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]

Abstract

This article explores the developing phenomenon of the ongoing collection and dissemination of personal identifying information (PII): first, explaining the nature and form of PII, including the consequences of its collection; second, exploring one of the greatest threats associated with data collection—unauthorized disclosure due to data breaches, including an overview of state and federal legislative reactions to the threats of data breaches and identity theft; third, discussing common law and constitutional privacy protections regarding the collection of personal information, revealing that United States privacy laws provide very little protection to individuals; and fourth, examining current practices by online commercial

* J.D., M.B.A. Assistant Professor, Department of Management & Marketing, University of Wyoming College of Business.
** J.D., M.A. Assistant Professor, Department of Ethics & Legal Studies, University of Denver Daniels 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.
[1] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 220 (1890).
[2] Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1412 (2001) (quoting JIM STERNE, WHAT MAKES PEOPLE CLICK: ADVERTISING ON THE WEB 255 (1997)).

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.

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, Congress has been slow to stake out a position and various states are attempting to pick up the slack.[4] The topic of this national debate is Personal Identifying Information, or PII—essentially, data that identifies 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.[5] Individuals have little to no control over

---

[3] *See* Patrick Thibodeau, *Privacy Again a Hot Button Issue for Legislators*, COMPUTERWORLD, Feb. 27, 2003, *available at* http://www.computerworld.com/securitytopics/security/privacy/story/0,10801,78887,00.html.

[4] Edmund L. Andrews, *U.S.-European Union Talks on Privacy are Sputtering*, N.Y. TIMES, May 27, 1999, at C6 ("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."); Saul Hansell, *Big Web Sites to Track Steps of Their Users*, N.Y. TIMES, Aug. 16, 1998, at 11 ("It is not illegal for Internet services to sell personal information about their customers and there are few laws protecting consumers' privacy in cyberspace."). *See infra* text accompanying notes 60–66, 82–86 (discussing the proliferation of state security breach notification laws but the inadequacies of federal legislation).

[5] *See* Corey Ciocchetti, *The Privacy Matrix,* 12 J. TECH. L. & POL'Y 245, 283–287 (2007). *See also*, Dan Mitchell, *Online Ads vs. Privacy*, N.Y. TIMES, May 12, 2007, at C5 (discussing the connection between collecting PII and online advertising, stating, "[t]o approach individuals with customized advertising, you have to know who they are.

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 data being collected and stored, so too are the lives they lead online, from shopping habits, to social interactions, to Web sites visited.[6] As one commentator noted, "[w]ho controls our data controls our lives."[7]

This paper explores the developing phenomena 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

---

Or at least, you have to gather enough personal information about them that their identity could be easily figured out.").

[6] Jim Puzzanghera, *Tough Cookies for Web Surfers' Trying to Protect Privacy*, L.A. TIMES, Apr. 19, 2008, *available at* http://articles.latimes.com/2008/apr/19/business/fi-privacy19 (discussing the desire of advertisers to track Web users' activities on the Internet); Vauhini Vara, *New Sites Make it Easier to Spy on Your Friends*, WALL ST. J., May 13, 2008, at D1 (discussing Web sites that aggregate personal information about individuals); Saul Hansell, *Charter Will Monitor Customers' Web Surfing to Target Ads*, N.Y. TIMES BITS BLOG, May 14, 2008, http://bits.blogs.nytimes.com/2008/05/14/charter-will-monitor-customers-web-surfing-to-target-ads/ (last visited Feb. 20, 2009) (discussing one Internet service provider's plans to track all Web surfing activities of its customers).

[7] Bruce Schneier, *Our Data, Ourselves*, WIRED, May 15, 2008, http://www.wired.com/politics/security/commentary/securitymatters/2008/05/securitymatters_0515 (last visited Feb. 20, 2009).

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 experience as websites store their information to facilitate navigation and purchases.[9] From a

---

[8] *See* Mark S. Ackerman et al., *Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences*, ACM CONF. ON ELECTRONIC COM. 1 (1999), *available at* http://www.eecs.umich.edu/~ackerm/pub/99b28/ecommerce.final.pdf (last visited Feb. 20, 2009) ("It is difficult, if not impossible, to complete a transaction without revealing some personal data—a shipping address, billing information, or product preference.").

[9] *See*, *e.g.*, Viktor Mayer-Schönberger, *The Cookie Concept*, COOKIECENTRAL.COM, http://www.cookiecentral.com/c_concept.htm (last visited Feb. 20, 2009) ("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.").

more nefarious standpoint, the collection of PII represents a prime target for identity thieves and other bad actors interested in obtaining the information for their financial benefit.[10]

The amount of personal identifying information collected in modern life is vast: transactional data is tracked, cell phones are monitored, Web surfing is recorded, and our moves in public are recorded by surveillance cameras.[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."[12] "Individually, each of these pieces 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."[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 . . . ."[14] Personal information can be collected directly through registration and transactional data, and surreptitiously by tracking users as they navigate the Internet via clickstream data.[15]

---

[10] *See*, FED. TRADE COMM'N, ABOUT IDENTITY THEFT, http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html (last visited Feb. 20, 2009) ("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 FTC estimates that as many as 9 million Americans have their identities stolen each year.").

[11] *See* JAMES B. RULE, PRIVACY IN PERIL 13 (Oxford University Press) (2007). *See also,* A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1475–76 (2000) (describing potential technological methods to collect personal identifying information).

[12] Solove, *supra* note 2, at 1394.

[13] Corey A. Ciocchetti, *E-Commerce and Information Privacy: Privacy Policies as Personal Information Protectors*, 44 AM. BUS. L.J. 55, 56 (2007). *See also*, Stan Karas, *Privacy, Identity, Databases*, 52 AM. U. L. REV. 393, 397 (2002) ("At some point during the accumulation of isolated transactional records, a recognizable portrait of us materializes.").

[14] Solove, *supra* note 2, at 1410.

[15] *Id.* at 1411.

An individual's digital footprint extends beyond transactional data.[16] "The digitization of public records and the increasing accuracy of search engines has made it eas[ier] . . . for the general population to join creditors, law enforcement, and other professional investigators . . . [to discover] individuals' personal information."[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.[18] In recent years, these so - called "data breaches" have grown in number, and have increased the risk of harm from credit card fraud and identity theft for a significant number of individuals.[19]

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."[20] Data breaches can occur in a number of ways, from unauthorized access of computer systems by outsiders, to the loss of portable

---

[16] *See* MARY MADDEN ET AL., PEW INTERNET & AM. LIFE PROJECT, DIGITAL FOOTPRINTS: ONLINE IDENTITY MANAGEMENT AND SEARCH IN THE AGE OF TRANSPARENCY 2 (2007), *available 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[,]" while other digital footprints are "passive," referring to "[p]ersonal data made accessible online with no deliberate intervention from an individual." *Id.* at 3–4.

[17] *Id.* at 3. *See also* Ciocchetti, *supra* note 13, at 55 (describing how, for $29.95, the author 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").

[18] *See* Jim Walden, et al., *Data Breaches: Expect a Rise in Litigation*, 239 N.Y.L.J. S4 (2008).

[19] *Id.*

[20] Richard Warner, *Surveillance and the Self: Privacy, Identity, and Technology*, 54 DEPAUL L. REV. 847, 865 (2005).

computers or portable storage devices.[21] Data breaches have been reported by businesses, financial groups, educational institutions, government entities, and medical and healthcare groups.[22]

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.[23] Initially, it was estimated that approximately 45 million records containing credit card information had been exposed to outsiders.[24] Subsequently, that estimate was raised to over 94 million records.[25]

The intruders were able to make fraudulent credit card purchases using the credit card account information of TJX customers.[26] Those losses, however, were borne by the banks that issued the credit cards rather than the customers.[27] One bank and credit union that had issued credit cards subjected to the TJX data breach filed suit individually and on behalf of a class of

---

[21] *See* Privacy Rights Clearinghouse, A Chronology of Data Breaches, http://www.privacyrights.org/ar/ChronDataBreaches.htm (last visited Feb. 20, 2009).
[22] *See generally* Identity Theft Resource Center, 2007 Data Breach Stats, http://idtheftmostwanted.org/ITRC%20Breach%20Stats%20Report%202007.pdf (last visited Feb. 20, 2009) (listing data breaches reported by various entities).
[23] Press Release, TJX Companies, The TJX Companies, Inc. Victimized by Computer Systems Intrusion; Provides Information to Help Protect Customers (Jan. 17, 2007) http://www.businesswire.com/portal/site/tjx/.
[24] Jaikumar Vijayan, *TJX Data Breach: At 45.6M Card Numbers, it's the Biggest Ever*, COMPUTERWORLD, Mar. 29, 2007, *available at* http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9014782.
[25] Ross Kerber, *Court Filing in TJX - Breach Doubles Toll: 94 Million Accounts were Affected, Banks Say*, BOSTON GLOBE, Oct. 24, 2007, at 1A. The TJX data breach may not be the largest; in early 2009, reports surfaced of a data breach at payment processor Heartland Payment Systems, which could be one of the largest breaches recorded. Brian Krebs, *Payment Processor Breach May Be Largest Ever*, WASH. POST SECURITY FIX, Jan. 20, 2009, *at* http://voices.washingtonpost.com/securityfix/2009/01/payment_processor_breach_may_b.html.
[26] *See* Vijayan, *supra* note 24 (reporting that credit and debit cards compromised in the TJX security breach were "being fraudulently used in several states in the U.S. and even overseas").
[27] Joseph Pereira, *Breaking the Code: How Credit-Card Data Went Out Wireless Door*, WALL ST. J., May 4, 2007, *available at* http://online.wsj.com/article/SB117824446226991797.html. *See also* 15 U.S.C. § 1643 (2000) (limiting credit-card holder liability for fraudulent charges to $50); 81 AM. JUR. 3d *Proof of Facts* § 4 (2008) (discussing liability protections for consumers). Banks and credit unions also had to block and reissue thousands of credit and debit cards as a result of the security breach. Vijayan, *supra* note 24.

similarly situated financial institutions against Fifth Third Bancorp and Fifth Third Bank ("Fifth Third") who had "acquire[d] and processe[d] Visa and MasterCard transactions for TJX as an 'Acquiring Bank.'"[28] 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.[29] 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;[30] 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.[31] The parties subsequently reached a 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.[32]

---

[28] Amended Consolidated Class Action Complaint at 2, In re TJX Cos. Retail Sec. Breach Litig., 527 F. Supp. 2d 209 (D. Mass. 2007) (No. 07-10162).

