Journal of Technology Law & Policy

Volume 12 | Issue 2 Article 4

December 2007

The Privacy Matrix

Corey Ciocchetti

THE PRIVACY MATRIX

Corey Ciocchetti[*]

* Assistant Professor at the Daniels College of Business in the Department of Business Ethics and Legal Studies, University of Denver.

I. INTRODUCTION

Vacationing in Victoria, British Columbia, I stepped into the province's Parliament Building expecting to encounter debates pertaining to land use, economic policy, and other territorially-relevant issues. Upon entering the legislative chamber, however, I found myself immersed in a detailed discussion of e-commerce and information privacy as the Members of Parliament questioned proposed privacy-based regulations regarding the electronic collection and transfer of medical records.[1] Meanwhile, the U.S. Congress continues to debate e-consumer privacy and identity theft legislation,[2] while the European Union gradually builds upon its comprehensive privacy protection regime.[3] This global focus on

1. *See* Health Statutes Amendment Act, 2004, Bill [29] 2006 (amending, *inter alia*, the Health Act (1996)), *available at* http://www.leg.bc.ca/38th2nd/1st_read/gov29-1.htm (last visited July 25, 2007).

2. *See, e.g.*, the Consumer Privacy Protection Act, H.R. 1263, 109th Cong. (2005) (requiring, among other things, most companies collecting, disclosing, selling, or utilizing PII for commercial purposes to create and post an electronic privacy policy describing the company's privacy practices and also require the FTC to put procedures in place that are designed to lighten the effects of identity theft on consumers) and the Safeguarding Americans from Exporting Identification Data Act, S. 810, 109th Cong. (2005) (protecting the privacy of an individual's PII by requiring certain privacy-enhancing protections to be put in place before PII is transmitted to foreign affiliates and foreign subcontractors).

3. Working Party 29 Opinion 2/2006 on Privacy Issues Related to the Provision of Email Screening Services (Feb. 21, 2006) (ruling in favor of individual privacy in e-mail communications and stating that it is unlawful for e-mail service providers to screen individual e-mails (even for evidence of unlawful activities), or to implement software monitoring the opening, forwarding or sending of e-mail, without prior consent or a "specific legal basis" such as public security), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/ wp118_en.pdf (last visited July 25, 2007). The Article 29 Working Party is not a legislative body, rather, it is made up of the:

> Data Protection Commissioners from the EU ... together with a representative of the EU Commission. The Working Party is independent and acts in an advisory capacity. The Working Party seeks to harmonise the application of data protection rules throughout the EU, and publishes opinions and recommendations on various data protection topics. It also advises the EU Commission on the adequacy of data protection standards in non-EU countries.

information privacy demonstrates the significance of protecting the vast amounts of personal information submitted into cyberspace from electronic privacy-invading threats (e-threats).

As technology advances and a greater percentage of commerce is conducted online,[4] web site visitors continually find themselves submitting more and more information about themselves via web site forms in order to conduct activities that recently required face-to-face encounters.[5] This data—often referred to as personally identifying information (PII)—has emerged as a valuable commodity both to individuals and organizations attempting to legally profit from its collection, processing and dissemination (the PII Processing Cycle).[6] Problematically, however, a shady and sophisticated underworld, consisting of technologically-savvy e-thieves and other unsavory actors, has developed alongside these legal

---

Office of Ireland's Data Protection Commissioner, *Article 29 Working Party*, http://www.dataprotection.ie/ViewDoc.asp?fn=/documents/european/article29.htm&CatID=31&m=u (last visited July 25, 2007).

4. Shop.org, *Statistics: U.S. Online Shoppers*, http://www.shop.org/learn/stats_usshop_general.asp (last visited July 25, 2007). E-commerce transactions in 2006 are projected to generate $198 billion and $316 billion in 2010. *Id.*

5. The number of worldwide Internet users surpassed one billion in 2005. *See* Computer Industry Almanac, *Worldwide Internet Users Top 1 Billion in 2005: USA Reach Nearly 200M Internet Users*, http://www.c-i-a.com/pr0106.htm (last visited July 25, 2007). Internet visitors across America may now enter personal information on particular web sites in order to, among other things, obtain a home mortgage, apply for a job or even hire a pet-watching service. *See, e.g.*, Ameriquest Mortgage Company, *Prequalify Now: Request A Loan*, https://www.ameriquestmortgage.com/loan.html?ad=ameriquest.com&requestLoan=true&miniForm=true (last visited July 25, 2007); Monster.com, *Create Account*, http://my.monster.com/Account/Account.aspx?jsinter=1 (last visited July 25, 2007); Camp Bowwow, *Send that Doggy to Camp!*, http://data.gointranet.com/cgi-bin/unitloc/cbw/locator.cgi?cpage=reservation.html&cu=Castle&cl=CBW%20Castle%20Rock (last visited July 25, 2007).

6. *See, e.g.*, *Datran Settles Spam Probe*, L.A. TIMES, Mar. 13, 2006, at C2 (quoting New York State Attorney General Eliot Spitzer's statement that "personal information equals marketing dollars" when discussing a settlement with an Internet marketing company accused of sending out millions of commercial e-mails based on PII obtained from different companies on violation of company privacy policies); ChoicePoint, Overview (employing over 5,000 people in over 60 locations whose primary purpose is to collect and sell PII), http://www.choicepoint.com/about/overview.html (last visited July 25, 2007). ChoicePoint states on its homepage that one of its "data products integrates ChoicePoint proprietary data with third-party data sources to provide unmatched coverage, depth and accuracy on more than 210 million consumers"). ChoicePoint Precision Marketing, http://www.choicepoint.com/business/direct/direct.html (last visited July 25, 2007); Jay MacDonald, *How Much are Your Personal Details Worth*, BANKRATE.COM, http://www.bankrate.com/brm/news/pf/20060221b1.asp (last visited July 25, 2007) (cataloging the "going price" on 46 separate items of PII stemming from a military record worth $35 to a phone number worth $0.25).

uses.[7] Over time, this underworld has come to dominate a section of cyberspace by propounding technologically-advanced e-threats specifically designed to obtain key pieces of PII for various criminal or otherwise unethical purposes.[8]

This Article identifies and categorizes the most dangerous contemporary e-threats—based on their ability to compromise PII—through a model entitled the Privacy Matrix. The Matrix demonstrates how each e-threat impacts consumer privacy during the primary stages of the PII Processing Cycle and explains how businesses, guided by an updated and balanced regulatory privacy regime, can create a safer e-commerce environment. I argue that e-threats targeting PII when businesses first attempt to collect such information from visitors—through a company's "front door"—are less invasive and less dangerous than e-threats targeting PII after its dissemination into cyberspace—through a company's "back door." Accordingly, what is needed is a comprehensive federal statute that is narrowly tailored to protect privacy against front door e-threats, but drafted to morph into a more comprehensive privacy protection regime as PII is shuttled towards a company's back door.

More specifically, the Privacy Matrix is introduced and interpreted in Part II. Part III focuses on the major front door e-threats and argues that a federal statute requiring the posting of a multilayered electronic privacy policy is sufficient to protect consumers at this stage because the decision to provide PII primarily rests with consumers. Part IV moves forward to the prominent e-threats targeting PII stored and processed inside the company and argues that the privacy policy statute must be supplemented with a provision—structured as a regulatory ceiling prohibiting more restrictive state laws—requiring companies to adequately protect stored and processed PII and to notify all PII providers of major security

---

7. Among these legal uses occurs when companies profit by amassing a detailed "digital dossier" containing as many pieces of PII as possible. *See* DANIEL SOLOVE, THE DIGITAL PERSON 1-10 (2004). *See, e.g.*, Jill Burcum, *Hackers' Assaults May Prod Wave of Reforms: Data-Selling Industry Comes Under Scrutiny*, STAR TRIB. (Minneapolis), at A-1 (describing the pieces of PII LexisNexis possessed on a certain individual such as: (1) a Social Security Number (including its date and state of issue); (2) a current employer; (3) every address [he] had lived at over the past twelve years ("including time spent in a California monastery"); (4) information on "past roommates, his brother and his parents, including their ages, past addresses, Social Security numbers and the value of their Twin Cities homes").

8. *See, e.g.*, John Moran, *Spam and the Taste of Money: How Junk E-Mailers Make Fortunes by Pushing Shady Goods to Eager Dupes*, S. FLA. SUN-SENTINEL, Jan. 30, 2005, at 24 (reviewing current literature on spam and the "Internet's seamy underside of bulk e-mail advertising on everything from cut-rate mortgages to penis-enlargement pills"); Tom Zeller Jr., *Countless Dens of Uncatchable Thieves*, N.Y. TIMES, Apr. 3, 2006, at B-3 (discussing international thieves that sell access to U.S. bank account numbers as well as other stolen PII).

breaches. This additional regulation is necessary to protect against the more serious e-threats lurking at this stage—an environment where the initial provider of the PII has less, but still some, control over the information. Part V introduces the e-threats targeting PII at the company's back door and argues that the privacy policy and security breach regulations must now be supplemented by stricter provisions that are specifically passed as regulatory floors allowing individual states room to thoroughly experiment with back door prevention tactics. Comprehensive regulation is necessary at this stage because PII exiting a company's back door is virtually irretrievable by the person it identifies and can be used to cause serious emotional and financial damage with the perpetrators, who nearly impossible to identify. Part VI concludes by summarizing the argument and suggesting areas for further research.

II. THE PRIVACY MATRIX

A matrix is an environment within which "something else originates, develops or takes form,"[9] or, a venue where multiple entities coexist and develop manners of interaction. This concept is appropriate for the e-commerce world where web site visitors, businesses, and Internet scam-artists all operate within an electronically-networked environment, continually collecting, processing, storing, and disseminating PII. This network has spawned a PII-based economy producing billions of dollars annually through the trading of data.[10] At the same time, this emerging market has proven susceptible to evolving e-threats and other sinister activities that interfere with business transactions.

To effectively combat these problems, Congress must address this national issue and enact a statute specifically designed to function within this environment. This approach would prove much more effective than sticking with the plethora of indirectly-related state and federal statutes currently on the books and hoping such a band-aid approach solves the problem.[11] The Privacy Matrix can help shape the design of such laws by

9. MERRIAM WEBSTER'S COLLEGIATE DICTIONARY 717 (10th ed. 2000).

10. In fact, many data-broker companies such as ChoicePoint and LexisNexis profit from the sale of PII. *See, e.g.*, Burcum, *supra* note 7, at A-1 (stating that "[f]or years, [data brokers] have made millions quietly selling personal information to law enforcement, corporations, attorneys, collection agencies and the news media.").

11. This plethora of laws problem occurred primarily because both federal and state legislators recognized the seriousness of these e-threats and rushed to enact legislation designed to protect consumers. Some e-threats were covered while some failed to merit protection. This patchwork approach, although undertaken with good motivations, is actually doing more harm than good as businesses struggle to comply with varying and expensive standards and as consumers

identifying particular e-threats while concurrently developing a regulatory framework designed to protect PII without excessively burdening e-commerce efficiency. In doing so, the Matrix identifies eleven of today's most prominent e-threats and then places each threat at a location where it most directly targets PII—at the front door, inside, or at the back door of a typical e-commerce company.

At their front doors, companies collect many different types of PII such as names, addresses, phone numbers, e-mails, usernames, passwords, credit card information and, sometimes, social security numbers. At this stage, the consumer ultimately chooses whether to visit a particular site and whether to divulge any PII. The Privacy Matrix demonstrates that front door e-threats—such as adware, spyware, phishing, pretexting and active/passive PII collection—should be combated primarily by a federal law mandating only that companies post readable electronic privacy policies. These policies must accurately disclose company privacy practices in understandable terms, thereby allowing individual consumers to make more informed PII-disclosure decisions.

Protecting against e-threats from within the company, on the other hand, lies primarily outside of the control of the consumer and requires stronger regulatory protections. It is not that threats to PII at this stage are more dangerous in and of themselves, rather, the lack of control over PII

---

struggle to understand the various ways and jurisdictions within which they are protected. *See, e.g.*, Joanne McNabb, *Stitching Together the Legislative Patchwork*, TRUSTE.ORG, http://www.truste.org/articles/legislative_patch.php (last visited July 25, 2007). McNabb argues that

> the states are creating a patchwork of incompatible laws that impose burdens and costs on business. California in particular has been criticized for enacting a large number of privacy laws—more than 40 since 1999—some of which effectively set a national standard even though they do not preempt other state or federal laws. In fact, the privacy quilt in the United States is even bigger and more complex. It encompasses a number of federal sectoral laws as well as the numerous laws and regulations of other countries.

Id.; *Privacy*, ARNOLD & PORTER, PRACTICES/INDUSTRIES LLP, http://www.arnoldporter.com/practice.cfm?practice_id=21 (last visited July 25, 2007). Arnold & Porter argue that

> [r]apid changes in technology and rising public concern have thrust information privacy and security to the top of the legal, regulatory, and policy agenda. . . . These same advances, however, pose new threats to individual privacy. Lawmakers at the federal, state, and international levels have responded to this problem by enacting sweeping laws to protect privacy. New privacy proposals are being introduced and debated in Congress, state legislatures, and foreign capitals on a regular basis.

Id.

merits greater regulation. The Matrix identifies that once PII is processed or stored inside a company, it is up to company officials to adequately protect the information from data mining, internally-connected and disconnected use violations, and external security breaches.

Finally, electronic threats to PII take on their most serious form if a company decides to sell or otherwise transfer PII it previously collected and processed and stored. At this point the PII is disseminated into cyberspace where it is virtually irretrievable without any recourse available to the individual it identifies. Privacy-enhancing regulations must strive to protect this information while serving as a regulatory floor from which individual states are allowed to experiment and enact stronger legislation to prevent spam attacks, identity theft and other privacy-invading external uses at this back door stage.

The following sections hone-in on each processing stage by discussing the relevant e-threats and identifying the proper regulatory structure, as defined by the Privacy Matrix, to best protect against them. Part II begins this process by covering the e-threats in existence at a company's front door.

