, rather unclear, manner: “As changing circumstances may require the revision of this Privacy Policy, we encourage our users to check our Privacy Policy from time to time.”).

178 See, e.g., Jonathan Krin, Online Data Gets Personal: Cell Phone Records for Sale, WASH. POST, June 8, 2005, at D1 (discussing the sale of personal identifying information):

A tool long used by law enforcement and private investigators to help locate criminals or debt-skippers, phone records are a part of the sea of personal data routinely bought and sold online in an Internet-driven, I-can-find-out-anything-about-you world. Legal experts say many of the methods for acquiring such information are illegal, but they receive scant attention from authorities.

In addition, “[s]uch records could be used by criminals, such as stalkers or abusive spouses trying to find victims.” _Id._

179 See, e.g., Lost in the Fine Print: Readability of Financial Privacy Notices, PRIVACY RIGHTS CLEARINGHOUSE, July 1, 2001, at http://www.privacyrights.org/arb/GBL-Reading.htm [hereinafter Lost in the Fine Print] (discussing a study of the readability of 60 financial privacy notices and finding they were written at a third- to fourth-year college reading level “instead of the junior high school level that is recommended for materials written for the general public.”).

180 An interesting study is posted on the Privacy Rights Clearinghouse website demonstrating that privacy policies drafted by financial institutions are often very difficult to read. **See, e.g., Take the Cloze Test: Readability of a Financial Privacy Policy, PRIVACY RIGHTS CLEARINGHOUSE, at http://www.privacyrights.org/fs/fs24b-ClozeFinancial.htm (last visited May 21, 2008) (providing readers an opportunity to actually read a sample privacy disclosure from a financial institution and gauge the readability themselves). See also Lost in the Fine Print, supra note 179 (concluding that “[c]onsumers will have a hard time understanding the notices because the writing style uses too many complicated sentences and too many uncommon words.”).**


183 See id. at 2-3 (describing the content of each of the different levels in a multi-layered privacy policy).

184 See id.

185 See id.

Companies win because multilayered notices easily build consumer trust. Research conducted in Hong Kong, Germany, the United Kingdom, and the United States shows that consumers prefer the template-based condensed notice to longer text-based notices. The US Postal Service changed its notice when the template-based notice scored highest in a survey of public trust. Consumers like multilayered notices because they like information that is clear, graphically appealing, and easy to compare.


Though Web sites regularly collect information on visitors, many Americans—even those who claim to understand Web site privacy policies—erroneously believe that sites with privacy policies will not share that information with other sites or companies, according to a new study by the Annenberg Public Policy Center of the University of Pennsylvania.

This information-rich medium [the World Wide Web] also serves as a source of vast amounts of personal information about consumers. Commercial Web sites collect personal information explicitly through a variety of means, including registration pages, user surveys, and online contests, application forms, and order forms. Web sites also collect personal information through means that are not obvious to consumers, such as “cookies.”

Corporate homepages are the most valuable real estate in the world. Space on a big company’s homepage is worth about 1,300 times as much as land in the business districts of Tokyo.

How is this valuable real estate allocated? Very inefficiently. Most pixels go to waste.

A homepage really has two main goals: to give users information, and to serve as their top-level navigation for information that’s inside the site. However, these two goals accounted for only 39% of the screen space across a sample of 50 homepages.

A third important homepage goal is to tell users the site’s purpose and where they are relative to the Web as a whole. Sites typically accomplish this using a logo and a tagline.

(emphasis in original).

See, e.g., Best Buy Privacy Policy, supra note 163:

As part of the policy modification, Best Buy also said it may share with third parties information collected from surveys or reviews on its site. … The shift raised the eyebrows of some privacy advocates. The changes are only the latest in a disturbing trend of companies revamping their privacy policies to the detriment of consumers, advocates say. Companies usually make such changes themselves, taking little input from customers and leaving them with little recourse.