> 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.

[29] *Id.* at 23–24. The PCI Data Security Standard is promulgated by the Security Standards Council to enhance payment account data security. *See generally* PCI Security Standards Council, About the PCI Data Security Standard (PCI DSS), https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml (last visited Feb. 20, 2009); PCI Security Standards Council, Welcome to the PCI Security Standards Council, https://www.pcisecuritystandards.org/ (last visited Feb. 20, 2009).

[30] Amended Consolidated Class Action Complaint, *supra* note 28, at 23–24.

[31] *Id.* at 25. In an October 2007 ruling on Fifth Third's motion to dismiss the lawsuit, the court dismissed the negligence claims on the basis that the damages sought were purely economic in nature and therefore "unrecoverable in tort . . . in the absence of personal injury or property damage." In re TJX Cos. Retail Sec. Breach Litig., 524 F. Supp. 2d 83, 90 (D. Mass. 2007) (citations omitted). But the court refused to dismiss the plaintiffs' negligent misrepresentation claim, "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," holding this was "a factual issue inappropriate for resolution on a motion to dismiss." *Id.* at 91–92.

[32] Jaikumar Vijayan, *Update: Proposed TJX Settlement Could Save Retailer Millions*, COMPUTERWORLD, Nov. 30, 2007, *available at*

Some of the data stored by TJX 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 victims of identity theft.[33] 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.[34]

The TJX data breach accounted for approximately 74% of the nearly 128 million records exposed in 2007 through data breaches,[35] and nearly half the total since 2005.[36] Even without the TJX data breach, millions of records, many potentially containing PII, are exposed each year through data breaches.[37] 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

---

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9050322. TJX also settled with MasterCard-issuing banks for $24 million to help defray the banks' costs resulting from the data breach. *Banks Agree to TJX Breach Settlement with MasterCard*, INTERACTIVE INVESTOR, May 14, 2008, http://www.iii.co.uk/news/?type=afxnews&articleid=6711624&action=article.

[33] *See* The TJX Companies, Inc., Annual Report (Form 10-K), at 7–10 (Mar. 28, 2007), *available at* http://www.sec.gov/Archives/edgar/data/109198/000095013507001906/b64407tje10vk.htm; Pereira, *supra* note 27. TJX has also entered a tentative settlement with a class of customers, in which TJX denied any wrongdoing and liability, and agreed to provide to customer claimants up to three years of free credit monitoring and identity theft insurance, reimburse the cost of replacement of driver's licenses for customer claimants, provide store vouchers for up to $30 for customer claimants, and hold a one-day "Special Event" in which prices on all merchandise in all TJX stores will be reduced by 15%. Settlement Agreement at 4–5, 13–17, In re TJX Cos. Retail Sec. Breach Litig., 527 F. Supp. 2d 209 (D. Mass. 2007) (No. 07-10162); Evan Schuman, *TJX Revises Consumer Settlement, Agrees to Pay Cash*, EWEEK, Oct. 9, 2007, http://www.eweek.com/c/a/Retail/TJX-Revises-Consumer-Settlement-Agrees-to-Pay-Cash/. The settlement will reportedly cost TJX $200 million. Evan Schuman, *Judge Inclined to Approve Revised TJX Settlement,* EWEEK, Oct. 10, 2007, http://www.eweek.com/c/a/Security/Judge-Inclined-to-Approve-Revised-TJX-Settlement/.

[34] *See* U. S. GOV'T ACCOUNTABILITY OFFICE, PERSONAL INFORMATION: DATA BREACHES ARE FREQUENT, BUT EVIDENCE OF RESULTING IDENTITY THEFT IS LIMITED; HOWEVER, THE FULL EXTENT IS UNKNOWN, 6, 9, 30 (June 2007), *available* at http://www.gao.gov/new.items/d07737.pdf [hereinafter *GAO Personal Information Report*].

[35] *See* Identity Theft Resource Center, *supra* note 22 at 6, 16 (showing that of the 127,725,343 records exposed in 2007, TJX represented 94 million).

[36] *See* Privacy Rights Clearinghouse, *supra* note 21 (showing that since 2005, there have been over 250,000,000 records exposed). A data breach analysis performed by a private company suggests that data breaches may be under-reported by a factor of 100. Press Release, *Consumer Data Losses: 100 Times Worse According to New Report*, EMEDIAWIRE, at http://www.emediawire.com/releases/2009/2/prweb2173994.htm (last visited Mar. 1, 2009).

[37] The first large data breach in 2008 involved the grocery chain Hannaford Bros. Co., in which 4.2 million customer accounts were allegedly compromised during the in-store credit card approval process. Clarke Canfield, *Supermarket Data Breach Still Unsolved*, MSNBC.COM, Mar. 18, 2008, http://www.msnbc.msn.com/id/23698169/.

a series of letters to the Maryland Office of the Attorney General, notifying the office of data breaches that could potentially affect Maryland residents.[38] On July 16, 2007, LPL learned that hackers had compromised the passwords of fourteen financial advisors, using the passwords to gain access to over 10,000 customer accounts, allegedly to solicit LPL customers in a stock scheme.[39] 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.[40] On December 11, 2007, five computers, containing PII of 444 LPL customers, were stolen from LPL's Diamond Bar, California office.[41] 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.[42]

Although the United States General Accounting Office has concluded that "[t]he extent to which data breaches result in identity theft is not well known,"[43] 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.[44] "[T]he median value of goods and services

---

[38] The letters were sent in compliance with Maryland's Personal Information Protection Act. MD. CODE ANN., COM. LAW §§ 14-3504—3508 (West 2008). *See infra* text accompanying notes 60–68 for a discussion of state data breach notification laws.

[39] Letter from Keith H. Fine, Senior Vice President, Assoc. Counsel, LPL Fin., to Douglas F. Gansler, Md. Attorney Gen. 1 (May 6, 2008) (Branch Office Break-in), http://www.oag.state.md.us/idtheft/Breach%20Notices/ITU-152079.pdf (last visited Feb. 23, 2009).

[40] *Id.* at 1–2.

[41] *Id.* at 1.

[42] Letter from Keith H. Fine, Senior Vice President, Assoc. Counsel, LPL Fin., to Douglas F. Gansler, Md. Attorney Gen. 1 (May 6, 2008) (Vehicle Break-in), http://www.oag.state.md.us/idtheft/Breach%20Notices/ITU-152082.pdf (last visited Feb 23, 2009).

[43] *See GAO Personal Information Report*, *supra* note 34 at 5.

[44] FED. TRADE COMM'N, 2006 IDENTITY THEFT SURVEY REPORT 3 (Nov. 2007), http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf. The survey also revealed that, in 2005, an additional 3.2 million American adults reported the misuse of one or more of their existing credit card accounts, and

[stolen] by the thieves was $1,350."[45] These costs do not include the hundreds of hours these victims spent resolving problems created by the identity theft,[46] such as being harassed by credit collectors, correcting credit mistakes, being denied loans, having utilities cut off, and even being criminally investigated.[47] Despite these direct and indirect costs, current law affords little to no remedy for a victim of a data breach or identity theft.[48]

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, exposing "confidential information of tens of thousands" of customers.[49] The plaintiffs sought "'[c]ompensation for all economic and emotional damages suffered as a result of the Defendants' acts which were negligent, in breach of implied contract or in breach of contract,'" plus credit monitoring services.[50] Indiana's security breach notification law[51] 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

---

an additional 3.3 million American adults reported discovering the misuse of one or more of their existing accounts other than credit cards (e.g., checking or savings accounts or telephone accounts). *Id.*

[45] *Id.* at 6.

[46] *See id.* at 7.

[47] *Id.* at 41.

[48] *See infra* text accompanying notes 52–57.

[49] Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 631 (7th Cir. 2007).

[50] *Id.* at 632 (citing R.37 at 5–6).