III. E-THREATS AT THE FRONT DOOR (PII COLLECTION)

E-commerce companies and e-consumers become acquainted and initiate business transactions through a World Wide Web interface (webpage) connected to the Internet.[12] This electronic interaction provides the initial opportunity for the visitor to provide, and for the company to collect, particular forms of PII.[13] Companies need some of this information—such as the purchaser's name, physical address, e-mail address, and credit card number—to fully and accurately process various

12. *See, e.g.*, Amazon.com, Homepage, http://www.amazon.com (last visited July 25, 2007) (stating that Amazon allows its customers to create an account, utilized to purchase Amazon products, that will open every time a customer opens Amazon's homepage on the same computer used to create the account).

13. *See, e.g.*, Amazon.com, *Registration*, https://www.amazon.com/gp/flex/sign-in/select.html/002-6636822-1893600?%5Fencoding=UTF8&protocol=https (last visited July 25, 2007) (stating that, upon the creation of a customer account, Amazon collects various forms of PII such as customer name, e-mail, birthday (submitting this PII is optional) and a newly-created (hopefully) password). Later on in the registration process, and in order to complete online purchases, Amazon will need to collect additional PII such as a physical address for billing, a physical address for shipping and a credit card number for each customer. *See, e.g.*, Amazon.com, Privacy Notice: What Personal Information About Customers Does Amazon.com Gather? (discussing the company's PII-collection practices), http://www.amazon.com/gp/help/customer/display.html?ie=UTF8&nodeId=468496 (last visited Dec. 18, 2007).

EXHIBIT 1—*The Privacy Matrix*

	PRIVACY MATRIX REGULATORY FRAMEWORK		
PRIVACY E-THREAT ↓ / PII PROCESSING STAGE →	Front Door (PII Collection)	Inside (PII Utilization)	Back Door (PII Dissemination)
Adware / Spyware	MANDATORY PRIVACY POLICY		
Data Mining		MANDATORY PRIVACY POLICY + REGULATORY CEILING	
Back Door Pretexting			MANDATORY PRIVACY POLICY + REGULATORY FLOOR
Identity Theft			MANDATORY PRIVACY POLICY + REGULATORY FLOOR
Internally-Connected Use		MANDATORY PRIVACY POLICY + REGULATORY CEILING	
Internally-Disconnected Use		MANDATORY PRIVACY POLICY + REGULATORY CEILING	
Phishing		MANDATORY PRIVACY POLICY + REGULATORY CEILING	
PII Collection (Active)	MANDATORY PRIVACY POLICY		
PII Collection (Passive)	MANDATORY PRIVACY POLICY		
Pretexting	MANDATORY PRIVACY POLICY		
Security Breach		MANDATORY PRIVACY POLICY + REGULATORY CEILING	
Spam			MANDATORY PRIVACY POLICY + REGULATORY FLOOR

online transactions.[14] Additionally, however, many companies desire other forms of PII—such as home and employment telephone numbers, social security numbers, mother's maiden name, personal income, or job field/description—merely to supplement a purchaser's database profile.[15] As mentioned previously, companies desire this information because detailed individual profiles are valuable as internal marketing resources as well as assets that may be sold to third parties in the future.[16]

All of this activity occurs at the front door of the company or stage one in the PII processing cycle. This data is typically collected via electronic forms and immediately transferred to company computers where it is processed by powerful databases.[17] Various e-threats operating at this stage can abuse PII by: (1) enticing visitors to voluntarily submit more PII than necessary to complete the transaction (active PII collection),[18] (2) placing cookies, spyware and web beacons on webpages that are able to secretly collect PII (passive PII collection)[19] and (3) obtaining information via the placing of deceptive phone calls/e-mails either by the company itself or by unrelated entities posing as legitimate businesses (pretexting).[20]

---

14. As mentioned above, Amazon would be unable to complete a purchase of a constitutional law textbook without some form of payment information and without some physical address to ship the textbook to. Submitting this information online is one of the major benefits to e-commerce (because textbooks may be rush-ordered at 1:00 am in the comfort of the home) and one of its downfalls (now Amazon has at least six pieces of my PII stored on its computers).

15. *See, e.g.*, *Electronic Edition Registration*, DENV. POST, https://www.post-newscustomercare.com/electronicedition/olivestep1.asp?pub=DP&bhcp=1 (last visited July 25, 2007) (showing that this electronic form is intended for people wishing to subscribe to the electronic version of the *Denver Post*. However, this form requires unnecessary additional PII such as a physical address to complete the subscription).

16. *See, e.g.*, Burcum, *supra* note 7, at A-1 (discussing the sale of PII).

17. American business spent over $15 billion in 2003 merely computerizing information collected on paper-based forms and are now competing to make their information gathering more efficient and more electronic. *See* David Becker, *Software Makers Look for Profits in E-Forms*, CNET NEWS.COM, Oct. 13, 2003, http://news.com.com/2100-1012-5089536.html. While large companies staff entire Information Technology Departments, smaller companies may outsource their electronic form creation and integration to companies like Logiforms.com; Logiforms.com creates an electronic form for a small business and any data provided via the form is stored in a "secured web-based database and can be accessed from anywhere." Logiforms.com, Data Management: Submissions Management, http://www.logiforms.com/index.lf/method/featuredetails/parent/data (last visited July 25, 2007).

18. *See supra* text accompanying note 15 (discussing the idea that the *Denver Post Electronic Edition* required an individual's physical address in order to subscribe).

19. *See infra* text accompanying notes 21-52 (detailing description and further resources on the e-threats of adware/spyware, cookie technology, and web beacons).

20. *See infra* text accompanying notes 53-64 (detailing description and further resources on the e-threat of pretexting).

Both active and passive PII collection are activities generally initiated and conducted by employees and independent contractors of the company collecting the information and can be classified as internally-created e-threats. On the other hand, pretexting is generally initiated by non-company-related individuals pretending to be associated with the company and is more properly classified as an externally-created e-threat. The following section describes each of these three e-threats in more detail beginning with the internally-created threats and then moving to the externally-created threats. This part concludes with the argument that a new federal law requiring all e-commerce businesses collecting, processing or disseminating PII in interstate commerce to post a standardized electronic privacy policy is the most efficient way to minimize the effectiveness of each kind of front-door e-threat.

A. *Internally-Created "Front Door" E-Threats*

E-commerce web sites collect PII in two ways: (1) actively and (2) passively.[21] Companies actively collect PII by requiring consumers to enter information through web site forms or by replying to e-mail registration messages.[22] During this active collection process, customers must "volunteer" all different types of information in order for the web site to process a transaction or create an account. The failure to enter PII into a

---

21. *See, e.g.*, MICRO-TEL, *Privacy Policy*, http://www. microcall.com/privacy.html (last visited July 25, 2007). MICRO-TEL discusses active and passive PII collection as follows:

> Active Personal Information Collection
>
> This Website collects your Personal Information using active collection methods, such as feedback forms, e-mail response mechanisms, or other forms where you are asked to provide Personal Information. This Web site will inform you at such information collection points as to what information is required to obtain the requested services and what information is optional.
>
> Passive Information Collection
>
> In addition to the active collection methods described above, this Website also passively collects other information from and about you using various technologies such as IP addresses, cookies, or GIFs, as those are discussed in this section.

Id. (disclosing in its privacy policy that the company conducts both types of collection).

22. *See, e.g.*, Johnson & Johnson Pharmaceutical Research and Development, *Privacy Policy*, http://www.jnjpharmarnd.com/privacy.html (last visited July 25, 2007) (discussing the fact that Johnson and Johnson actively collects PII from web site visitors in the form of e-mail, electronic forms provided to conduct transactions, promotions and sweepstakes, and chat rooms).

required field will delay or end the web session causing consumers to miss the opportunity they went online to obtain in the first place. Active PII collection is generally benign and necessary to conduct online transactions. The threats to privacy occur when companies require the submission of unnecessary information to complete a transaction.

Passive PII collection, on the other hand, occurs when web sites collect PII via covert programs without the knowledge or consent of the visitor. Despite the mysterious nature of these collection instruments, e-commerce operations commonly utilize passive PII collection and are able to collect much more PII from consumers than a similar brick-and-mortar business could obtain.[23] Passive PII collection most commonly occurs through cookies, web beacons, spyware, and adware. Problematically, if a user chooses to disable cookies or monitor the source code of web sites only choosing those locations without web beacons, spyware, or adware, most of the World Wide Web becomes off-limits.[24] While active collection is obvious to all parties, the instruments of passive PII collection are nearly invisible and deserve more analysis.

A cookie is:

> A message given to a Web browser by a Web server. The browser stores the message in a text file. The message is then sent back to

---

23. *See, e.g., id.* (laying out how the company collects information—via cookies, web beacons and other "navigational data"—without web site visitors purposefully submitting any PII); Rachel Zimmerman, *Note: The Way the Cookies Crumble: Internet Privacy and Data Protection in the Twenty-First Century*, 4 N.Y.U. J. LEGIS. & PUB. POL'Y 439, 442 (2001) (stating that "when people log on to the Internet and visit Web sites, a great deal of personal information is collected through both active user participation and passive collection techniques"); Andrew Shen, *Symposium: Online Activities and their Impact on the Legal Profession: The Current State of Online Privacy*, 16 ST. JOHN'S J.L. COMM. 621, 621-622 (2002) (stating that the architecture of the Internet allows much more information to be collected passively than currently occurs in the offline world).

24. Techsoup.org, *Cookies: You are Never Alone on the Internet: Tiny Text Files on Your Hard Drive can be Revealing*, http://www.techsoup.org/learningcenter/internet/page5051.cfm (last visited May 28, 2006). Techsoup.org discusses cookies and the idea a web surfer is likely to be frustrated with the results of disabling cookies:

> > You can disable cookies entirely, but that is probably not a good idea, as many sites depend on cookies to function properly. If you use a Web-based e-mail program, you must have cookies enabled. Any site where you have to register to use its content needs cookies. You can set the browser to warn you or ask permission to send cookies, but that can be intrusive, and you may be driven to distraction by the number of times you are asked to accept a cookie before a site will serve up a page.
>
> *Id.*

> the server each time the browser requests a page from the server. . . . The main purpose of cookies is to identify users and possibly prepare customized Web pages for them. When you enter a Web site using cookies, you may be asked to fill out a form providing such information as your name and interests. This information is packaged into a cookie and sent to your Web browser which stores it for later use. The next time you go to the same Web site, your browser will send the cookie to the Web server. The server can use this information to present you with custom Web pages.[25]

There are two types of cookies: (1) persistent cookies and (2) session cookies.[26] Persistent cookies are stored on a web site visitor's computer and are not deleted when the browser session is closed.[27] Because the text file remains on the user's computer, it may be used to identify the user on return visits to the web site and return the browser to the format the web site was in when the user last visited.[28] This customization effect allows for a more user-friendly experience, but it also presents a threat as it allows companies to track user behavior over long periods of time.[29]

---

25. Webopedia.com, *Cookie*, http://www.webopedia.com/TERM/c/cookie.html (last visited July 25, 2007). Cookies were developed in 1995 by Netscape Communications Corporation and are allegedly named after a programming term called a "magic cookie"—a "piece of information shared between co-operating software." Aboutcookies.org, *Cookies: Frequently Asked Questions*, http://www.aboutcookies.org/Default.aspx?page=5 (last visited July 25, 2007). Cookies are stored on a web site visitor's hard drive as .txt or text files. *Id.*

26. *See* Michael Siebecker, *Cookies and the Common Law: Are Internet Advertisers Trespassing on Our Computers?*, 76 S. CAL. L. REV. 893, 897 (defining the terms session cookies and persistent cookies and discussing how cookies operate and are placed on a web site visitor's hard drive).

27. *See* Aboutcookies.com, *supra* note 25 (discussing the fact that persistent cookies are designed to track individual users for long periods of time—"in some cases many years into the future").

28. *Id.* (stating that persistent cookies provide cumulative data which may be used to analyze the user's behavior while surfing the particular web site).

29. Cookies allow web sites to track individual as well as overall visitor behavior. For instance, companies utilize databases and cookies to track individual visitors in the following manner:

> The first time a visitor arrives, the site creates a new ID in the database and sends the ID as a cookie. The next time the user comes back, the site can increment a counter associated with that ID in the database and know how many times that visitor returns.

Marshall Brain, *How Internet Cookies Work*, HOWSTUFFWORKS.COM, http://computer.howstuffworks.com/cookie3.htm (last visited July 25, 2007). As for tracking overall web site

Session cookies, on the other hand, are stored in the computer's memory and are deleted when the browser session is closed.[30] Session cookies also track user information, but only for brief periods of time. Additionally, technology exists that allows digital advertising companies such as DoubleClick[31] to place a cookie on hard drives in order to monitor web-surfing over numerous web sites and thereby create a larger profile of an individual's Internet activities.[32] In fact, DoubleClick recently caused a privacy firestorm when it announced that it would link these rich profiles to names and addresses through a business transaction with a marketing company called Abacus Direct.[33]

---

visitation, the implementation of cookies allows a company to trace the overall number of visitors of a specific period of time. Web sites can

> accurately determine how many people actually visit the site. It turns out that . . . the only way for a site to accurately count visitors is to set a cookie with a unique ID for each visitor. Using cookies, sites can determine: [h]ow many visitors arrive; [h]ow many are new vs. repeat visitors; [and how] often a visitor has visited.

Id.

30. *See* Aboutcookies.com, *supra* note 25 (discussing that session cookies are particularly helpful on web sites containing a shopping cart that will keep track of selected items until the check-out process is completed).

31.

> DoubleClick places advertisements on Web sites belonging to the DoubleClick network. DoubleClick then tracks the Internet users who receive the ads at the various Web sites and assigns the user a unique number. DoubleClick records the number in a cookie file. Advertisers then can use the cookie file to target specific users.

FTC Ends DoubleClick Investigation, CONSUMER FIN. SERVICES L. REP., Feb. 20, 2001, at 15 [hereinafter *DoubleClick Investigation*].