See, e.g., AT&T Revises Privacy Policy for Customer Data, N.Y. TIMES, June 22, 2006, at C7 (stating that the “nation’s largest telephone company, AT&T, has revised its privacy policy for its television and Internet customers, clarifying that the personal information it collects is owned by the company and may be shared in response to court orders and other legal processes.”).


- This privacy policy supersedes and replaces all previously posted privacy policies.
- We want you to be aware of the information we collect, how we use it and under what circumstances, if any, we disclose it. We reserve the right to update this privacy policy to reflect any changes we make in order to continue to serve the best interests of our customers and Web visitors and will timely post those changes. If we make a material change to this privacy policy, we will post a prominent notice on our Web sites.
- If we intend, however, to use personal identifying information in a manner materially different from that stated at the time of collection, we will attempt to notify you at least 30 days in advance using an address or e-mail address, if you have provided one, and by posting a prominent notice on our Web sites, and you will be given a choice as to whether or not we use your information in this different manner.
- Please periodically check our Web sites for changes to this privacy policy.

(emphasis added).

See id.

Id. (providing exceptions to this commitment such as in cases where the company is required by law to provide certain information).

See supra, note 57 and accompanying text.


Personal information is provided by website visitors in numerous ways. From the simple act of providing an email address for the purpose of receiving an email newsletter, to the provision of a credit card number and mailing address to facilitate a purchase, to the most risky provision of social security numbers and other financial information to a bank in order to apply for a loan, personal information is given freely and often in the ever-growing online American market.
This is evidence that companies are conducting market analysis of a multi-layered policy template and that consumers desire such a change.

A material privacy policy amendment is any change that would make a difference to a reasonable e-consumer in the process of deciding whether to submit PII. Under this standard, any change pertaining to PII collection, use, storage or dissemination would clearly be material. On the other hand, merely changing the webpage location of the full text privacy policy would not be material as long as the homepage link is accurate.

Michelin’s privacy policy would be insufficient under the Model Law because Michelin makes no claims about contacting current customers with notification of policy amendments. See supra, note 203.

Some companies are already making efforts to notify existing customers about material amendments. See, e.g., Privacy and Security: Amendments, HEADSPROUT, at http://www.headsprout.com/legal/ (last visited May 10, 2008) (discussing privacy policy amendments: Headsprout may amend this Privacy Policy from time to time. We will notify you by email regarding any material changes to our privacy and security practices. Please review all revisions to the Privacy Policy. Your continued use of the Web Site and the Reading Programs after the date Headsprout has emailed such notices will be deemed to be your agreement to the changed terms). (emphasis added).

A few states (Arkansas, California, Oregon, Rhode Island, and Utah) include additional requirements, such as the destruction of PII once it is no longer needed.

See A Chronology of Data Breaches, supra note 19 (maintaining a regularly updated listed of data breaches). In addition, encryption is not an absolute protection for data. See, e.g., http://www.wiebetech.com/products/HotPlug.php (describing a product that allows a computer to be moved without turning off the power, thereby preserving unencrypted data that has been accessed on the computer); George Ou, Cryogenically Frozen RAM Bypasses all Disk Encryption Methods, ZDNET, Feb. 21, 2008, at http://blogs.zdnet.com/security/?p=900 (describing how a $7 can of compressed air can freeze memory chips, preserving unencrypted data stored in the chips).

See supra, note 86 and accompanying text.


214 See id. The settlement also requires Life is good to retain an independent, third-party security auditor to assess its security program on a biennial basis for the next 20 years. The auditor will be required to certify that Life is good’s security program meets or exceeds the requirements of the FTC’s order and is operating with sufficient effectiveness to provide reasonable assurance that the security of consumers’ personal information is being protected. The settlement also contains bookkeeping and record keeping provisions to allow the FTC to monitor compliance with its order. See id.


219 See supra, notes 86-90 and accompanying text.