[51] IND. CODE ANN. §§ 24-4.9-1-1, -3-1 to -3-4 (West 2008).

wake of a breach."[52] In particular, the law "imposes no duty to compensate affected individuals for inconvenience or potential harm to credit that may follow [a data breach]."[53] Further, the plaintiffs were not able to show that 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."[54]

On a different front, victims of identity theft have attempted to hold banks liable for issuing credit cards to impostors (using the victim's identity) under a theory of negligent enablement of impostor 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 impostor fraud.[55] A New York Appellate Division court upheld summary judgment against the plaintiffs because the defendant credit card issuers "had no special 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."[56] Similarly, the

---

[52] *Pisciotta*, 499 F.3d at 637.
[53] *Id.*
[54] *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 an identity theft context, that "an alleged increase in risk of future injury is not an 'actual or imminent' injury"); Kahle v. Litton 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, 7–11 (D.D.C. 2007) (remanding plaintiffs' complaint without prejudice, and 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, No. 08-0560, 2008 U.S. Dist. LEXIS 25563, at *2 (D.D.C. Mar. 20, 2008) (finding plaintiff's claim to be similarly speculative). *But see* Pinero v. Jackson Hewitt Tax Service, Inc., No. 08-3535, 2009 U.S. Dist. LEXIS 660 (E.D. La. Jan. 7, 2009) (holding that although a mere possibility that personal information may be at increased risk does not constitute actual injury sufficient to maintain a claim for negligence under Louisiana law, the court denied the defendant's motion to dismiss the plaintiff's allegations that using false promises of data protection to lure customers to enter into a consumer services contract was an unfair trade practice under Louisiana law, in a case in which the plaintiff's tax returns were found by a third party in an unsecured dumpster outside a tax preparer's office).
[55] *See* Polzer v. TRW, Inc., 682 N.Y.S.2d 194, 195 (App. Div. 1998).
[56] *Id.* at 195.

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 the *Polzer* court and "decline[d] to recognize a legal duty of care between credit card issuers and those individuals whose identities may be stolen."[57]

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 a patient) allegedly gained access to the plaintiff's medical file and shared private information with third parties.[58] 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 use that code to access and obtain the plaintiff's confidential medical records.[59]

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.

---

[57] Huggins v. Citibank, N.A., 585 S.E.2d 275, 277 (S.C. 2003). *But see* Wolfe v. MBNA Am. Bank, 485 F. Supp. 2d 874, 882 (W.D. Tenn. 2007) ("[U]nder 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]."). *See 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, 245 (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, 1557 (2005) (arguing for a tort of negligent enablement as a remedy for computer intrusions due to defective software).

[58] Acosta v. Byrum, 638 S.E.2d 246, 249–50 (N.C. App. 2006).

[59] *Id.* at 251–52. *See also* Randi A.J. v. Long Island Surgi-Center, 842 N.Y.S.2d 558, 565 (App. Div. 2007) (holding that the medical center's wrongful disclosure of confidential medical information to patient's parents was sufficient evidence for a jury to conclude that the conduct amounted to recklessness, gross negligence, and callousness, supporting a punitive damages award).

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.[60] California residents who were victims of the ChoicePoint data breach were notified that their personal information may have been compromised thanks to California's security breach notification law,[61] which has since been used as a model by numerous states in response to the ChoicePoint data breach.[62] California's breach notification law requires businesses conducting business within the state to promptly notify individuals if the individuals' unencrypted personal information is acquired by an unauthorized individual.[63] Personal information, under the California statute, means information regarding name, social security number, driver's license or state identification card number, account number, credit or debit card number, medical information, or health insurance information.[64]

All but six states[65] and the District of Columbia have since passed legislation[66] requiring entities, particularly businesses that maintain computerized PII of state residents, to notify those

---

[60] *See Alert: The ChoicePoint Security Breach (Feb. '05): What it Means for You*, PRIVACY RIGHTS CLEARINGHOUSE, http://www.privacyrights.org/ar/CPResponse.htm (last visited Feb. 23, 2009). It is estimated that approximately 163,000 records were exposed in this particular data breach. *See* Privacy Rights Clearinghouse, *supra* note 21.

[61] *See* CAL. CIV. CODE § 1798.82 (West 1998 & Supp. 2008).

[62] Kathleen Hunter, *California Law on ID Theft Seen as Model*, STATELINE.ORG, Apr. 4, 2005, http://www.stateline.org/live/ViewPage.action?siteNodeId=136&languageId=1&contentId=22828.

[63] CAL. CIV. CODE § 1798.82(a) (West 1998 & Supp. 2008). Section 1798.82 was amended 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. CA.gov, Privacy Legislative Update, http://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/PrivacyLegislation.aspx (last visited Feb. 23, 2009).

[64] CAL. CIV. CODE § 1798.82(e) (West 1998 & Supp. 2008).

[65] Alabama, Kentucky, Mississippi, Missouri, New Mexico, and South Dakota. Jim Graves, *The Six States Without Data Breach Notification Laws*, GRAVES CONCERNS, July 23, 2008, http://blog.subjunctive.com/2008/07/23/the-six-states-without-data-breach-notification-laws/. *See also* Proskauer Rose LLP Privacy Law Blog, *Northern Disclosure: Alaska Enacts 44th State Breach Notification Law*, July 23, 2008, http://privacylaw.proskauer.com/2008/07/articles/security-breach-notification-l/northern-disclosure-alaska-enacts-44th-state-breach-notification-law/ (last visited Feb. 23, 2009).

residents if their PII has been disclosed through a data breach.[67] 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.[68] 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."[69] 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

---

[66] Arizona, ARIZ. REV. STAT. ANN. § 44-7501 (LexisNexis 2008); Arkansas, ARK. CODE ANN. § 4-110-105 (LexisNexis 2008); California, CAL. CIV. CODE § 1798.82 (West 1998 & Supp. 2008); Colorado, COLO. REV. STAT. ANN. § 6-1-716 (LexisNexis 2007); Connecticut, CONN. GEN. STAT. ANN. § 36a-701b (LexisNexis 2008); Delaware, DEL. CODE ANN. tit. 6, § 12B-102 (LexisNexis 2008); District of Columbia, D.C. CODE ANN. § 28-3852 (LexisNexis 2008); Florida, FLA. STAT. ANN. § 817.5681 (LexisNexis 2008); Georgia, GA. CODE ANN. § 10-1-912 (LexisNexis 2008); Hawaii, HAW. REV. STAT. ANN. § 487N-2 (LexisNexis 2008); Idaho, IDAHO CODE ANN. § 28-51-105 (LexisNexis 2008); Illinois, 815 ILL. COMP. STAT. ANN. § 530/10 (LexisNexis 2008); Indiana, IND. CODE ANN. § 24-4.9-3-1 (LexisNexis 2008); Iowa, IOWA CODE ANN. § 715C.2 (West 2008); Kansas, KAN. STAT. ANN. § 50-7a02 (LexisNexis 2006); Louisiana, LA. REV. STAT. ANN. § 51:3074 (LexisNexis 2008); Maine, ME. REV. STAT. ANN. tit. 10, § 1348 (LexisNexis 2008); Maryland, MD. CODE ANN., COM. LAW § 14-3504 (LexisNexis 2008); Massachusetts, MASS. GEN. LAWS ANN. ch. 93H, § 3 (LexisNexis 2008); Michigan, MICH. COMP. LAWS ANN. § 445.72 (LexisNexis 2008); Minnesota, MINN. STAT. ANN. § 325E.61 (LexisNexis 2007); Montana, MONT. CODE ANN. § 30-14-1704 (LexisNexis 2007); Nebraska, NEB. REV. STAT. ANN. § 87-803 (LexisNexis 2008); Nevada, NEV. REV. STAT. ANN. § 603A.220 (LexisNexis 2008); New Hampshire, N.H. REV. STAT. ANN. § 359-C:20 (LexisNexis 2008); New Jersey, N.J. STAT. ANN. §§ 56:8-163 (LexisNexis 2008); New York, N.Y. GEN. BUS. LAW § 899-aa (LexisNexis 2008); North Carolina, N.C. GEN. STAT. § 75-65 (LexisNexis 2008); North Dakota, N.D. CENT. CODE § 51-30-02 (LexisNexis 2008); Ohio, OHIO REV. CODE ANN. § 1349.19 (LexisNexis 2008); Oklahoma, OKLA. STAT. ANN. tit. 74, § 3113.1 (LexisNexis 2008) (as originally enacted, Oklahoma's statute only applied to state government agencies; House Bill 2245, signed by the Governor on May 2, 2008, amended Oklahoma's statute to apply to businesses holding computerized personal data of state residents (Committee Substitute for H.B. 2245 (Ok. 2008))); Oregon, OR. REV. STAT. § 646A.604 (LexisNexis 2007); Pennsylvania, PA. CONS. STAT. ANN. § 2303 (LexisNexis 2008); Rhode Island, R.I. GEN. LAWS § 11-49.2-3 (LexisNexis 2008); South Carolina, S.B. 453, 117th S.C. Gen. Assemb., Reg. Sess. (Sc. 2008); Tennessee, TENN. CODE ANN. § 47-18-2107 (LexisNexis 2008); Texas, TEX. BUS. & COM. CODE ANN. § 48.103 (LexisNexis 2007); Utah, UTAH CODE ANN. § 13-44-202 (LexisNexis 2008); Vermont, VT. STAT. ANN. tit. 9, § 2435 (LexisNexis 2007); Virginia, VA. CODE ANN. § 18.2-186.6 (LexisNexis 2008); Washington, WASH. REV. CODE ANN. § 19.255.010 (LexisNexis 2008); West Virginia, W. VA. CODE § 46A-2A-102 (LexisNexis 2008); Wisconsin, WIS. STAT. ANN. § 895.507 (LexisNexis 2007); and Wyoming, WYO. STAT. ANN. § 40-12-502 (LexisNexis 2008).