32. *See* Brain, *supra* note 29. Brain states that

> [t]here are certain infrastructure providers that can actually create cookies that are visible on multiple sites. DoubleClick is the most famous example of this. Many companies use DoubleClick to serve banner ads on their sites. DoubleClick can place small (1x1 pixels) GIF files on the site that allow DoubleClick to load cookies on your machine. DoubleClick can then track your movements across multiple sites. It can potentially see the search strings that you type into search engines (due more to the way some search engines implement their systems, not because anything sinister is intended). Because it can gather so much information about you from multiple sites, DoubleClick can form very rich profiles.

Id.

33. *See Company News: DoubleClick to Buy Retailing Data Base Keeper*, N.Y. TIMES, June 15, 1999, at C-4 (discussing DoubleClick's plans in 1999 to acquire Abacus Direct Corp., a company that manages data on items people purchase, in an effort to utilize Abacus's database "of

Functionally, cookies are not particularly dangerous[34] and can actually create a more efficient Web-surfing experience as users are not required to continually enter usernames and passwords and click back through to their desired webpage during new sessions. However, the covert collection of information and the potential dissemination to third parties is problematic because web sites can covertly collect more information from an individual than a brick-and-mortar establishment executing a traditional transaction.[35] This excessive collection of PII may lead to more information being sold in the open market to willing buyers, which may include e-thieves.[36] Although users can disable cookies via a browser tool if they are uninterested in the benefits, web sites also should bear some responsibility for clearly disclosing the fact that cookies are used to passively collect PII.[37]

---

consumer behavior to better direct advertising to consumers"). Upon announcement of the deal shares, DoubleClick's stock "fell $18.0625, to $70.75, and shares of Abacus were down $7.0625, to $67.50." *Id.* As for the outrage, see, e.g., *Privacy Groups See Danger in a Merger*, N.Y. TIMES, June 22, 1999, at C-6. This *New York Times* article states that

> [l]eading privacy advocates . . . blasted the $1 billion merger of the Internet advertising firm Doubleclick Inc. with the Abacus Direct Corporation, a consumer data collector, arguing that the combination would collect far too much personal information about consumers. The nonprofit Electronic Privacy Information Center and the privacy-oriented Web site Junkbusters . . . said they would probably ask regulators to block the deal if the companies proceeded.

Id. Later, the FTC commenced, and subsequently dropped, an investigation into whether these actions by DoubleClick violated its privacy policy that claimed that PII collected by DoubleClick would remain confidential. *See DoubleClick Investigation*, *supra* note 31 (stating that the FTC claimed that it ended its investigation because the evidence demonstrated that DoubleClick did not violate its privacy policy or the FTC Act which prohibits deceptive commercial practices).

34. *See* Aboutcookies.com, *supra* note 25 (discussing the idea that cookies are merely text files that cannot be used to scan a user's hard drive or to transmit viruses and may be shut down by the user through a browser function).

35. *See, e.g.*, Brain, *supra* note 29. Brain states that,

> [o]n a Web site, the site can track not only your purchases, but also the pages that you read, the ads that you click on, etc. If you then purchase something and enter your name and address, the site potentially knows much more about you than a traditional mail order company does. This makes targeting much more precise, and that makes a lot of people uncomfortable.

Id.

36. *See id.* (arguing that e-commerce companies sell PII obtained via cookies in the marketplace in a similar manner as traditional collectors of information); Shen, *supra* note 23.

37. *See* discussion *infra* Part III.C. A few states have sued companies alleging that covert collection of PII constituted an invasion of privacy. *See, e.g.*, Aaron Chambers, *Web Ventures*

A web beacon can be described as follows:[38]

> Used in combination with cookies, a Web beacon is an often-transparent graphic image, usually no larger than 1 pixel x 1 pixel, that is placed on a Web site or in an e-mail that is used to monitor the behavior of the user visiting the Web site or sending the e-mail. When the HTML code for the Web beacon points to a site to retrieve the image, at the same time it can pass along information such as the IP address of the computer that retrieved the image, the time the Web beacon was viewed and for how long, the type of browser that retrieved the image and previously set cookie values.[39]

Web beacons are relatively simple to create and are generally embedded inconspicuously into a webpage.[40] Therefore, when web site visitors

---

Accused of Cookie Fraud, CHI. DAILY LAW BULL., Dec. 12, 2000, at 1 (discussing a lawsuit initiated by the state's attorney's office in Cook County Illinois against DoubleClick, Inc. and ClearStation Inc. "for violating the Illinois Consumer Fraud and Deceptive Business Practices Act by misleading Internet users about their practice of sending small bits of data—called cookies—to the user's computer when the user visits ClearStation's Web site."). *But see Court Dismisses Suit Against Internet Advertising Firm DoubleClick*, CONSUMER FIN. SERVICES L. REP., May 14, 2001, at 21 (discussing the dismissal of a class action lawsuit filed by individuals who claimed that DoubleClick's accessing of cookies on their computer hard drives violated, *inter alia*, the Electronic Communications Privacy Act); *Attorneys General Reach Agreement with Internet Company to Protect Consumer Privacy,* NAAG AG BULL., Aug. 2002 (discussing a settlement between the attorneys general of nine states (Arizona, California, Connecticut, Massachusetts, Michigan, New Jersey, New Mexico, New York, Vermont, and Washington) and DoubleClick whereby the company promised not to use certain pieces of PII obtained from cookies in placing web-based advertisements).

38. Web beacons are also commonly referred to as web bugs, clear gifs, and pixel tags. *See, e.g.*, Thomas Fitzgerald, *Microsoft Swats at Stealthy Web Bugs*, N.Y. TIMES, June 12, 2003, at G-4.

39. Webopedia.com, *Web Beacon* [hereinafter *Web Beacon*], http://www.webopedia.com/TERM/W/Web_beacon.html (last visited July 25, 2007).

> Many Web bugs work in tandem with cookies, which are different creatures. Web bugs are usually invisible images on a Web page; cookies are text files that Web sites place on our computers to identify us. Marketers use Web bugs to signal to sites other than the ones you're visiting to put a cookie on your computer.

Leslie Walker, *Bugs that Go Through Computer Screens*, WASH. POST, Mar. 15, 2001, at E-1. A recent search for the number of web beacons in existence on the Web (researched through an examination of fifty-one million webpages) discovered that "seventy-four percent had bugs that tracked visitors from third-party Web sites." *Id.*

40. *Web Beacon*, *supra* note 39. Web beacons are easily detectable by someone with a computer science background and "can be detected by viewing the source code of a Web page and looking for any IMG tags that load from a different server than the rest of the site." *Id.* "Turning off the browser's cookies will prevent Web beacons from tracking the user's activity. The Web

browse the webpage, certain pieces of personal information are collected without notification.[41] These bits of data may later be aggregated with PII actively collected, or PII obtained from another passive collection technique, to form a more complete picture of the visitor that may be sold in the data marketplace.[42] Web beacons present a threat because PII is being collected covertly and for purposes unrelated to the transaction or webpage viewing at hand.

Spyware is:

> [S]oftware that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet . . . Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can also gather information about e-mail addresses and even passwords and credit card numbers.[43]

Spyware possesses the capability to, among other things, monitor keystrokes, scan hard drive and other program files, install other spyware

---

beacon will still account for an anonymous visit, but the user's unique information will not be recorded." *Id.*

41. *See, e.g.*, David Lazarus, *Now Taxes Can Really Bug You*, S.F. CHRON., Apr. 13, 2005, at C-1 (quoting a representative from an Internet company charged with monitoring data collected by this technology who was discussing web bugs and who stated: "We could capture your name, your Social Security number or any other information that you willingly pass to a Web site [through a web bug]"). This collection is serious as a reporter from the *Washington Post* who claimed:

> I picked up the bug by visiting [an Internet company's web site containing web beacons], and it managed to slip past the 'fire wall' and anti-virus software that is supposed to protect both of my machines. During the test, the bug sent copies of two personal files back to [the company] and left behind a hidden file on my hard drive.

Walker, *supra* note 39 (discussing the idea that these web beacons can collect PII).

42. *See, e.g.*, David Lazarus, *Web Bugs May Break State Law*, S.F. CHRON., Apr. 20, 2005, at C-1 (discussing the placement of web beacons onto webpages where people conduct online tax preparation and the idea that outside disclosure of PII gained from a tax return, or from the preparation of a tax return, may violate the California Business and Professions Code unless consented-to by the customer).

43. Webopedia.com, *Spyware*, http://www.webopedia.com/TERM/s/spyware.html (last visited July 25, 2007).

programs and read cookie files.[44] Adware is "a form of spyware that collects information about the user in order to display advertisements in the Web browser based on the information it collects from the user's browsing patterns."[45] Adware is often programmed to go out of control and display endless advertisements. This barrage of pop-ups often connect a browser to a particular homepage instead of the homepage the user desires typically when the "home" button is clicked the user is automatically taken to the new homepage even though she desires her selected homepage.[46] At its worst, adware hinders an Internet user from conducting any business whatsoever online.

These two programs are threats to e-commerce because of their ability to covertly monitor an individual's web activities and collect and store valuable PII such as usernames, passwords, and credit card information.[47] On the other hand, it is important to keep in mind that spyware and adware, like cookies, are not always privacy-invasive technologies.[48] Many companies bundle adware with software they distribute for free and disclose this fact on their web sites.[49] Therefore, if a user is fully aware of an adware program on a computer and chooses to install free software, such user has consented to the web monitoring and may even appreciate the targeted advertisements generated in return for the free software.

Businesses often install their own, or allow third parties to install, separate spyware on customers' computers when such individuals download a program or visit a web site—in other words, at the front

44. *See, e.g.*, Webopedia.com, *The Difference Between Adware & Spyware*, http://www.webopedia.com/DidYouKnow/Internet/2004/spyware.asp (last visited July 25, 2007) [hereinafter *Difference Between Adware & Spyware*] (describing all of the malicious activities that spyware may conduct).

45. Webopedia.com, *Adware*, http://www.webopedia.com/TERM/a/adware.html (last visited July 25, 2007).

46. Cliff Joseph, *Spyware Under the Microscope*, VNUNET.COM, Sept. 26, 2005.

47. *Id.* (comparing the threat of spyware to the threat of computer viruses). The fact that spyware is a threat is why it has also been given the name "malware" which stands for "malicious software." *Id.*

48. For a recap of the difference between adware and spyware, see *supra* text accompanying 43-47 (describing adware as a "legitimate alternative offered to consumers who do not want to pay for software"). Properly functioning adware should disable itself when the software program is closed. *Id.*

49. *See, e.g.*, Eudora.com, *Three Modes: Choose the Eudora That's Best for You*, http://www.eudora.com/email/modes/ (last visited July 25, 2007) (distributing an e-mail software program in three ways, two of which allow users to download and use the software for free in return for the installation of adware containing an advertisement window and up to three sponsored toolbar links); Google, *About Gmail*, http://mail.google.com/mail/help/intl/en/about.html (last visited July 25, 2007) (demonstrating that this free e-mail service offered by Google places small text advertisements on e-mail correspondence based on the content of user e-mails which can be considered a form of adware).

door.[50] In fact, many End User License Agreements (EULA) state that the company providing the software or the download at issue are free to also pass on "third party software" to the visitor's computer.[51] Often, this third party software is some form of spyware or adware.[52] Therefore, bundling of spyware with downloaded software may produce a treasuretrove of valuable information by which the company may then target its marketing efforts or sell to third parties.

While these company-initiated e-threats may seem innocuous at first, it is important to keep in mind that, when combined together, these e-threats can lead to a complete digital profile of web site visitors. These profiles allow companies to tailor targeted marketing packages at specific individuals. These profiles are also valuable commodities that can be sold on the open market. If such profiles fall into malicious hands, serious invasions of privacy loom on the horizon.

B. *Externally-Created "Front Door" E-Threats*

Pretexting is the practice of collecting PII utilizing false pretenses and is a much more serious threat than active or passive PII collection. According to the Federal Trade Commission (FTC), pretexters use a variety of tactics to get your personal information:

---

50. *See* CIBC.com, *Spyware: What is Spyware*, http://www.cibc.com/ca/legal/spyware-info.html (last visited July 25, 2007) (stating that spyware "has become a leading security problem for Internet users and is now more widespread than spam or virus infections").

51. *See, e.g.*, Google Labs, *Picasa End User License Agreement*, http://picasa.google.com/linux/eula.html (last visited July 25, 2007). Google Labs discusses the issue of third party software in the EULA for Picasa's photo management software:

> Thank you for trying out the Picasa software! By using this software, including certain third party software made available in conjunction with this software but not including software provided in source form and expressly licensed under other terms as set forth at http://code.google.com . . . you agree to accept a license under and be bound by the following terms and conditions of this agreement . . . with Picasa LLC and Google Inc. . . .).

Id.

52. *See, e.g.*, Jeffrey Benner, *Spyware, In a Galaxy Near You*, Wired.com, Jan. 24, 2002, http://www.wired.com/news/technology/0,49960-0.html (discussing a third party software spyware program covertly bundled with a popular screensaver download); Peter Rojas, *Kazaa Lite: No Spyware Aftertaste*, WIRED.COM, Apr. 18, 2002, http://www.wired.com/news/mp3/0,1285,51916,00.html (reporting that users of Kazaa's Media Desktop—a file-sharing program for electronic entertainment files—had unknowingly downloaded third party spyware along with the Media Desktop software).

> For example, a pretexter may call, claim he's from a survey firm, and ask you a few questions. When the pretexter has the information he wants, he uses it to call your financial institution. He pretends to be you or someone with authorized access to your account. He might claim that he's forgotten his checkbook and needs information about his account. In this way, the pretexter may be able to obtain personal information about you such as your SSN, bank and credit card account numbers, information in your credit report, and the existence and size of your savings and investment portfolios.[53]

Pretexting may come in the form of a phone call where the caller pretends to be someone else, or in the form of an e-mail whereby the sender appears to represent someone else. Legitimate businesses will not utilize deceptive practices to obtain additional customer PII; however, pretexters are successful because individuals or businesses possessing PII are not fully aware of this fact and often believe that the party contacting them is legitimate.[54] Pretexting violates at least two federal laws: (1) The Federal Trade Commission Act (FTCA)[55] and the Gramm-Leach-Bliley Act (GLBA).[56] The FTC is actively pursuing violations of these statutes from pretexting, especially as it pertains to the fraudulent collection of financial PII, and has brought several high profile pretexting-related enforcement actions beginning in 1999.[57]

---

53. FTC, Facts for Consumers: Pretexting: Your Personal Information Revealed [hereinafter FTC, Facts for Consumers], http://www.ftc.gov/bcp/conline/pubs/credit/pretext.htm (last visited July 25, 2007).