[67] 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 38–42 and accompanying text.

[68] *See, e.g.*, CAL. CIV. CODE § 1798.84(b) (West 1998 & Supp. 2008) (providing a cause of action for damages for customers injured by a violation of the disclosure requirements of the statute).

[69] Pereira, *supra* note 27.

another which files had already been copied and avoid duplicating work."[70] 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 nine of the data breach notification statutes[71] provide an encryption safe harbor, making the notification requirements inapplicable if the breached data is encrypted.[72]

And in the few states that do provide civil damages against a company that has had a data breach,[73] 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.[74] Horne alleged that Pfizer had violated Louisiana's Security Breach Notification law[75] because nine weeks elapsed between the data breach and the notification of the breach.[76] 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.[77] As with the common law remedies sought as a result of data breaches that were discussed above,[78] the

---

[70] *Id.*
[71] District of Columbia, Louisiana, New Hampshire, New York, North Carolina, Ohio, Texas, Wisconsin, and Wyoming. *See* Scottandscottllp.com, State Data Breach Notification Laws, http://www.scottandscottllp.com/resources/state_data_breach_notification_law.pdf (last visited Feb. 23, 2009).
[72] Encryption is a method of scrambling data, which then requires a "key" to unscramble the data. *See* SearchSecurity.com, Encryption Definition, http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci212062,00.html (last visited Feb. 23, 2009).
[73] California, Delaware, District of Columbia, Hawaii, Illinois, Louisiana, Maryland, Nevada, North Carolina, Rhode Island, Tennessee, and Washington. *See* Scottandscottllp.com, *supra* note 71.
[74] Ponder v. Pfizer, Inc., 522 F. Supp. 2d 793, 794 (M.D. La. 2007). Or, as was so eloquently phrased by the court, "[s]ometime 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. *Id.* at 794, n.1.
[75] LA. REV. STAT. ANN. § 51:3074 (LexisNexis 2008).
[76] Ponder, 522 F. Supp. 2d at 796.
[77] *Id.* at 798.
[78] *See supra* notes 48–59 and accompanying text.

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."[79]

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,[80] the continuing number of data breaches indicates otherwise.[81] With the emphasis state data breach notification laws place 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 three 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."[82] Since the Gramm-Leach-Bliley Act applies only to financial institutions, such as banks, credit unions, savings and loans, insurance companies and investment companies,[83] 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 amend the Fair Credit Reporting Act to protect against identity theft.[84] Specifically, the FACT Act requires that merchants providing an

---

[79] *Ponder*, 522 F. Supp. 2d at 798. Indeed, the court noted it was following *Pisciotta v. Old National Bancorp* in reaching its conclusion. *Id. at* 798 n.5 ("[T]he injury accrues when the compromised data are actually used by a third party to steal someone's identity.").
[80] *See, e.g.*, Lilia Rode, Comment, *Database Security Breach Notification Statutes: Does Placing the Responsibility on the True Victim Increase Data Security?*, 43 HOUS. L. REV. 1597, 1627–30 (2007).
[81] *See* Privacy Rights Clearinghouse, *supra* note 21.
[82] 15 U.S.C. § 6801(b)(1) (2000).
[83] *See* 15 U.S.C. § 6805(a) (2000).
[84] Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952 (2003).

electronically printed credit card receipt truncate the card number so that no more than the last five digits are printed, and refrain from printing the expiration date of the credit card as well.[85]

Although Senator Leahy introduced the Identity Theft Enforcement and Restitution Act in 2007, it was not enacted until he inserted it into the Former Vice President Protection Act of 2008.[86] The Act amends Title 18 of the United States Code to allow victims of identity theft the ability to seek restitution for the loss of time and money spent restoring credit and remedying the harms of identity theft,[87] and establishes federal jurisdiction even where the victim's and the thief's computers are located in the same state.[88]

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, plus some potential restitution remedies. 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

---

[85] 15 U.S.C. § 1681c(g)(1) (2008). The Federal Trade Commission and additional agencies have promulgated "red flag" rules to also combat identity theft. *See* Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, 72 Fed. Reg. 63718, 63769-71 (Nov. 9, 2007) (FTC rules codified at 16 C.F.R. § 681.1). The red flag rules essentially require financial institutions to develop procedures to identify discrepancies between credit reports and information provided by or about an individual. *Id.*

[86] Pub. L. No. 110-326, Tit. II, 122 Stat. 3560.

[87] 18 U.S.C. § 3663(b).

[88] 18. U.S.C. § 1030(e)(2)(B). The Act also makes it illegal to employ spyware or keylogger software which can be used to collect PII. *Leahy-Authored Anti-Cyber Crime Provisions Set To Become Law*, Sept. 15, 2008, *at* http://leahy.senate.gov/press/200809/091508b.html. Senator Leahy had previously introduced the Personal Data Privacy and Security Act, which took a more comprehensive approach to data protection by requiring non-financial businesses to develop and implement administrative, technical, and physical safeguards to protect the security of sensitive PII. S. 495, 110th Cong. § 301 (2007). The proposed Act never went to a vote before the Senate. Tangentially, 18 U.S.C. § 1028A(a)(1), Aggravated Identity Theft, provides additional penalties for anyone who uses the identity of another in the commission of certain enumerated felonies.

federal privacy statutes.[96] Although PII exposure as a result of a private-entity data breach does not infringe upon constitutional rights, the constitutional right to privacy influences the overall approach to legal protections of privacy in the United States.[97] 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,"[98] enforceable through legal protection from "injurious disclosures as to private matters."[99] 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.[100] In particular, Warren and Brandeis expressed concern not only over the aggressive activities of the press, but their accompanying technology as well.[101] 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

[96] *See* Neil M. Richards, *The Information Privacy Law Project*, 94 GEO. L.J. 1087, 1089 (2006).
[97] *See id.* at 1118–19.
[98] Warren & Brandeis, *supra* note 1, at 193. *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) ("Despite near unanimity among courts and commentators that . . . [*The Right to Privacy*] created the structural and jurisprudential foundation of the tort of invasion of privacy . . . .").
[99] Warren & Brandeis, *supra* note 1, at 204.
[100] *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 95, at 893 (noting that Warren's first daughter would not have been more than seven years old in 1890, and speculating the newspaper story in question may have covered the wedding of one of Mrs. Warren's cousins). *See also* DANIEL J. SOLOVE, THE FUTURE OF REPUTATION 109 (Yale University Press 2007) (discussing same).
[101] *See* Warren & Brandeis, *supra* note 1, at 195.

or sounds."[102] "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.'"[103]

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.[104] A confidential relationship requires just that—a relationship (either through contract, trust, or both).[105] 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."[106] But by the late 1800s, instantaneous photography allowed for surreptitious photographs, eliminating any sort of "relationship between photographer and subject."[107] 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.[108] For Warren and Brandeis, this type of privacy did not arise "from contract or from special trust, but are rights as against the world."[109]

By the mid-twentieth century, based in large part on *The Right to Privacy*, the majority of states recognized a common law right to privacy.[110] In 1960, Prosser identified four distinct types of invasion of privacy recognized by the courts: "(1) [i]ntrusion upon . . . seclusion . . . [;]

---

[102] *Id.* at 206.
[103] *Id.* at 195.
[104] *See* Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 127–128 (2007).
[105] *See id.* at 132.
[106] Warren & Brandeis, *supra* note 1, at 211.
[107] Richards & Solove, *supra* note 101, at 132. *See* Warren & Brandeis, *supra* note 1, at 211.
[108] Warren & Brandeis, *supra* note 1, at 204.
[109] *Id.* at 213. *See also* Richards & Solove, *supra* note 101, at 132.
[110] Prosser, *supra* note 97, at 386–88.

(2) [p]ublic disclosure of embarrassing private facts . . . [;] (3) [p]ublicity which places the plaintiff in a false light in the public eye[; and] (4) [commercial a]ppropriation . . . of the plaintiff's name or likeness."[111] But an additional requirement had become ingrained in the first three types of invasion of privacy—highly offensive conduct.[112]

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.[113] Given circumstances approximating an intrusion upon seclusion, the *De May* court acknowledged the woman's right to privacy during "a most sacred" occasion, ruling that "[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."[114] 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."[115] 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, faced the publication of these facts.[116] 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,

---

[111] *Id.* at 389.
[112] *See* RESTATEMENT (SECOND) OF TORTS § 652D cmt. c (1977).
[113] De May v. Roberts, 9 N.W. 146, 146–47 (1881).
[114] *Id.* at 148–49.
[115] Warren & Brandeis, *supra* note 1, at 214.
[116] Melvin v. Reid, 297 P. 91, 91 (Cal. Ct. App. 1931).

coupled with her true name, was not justified by any standard of morals or ethics known to [the court]."[117]

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."[118] 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."[119] 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 [when] there is highly personal portrayal of . . . intimate private . . . conduct."[120] 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*.[121] 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."[122]

United States privacy law is based on a paradigm that understands privacy as protecting against highly offensive "invasions into [a person's] hidden world."[123] As such, it does little to protect against the collection, use, and dissemination of PII. For example, in *Dwyer v. American*

---

[117] *Id.* at 93.
[118] RESTATEMENT (SECOND) OF TORTS § 652B (1977).
[119] *Id.* at § 652D.
[120] Prosser, *supra* note 97, at 397.
[121] *See id.*
[122] RESTATEMENT (SECOND) OF TORTS § 652E (1977). *See also id.* at § 652C (discussing how 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 . . .").
[123] Solove, *supra* note 2, at 1431.

Express Co., 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.[124] The court stated that "[b]y using [] the card, a cardholder is voluntarily, and necessarily, giving information to defendants that, if analyzed, will reveal a cardholder's spending habits and shopping preferences."[125] 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."[126]

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."[127] 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,"[128] *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 that "[t]he right of privacy does not extend to the mailbox,"[129] relying on a Federal District Court's admonition: "[t]he mail box, 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.'"[130]

---

[124] Dwyer v. Am. Express Co., 652 N.E.2d 1351, 1354 (Ill. App. Ct. 1995).
[125] *Id.*
[126] *Id.*
[127] Solove, *supra* note 2, at 1432.
[128] *Id.*
[129] Shibley v. Time, Inc., 341 N.E.2d 337, 339 (Ohio Ct. App. 1975) (holding that the sale of "personality profiles" based on subscription lists is not an invasion of privacy).
[130] Lamont v. Comm'r of Motor Vehicles, 269 F. Supp. 880, 883 (S.D.N.Y. 1967) (upholding the constitutionality of N.Y. VEH. & TRAF. LAW § 202(4) (McKinney 2006) (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 (2000) (prohibiting states from selling driver's license information without prior consent; however, prior

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 . . . ."[131] In addition, as noted above, this invasion of privacy is concerned with public disclosure of highly personal portrayals of intimate private conduct.[132] Finally, invasion of privacy from public disclosure requires private facts.[133] "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."[134] "Certainly no one can complain when publicity is given to information about him which he himself leaves open to the public eye . . . ."[135] For similar reasons, dissemination of PII would not constitute a "false light" invasion, as the disclosure would most likely not be considered highly offensive. "[F]alse light protect[s] one's reputation, but the type of information collected in databases often is not harmful to one's reputation."[136]

The fourth type of invasion, commercial appropriation of a person's name or likeness,[137] "is designed to protect a person from having his name or image used for commercial purposes

---

consent actually means electing to opt-out). *See, e.g.*, N.Y. VEH. & TRAF. LAW § 202(4)(b) (McKinney 2006) (allowing the sale of information unless a registrant requests the deletion of his or her information from the records to be sold).

[131] Solove, *supra* note 2, at 1433.

[132] *See* Warren & Brandeis, *supra* note 1, at 214–15 (stating that the law should prevent, "so far as possible," the occurrence of a person's private life from being made public against their will).

[133] *See* Keith J. Hilzendeger, *Unreasonable Publicity: How Well Does Tort Law Protect the Unwarranted Disclosure of a Person's HIV-Positive Status?*, 35 ARIZ. ST. L.J. 187, 195 (2003) (stating that the invasion of privacy involves unwanted disclosure of private facts).

[134] Solove, *supra* note 2, at 1433.

[135] Prosser, *supra* note 97, at 394.

[136] Solove, *supra* note 2, at 1433.

[137] *See* RESTATEMENT (SECOND) OF TORTS § 652C (1977).

without consent."[138] 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 that his or her individual information may possess.[139]

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, some 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 an option preventing the broadcast).[140] In addition, companies using this feature could also display the Facebook member's photograph next to the purchase information.[141] 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

---

[138] Dwyer v. American Express Co., 652 N.E.2d 1351, 1355 (Ill. App. 1 Dist. 1995) (citations omitted).
[139] *See id.* at 1356; *see also* Shibley v. Time, Inc., 341 N.E.2d 337, 339 (Ohio Ct. App. 1975) (denying plaintiffs' "invasion of privacy" claim arising from defendants' alleged unjust enrichment by selling "personality profiles" based on plaintiffs' data).
[140] *See* Anick Jesdanun, *Facebook Users Raise Privacy Complaints Over New Tracking*, S. F. CHRONICLE, Nov. 21, 2007, *available at* http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2007/11/21/financial/f122538S55.DTL; *see also* Louise Story & Brad Stone, *Facebook Retreats on Online Tracking*, N.Y. TIMES, Nov. 30, 2007, at C1.
[141] *See* Jesdanun, *supra* note 137.

inform the discussion. Although the U.S. Supreme Court had previously ruled that sealed letters[142] and private papers[143] were subject to Fourth Amendment warrant requirements when it encountered its first electronic wiretapping case, it ruled that telephone conversations were outside the Fourth Amendment's warrant requirement.[144] The Fourth Amendment's language refers to seizing people or things, or searching places.[145] 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.[146]

Recognizing that one's subjective expectation of privacy—reasonable under the circumstances—determines the extent of privacy protection, the Supreme Court reversed its prior decision in *Katz v. United States.*[147] In *Katz,* the Court held that "[t]he Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment."[148] 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."[149] Privacy in America is about reasonable expectations of keeping information secret.

---

[142] *Ex parte* Jackson, 96 U.S. 727, 732–34 (1877).
[143] Boyd v. United States, 116 U.S. 616, 621–23 (1886).
[144] Olmstead v. United States, 277 U.S. 438, 465–66 (1928).
[145] *See* U.S. CONST. amend. IV.
[146] *Olmstead*, 277 U.S. at 464–66.
[147] Katz v. United States, 389 U.S. 347 (1967).
[148] *Id.* at 353.
[149] *Id.* at 351 (citations omitted).

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.[150] The Court concluded that phone customers have no legitimate expectation of privacy regarding 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.[151] 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 the "to/from addresses of e-mail messages, the IP addresses of websites visited and the total amount of data transmitted to or from an account[,]" is not considered a Fourth Amendment search.[152]

The U.S. Supreme Court has also limited privacy rights in records maintained by third parties. In *United States v. Miller*, the defendant was the subject of a tax evasion investigation and tried to prevent the government from using his bank records in the investigation.[153] The Supreme Court concluded that Miller had no privacy interest in his bank records because they were not his personal papers which he owned or possessed—they were the business records of the bank.[154] 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,

---

[150] Smith v. Maryland, 442 U.S. 735, 736 n.1, 745–46 (1979).
[151] *See id.* at 742.
[152] United States v. Forrester, 495 F.3d 1041, 1048–49 (9th Cir. 2007).
[153] United States v. Miller, 425 U.S. 435, 436 (1976).
[154] *See id.* at 440. United States v. Miller was superseded by the Right to Financial Privacy Act, 12 U.S.C. §§ 3401-22 (2007), which "defines the conditions in which government officials may access an individual's financial records." Lopez v. First Union Nat'l. Bank of Fla., 129 F.3d 1186, 1190 (11th Cir. 1997).

for we assume the risk that the third party might relay it to others."[155] And following *Miller* and *Smith*, 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."[156]

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.[157] 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 "applies only to federal, not state and local agencies[;]" information can be disclosed to "law enforcement entities" and "consumer reporting agencies[;]" and "information may be disclosed for any 'routine use' if disclosure is 'compatible' with the purpose for which the agency collected the information."[158] The "routine use" exception is a significant loophole which has done little to bar external disclosure of personal information.[159]

A principal method in which web pages track user browsing is through cookies—files stored by websites on users' computers.[160] For example, DoubleClick, Inc., a company which

---

[155] Joseph T. Thai, *Is Data Mining Ever a Search Under Justice Stevens's Fourth Amendment?*, 74 FORDHAM L. REV. 1731, 1733 (2006) (citations omitted).
[156] United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008) (referencing federal cases that have held the same).
[157] 5 U.S.C. § 552a (2006).
[158] Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1167 (2002) (citing 5 U.S.C. § 552a(b)(3)).
[159] *Id.*
[160] *See* CookieCentral.com, Cookies and Privacy FAQ, http://www.cookiecentral.com/n_cookie_faq.htm (last visited Feb. 24, 2009).

"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.[161] 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 (hereinafter "ECPA" or "Act").[162] 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."[163] The plaintiffs alleged DoubleClick violated Title II because placing cookies on the plaintiffs' computer hard drives constituted unauthorized access.[164]

However, "DoubleClick's cookies only collect information" concerning users' activities on DoubleClick-affiliated websites.[165] Therefore, the court's focus was not on DoubleClick's access of cookies on users' computers, but whether the affiliated websites authorized DoubleClick to access those communications.[166] The court found it "implausible" that DoubleClick's affiliated websites would not authorize DoubleClick to access information collected as a result of that affiliation.[167]

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.[168] Reviewing the legislative history of the Act, the court determined that Congress' intent in passing Title II was

---

[161] *See In re* DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497, 500, 502–03 (S.D.N.Y. 2001).
[162] Electronic Communications Privacy Act, 18 U.S.C. §§ 2701–11 (1986); *In re DoubleClick*, 154 F. Supp. 2d at 507.
[163] *In re DoubleClick,* 154 F. Supp. 2d at 507 (citing 18 U.S.C. § 2707 (1986)).
[164] *Id.*
[165] *Id.* at 504.
[166] *Id.* at 510.
[167] *Id.*
[168] *Id.* at 511.