54. *See, e.g.*, Fed. Trade Comm'n v. Information Search, Inc & David Kacala, *Complaint for Injunctive and Other Equitable Relief*, Civil Action No. AMD-01-1121 (D. Md. N.D.), Apr. 18, 2001, 3-4 (demonstrating that, in this civil lawsuit that ended in a negotiated settlement, the FTC claimed that an information data broker utilized pretexting techniques such as false pretenses, fraudulent statements and impersonations to successfully obtain and later sell confidential financial information in the form of bank account statements and balances).

55. 15 U.S.C. § 57a(a)(1)(B) (2000).

56. Pub. L. No. 106-102, 113 Stat. 1338 (Nov. 12, 1999) (codified as amended in scattered sections of 12 and 15 U.S.C.).

57. *See, e.g.*, Fed. Trade Comm'n v. James Rapp & Touch Tone Information, Inc., Complaint for Injunction and Other Equitable Relief, Civil Action No. 99-WM-783 (D. CO), Apr. 21, 1999 [hereinafter *Touch Tone*], *available at* http://www.ftc.gov/os/1999/04/touchtonecomplaint.htm (demonstrating that, in a case that later settled, the FTC complained that Touch Tone Information violated § 5 of the FTCA by utilizing pretexting in the form of false statements to employees of financial institutions in various attempts to obtain financial account information that the company would later sell); Fed. Trade Comm'n v. 30 Minute Mortgage, Inc., Civil Action No. 03-60021 (S.D. FL.), Complaint for Injunctive and Other Equitable Relief, Jan. 8, 2003, 3-5, [hereinafter *30 Minute Mortgage*], *available at* http://www.ftc.gov/os/2003/03/30mincmp.pdf (demonstrating that,

To see why pretexting can constitute a serious e-threat, one must only consider the tragic story of Amy Boyer. A former junior high school classmate of Boyer hired a private investigation service, Docusearch.com, in an effort to determine her current whereabouts.[58] For $150,[59] Docusearch searched various public records databases and obtained pieces of PII concerning Boyer, including her social security number, but failed to locate her employment address. In order to obtain this information, someone from the investigative service placed a phone call to Boyer pretending to be from her insurance company—a classic form of pretexting.[60] Boyer, believing that the caller was legitimate, responded with the desired information that was transmitted to her

---

in a case that would later settle, the FTC complained that 30 Minute Mortgage engaged in pretexting and violated, among other statutes, § 5 of the FTCA when the company sent out e-mails pretending to be a national mortgage lender when, in fact, the company merely collected PII in the form of addresses, phone numbers, social security numbers. Income and mortgage information and bank account types and balances and then sold this information to actual mortgage lending companies). Additionally, in January 2001, the FTC announced the kick-off of its "Operation Detect Pretext." Fed. Trade Comm'n, *FTC Kicks Off "Operation Detect Pretext,"* Jan. 31, 2001, *available at* http://www.ftc.gov/opa/2001/01/pretexting.htm. In this effort, aimed at actively looking for companies selling financially-related PII online and advising such companies that pretexting is illegal under the GLBA, the FTC looked at over 1,000 web sites and 500 print advertisements and sent over 200 letters advising these firms of their obligations under the GLBA. *Id.*

58. *See* Robin Washington, *Online Trail to Murder: Slain Girl's Kin Sue Internet Co. for Selling Data to Killer*, BOSTON HERALD, Apr. 28, 2000, at 5 (stating that Boyer's family sued the data trading company for wrongful death for providing "the private information he used to track her down and kill her."). This lawsuit was eventually settled for 85,000. *See* Holly Ramer, *Mother of Slain Woman Settles Lawsuit Against Info-Broker*, USA TODAY, Mar. 10, 2004, http://www.usatoday.com/tech/news/internetprivacy/2004-03-10-boyer-suit-settled_x.htm (discussing that, in the case, Docusearch.com claimed that none of the information it sold on Boyer was private).

59. *See* Holly Ramer, *Mother of Slain Woman Settles Lawsuit Against Info-Broker*, USA TODAY.COM (Mar. 10, 2004) (discussing the fact that the killer paid $150 to obtain this information), http://www.usatoday.com/tech/news/internetprivacy/2004-03-10-boyer-suit-settled_x.htm.

60. *See* Electronic Privacy Information Center.org, *Amy Boyer Case,* Resinburg v. Docusearch, http://www.epic.org/privacy/boyer/ (last visited July 25, 2007).

> Docusearch obtained Boyer's work address by having a subcontractor, Michelle Gambino, place a "pretext" call to Boyer. Gambino lied about who she was and the purpose of her call in order to convince Boyer to reveal her employment information—Gambino pretended to be affiliated with Boyer's insurance company, and requested "verification" of Boyer's work address in order to facilitate an overpayment refund. Docusearch charged [Ms. Boyer's murderer] $109 for this information.

Id.

stalker/Docusearch's client and used to track her down at work where she was subsequently shot and killed.[61]

Boyer's parents filed a civil lawsuit against Docusearch for wrongful death and invasion of privacy among other claims.[62] Four years later, the New Hampshire Supreme Court ruled that information brokers such as Docusearch.com must exercise "reasonable care in disclosing a third person's personal information to a client."[63] Although the case of Amy Boyer clearly represents an extreme situation of pretexting gone bad, many other cases of pretexting have led to cases of identity theft and have caused much more PII to exist in cyberspace.[64] Pretexting has fast become a serious e-threat.

C. *U.S. Law Operating at the Front Door*

A company's front door is the only stage of the PII processing cycle where web site visitors maintain primary control over submission of their PII into cyberspace. At the front door, no individual is forced to conduct an online transaction and every web-surfer has the option of leaving a web site before entering personal information.[65] In a perfect online world, consumers would rationally make this decision after being accurately informed of the kinds of PII collected, the uses the information may be put

---

61. The killer then turned the gun on himself and committed suicide. *Id.* (stating that the killer even wrote the following on a web site dedicated to his obsession with Boyer: "I found an internet site to do that, and to my surprize [sic] everything else under the Sun. Most importantly: her current employment. It's accually obsene [sic] what you can find out about a person on the internet." *See* Washington, *supra* note 58).

62. *See, e.g., id.* (stating that the wrongful death claim against Docusearch alleged that the company owed a duty to Boyer to not reveal her PII to a client for non-legitimate purposes and the invasion of privacy claims alleged an intrusion upon seclusion and a commercial appropriation of private information).

63. Remsburg v. Docusearch, Inc., 816 A.2d 1001, 1009 (N.H. 2003) (discussing the court's statement that "this is especially true when . . . the investigator does not know the client or the client's purpose in seeking the information.").

64. *See, e.g.*, FTC, Facts for Consumers, *supra* note 53 (stating that the FTC has dedicated an entire webpage to the issue of pretexting offering tips on how to avoid becoming a victim and providing contact information for complaints).

65. Remember, passive PII collection may occur from the first instance a webpage is loaded onto the visitor's computer screen through cookies, web beacons, spyware, and adware. However, these programs alone cannot collect the massive amounts of information that active collection can and users exiting a web site without volunteering any information will generally avoid major pitfalls. This could all change, however, as passive PII collection devices become more sophisticated and able to collect more PII. *See* Thomas A. Hemphill, *Identity Theft: A Cost of Business?* 106 BUS. & SOC'Y REV. 1, 53 (2001) (discussing identity theft—a prominent e-threat—and stating that "protecting personal identifying information from public consumption is initially the responsibility of the consumer.").

to, and other important privacy aspects of the e-commerce relationship. Unfortunately, the contemporary online environment is far from perfect. Today, many web site visitors do not understand the privacy implications of entering their information online and have little idea how web sites plan to use this information. Compounding this problem is the fact that company privacy policies—a company's primary, and sometimes only, vehicle for relaying its privacy practices to the general public—are often inconspicuously linked at the bottom of homepages, written in small print and filled with legalese. These attributes make the terms and conditions of such policies very difficult to read and interpret. In order for e-consumers to take responsibility for their actions on the Web—a situation that policymakers should encourage—fair information practices should require standardized and readable e-commerce privacy policies. The current United States information privacy regulatory regime does not require these types of privacy polices and, subsequently, is not fostering an environment where e-consumers can legitimately make educated decisions concerning their PII at the front door stage.

To help remedy this problem, this Article argues that the U.S. Congress should enact a statute focused only on protecting PII from the various types of e-threats that threaten such information throughout the PII processing cycle.[66] The front door section of this regulation should require that all companies conducting business online and operating in interstate commerce (covered companies) post a link to a standardized, multilayered and readable privacy policy on their web site homepage. Although covered companies should not be required to adopt particular privacy-enhancing policy terms at this early stage, every aspect of their actual privacy policy, even if privacy-invasive and potentially unpopular, must be described accurately. Granting businesses greater flexibility to choose their own privacy terms at the front door is appropriate because consumers retain control over their PII at this stage and bear some of the responsibility for protecting it. This section of the law will encourage consumer diligence as web site visitors, armed with the information they obtain from reading and understanding the basics of the simplified policy, will be able to make more informed decisions as to whether the company's policies warrant the disclosure of any PII. At the same time, businesses will retain the freedom

66. Any statute that is to effectively target these dangerous e-threats must be drafted specifically for this purpose. Today's patchwork regulatory scheme that indirectly targets these threats is insufficient—especially as the threats grow more technologically advanced. As mentioned previously, the statute proposed in this Article will consist of three primary parts: (I) regulation targeting front door e-threats; (II) regulation targeting inside the company e-threats; and (III) regulation targeting back door e-threats. Its sole purpose will be to mitigate or eliminate the various e-threats at each stage of the PII processing cycle.

to structure their privacy policies free from excessive regulation. At this early stage in the PII processing cycle, both sides should be satisfied with this compromise approach.

To bring this vision to fruition, the proposed law should require that all covered companies post electronic privacy policies that: (1) are standardized and multilayered, (2) contain specific sections but not specific language, and (3) are understandable to the typical web site visitor. Finally, the law must be structured as a regulatory ceiling to allow for maximum effectiveness at this early stage.

1. Privacy Policies Must be Standardized and Multilayered

Multilayered privacy policies represent the future of online privacy disclosure.[67] This is an encouraging trend because such policies are easier

---

67. *See, e.g.*, Marty Abrams & Malcolm Crompton, *Multi-Layered Privacy Policies: A Better Way*, PRIVACY L. BULL., May/June 2005, at 1. Abrams & Crompton state that:

> Privacy notices are the windows to how organisations collect, use, share and protect the information that pertains to individuals. As information processes have become more complex, privacy notices have become very long, mirroring this complexity. The effect has been to obscure the content that individuals need to know when making judgments about with whom they will do business. The lack of clarity has been an impediment to online commerce.

Id. This Article describes a framework for assuring that notices are easy both to understand and follow as well as to complete. These objectives are achieved by layering up to three documents as part of a notices package. This approach, supported by an ad hoc group of civic, business, and government participants, has been adopted by the European Union's Art 29 working party in Opinion WP100, issued in 2004.). The Center for Information Policy Leadership has taken the lead in the United States to promote the usage of multilayered privacy policies. *See, e.g.*, *Multi-Layered Notices Explained*, Center for Information Policy Leadership White Paper, Feb. 2005, http://www.hunton.com/files/tbl_s47Details/FileUpload265/1303/CIPL-APEC_Notices_White_Paper.pdf (describing the problems with contemporary privacy policies and the process of creating a multilayered privacy policy); *Ten Steps to Develop a Multilayered Privacy Notice*, Center For Information Privacy Leadership, Feb. 16, 2006 [hereinafter *Ten Steps*], http://www.hunton.com/files/tbl_s47Details/FileUpload265/1405/Ten_Steps_whitepaper.pdf. Additionally, the concept of a multilayered privacy policy is becoming standard-fare for government webpages. *See, e.g.*, Melanie Goldwater, *Privacy Commissioner Releases New Multi-Layered Privacy Policy for Her Office*, Minter Ellison, Aug. 31, 2006, http://www.minterellison.com/public/connect/Internet/Home/Legal+Insights/Newsletters/Previous+Newsletters/A-E-Privacy+Commissioner+releases+new+multi-layered+privacy+policy+for+her+Office. Goldwater states that

> The Privacy Commissioner [of Australia], Karen Curtis has announced that her Office will adopt a multi-layered privacy policy. The new format includes two versions of the organisation's privacy policy: a condensed "snapshot" of the Office's practices; and a full version of its privacy policy, which contains detailed information about the Office's legal obligations. Ms Curtis has indicated that the

to understand and present a far more standardized privacy picture than their contemporary counterparts. Web site visitors viewing a multilayered policy are better able to evaluate the actual privacy practices of the e-commerce web sites they visit. Additionally, the creation of such policies is inexpensive and relatively simple. A multilayered privacy policy consists of three versions (layers) specifically tailored to the environment where the policy will be posted. The process of tailoring the policy format to the viewing environment is designed to promote the visibility of privacy terms and to encourage people who notice the policy terms to actually read them.

Companies that desire to create a compliant multilayered privacy policy should start by drafting a comprehensive policy before creating any subsequent layers. This version of the privacy policy will be the most lengthy of the three and must contain seven specific headings designed to cover subjects such as a summary of the major pieces of PII collected, the utilization of such information, and a short discussion of other relevant privacy information.[68] This document is referred to as the third layer in this tripartite format and should be linked to the company's homepage. There is no length requirement for this third layer, although companies must draft the policy so that it can be read and understood by the average web site visitor.[69] As mentioned previously, the proposed federal law should not require companies to adopt any specific privacy practices at this early stage in the PII processing cycle, only that they post a multilayered policy that accurately discloses actual privacy practices.