"to protect communications held in interim storage by electronic communication service providers."[169] The court ruled that since DoubleClick's cookies remained on users' computers indefinitely, they "are never in 'electronic storage' under the ECPA, [and therefore] they are not protected by Title II . . . ."[170]

There are a scattering of federal privacy laws that do provide some privacy protection related to data collection.[171] 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.[172]

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 collectors of PII, particularly on the internet, agree to safeguard PII.

---

[169] *Id.* at 512.
[170] *Id.* at 513.
[171] *See generally* Gramm-Leach-Bliley Act, 15 U.S.C. § 6802 (1999) (limiting information sharing by financial institutions with third parties without prior consent by customers); Privacy Protection Act, 42 U.S.C. § 2000aa (1980) (restricting the search or seizures of work product materials in the possession of third parties by government officers); Cable Communications Policy Act, 47 U.S.C. § 551 (1984) (requiring notice to cable customers of any disclosure of PII); Video Privacy Protection Act, 18 U.S.C. § 2710 (1988) (prohibiting video rental stores from disclosing customer video rental and purchase information); Computer Matching and Privacy Protection Act of 1988, Pub. L. No. 100-503, 102 Stat 2507 (1988) (regulating the federal government's practice of comparing individual information stored across different agency computer databases); Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat 1936 (1996) (regulating the disclosure of health information).
[172] *See* Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1148 (2002).

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.[173] Although brick and mortar establishments often draft privacy policies, the e-commerce world has made them famous.[174] In today's e-commerce arena, it is common for most legitimate e-commerce companies to post their privacy policies on their websites.[175] 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.[176]

---

[173] *See, e.g., Your Online Privacy Policy, An Informational Paper about Drafting Your First Privacy Statement or Improving Your Existing One*, TRUSTe, 2004, *available at* http://www.truste.org/pdf/WriteAGreatPrivacyPolicy.pdf [hereinafter *TRUSTe Online Privacy*]. "A privacy statement is a communication to consumers about how a company uses their personal information. . . . These statements are unique in that they are wholly public: they can be viewed by anyone, at any time, and apply to anyone visiting the Web site on which they are displayed." *Id.* at 3.

> [A] document that provides notice and details exactly how a company (i.e. a website) uses any information provided by the user or gathered by the site about the user. The company will generally explain how information is collected, how it is used, whether it is shared with any third parties, who the third parties might be, whether the site uses cookies or other tracking methods, and any other relevant policies.

FindLegalForms, Inc., *What is a Privacy Policy?*, http://www.findlegalforms.com/articles/form-encyclopedia/what-is-a-privacy-policy (last visited Feb. 24, 2009).

[174] Some companies have a privacy policy that covers PII collected online and in its brick and mortar establishments. *See, e.g.,* Troy Wolverton, *Best Buy Changes Privacy Policy*, C|NET NEWS, June 4, 2002, *available at* http://www.news.com/2100-1017-932157.html [hereinafter *Best Buy Privacy Policy*].

> 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.

Id.

[175] *See, e.g.*, *TRUSTe Online Privacy*, *supra* note 170, at 6 ("Posting a privacy statement online is the industry standard. Most Web sites now post an online privacy statement.").

[176]

> 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.

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.[177] Through its policy, a company could accurately describe the collection, storage, and uses of PII.[178] 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.[179] Along those same lines, visitors could click on a privacy policy link, read these disclosures, and surf the web accordingly.[180] This communication between company and customer was supposed to build trust and make individuals feel more comfortable when transacting business online.[181] In reality, quite a different story emerged and the idealistic promise of privacy policies faded from memory.[182]

---

[177] *See, e.g.,* HUNTON & WILLIAMS, CENTER FOR INFORMATION POLICY LEADERSHIP, MULTI-LAYERED NOTICES EXPLAINED 2, *available at* http://www.hunton.com/files/tbl_s47Details/FileUpload265/1303/CIPL-APEC_Notices_White_Paper.pdf [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 with whom they will do business. This has been an impediment to on-line commerce.").

[178] If there is ever a place for such disclosure it is in a company's self-titled privacy policy. *See id.* ("Privacy notices are the windows to how organizations collect, use, share, and protect the information that pertains to individuals.").

[179] *See, e.g.*, *TRUSTe Online Privacy*, *supra* note 170, 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.").

[180] *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.").

[181] *TRUSTe Online Privacy*, *supra* note 170, at 4.

> 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.

Id.

[182] *See, e.g.,* Ciocchetti, *supra* note 13, at 68–70 (discussing how contemporary privacy policies have failed to live up to their expectations).

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.[183] Exacerbating this problem is the fact that the vast majority of companies collect PII on their websites.[184] 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.[185] Other information is collected passively through technology such as cookies and web beacons.[186] These devices are able to collect information

---

[183] *See, e.g.*, Center for Democracy and Technology, Data Privacy, CDT's 1997 Privacy Survey Results, http://www.cdt.org/privacy/survey/findings/results.shtml (last visited Feb. 24, 2009) (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., looked for and/or read) a privacy policy from their online service provider. *Id.*

[184] *See generally* Joseph Turow, Ph.D., *Americans & Online Privacy, The System is Broken*, ANNENBERG PUB. POL'Y CTR. 5–6 (2003), *available at* http://www-personal.si.umich.edu/~rfrost/courses/SI110/readings/Privacy/Annenberg_Privacy_Study.pdf (discussing the numerous methods that many companies employ to exploit and troll for PII).

[185] *See, e.g.,* Steelcase, Inc., Steelcase Privacy Policy, http://www.steelcase.com/na/privacy_policy_cnav.aspx?f=10033 (last visited Feb. 24, 2009). 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.

[186] *See, e.g.,* Apartments.com, Privacy Statement, http://www.apartments.com/privacy.htm (last visited Feb. 24, 2009). 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).

without notification to or knowledge of the person visiting the website.[187] In addition, companies often reserve the right to amend their privacy policies at any time and bind such amendments on visitors who entered their PII under previous privacy terms.[188] Other policies are unclear about whether privacy policy amendments are binding on visitors.[189] 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.[190] 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.

---

[187] *See, e.g.*, Brian Quinton, *Study: Users Don't Understand, Can't Delete Cookies*, May 18, 2005, DIRECT, *available at* http://searchlineinfo.com/InsightExpress_cookie_study/ ("[One] 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.").

[188] *See, e.g.*, The Weather Channel, Privacy Statement, Changes to the Privacy Policy (effective June 5, 2008), http://www.weather.com/common/home/privacy.html?from=footer (last visited Feb. 24, 2009) (discussing privacy policy amendments in a manner that indicates such amendments are binding).

> *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.*

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

[189] *See, e.g.,* Google.com, Privacy Policy, Changes to Privacy Policy (last modified Aug. 7, 2008), http://www.google.com/intl/en/privacypolicy.html (showing how notification will be given for any changes to the privacy policy but never mentioning whether or not the customers will be automatically bound to these changes).

[190] *See, e.g.,* Jonathan Krim, *Online Data Gets Personal: Cell Phone Records for Sale*, WASH. POST, July 8, 2005, at D01, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2005/07/07/AR2005070701862.html (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.
>
> . . . .
>
> Such records could be used by criminals, such as stalkers or abusive spouses trying to find victims.

Id.

Privacy Policy Terms

Reading through many contemporary privacy polices 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.[191] 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.[192] 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.[193] The most current trend in policy creation occurs in the form of a multi-layered privacy policy.[194] Multi-layered policies come in at least two stages (layers),

---

[191] *See, e.g.*, Mark Hochhauser, Ph.D., *Lost in the Fine Print: Readability of Financial Privacy Notices*, PRIVACY RIGHTS CLEARINGHOUSE, July 2001, http://www.privacyrights.org/ar/GLB-Reading.htm [hereinafter *Lost in the Fine Print]* ("Readability analyses of 60 financial privacy notices found that they are written at a 3rd-4th year college reading level, instead of the junior high school level that is recommended for materials written for the general public.").

[192] *See* Turow, *supra* note 181, at 9–10 (discussing problems with privacy policy language).
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.*, Mark Hochhauser, Ph.D., *Take the Cloze Test: Readability of a Financial Privacy Policy*, PRIVACY RIGHTS CLEARINGHOUSE, July 2004, http://www.privacyrights.org/fs/fs24b-ClozeFinancial.htm (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 188 ("Consumers will have a hard time understanding the notices because the writing style uses too many complicated sentences and too many uncommon words.").

[193] *See, e.g.*, IBM.com, IBM Privacy Practices on the Web, http://www.ibm.com/privacy/us/en/ (last visited Feb. 24, 2009) (demonstrating the clarity and readability of a more recent privacy policy trend called a multi-layered privacy policy, which contains a summary of the policy terms that appears as a separate statement apart from the full privacy policy).