The second layer consists of a condensed version of a company's third layer privacy policy. It should contain only a summary of the privacy terms located under the seven required headings in the comprehensive policy.[70] This second layer is intended to supply the major attributes of the policy without overburdening the reader with excessive information.[71] The idea is that this second layer will be the layer that the vast majority of online visitors will actually take the time to read. Therefore, the summary

---

> multi-layered approach should serve as a model for other agencies and organisations. "Research has shown that individuals find privacy notices long and difficult to read and most do not read them at all," Ms Curtis said.

Id.

68. *See infra* Part III.C.2 (describing these seven privacy policy headings in detail).

69. *See infra* Part III.C.3 (describing the readability and understandability aspects of compliant privacy policies).

70. The second layer should also be required to contain each of the seven headings contained in the third layer policy. *See infra* Part III.C.2.

71. A hypothetical second layer privacy policy is reprinted at the end of this Article as Exhibit 3.

it includes must provide the essence of the comprehensive policy. The second layer should be posted in areas with more screen space than an automated teller machine or a cellular phone where placement of the comprehensive policy is not feasible. For example, companies can place their second layer privacy policy in its entirety on their homepage or in correspondence with customers and account holders. It should also be acceptable under the proposed regulation for a company to place a clear and conspicuous hyperlink to its second layer policy on its homepage.[72]

Finally, the first layer of a multilayered privacy policy is created specifically for small screen viewing areas such as automated teller machines and cellular phones. This first-layer policy must be very short—between one and four lines—and merely make viewers aware that the company they are transacting with collects PII and that the full policy can be viewed at a particular webpage.[73] The first layer, in and of itself, is not sufficient under the statute proposed in this Article and companies should be required to at least create and post a second and a third layer policy.[74]

Today, even without any specific legal provisions requiring them to do so, companies are beginning to buy into this multilayered privacy policy approach.[75] The proposed federal law can validate this buy-in by requiring

---

72. The terms clear and conspicuous for the purposes of this legislation should mean that the link is located on the company's homepage in a manner where it is set apart from other links and where visitors can clearly understand that the privacy policy is located by clicking on it. The second layer privacy policy can then link to the third layer, comprehensive policy or a company can link to both the second and third payer policies from its homepage. As long as visitors can easily navigate to the comprehensive privacy policy, then a company should be considered compliant.

73. A hypothetical first layer privacy policy is reprinted at the end of this Article as Exhibit 2.

74. In fact, a covered company is only required to create and post a first-layer privacy policy when it transacts business in small screen environments such as on automated teller machines or cellular phones. All covered companies, however, should be required to create and post a second- and third-layer policy regardless of the environment where they conduct business.

75. *See, e.g.*, IBM.com, *Privacy: IBM Privacy Practices on the Web*, http://www.ibm.com/privacy/us/ (last visited July 25, 2007) (demonstrating that IBM placed its second-layer privacy policy on a separate webpage linked directly from the bottom of its homepage); *Ten Steps*, *supra* note 67, at 1 (discussing that consumers need clear, comprehensible, short yet comprehensive privacy policies and that multilayered privacy policies are becoming a popular way of satisfying these seemingly mutually-exclusive objectives:

> Experts agree that good privacy begins with effective transparency. Transparency requires privacy notices that are easy to understand, facilitate comparison, and are actionable. Privacy notices must also comply with legal requirements that may differ from country to country, and jurisdiction to jurisdiction. Research on how people learn has shown that for notices to be easy to read and understand, they must be short, use plain language, and be presented in a common format. Complete notices tend to be longer and more complex, so it is impossible to have

covered companies to create at least a second- and third-layer of a multilayered privacy policy and then post a link to these layers on their homepages. This requirement will standardize privacy policy formats across e-commerce companies. Over time, web site visitors will become more comfortable locating the policy itself, scanning its second or third layer and understanding the implications of key privacy terms and conditions. A standardized privacy policy, in and of itself, is not enough to provide visitors with the information they need to combat the e-threats that face them at a company's front door. These multilayered privacy policies also must be standardized and readable to maximize their effectiveness.

2. Privacy Policies Must Contain Specific Sections But Not Specific Language

The multilayered privacy policies that companies are required to create under this proposed federal law should be standardized to facilitate consumer understanding and familiarity. The type of standardization required is similar to the federal nutritional labeling requirements required by the U.S. Food and Drug Administration (FDA). Under the proposed federal law, legally-sufficient privacy policies must provide information pertaining to the following subheadings:

1) Types of Personal Information Collected;
2) Personal Information Uses;
3) Your Consent Options;
4) Personal Information Security,
5) Accessing/Changing/Removing Personal Information;
6) Privacy Policy Changes; and
7) Other Important Information.[76]

> both sets of requirements in one document. A multilayered notice is made up of a condensed notice that contains all the key factors in a way that is easy to understand and is actionable, and a complete notice with all the legal requirements. A growing number of privacy officials and experts agree that multilayered notices meet the transparency objective. Corporate and government sponsored research shows that multilayered notices build both trust and compliance. The work of the European Article 29 Working Party gives us confidence that layering a privacy notice is legally complaint [sic].

Id.

76. It is important that every privacy policy covered under this proposed statute utilize the exact same title names for these seven subheadings so that consumers become accustomed to finding the same types of information in the same place from privacy policy to privacy policy.

The continual use of these same headings will lead to a privacy policy template similar to the "Nutritional Facts" template as required under the Nutrition Labeling and Education Act.[77] For example, by law, the vast majority of food products must contain a "Nutrition Facts" label that states the total calories, total calories from fat, total fat, saturated fat, cholesterol, sodium, total carbohydrates, dietary fiber, sugars, protein, Vitamin A, Vitamin C, calcium and iron.[78] These standardized headings—always placed in the same order on the nutritional label—help consumers understand the nutritional implications of the foods they consume.[79] Without the standardized labels, consumers would face a plethora of nutritional descriptions or none at all; they would be hard-pressed to understand the nutritional implications of the food they are about to consume. Research into why consumers understand and appreciate the nutritional facts template demonstrates that any information given to the public must be concise (cover no more than seven topics), use common language and appeal to the consumer's short- and long-term memories at

---

77. Nutrition Labeling and Education Act of 1990, Pub. L. No. 101-535, 104 Stat. 2353 (codified at 21 U.S.C. 343 (2000) [hereinafter NLEA]. Before enactment of the NLEA, the

> Food, Drug, and Cosmetic Act ("FDCA") expanded the regulatory scope of the [Food and Drug Administration] FDA by granting it the power to protect foods from adulteration or misbranding. Congress first created optional standards for nutritional labels on foods in 1973, putting the FDA in charge of implementing and enforcing them. Under these rules, only producers who chose to make affirmative health and nutritional claims had to put nutritional information on their packaging.

Rebecca S. Fribush, Note: *Putting Calorie and Fat Counts on the Table: Should Mandatory Disclosure Laws Apply to Restaurant Foods?*, 73 GEO. WASH. L. REV. 377, 379 (2005) (internal citations omitted).

78. 21 C.F.R. § 101.9 (2002). There are also some voluntary nutritional information that are often included such as: calories from saturated fat, polyunsaturated fat, monounsaturated fat, potassium, soluble fiber, insoluble fiber, sugar alcohol, other carbohydrate, percent of vitamin A present as beta-carotene, other essential vitamins and minerals. *See* U.S. Food and Drug Administration, *The Food Label*, May 1999, http://www.fda.gov/opacom/backgrounders/foodlabel/newlabel.html (stating that, "[i]f a claim is made about any of the optional components, or if a food is fortified or enriched with any of them, nutrition information for these components becomes mandatory."). Additionally, "these mandatory and voluntary components are the only ones allowed on the Nutrition Facts panel. The listing of single amino acids, maltodextrin, calories from polyunsaturated fat, and calories from carbohydrates, for example, may not appear as part of the Nutrition Facts on the label." *Id.* (demonstrating that this limitation is important because it helps with the standardization of nutritional labeling).

79. Nutrition and Diet Services, *Sample Nutrition Labels*, http://www.nutrition-dietservices.com/samlabel.html (last visited July 30, 2007) (complying with governmental standards so the label is familiar to the vast majority of Americans).

the same time ("the notice seen yesterday must help consumers understand the notice they see today").[80]

The same logic holds true in the world of electronic privacy policies.[81] The short aspect of effective privacy policies is covered by the multilayered approach described above. The common language aspect of effective privacy policies is discussed in the plain English section below and the short- and long-term memory aspect of effective privacy policies are covered by the seven standardized headings covered in this section.

The first section (Types of Personal Information Collected) must state exactly what types of PII the web site collects—both actively and passively. The type of information collected (such as name, address, social security number) and the collection method (such as via web forms, cookies, or web beacons) must be addressed in this section. Although the operation and terminology surrounding some prominent data collection techniques, such as cookies, is sometimes complicated and dense, companies should be required to describe these techniques clearly and concisely.[82] Similarly, descriptions of cookies and web beacons that make a reader more confused after reading them are contrary to the intent of this legislation and must be avoided. If the web site does not collect any forms of PII, this fact must be disclosed under this first section heading and the heading cannot be omitted from the privacy policy.

The second section (Personal Information Uses) must state how the company plans to utilize the PII that it collects. For instance, a company planning to sell specific pieces of data to unrelated third parties must disclose this fact in this section. The most common PII uses that will be disclosed are transaction processing, account creation and maintenance, storage, internal marketing purposes, dissemination to related entities, and dissemination to unrelated entities or individuals. Any changes to the utilization of PII that a company has previously disclosed in its privacy policy (as might occur when a company changes its business plan and subsequently decides to sell information that it promised not to sell in this section) must be reflected by an amended privacy policy.[83] Over time, web site visitors should become more accustomed to reading and understanding the terms as they are laid out in this section in order to determine if the company's practices meet their privacy expectations.

The third section (Your Consent Options) deals with a web site visitor's options as to how the information collector can use the PII.

---

80. *Id.*

81. *See, e.g.*, Abrams & Crompton, *supra* note 67, at 2 (drawing the analogy between electronic privacy policies and nutritional facts food labels).

82. *See* discussion, *infra* Part III.C.3.

83. The sixth required heading, to be discussed below, deals with amending a privacy policy.

Companies may require a customer to affirmatively contact them to request that PII not be utilized for any purpose aside from the transaction it was obtained to consummate (a secondary use). These are referred to as "opt-out" provisions and are not considered strong privacy protectors as evidence demonstrates that many customers choose not to take the time to opt-out even if such an option is their privacy preference. The alternative to an opt-out policy is an opt-in policy. Under an opt-in policy, companies may be forced to request affirmative customer consent to utilize PII for any or all secondary uses. Recall that under the law proposed in this Article, neither an opt-out nor an opt-in is required because the relationship is still at the front door stage and consumers disliking the company's chosen approach need not submit their PII and may take their business elsewhere. Under the proposed law, the heading along with the accurate disclosure of the company's consent options are of primary importance.

The fourth section (Personal Information Security) must detail how the company will secure any PII once it is collected, processed, or stored in company databases. As will be demonstrated in subsequent parts of this Article, information security breaches are serious threats and can occur internally—from rouge or careless employees—or externally—from remotely-located database hackers.[84] Customers submitting their PII deserve to understand the security practices companies implement before they choose to submit any information. This section of the privacy policy will aid in this process by requiring a clear and accurate description of such practices. As with passive PII collection techniques, the task of accurately describing information security practices can become very complicated and companies must strive to keep this section understandable and free of tech-speak.

The fifth section (Accessing/Changing/Removing Personal Information) must cover the visitor's ability or inability to access, change, or remove PII from company databases once it has been submitted. A customer may wish to access stored PII to make sure it is accurate, change PII to reflect a move, or remove PII due to a change in privacy preferences. Companies must detail how they deal with these issues in this section of their privacy policy and then adhere closely to these terms unless the policy is amended. For instance, it would be an unfair practice under the proposed statute if a company states that it allows customers to delete their PII at any time and then makes the process unbearably complicated or more limited than previously disclosed to discourage such removal.

84. *See infra* Parts IV.A.2 & IV.B.2 (discussing both internal and external security breaches).

The sixth section (Privacy Policy Changes) should detail exactly how a company will notify its customers of changes to its privacy policy, as well as how such changes will retroactively affect PII previously submitted. This becomes a serious issue when PII collected under an initial privacy policy is dealt with in a markedly different manner under the terms of a subsequent policy. For example, a company may state that it will not sell any collected PII as an asset in bankruptcy and then amend this policy a year later to allow such sales. Nothing in the proposed law will prevent this change in strategy, and businesses must be able to flexibly change their business strategies when they choose. However, the law should require that customers who entered data based on the previous terms be notified as to how their information will be affected by such changes.[85] To make this notification more effective, companies will be required to notify all existing customers of such changes and also clearly identify the differences between the two policies.

The final section (Other Important Information) is a catch-all category designed for unique privacy policy terms that do not fit comfortably under the other six headings. For example, this is the best place for a company to disclose that it belongs to a privacy webseal program[86] and to place the

85. Companies choosing to sell information under the terms of an amended privacy policy that formerly restricted such sales are acting in a privacy-invading manner. Although this proposed law will do nothing to stop this type of practice aside from mandating its accurate disclosure, the public scrutiny that will arise when word spreads of this practice will discourage companies from implementing such a strategy.

86. Privacy webseal programs are designed to build consumer trust in a company's PII privacy practices. Companies voluntarily submit to following certain privacy protocols in order to receive permission to display the webseal on their homepages. Webseal providers conduct audits of company privacy policies to ensure that the seal privacy requirements are met. One of the major players in the webseal market is TRUST-e, which describes its webseal program as follows:

> The seal marks companies that adhere to TRUSTe's strict privacy principles, and comply with the TRUSTe Watchdog dispute resolution process. Principles include:
>
> 1. Creating a privacy policy to be reviewed by TRUSTe
> 2. Posting notice and disclosure of collection and use practices of personally identifiable information
> 3. Giving users choice and consent over how their information is used and shared

TRUST-e.com, *What's the Difference Between You and Your Competition*, http://www.truste.org/businesses/web_privacy_seal.php (last visited July 20, 2007).

link to the other layers of its privacy policy.[87] A company need not provide information in this section if it feels that all of its privacy policies are adequately disclosed in the remainder of the policy.

3. Privacy Policies Must be Understandable to the Typical Visitor

Finally, the proposed statute should require that all covered companies produce privacy policies that are understandable to the average web site visitor or at least to the average web site visitor who makes a good faith effort to understand such policies.[88] The best way to accomplish this objective is to require all covered privacy policies to be written in plain English. This concept, recognizable from federal securities regulation,[89] urges document drafters to write clearly, use concise sentences, place only one issue per sentence and avoid legalese whenever possible.[90] This

87. A link to the third-layer of the privacy policy must be conspicuously placed on a company's homepage as well as on any copy of its second-layer privacy policy. The Other Important Information section is a good place to include this link.

88. *See, e.g.*, Carlos Jensen & Colin Potts, *Privacy Policies Examined: Fair Warning or Fair Game?*, GEORGIA INSTITUTE OF TECHNOLOGY GVU TECHNICAL REPORT-03-04, 2 (2003), http://hdl.handle.net/1853/3215.

89. The Securities and Exchange Commission (SEC) requires some prospectus documents that must be distributed to potential investors by public companies and mutual funds to possess certain sections drafted in plain English. *See, e.g.*, SEC Release 33-7497 (and SEC Releases 34-39593 and IC-23011), *available at* http://www.sec.gov/rules/final/33-7497.txt. *See also* SEC, *Plain English Disclosure*, 17 C.F.R. Pts. 228, 229, 230, 239 and 274, 1998.

> The [plain English] rule requires issuers to write the cover page, summary, and risk factors section of prospectuses in plain English.... We are also giving issuers more specific guidance on how to make the entire prospectus clear, concise, and understandable. We believe that using plain English in prospectuses will lead to a better informed securities market—a market in which investors can more easily understand the disclosure required by the federal securities laws.

Id.

90. *See, e.g.*, SEC, *A Plain English Handbook: How to Create Clear SEC Disclosure Documents*, Aug. 1998, *available at* http://www.sec.gov/pdf/handbook.pdf. The SEC is not the only organization interested in the concept of plain English. The U.S. government created a web site dedicated to promoting the use of plain language. PlainLanguage.gov, *Homepage*, http://www.plainlanguage.gov/ (last visited July 30, 2007). The web site was started in 1995 by a group of federal employees dedicated to crafting more readable government documents. PlainLanguage.gov *History of Plain Language in the United States*, http://www.plainlanguage.gov/whatisPL/history/index.cfm (last visited July 30, 2007) (stating that "many definitions of plain language exist. Fundamentally, when we write in plain language, we present information in a way that makes it as easy as possible for people to understand. All definitions emphasize the importance of audience, clarity, and comprehension"). PlainLanguage.gov, *Definitions of Plain Language*, http://www.plainlanguage.gov/whatisPL/definitions/index.cfm. More globally, the Plain English Campaign (PEC) is a British organization dedicated to helping companies produce clear public

simplified writing style is crucial whenever a document is designed to be read by the typical web site visitor in an abbreviated period of time. Plain English will help readers understand the complex issues that must be disclosed in a privacy policy and generate a better understanding of the implications of PII submissions. It is important to remember that the average adult American reads at around an eighth- or a ninth-grade level[91] while the majority of contemporary privacy policies are written at a second-year college reading level.[92] Although studies show that the typical Internet user reads at the fourteenth-grade level (equivalent to the second year in college), as the Internet becomes more and more mainstream, the average reading level of its users will fade lower toward the average literacy rate of the general population.[93] This plain English requirement will not only simplify the reading level of privacy policies but also increase comprehension level regardless of the visitor's educational attainment.

On the other hand, plain English is not an excuse to dumb-down a document to the point where nothing of substance remains. Instead, the concept merely encourages authors to express complex issues as clearly as possible and to separate tough concepts into separate sentences. For example, consumers reading privacy policy documents need to be aware of the different ways their PII is collected and used. A privacy policy

---

information documents. *See Plain English Campaign: About the Campaign*, http://www.plainenglish.co.uk/facts.htm (last visited July 30, 2007) (claiming that "[t]hanks to our lobbying in Europe, it is now impossible to enforce consumer contracts that are not in 'plain, intelligible language.'"). The PEC defines plain English as "writing that the intended audience can read, understand and act upon the first time they read it. Plain English takes into account design and layout as well as language." Plain English Campaign, *Frequently Asked Questions*, http://www.plainenglish.co.uk/faqs.htm (last visited July 30, 2007). The PEC implemented its Crystal Mark program entice companies to draft important documents in plain English; documents that have been "written and designed as clearly as possible" are eligible to receive the Crystal Mark. Plain English Campaign, *Crystal Mark*, http://www.plainenglish.co.uk/crystalmark.htm (last visited July 30, 2007) (claiming that over 14,000 documents carry its Crystal Mark and that prominent corporations such as AT&T, Bank One, and Fortis Group participate in the program).

91. *See, e.g.*, Norman M. Goldfarb, *How Well Does the Average U.S. Adult Read?*, 9 J. CLINICAL RES. BEST PRACTICES 3 (2005), *available at* http://firstclinical.com/journal/2005/0509_Literacy.pdf (citing 1992 findings on American literacy and claiming that the ninth grade literacy level may be optimistic); Frank Grazian, *Frequently Asked Questions (FAQ) About Readability*, 41 PUB. REL. Q. 19 (1996) (discussing readability and the idea that the average American reads at the ninth grade level). *See generally* Irwin S. Kirsch et al., *Adult Literacy in America: A First Look at the Results of the National Adult Literacy Survey*, U.S. DEP'T EDUC.: NAT'L CENTER FOR EDUC. STAT. (Sept. 1993), *available at* http://nces.ed.gov/pubs93/93275.pdf.

92. *See, e.g.*, Jensen & Potts, *supra* note 88, at 4.

93. *See, e.g.*, *id.* at 3 (stating that this reading level is higher than high school but lower than a bachelor's degree but that, as the Internet becomes more and more mainstream, the literacy rate of its users will decrease back towards the literacy rate of the American population in general).

section that fails to describe the use of cookies and web beacons because the concepts are difficult to grasp is all but useless from a privacy-protection point of view. Instead, such collection techniques should be described in a clear and concise fashion rather than being avoided because of their complexity.[94] The following example from IBM's privacy policy shows how plain English principles make these statements relatively easy to read and understand:

> Personal Information
>
> In general, you can visit IBM on the Internet without telling us who you are and without giving any personal information about yourself. There are times, however, when we or our partners may need information from you.
>
> You may choose to give us personal information in a variety of situations. For example, you may want to give us information, such as your name and address or e-mail id, to correspond with you, to process an order, or to provide you with a subscription. You may give us your credit card details to buy something from us or a description of your education and work experience in connection with a job opening at IBM that you wish to be considered for. We intend to let you know how we will use such information before we collect it from you; if you tell us that you do not want us to use this information to make further contact with you beyond fulfilling your requests, we will respect your wishes. If you give us personal information about somebody else, such as a spouse or work colleague, we will assume that you have their permission to do so.[95]

---

94. *See, e.g.*, IBM.com, *IBM Privacy Practices on the Web* [hereinafter *IBM Privacy Policy*], http://www.ibm.com/privacy/details/us/#section_1 (last visited July 30, 2007).

> We collect the information we mentioned in the previous paragraphs through the use of various technologies, including one called "cookies." A cookie is a piece of data that a Web site can send to your browser, which may then be stored on your computer as an anonymous tag that identifies your computer but not you. Some IBM pages use cookies, sent by IBM or its third party vendors, or other technologies to better serve you when you return to the Web site. You can set your browser to notify you before you receive a cookie, giving you the chance to decide whether to accept it. You can also set your browser to turn off cookies. If you do so, however, some Web sites may not work properly.

Id.

95. *Id.*

Please keep in mind that plain English is not a comprehensive set of written rules that must be followed in every instance (i.e., there is no plain English stylebook that regulators will look at to determine whether sentences are too long or whether too many ideas are expressed in one sentence). Rather, plain English merely requires that privacy policy drafters attempt to make their policies as readable as possible without compromising the integrity of the main concepts. Regulators at the FTC will be tasked with promulgating a final rule describing the types of plain English principles that comply with the terms of the proposed federal law. The FTC also will be tasked with the determination as to whether or not a company's policy complies with its final rule.[96]

Adopting a plain English-type standard in the United States is not a groundbreaking proposition. In fact, in 1978, President Jimmy Carter issued an executive order urging that "regulations should be as simple and clear as possible."[97] In 1998 President Bill Clinton drafted a memorandum for the heads of all Executive departments and agencies requiring these particular bodies to draft certain documents in plain English.[98] This

96. Administrative agencies such as the FTC are capable of determining whether a document complies with plain English principles. In 2003, the SEC ordered 350 of the Fortune 500 companies to redraft some parts of their annual reports or at least promise to make such reports clearer in the future. SEC, *Summary by the Division of Corporation Finance of Significant Issues Addressed in the Review of the Periodic Reports of the Fortune 500 Companies*, Feb. 27, 2003, *available at* http://www.sec.gov/divisions/corpfin/fortune500rep.htm (stating that one of the factors that the SEC looked at when analyzing these annual reports was the clarity of a company's disclosure).

97. Exec. Order No. 12044 (Mar. 23, 1978). This Executive Order was followed by another in 1979 which urged that government forms "should be as short as possible and should elicit information in a simple straightforward fashion." *See* Exec. Order No. 12174 (Nov. 30, 1979).

98. In an effort to make the federal government more "responsive, accessible, and understandable in its communications with the public," President Clinton mandated that executive department and agency heads ensure that plain language be used in all public documents where citizens can request a benefit or service, learn how to comply with a requirement and in all proposed and final rulemakings published in the Federal Register. Bill Clinton, *Plain Language in Government Writing*, WHITE HOUSE MEMORANDUM, June 1, 1998, http://www.plainlanguage.gov/whatisPL/govmandates/memo.cfm.

> The Vice President and I have made reinventing the Federal Government a top priority of my Administration. We are determined to make the Government more responsive, accessible, and understandable in its communications with the public.
>
> The Federal Government's writing must be in plain language. By using plain language, we send a clear message about what the Government is doing, what it requires, and what services it offers. Plain language saves the Government and the private sector time, effort, and money.

document defined plain language as "common, everyday words, except for necessary technical terms: 'you' and other pronouns: the active voice; and short sentences."[99] Approximately ten states have laws mandating clear language in certain public documents.[100] New York passed America's first general plain language law that requires all residential leases and certain commercial contracts be written in "a clear and coherent manner using words with common and everyday meanings" and "appropriately divided and captioned by its various sections."[101] In addition, the concept of plain

---

> Plain language requirements vary from one document to another, depending on the intended audience. Plain language documents have logical organization, easy-to-read design features, and use:
>
> 1. common, everyday words, except for necessary technical terms:
> 2. "you" and other pronouns:
> 3. the active voice; and
> 4. short sentences.

Id.

99. *Id.*

100. *See, e.g.*, CAL. GOV'T CODE § 11340 (Deering 2006); CAL. INS. CODE § 10291.5 (Deering 2006); CONN. GEN. STAT. § 42-152 (2007); FLA. STAT. ANN. § 627.4145 (2007); MINN. STAT. ANN. § 144.056 (West 2006); N.Y. GEN. OBLIG. LAW § 5-702 (Consol. 2007); PA. STAT. ANN. tit. 73, § 2201 (West 2007).

101. N.Y. GEN. OBLIG. LAW § 5-702(a) (Consol. 2007).

> Every written agreement entered into after November first, nineteen hundred seventy-eight, for the lease of space to be occupied for residential purposes, for the lease of personal property to be used primarily for personal, family or household purposes or to which a consumer is a party and the money, property or service which is the subject of the transaction is primarily for personal, family or household purposes must be:
>
> 1. Written in a clear and coherent manner using words with common and every day meanings;
> 2. Appropriately divided and captioned by its various sections.
>
> Any creditor, seller or lessor who fails to comply with this subdivision shall be liable to a consumer who is a party to a written agreement governed by this subdivision in an amount equal to any actual damages sustained plus a penalty of fifty dollars. . . . No action under this subdivision may be brought after both parties to the agreement have fully performed their obligation under such agreement, nor shall any creditor, seller or lessor who attempts in good faith to comply with this subdivision be liable for such penalties. . . . It also shall not apply to agreements involving amounts in excess of fifty thousand dollars nor prohibit the use of words or phrases or forms of agreement required by state or federal law, rule or regulation or by a governmental instrumentality.

English has worked well for the SEC as company prospectuses are much easier to read and comprehend.[102]

4. The Law Must be Structured as a Regulatory Ceiling

Finally, any new federal law proposing to protect PII entering a company's front door must create an unambiguous national standard that clearly lays out the requirements placed upon covered companies and by requiring such companies to clearly define the privacy protections online consumers will receive. Conflicting or more stringent state and local laws over-regulate, confuse consumers, and increase compliance costs in this early stage in the PII processing cycle—a stage where web site visitors can adequately protect themselves once they understand the implications of submitting their PII into cyberspace. One national standard can provide web site visitors with the necessary knowledge to drastically reduce the power of the various e-threats lurking at a company's front door. With this in mind, the legislation proposed by this Article should be drafted as a regulatory ceiling as opposed to a regulatory floor.

Regulatory ceilings are created when federal laws preempt more restrictive state laws regulating the same topic. Such preemption is particularly helpful in creating a national standard and eliminating the chance of fifty different state laws enacted to solve the same problem.[103] Differing state laws are problematic from both a compliance and a consumer-understanding standpoint. First, companies struggling to comply with varying state standards often choose the most stringent state law and abide by its terms in every state where it operates. This allows the state legislature of one particular state to set a de-facto national standard without any of its members being elected nationally. A federal law, on the other hand, originates from legislators elected from states representing the entire country—a more proper way of setting a national standard. Second, varying state laws will cause company privacy statements to take different forms, include different topics and discuss privacy concepts in different ways. This makes it even more difficult for web site visitors to understand privacy policy terms. Under one federal standard, privacy policy templates would begin to resemble nutritional content templates required by the FDA under the federal Nutrition Labeling and Education Act as discussed previously.