[194] *See, e.g.*, HUNTON & WILLIAMS LLP, CENTER FOR INFORMATION PRIVACY POLICY LEADERSHIP, TEN STEPS TO CREATE A MULTILAYERED PRIVACY NOTICE 1–2, *available at* http://www.hunton.com/files/tbl_s47Details/FileUpload265/1405/Ten_Steps_whitepaper.pdf [hereinafter TEN STEPS

beginning with a summary of policy terms in the first layer and followed by the full privacy policy in the second layer.[195] 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.[196] 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 it's PII, and that a glance is better than no glance at all.[197] Additionally, companies that choose to create a multi-layered policy—it is not currently required by any state or federal law[198]—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.[199]

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.[200] 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

---

TO CREATE A MULTILAYERED PRIVACY NOTICE] (discussing the idea of a multi-layered privacy policy and providing businesses with an approach to drafting such statements).

[195] *See id.* at 2–3 (describing the content of each level in a multi-layered privacy policy).

[196] *See id.*

[197] *See id.* at 3–4.

[198] *See* Turow, *supra* note 181, at 9.

[199] *See* TEN STEPS TO CREATE A MULTILAYERED PRIVACY NOTICE, *supra* note 191, at 1, 3–4.

> 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.

[200] *See, e.g.*, Turow, *supra* note 181, at 3 (stating that many Americans "believe incorrectly that when a website has a privacy policy, it will not share their personal information with other websites or companies").

without the exchange of valuable PII.[201] This situation results in a dilemma where a consumer does not want to or 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.[202] 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, so they generally place a link to their policy on the homepage.[203] This is an acceptable compromise because homepages are valuable web real estate and should be utilized in the most effective manner possible.[204] However, some companies abandon this compromise and

---

[201] *See, e.g.,* Federal Trade Commission, History and Overview, Consumer Privacy Online (last modified June 25, 2007), *available at* http://www.ftc.gov/reports/privacy3/history.shtm (stating that online consumers forgo products or services because they do not wish to give the Web site their personal information, thus implying that the product or service is not available online without the disclosure of the consumer's personal information).

> . . . *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.'"

Id. (internal citations omitted) (emphasis added).

[202] *See e.g.,* Gmail, http://www.gmail.com (follow "Create an Account" link) (last visited Feb. 24, 2009) (showing that a user must enter personal information such as secondary email and location before setting up an account).

[203] *See, e.g.*, Ernst & Young, http://www.ey.com/global/content.nsf/International/Home (Follow "Privacy Policy" link) (last visited Feb. 24, 2009) (showing an unwillingness to use homepage space for the privacy policy by allocating only a minimal amount of space for the privacy policy link near the bottom of the page).

[204] *See, e.g.*, Jakob Nielson, *Homepage Real Estate Allocation*, USEIT.COM, Feb. 10, 2003, http://www.useit.com/alertbox/20030210.html.

> 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.

are reluctant to post a conspicuous link to their privacy policy on their homepages.[205] Other companies force users to click on numerous links before they even arrive at the actual privacy policy statement.[206] 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.[207] 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

---

> 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.

Id. (emphasis in original).

[205] *See, e.g.*, FreshDirect, http://www.freshdirect.com (last visited Feb. 24, 2009) (failing to post a link to the privacy policy anywhere on the homepage).

[206] *See, e.g.*, AT&T, http://www.att.com, (last visited Feb. 24, 2009) (user must click on two links before he or she reaches the full text of the Privacy Policy).

[207] *See, e.g.*, Turow, *supra* note 181, at 17–18 (showing that approximately 30% of people do not look to see if a website has a privacy policy, and a great number of the people that do look do not even read the policies anyway because they do not understand them).

any time and without much in the way of notice.[208] 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.[209]

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.[210] The new policy terms also require visitors to agree to the revised policy before they proceed on the website or use AT&T services.[211] 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.[212] If the change is material then the

---

[208] *See, e.g.*, Facebook, Terms of Use, Notices and Revisions, http://www.facebook.com/policy.php (last visited Feb. 24, 2009) (stating that they will only notify you of changes, which take effect 30 days after posting at the latest, through the online privacy policy page or through a notice on the home page; thus requiring a customer to continually check the privacy policy for changes).

[209] *See, e.g.*, *Best Buy Changes Privacy Policy*, *supra* note 171174.

> As part of the policy modification, the company 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.

Id.

[210] *See AT&T Revises Privacy Policy for Customer Data*, N.Y. TIMES, June 22, 2006, at C7 ("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.").

[211] *See* AT&T, *Congrats. Your Computer Is Almost a TV*, https://att.mobitv.com/fe/att-bb/signup.do (last visited Feb. 24, 2009) (requiring customers to "agree and consent" to the company's privacy policy before signing up for services).

[212] *See* AT&T, *AT&T Privacy Notice* (effective June 16, 2006), *available at* http://www.att.com/gen/privacy-policy?pid=7666 (providing "updates" in the penultimate section of its privacy policy).

> • 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*.

company promises to "attempt" to notify individuals within thirty 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.[213] 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."[214] 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.[215] In fact, an entire data brokerage industry has sprung up around such data sales.[216] External PII transfers raise some very serious threats. First, once data is disseminated outside of the possession of the

---

> • 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*.

Id. (emphasis added).

[213] *See id.*

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

[215] *See* Jonathan P. Cody, Comment, *Protecting Privacy Over the Internet: Has the Time Come to Abandon Self-Regulation?*, 48 CATH. U. L. REV. 1183, 1184–85, 1223–24 (1999) (citations omitted).

[216] *See, e.g.* Net-Trace, Information Brokers, http://www.nettrace.com.au/resource/search/info.html (last visited Feb. 24, 2009) (providing a list of information brokers who offer search services for PII for a fee).

individual it identifies and its collector, it becomes virtually irretrievable.[217] 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.[218] 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.[219] Finally, PII sharing can be done at a very low cost in terms of time and money.[220] 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 disclose 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

---

[217] *See* Ciocchetti *supra* note 13, at 57 (stating that once PII is distributed into cyberspace, "such information is virtually irretrievable and may be intercepted or purchased by commercial entities, governments, or individuals for marketing or other more sinister purposes").
[218] *Your Privacy for Sale*, CONSUMER REPORTS, Oct. 2006 *available at* http://www.consumerreports.org/cro/money/credit-loan/data-privacy-10-06/overview/1006_privacy_ov1_1.htm.
[219] *See* PRIVACY RIGHTS CLEARINGHOUSE, *supra* note 60 and accompanying text.
[220] *See* Cody, *supra* note 212, at 1184 ("[T]he collection and use of personal identifiable information have never been cheaper or easier.") (citations omitted).

(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.[221] 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

[221] *See supra* notes 174–76 and accompanying text.

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.[222] More specifically,

---

[222] *See, e.g.*, Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control Over Personal Information?*, 111 PENN. ST. L. REV. 587, 590–91 (2006-2007) (citations omitted) (discussing the multifarious ways that e-consumers use the Web).

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 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

---

> 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.

Id. (citations omitted).

prose and content in written materials disclosing securities information to the general public.[223] 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.[224] Instead, the concept of

> [p]lain 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.[225]

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

---

[223] *See* U.S. SECURITIES AND EXCHANGE COMMISSION, OFFICE OF INVESTOR EDUCATION AND ASSISTANCE, A PLAIN ENGLISH HANDBOOK, HOW TO CREATE CLEAR SEC DISCLOSURE DOCUMENTS 3, (Aug. 1998), *available at* http://www.sec.gov/pdf/handbook.pdf [hereinafter PLAIN ENGLISH HANDBOOK].
[224] *See id.* at 5.
[225] *Id.*

9. Unreadable design and layout"[226]

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[227] 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 is posted in at least the same font, style, and size as any surrounding links.[228] 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

---

[226] *Id.* at 17.
[227] *See* Nielson, *supra* note 201 (discussing the value of a company's homepage).
[228] *See* THE NEW OXFORD AMERICAN DICTIONARY 367 (2001) (defining "conspicuous" as "standing out so as to be clearly visible").

nearby.[229] 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.[230]

Amendments

Third, the Model Law requires all Covered Policies to properly notify consumers about any material privacy policy amendment.[231] 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.[232] Neither of these options is acceptable in an e-commerce environment where people do not read privacy policies in the first place and where

---

[229] *See, e.g.,* Google.com, http://www.google.com/ (last visited Feb. 24, 2009) (revealing that Google places a link to its privacy policy on the bottom of its homepage in a smaller font, which would violate the Model Law).

[230] Additionally, as the e-commerce industry moves towards the multi-layered privacy policy format, the posting of a privacy policy link on a homepage will take the visitor to the next level—the policy summary—and then eventually to the entire text of the policy. The Model Law can easily include a multi-layered policy requirement but this may not be necessary as the industry appears to be self-regulating in this direction. *See, e.g.*, MULTI-LAYERED NOTICES EXPLAINED, *supra* note 174, at 4.

> . . . [Multi-layered notices] have been tested with focus groups in the US, Germany and Hong Kong. The US research was led by P&G and . . . found that 1) consumers believed that long notices were obscuring important information and 2) that they preferred the [multi-layered] template that allows them to compare the practices of different companies.

Id.

This is evidence that companies are conducting market analysis of a multi-layered policy template and that consumers desire such a change.

[231] 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. *See, e.g.*, BLACK'S LAW DICTIONARY 998 (8th ed. 2004) (defining "material" as "of such a nature that knowledge of the item would affect a person's decision making.").

[232] *See, e.g.*, Michelin, Privacy Policy, Amendments, http://www.michelin-us.com/policies/privacy.htm (last visited Feb. 24, 2009) (discussing privacy policy amendments and stating that "[t]his Policy became effective on May 21, 2004. Any amendments will be posted at this URL and will be effective when posted."); Cobimobi.com, Privacy Policy/Terms & Conditions, http://www.cobimobi.com/privacy.html (last visited Feb. 24, 2009) ("This Privacy Policy is subject to change by us at any time . . . . It is your responsibility to check regularly to determine whether these Terms and Conditions have been changed each time you use the Website.") This implies that notification for amendments will not be given. *Id.*

these same people are extremely unlikely to look to privacy policies for any amendments.[233] Making matters worse, companies often claim that policy amendments are binding on all users—past and present—when posted regardless of the fact that no notice has been provided.[234]

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 for any changes that affect their PII.[235] 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.[236] For those people who cannot be notified via e-mail (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,

---

[233] *See* Keith Regan, *Does Anyone Read Online Privacy Policies?*, E-COMMERCE TIMES, June 15, 2001, *available at* http://www.ecommercetimes.com/story/11303.html?welcome=1210544891.

> Though the public's desire for privacy protection within e-commerce is well-documented, the vast majority of online shoppers appear unwilling to take the time to read an e-tailer's privacy policy.
>
> "Some people read privacy policies, but it's a tiny minority," Susannah Fox, director of research at the Pew Internet and American Life Project in Washington, D.C., told the E-Commerce Times. "People aren't that aggressive when it comes to protecting their own privacy."
>
> In fact, Forrester Research analyst Christopher Kelley told the E-Commerce Times that less than 1 percent of the visitors to six major online travel sites during April actually read privacy policies.
>
> "Consumers are incredibly concerned about privacy," Kelley said. "But they don't want to lift a finger to protect their own privacy."

Id.

[234] *See* Cobimobi.com, *supra* note 229 (stating that the company reserves the right to modify the Terms and Conditions and the Privacy Policy at any time, effective upon posting on the website).

[235] 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* Michelin, *supra* note 229.

[236] Some companies are already making efforts to notify existing customers about material amendments. *See, e.g.*, Headsprout, Privacy and Security, http://www.headsprout.com/legal/ (last visited Feb. 24, 2009) (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.

Id. (emphasis added).

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 that 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 that 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.[237] 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.[238]

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;

---

[237] 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). ARK. CODE ANN. § 4-110-104(a) (2005); CAL. CIV. CODE § 1798.81 (2000); OR. REV. STAT. § 646A.622(1) (2007); R.I. GEN. LAWS § 11-49.2-2 (2005); UTAH CODE ANN. § 13-44-201(2006).

[238] *See A Chronology of Data Breaches*, *supra* note 21 (maintaining a list of data breaches updated twice a week). In addition, encryption is not an absolute protection for data. *See, e.g.*, WiebeTECH, Hot Plug, http://www.wiebetech.com/products/HotPlug.php (last visited Feb. 24, 2009) (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); Posting of George Ou, *Cryogenically Frozen RAM Bypasses All Disk Encryption Methods*, ZDNET, Feb. 21, 2008, *available 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).

3. Vulnerability testing and modernization; and

4. Financial penalties for noncompliance.

This is the approach the federal government is beginning to pursue through enforcement actions by the Federal Trade Commission ("FTC"). For example, in *In re Life is good, Inc.*, the FTC brought a complaint against the company alleging that it "failed to provide reasonable and appropriate security for the consumer information stored on their network, including credit card numbers, expiration dates, and security codes."[240] In particular, the Life is good, Inc. Privacy Policy stated PII was stored in a secure file when, in fact, it was stored in "clear, readable text."[241]

In a consent agreement, Life is good, Inc. agreed to "establish and implement, and thereafter maintain[] a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers."[242] Implementation and maintenance of the security program requires Life is good, Inc. to: (1) designate "an employee or employees to coordinate . . . the information security program;" (2) identify "internal and external risks to the security, confidentiality, and integrity of personal information," and assess the safeguards already in place; (3) design and implement safeguards "to control the risks identified through 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, Inc. customers; and (5) evaluate and adjust its

---

[240] Complaint at ¶ 8, *In re* Life is Good, Inc., (Fed Trade Comm'n, 2007) (No. 0723046) *available at* http://www.ftc.gov/os/caselist/0723046/080117complaint.pdf. The FTC based its complaint on an allegation that the acts and practices of Life is good, Inc. violated Section 5(a) of the Federal Trade Commission Act. *Id.* at ¶ 12.
[241] *Id*. at ¶¶ 7–8.
[242] Agreement Containing Consent Order at 3, *In re* Life is good, Inc., (Fed Trade Comm'n 2007) (No. 0723046) *available at* http://www.ftc.gov/os/caselist/0723046/080117agreement.pdf.

"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.[243]

The FTC has brought similar actions and reached similar agreements with three additional businesses: Goal Financial, LLP,[244] Reed Elsevier, Inc.,[245] and TJX.[246] These actions by the FTC 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 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 twenty years.[247] There have been no monetary fines. While a large fine could arguably be a significant incentive for smaller companies to implement adequate security measures to protect PII, recent evidence

---

[243] *Id.* at 3–4. The settlement also requires Life is good, Inc. to retain an independent, third-party security auditor to assess its security program on a biennial basis for the next twenty years. The auditor will be required to certify that Life is good, Inc.'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. *Id.* at 4–5.

[244] *See* Complaint at 2, *In re* Goal Financial, LLC, (Fed. Trade Comm'n, 2008) (No. C-4216), *available at* http://www.ftc.gov/os/caselist/0723013/080415complaint.pdf; Decision and Order at 3–4, *In re* Goal Financial, LLC, (Fed. Trade Comm'n, 2008) (No. C-4216), *available at* http://www.ftc.gov/os/caselist/0723013/080415decision.pdf.

[245] *See* Complaint at 3, 5, *In re* Reed Elsevier, Inc. and Seisint, Inc., (Fed. Trade Comm'n 2008) (No. 0523094), *available at* http://www.ftc.gov/os/caselist/0523094/080327complaint.pdf; Agreement Containing Consent Order at 4–5, *In re* Reed Elsevier, Inc. and Seisint, Inc., (Fed. Trade Comm'n, 2008) (No. 0523094), *available at* http://www.ftc.gov/os/caselist/0523094/080327agreement.pdf. Reed Elsevier, Inc. acquired Seisint, Inc. in September 2004. Complaint at 1, *In re* Reed Elsevier, Inc., and Seisint, Inc., (Fed. Trade Comm'n, 2008) (No. 0523094), *available at* http://www.ftc.gov/os/caselist/0523094/080327complaint.pdf

[246] *See* Complaint at 2–3, *In re* TJX Companies, Inc., (Fed. Trade Comm'n, 2008) (No. 072-3055), *available at* http://www.ftc.gov/os/caselist/0723055/080327complaint.pdf; Agreement Containing Consent Order at 3–4, *In re* TJX Companies, Inc., (Fed. Trade Comm'n, 2008) (No. 072-3055), *available at* http://www.ftc.gov/os/caselist/0723055/080327agreement.pdf.

[247] *See, e.g.*, Agreement Containing Consent Order at 4, 15, *In re* Life is good, Inc., (Fed. Trade Comm'n, 2007) (No. 072-3046), *available at* http://www.ftc.gov/os/caselist/0723046/080117agreement.pdf ("[R]espondents shall obtain initial and biennial assessments and reports . . . from a qualified, objective, independent professional, who uses procedures and standards generally accepted in the profession.").

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."[249] And that is the estimated approximate cost required to settle the incident with the various parties involved.[250] 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.[251] 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 loss 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

---

[249] The TJX Companies, Inc., Quarterly Report (Form 10-Q), at 2 (July 2007), *available at* http://www.sec.gov/Archives/edgar/data/109198/000095013507005281/b66678tje10vq.htm.
[250] *See* Evan Schuman, *TJX Judge Inclined to Approve Revised Cash Settlement Deal,* STOREFRONTBACKTALK, Oct. 10, 2007, *available at* http://storefrontbacktalk.com/story/101007judgelikessettlement (noting a settlement amount of approximately $200 million).
[251] *See* Thomas Wailgum, *How TJX Avoided Wall Street's Wrath*, CIO, Feb. 5, 2008, *available at* http://www.cio.com/article/179603; Ben Worthen, *TJX Earnings Suggest that Data Security Doesn't Worry Consumers*, WALL ST. J., May 13, 2008, *available at* http://blogs.wsj.com/biztech/2008/05/13/tjx-earnings-suggest-that-data-security-doesnt-worry-consumers/?mod=WSJBlog.

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 that would at least require comprehensive internal data protection procedures, coupled with substantial fines for failing to implement and maintain such procedures.. This 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 programs in place.