Id.

102. *See supra* note 89 (discussing the SEC and its plain English rules).

103. The number of similar laws governing one area can multiply exponentially if local regulations are considered and not preempted by state or federal laws.

State governments and privacy advocates correctly argue that regulatory floors limit the ability of state and local legislatures to experiment with creative solutions to PII-privacy problems and, thereby, less privacy is protected. While the creative solutions of this argument is true, a non-intrusive national standard is far more important at this point in the PII processing cycle than state experimentation. The experimentation-regulatory angle becomes more important as the e-threats become more serious at the back door stage of the PII processing cycle.

This first segment of the proposed federal law provides a workable framework to defend an individual's PII against the dangerous e-threats lurking at the front door. As the next part will demonstrate, however, different e-threats present serious problems as PII moves from a company's front door to inside the company's infrastructure. At this point, the individual the PII identifies has lost a great deal of control over the processing, usage, and dissemination of the information. Therefore, more comprehensive regulatory protection is necessary at this middle stage of the cycle. Fortunately, the same statute that protects against front door e-threats also can protect against these threats from inside the company.

IV. THREATS INSIDE THE COMPANY (PII UTILIZATION)

After entering a company's front door, PII is generally stored electronically and processed internally to complete transactions and conduct marketing activities.[104] The information is now "inside the company" from this point forward until a decision is made either to disseminate it to unrelated entities[105] or destroy it completely.[106] At this

104. *See, e.g.*, Agilent Technologies, *Customer Privacy Statement*, http://www.home.agilent.com/cgi-agilent/editorial.jspx?pmode=Privacy&cc=US&lc=eng (last visited Aug. 24, 2006) (providing an example of a company collecting and storing PII for both transactional and marketing purposes. Agilent's privacy policy section on uses of PII states in part:

> Agilent uses your personal information to better understand your needs and provide you with better service. Specifically, *we use your personal information to help you complete a transaction*, to communicate back to you, provide updates on service and benefits, and to personalize our web sites and communications with you. . . . *From time to time, we may also use your information to contact you for market research or to provide you with marketing information we think would be of particular interest.*

Id. (emphasis added)).

105. *See, e.g.*, Holden Lewis, *Banks are Selling your Private Information*, BANKRATE.COM (Oct. 8, 1999), http://www.bankrate.com/brm/news/bank/19991008.asp (discussing banks and their collection and eventual dissemination of PII for a fee by stating that:

stage, PII is exposed to three serious e-threats: (1) data mining, (2) security breaches (internal and external) and (3) phishing attacks. Similar to the e-threats lurking at the front door, inside-the-company e-threats are initiated by both internal sources (data mining and internal security breaches) and

---

> In fact, banks sell all sorts of information—including Social Security numbers and checking and credit card account numbers—to whoever has the money to pay for the data. The information might be provided to an affiliated brokerage selling mutual funds (just as your certificate of deposit is about to expire) or to a telemarketer who calls you at dinnertime to sell you a health club membership.).

Id.

106. As of June 1, 2005, a recent FTC regulation requires any businesses utilizing or deriving information from consumer reports to dispose of this information in a manner that is reasonable and appropriate to prevent unauthorized access. Fed. Trade Comm'n, *Disposal of Consumer Report Information and Records Rule*, 16 C.F.R. pt. 682 (June 1, 2005) [hereinafter FTC, *Disposal Rule*] (this rule stems from a requirement in the Fair and Accurate Credit Transactions Act of 2003 (15 U.S.C. § 1681(w) (2000) [hereinafter FACTA]) requiring the FTC, among other federal governmental entities, to promulgate rules regarding the proper disposal of consumer report information). *See also* FTC, *Consumer Alert: Disposing of Consumer Report Information? New Rule Tells How* [hereinafter FTC, *Consumer Alert*], http://www.ftc.gov/bcp/conline/pubs/alerts/disposalalrt.shtm (last visited July 30, 2007) (summarizing the new rule and providing relevant links). The method of disposal is left to the company to decide, however the FTC states that a few reasonable and appropriate methods would include: (1) burning, pulverizing, or shredding paper documents and (2) destroying or erasing digital documents. *See* FTC, *Disposal Rule*, *supra*, § 682.3(b); FTC, *Consumer Alert*, *supra* (stating that companies could conduct due diligence reviews of their disposal policies and hire a "document destruction contractor" to dispose of this material). This rule is rather broad in that it covers any business that utilizes consumer report information—a list of companies that can include:

> Consumer reporting companies, Lenders, Insurers, Employers, Landlords, Government agencies, Mortgage brokers, Automobile dealers, Attorneys or private investigators, Debt collectors, Individuals who obtain a credit report on prospective nannies, contractors, or tenants [and entities] that maintain information in consumer reports as part of their role as service providers to other organizations covered by the [FTC Disposal] Rule.

Id. Even with such regulations in place, a recent interview with a former Department of Homeland Security (DHS) Chief Privacy Officer (CPO) covered the knowledge level of consumer financial firms concerning the protection of PII and concluded that although these firms tend to care about information privacy, the official has "observed that businesses are not always completely advised on the overlap in their civil and criminal risk liability for particular behaviors or failures in their internal control processes [when it comes to protecting PII."]. *What You Don't Know about Privacy Can Hurt You*, 10 CONSUMER FIN. SERVICES L. REP. 6 (2006); *Hackers Keen on Credit Unions*, 10 CONSUMER FIN. SERVICES L. REP. 1 (2006) [hereinafter *Credit Unions*] (interviewing Maureen C. Cooney—the retiring DHS CPO and former corporate attorney and FTC official). This lack of knowledge may lead firms to take the protection of PII less seriously than they would if they were adequately informed of current regulations as well as the litigation risks involved with sloppy PII protection.

external sources (phishing and external security breaches).[107] At this middle point in the PII processing cycle, responsibility for protecting against inside-the-company e-threats must slide toward the businesses collecting PII and away from the individuals submitting it because the information is primarily out of the hands of the individual it identifies and primarily within the control of its collector.[108]

The following sections elaborate upon these inside the company e-threats and argue that the proposed federal law must also contain a second substantive section specifically designed to protect PII during this stage. Also enacted as a regulatory ceiling preempting conflicting state and local laws, these statutory provisions should place a more significant burden on PII utilizers to protect against these inside-the-company e-threats than was necessary at the front-door stage.

A. *Internally-Created "Inside the Company" Threats*

The two major internally-created e-threats targeting PII inside the company are data mining and internal security breaches. While the major information security breaches over the past two years—such as Bank of America,[109] LexisNexis[110] and ChoicePoint[111]—take up much of the

107. *See* discussion, *supra* Part III.A & B (covering both internal and external front-door e-threats).

108. At this stage, companies may allow submitters of PII to amend or delete their information from company databases but are under no legal obligation to do so. If a company does not allow such individual control, individuals submitting information are at the mercy of companies to protect their data. This is in stark contrast to the front door where individuals made the primary decision as to whether or not to submit any information. The silver lining at this stage is that companies are bound to follow their stated privacy policies and may be charged with an unfair or deceptive practice by the FTC for breaching such promise. *See* FTC, *Privacy Initiatives: Introduction*, http://www.ftc.gov/privacy/index.html (last visited July 30, 2007). The dark cloud surrounding the silver lining, however, is that most e-commerce companies are not required to post an electronic privacy policy in the first place. Also important is the fact that e-threats become even more dangerous once PII is disseminated into cyberspace because, at this point, neither the submitter nor the initial collector can protect the information from abuse. *See* discussion, *infra* Part V (discussing e-threats occurring after PII is disseminated through a company's back door).

109. *See Bank of America Loses Customer Data* (Mar. 1, 2005), http://www.msnbc.msn.com/id/7032779/ (discussing a major security breach at Bank of America and stating that the company "lost computer data tapes containing personal information on up to 1.2 million federal employees, including some members of the U.S. Senate. The lost data includes Social Security numbers and account information that could make customers of a federal government charge card program vulnerable to identity theft").

110. *See* Heather Timmons, *Security Breach at LexisNexis Now Appears Larger*, N.Y. TIMES, Apr. 13, 2005, at C-7 (discussing the theft of the social security numbers, driver's license numbers, and addresses of over 310,000 people when hackers compromised a database at Seisint's—a unit of LexisNexis—utilizing a computer virus and stolen passwords). Lexis first claimed that 32,000 individuals had their PII compromised and then revised the estimate to the current 310,000. *See*

spotlight in the popular press,[112] data mining also can be a powerful threat to privacy.

1. Data Mining

Data mining is:

> A class of database applications that look for hidden patterns in a group of data that can be used to predict future behavior. For example, data mining software can help retail companies find customers with common interests. The term is commonly misused to describe software that presents data in new ways. True data mining software doesn't just change the presentation, but actually discovers previously unknown relationships among the data. Data mining is popular in the science and mathematical fields but also is utilized increasingly by marketers trying to distill useful consumer data from Web sites.[113]

Press Release, *LexisNexis Concludes Review into Unauthorized Access to U.S. Databases*, (Apr. 12, 2005), http://www.reed-elsevier.com/index.cfm?articleid=1319&articleaction=print&type. The Press Release states that a comprehensive review analyzed

> data search activity going back over the last two full years and concluded that there were 59 incidents where [unauthorized], predominantly using IDs and passwords of legitimate customers of Seisint, may have fraudulently acquired personal identifying information from its U.S. risk management databases. LexisNexis estimates that information on approximately 310,000 U.S. individuals in total may have been accessed.

Id.; Malini Guha, *Reed Elsevier's Estimate of Identity-Theft Victims Jumps*, FIN. TIMES (London), Apr. 13, 2005, at 21.

111. *See ChoicePoint: More ID Theft Warnings*, CNNMONY.COM (Feb. 17, 2005), http://money.cnn.com/2005/02/17/technology/personaltech/choicepoint/ (describing a situation where ChoicePoint sold PII—in the form of names, addresses, social security numbers and credit reports on over 144,000 individuals—to criminals posing as legitimate business operators).

112. A study by the Privacy Rights Clearinghouse found that over 90,995,000 PII records were compromised since February 15, 2005. *See A Chronology of Privacy Breaches*, PRIVACY RIGHTS CLEARINGHOUSE, http://www.privacyrights.org/ar/ChronDataBreaches. htm (last visited July 30, 2007) (emphasis added) [hereinafter *Chronology of Privacy Breaches*] (labeling each major security breach since early 2005, provides the name of the victimized company and its location, discusses the types of breaches which occurred and totals the number of PII records lost). Interestingly, over 80 of the security breaches occurred at universities and were evenly spread between 2005 and 2006 indicating that this e-threat is not confined only to e-commerce businesses. *Id.*

113. Webopedia.com, *Data Mining*, http://www.webopedia.com/ TERM/d/data_mining.html (last visited July 30, 2007). According to sources in the technology industry, the demand for data mining software is rapidly growing. *See, e.g.*, Michelle Kessler, *Data Miners Dig a Little Deeper;*

Companies engaged in data mining utilize sophisticated software programmed to analyze and correlate scattered pieces of PII in ways its submitters may not fathom.[114] This combing through of collected data results in the creation of detailed profiles forecasting an individual customer's needs, interests, and desires.[115] These dossiers are utilized to develop targeted marketing materials and potentially sold to interested

---

Companies may Know a lot More about You Than You Think—or Want, USA TODAY, July 12, 2006, at B-1; James Rosen, *Big Business is Old Hand at Mining Personal Data*, SACRAMENTO BEE (California), May 22, 2006, at A-10 (citing a study by a college professor finding "a 30-fold increase in corporate data collection between 1999 and 2004. Wal-Mart . . . gathers and analyzes information on about 20 million transactions—a day.").

114. *See, e.g.*, Duane Stanford, *All Our Lives are on File for Sale*, ATLANTA-J. CONST., Mar. 21, 2004, at A-1 (describing data mining, giving examples of the practice and discussing the interesting data mining tactics of the Internet portal Abika stating that the company conducts:

> [A] media sweep of newspaper and magazine articles [and] purchases databases from companies that offer anything from subscriber lists to club membership rosters. . . . Most of the databases prohibit Abika from reselling the raw information. Instead, Abika plugs the data into a mathematical formula . . . that compares the subject with more than 60,000 profiles that have been verified as accurate. The program then spits out a supposed map of the subject's character. [Abika] constantly fine-tunes the program based on feedback, and . . . admits the profiles can be wrong or incomplete.

Id. E-commerce companies are also utilizing an older direct marketing approach in scanning customer information—abbreviated as RFM or receny/frequency/monetary value—in their data mining applications. *See* Simon Pohlen, *Data Mining for the Profitable Veins of Gold*, DOMINION POST (New Zealand), Aug. 9, 2004, at 2. The article describes the following terms as follows:

> "Recency" is the time since you last saw the customer; "frequency" applies to how often you see them; and "monetary value" applies to the amount they generate for your business—revenue or profit. The way this is applied will vary between industries but the data that is collected serves the same purpose—it helps drive value in the business.

Id. These categories are then combined with specific pieces of PII to form a picture of customer needs and interests.

115. *See, e.g.*, Stanford, *supra* note 114.

> [E]very time you visit an Internet site, apply for credit or send in a product registration card, you leave behind bread crumbs of information that are swept up, compiled and stored by people you don't know. And it's all for sale to someone. Hundreds of companies are selling and swapping information—everything from your phone number to what you buy at the supermarket—and storing it in databases to be cross-referenced again and again.

Id.

third parties. Today, data mining presents an opportunity for companies to mine electronic gold from their cache of stored PII.[116]

A hypothetical example readily illustrates the power of data mining technology. Assume a registered Yahoo! customer living in an upper-middle class neighborhood in Westminster, Colorado[117] frequently searches the Yahoo! search engine for the newest BMW sports car models. Utilizing data mining software, Yahoo! can instantly aggregate these separate pieces of information and place a specifically targeted banner advertisement for the new BMW 650 as well as automobile financing options the next time the user checks the Dow Jones Industrial Average on the Yahoo! Finance homepage.[118] Without a data mining program to quickly correlate this information and the technology to automatically place the appropriately-tailored advertisement, Yahoo! would have a difficult time correlating this customer's interests with its advertiser's products. Therefore, effectively utilizing data mining technology increases a company's chances of generating more banner advertisement revenue. Or, to put it differently:

> Somewhere in America, powerful computers ingest crumbs of data about your personal life. Your income level. The kind of car you drive. Your home address. Your credit rating. All input, assimilated and analyzed at lightning speed. The result: A piece of paper arrives in your mailbox offering you 10 percent off an oil change at your local service station.[119]

As with some of the other potential e-threats mentioned previously—such as cookies and adware—data mining technology contains advantageous features. For instance, data mining allows individuals to receive targeted advertisements more closely tailored to their interests as opposed to annoying advertisements for products and services they would never consider purchasing. On the flip side, however, data mining technologies

---

116. *See, e.g.*, Pohlen, *supra* note 114 (discussing the tendencies of businesses to mine the PII of their customers).

117. Westminster, Colorado is a quaint, upper middle class city north-west of Denver that was named the twenty-fourth best small city in America by *Money Magazine*. *Best Places to Live: Westminster, CO*, CNNMONEY.COM (2006), *available at* http://money.cnn.com/magazines/moneymag/bplive/2006/snapshots/PL0883835.html.

118. *See* Kessler, *supra* note 113. A different Yahoo! customer that has never searched for sports cars on the Yahoo! search engine will likely see a banner advertisement targeted more towards his interests on his next trip to the Yahoo! Finance homepage.

119. Matthew B. Stannard, *U.S. Phone-Call Database Ignites Privacy Uproar: Data Mining Commonly Used in Business to Find Patterns, It Rarely Focuses on Individuals*, S.F. CHRON., May 12, 2006, at A-1.

can be privacy-invading depending upon the mining company's utilization of its created profiles.[120] If detailed profiles containing many different pieces of PII are created, mined for trends and then sold on the open market, more PII than is necessary to commit identity theft or other forms of fraud will linger in cyberspace outside of the control of the individual it identifies.[121]

2. Internal Security Breaches

Security breaches are the most widespread e-threats targeting PII at the inside-the-company stage.[122] An internal security breach occurs when stored PII is accessed or distributed inappropriately by rouge employees or through some form of human error.[123] While rogue employees definitely cause damage,[124] the cases concerning human error garner the most

120. *See, e.g.*, Brad Daisley, *Electronic "Data Mining:" Privacy Concerns Trigger Legislation*, LAW. WKLY., June 25, 1999, at 8 (stating that "new electronic data mining techniques have led to a worldwide concern for privacy and new legislation from several countries restricting the sale and transfer of personal data.").

121. *See* Daisley, *supra* note 120. Daisley states that:

> data can be collected from almost any source, such as telephone records or credit card transactions, and sold to any number of organizations without the individual knowing . . . It can also be processed into very specific databases . . . [in fact,] one American direct marketing company is advertising mail listings based on everything from age and sex to ethnicity.

Id.

122. *See Chronology of Privacy Breaches*, *supra* note 112 (discussing a study by the Privacy Rights Clearinghouse finding that over 90,995,000 PII records have been compromised since February 15, 2005).

123. Human error encompasses instances of careless treatment of PII. Oftentimes, such careless treatment of PII is found when the data is accidentally disseminated by an internal source; these situations occur when an employee leaves a file cabinet/office unlocked, a laptop in an automobile or a hotel room, or leaves a computer terminal and database application without password protection enabled. Although this accidental-dissemination occurs more infrequently than hacker attacks, such dissemination can be "disruptive, hurt the organization's morale and public relations, and take a lot of time and money to repair." *How HR is Coping with Employee Data Privacy*, HRFOCUS, (July 2006), at 7 [hereinafter *How HR is Coping*] (discussing the many types of PII possessed by a typical HR department such as: "Social Security numbers, home addresses and telephone numbers, bank accounts for payroll direct deposits, garnishments, investment information for 401(k) plans, and personnel reviews and disciplinary records" and instances of accidental dissemination). Although instances of accidental dissemination of employee PII are more heralded in the press, the accidental dissemination of customer PII can be just as disruptive because, in both instances, an individual's PII is compromised.

124. *See, e.g.*, Michael Krauss, *Tech-Security Legal Guru Expects Growth of Fraud*, CHI. SUN TIMES, May 22, 2006, at 64. Krauss quotes San Francisco lawyers discussing situations where

prominent press coverage. A recent example of human error occurred when a laptop computer containing the "name, Social Security Number and birth date of every living veteran since 1975"—over 26.5 million United States individuals—was stolen in a random burglary of the home of a Department of Veterans Affairs staffer who brought the computer home from work.[125] With this information compromised and subject to misuse, 26.5 million people stood at a greater risk of fraud than they had before the laptop was stolen.[126] Skeptics, referencing the woes of governmental bureaucracy in general, should understand that security breaches caused by human error are not merely a bureaucratic phenomenon. In fact, over the past two years, the private sector has provided more than its fair share of security breaches.[127] Once the data is compromised by a security breach, it is vulnerable to dissemination outside the company through the back door and exposed to the serious e-threats facing PII at that stage.[128]

> angry employees hack computer systems to steal the identity of a disliked senior exec to defame him . . . [or where a rouge] employee read his bosses' e-mails to find company secrets, and pass them along. There was even a group of IT execs who tried to hold their company hostage to avoid an outsourcing deal.

Id.; Peter H. Lewis, *Threat to Corporate Computers is Often the Enemy Within*, N.Y. TIMES, Mar. 2, 1998, at D-1 (discussing the story of a "computer supervisor at a Midwestern engine manufacturing company [who] approached his bosses . . . and made them an offer they could not refuse. Either they gave him a big raise immediately and agreed to a list of other job demands, or he would shut the company down"); *Computer Security Breaches: the Enemy is Within*, BUS. TIMES (Singapore), Aug. 4, 1997, at 10 (stating that "outgoing employees, before leaving a company, may sabotage the company in various ways . . . [including] stealing the company's digital assets, intellectual property, databases and financial information.").

125. *See* David Lazarus, *Where is the Security for Our Personal Data*, S.F. CHRON., May 24, 2006, at C-1.

126. The Department of Veterans Affairs claimed that the laptop was recovered and that the data was not accessed inappropriately. *See, e.g.*, Christopher Lee & Zachary A. Goldfarb, *Computer with Missing Vet Data Found*, WASH. POST, June 30, 2006, at A-1.

127. *See Chronology of Privacy Breaches*, *supra* note 112 (providing examples of both internal and external security breaches at American corporations, educational institutions and governmental agencies since Feb. 15, 2005); *supra* text accompanying notes 69-71 (providing background information on three prominent security breaches recently occurring at major American corporations). In one of the most recent cases involving human error, professional services firm Ernst & Young lost sensitive PII when a laptop containing social security numbers was stolen from an employee's car. *See* Carrie Kirby, *Another Security Breach Reported: Stolen Laptop Had Client's Private Data, Says Ernst & Young*, S.F. CHRON., Feb. 25, 2006, at C-1 (discussing a security breach at Deloitte & Touche, a competitor of Ernst & Young, when a compact disc was left in an airplane seat-pocket by an auditor; the disc contained, among other pieces of data, 9,000 names and social security numbers of McAfee employees collected for a McAfee audit).

128. *See* discussion, *infra* Part V.

Over time, the FTC began to take notice of the danger caused by internal security breaches and acted rather quickly to protect stored PII. Over the past few years, the FTC has brought thirteen enforcement actions against companies alleging poor PII-protection practices.[129] In its most recent case, the FTC filed a complaint against a large real estate title company, Nations Title Agency (Nations), with operations in forty-four states.[130] The complaint alleged that Nations collected pieces of PII necessary to complete real estate financing deals,[131] but then breached a privacy policy promise to safeguard PII. The FTC claimed that Nations breached its protection promise by, among other things, discarding old mortgage applications containing sensitive PII into an open trash dumpster behind the building and failing to implement adequate computer network security procedures.[132] The FTC alleged that these practices failed to reasonably protect PII and, thereby, violated the Federal Trade Commission Act (FTC Act), the FTC's Privacy Rule,[133] as well as the

129. *See, e.g.*, FTC, *In the Matter of* Nations Title Agency, Inc., Nations Holding Company and Christopher M. Likens, Complaint, Docket No. C-4161 (June 19, 2006) [hereinafter *Nations Title*] (alleging, in the most recent FTC enforcement action, that the practice of placing customer home loan applications into an open dumpster violated its promise to utilize "physical, electronic and procedural safeguards" to protect confidential financial information). *See also Rules and Regulations: FTC Closes Lid on Title Company*, 10 CONSUMER FIN. SERVICES L. REP. 1, May 31, 2006) (describing the FTC action against Nations Holding Company as the thirteenth "case that the FTC has brought challenging faulty data security practices.").

130. *Nations Title*, *supra* note 129.

131. This information included: "Consumer names, Social Security numbers, bank and credit card account numbers, mortgage information, loan applications, purchase contracts, refinancing agreements, income histories, and credit histories." *Nations Title*, *supra* note 129, at 2.

132. *See id.* at 2. The discarded documents contained intact pieces of PII and were found by a Kansas City news crew in an unsecured dumpster. *Id.* at 3. The complaint also alleged that the company failed to adequately protect its computer network from hacker attacks because a hacker was able to use a common web site attack to gain unauthorized access to Nations' computer network. *Id.* at 2. This is an interesting case where a company falls victim to both an internal and external security breach at the same time.

133. FTC, *Privacy of Customer Financial Information Rule*, 16 C.F.R., pt. 313 (effective July 1, 2001) [hereinafter *Privacy Rule*] (stating that the FTC's *Privacy Rule* requires financial institutions to provide customers—at the point when the customer relationship is formed and then annually thereafter—with a "clear and conspicuous" statement that "accurately reflects" the institution's privacy policies.). The *Privacy Rule* also was promulgated under the authority of the GLBA. GLBA §§ 6801-6809. The complaint alleged that Nations' privacy policy did not accurately describe the actual handling of PII and, therefore, violated the *Privacy Rule*. *See Nations Title*, *supra* note 129, at 4. Nations' privacy policy contained the statement that the company "at all times, strives to maintain the confidentiality and integrity of the personal information in its possession and has instituted measures to guard against its unauthorized access. We maintain physical, electronic and procedural safeguards in compliance with federal standards to protect the information." *Id.* at 4.

FTC's Safeguards Rule.[134]

Buoyed by the many occurrences of internal security breaches making national news, professional studies also suggest that internal security breaches are much more common than external security breaches.[135] With this in mind, the vast amount of money companies pour into protecting against external attacks—to create sophisticated firewalls,—becomes less meaningful in preventing an internal security breach.[136] With over 165

---

134. FTC, *Standards for Safeguarding Customer Information Rule*, 16 C.F.R., pt. 314 (May 23, 2002) [hereinafter *Safeguards Rule*]. This rule was promulgated by the FTC to implement a provision in the Gramm-Leach-Bliley Act (GLBA) and requires financial institutions to protect the security, integrity, and confidentiality of customer PII by devising a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards. *Id.* at 3. *See also* 15 U.S.C. § 6801(b) (2000) (Section 6801(b) required the FTC to promulgate the *Safeguards Rule*).

135. *See* Maija Pesola, *Hackers at Bay as Defences Improve*, FIN. TIMES (London), June 22, 2005, at 8 (citing a Deloitte study of the world's top 100 financial institutions finding that internal security breaches are more common today than external hacking attacks), Peter H. Lewis, *Threats to Corporate Computers is Often the Enemy Within*, N.Y. TIMES, Mar. 2, 1998.

> According to an informal survey conducted by the Computer Security Institute . . . computer attacks by insiders were more common [in 1997] than external Internet-based attacks. More than 87 percent of the corporate, financial, government and university information security managers polled by the survey said disgruntled employees were the most likely cause of data security incidents, ranging from sabotage, fraud and theft of proprietary information to unauthorized snooping in a colleague's E-mail or the storing of digital pornography on a company computer.

See also discussion, *infra* Part V.B.2 (discussing external security breaches); Zachary Wilson, *Hacking: The Basics*, SANS INSTITUTE (updated June 27, 2006), http://www.sans.org/reading_room/whitepapers/hackers/955.php (SANS stands for SysAdmin, Audit, Network, and Security). The SANS Institute is

> the most trusted and by far the largest source for information security training and certification in the world. It . . . develops, maintains, and makes available at no cost, the largest collection of research documents about various aspects of information security, and it operates the Internet's early warning system—Internet Storm Center.

SANS Institute, *About SANS*, http://www.sans.org/about/sans.php (last visited July 30, 2007). A recent SANS report recounted a statistic that "insiders [motivated generally by either greed or revenge] commit 80% of security breaches." Wilson, *supra*, at 1.

136. *See* Li Yuan, *Companies Face System Attacks from Inside, Too*, WALL ST. J. ABSTRACTS, June 1, 2005, at B-1.

> While companies spend billions of dollars a year to protect their computer systems from outside attack, many of those defenses can be rendered useless by internal abuse from employees and contractors; a January survey . . . found that 23% of

million PII records compromised over the past two years,[137] clearly the self-regulatory structure governing most PII storage needs some assistance.

B. *Externally-Created "Inside the Company" Threats*

Similar to one of the primary e-threats lying in wait at a company's front door (such as pretexting), two externally-initiated threats target PII at the inside-the-company stage. While data mining and internal security breaches stem from actions initiated by sources located within a company, both phishing and external security breaches stem from actions initiated by outside bad actors seeking stored PII for nefarious purposes.

1. Phishing

Phishing is:

> The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information.[138]

---

229 U.S. organizations with 1,000 or more employees had at least one internal security breach in 2004.

Id. To alleviate some of the costs of internal security breaches, companies are buying insurance against such instances. *See* Erika Gonzalez, *Latest Insurance Protects Businesses from Web Problems*, DENV. ROCKY MOUNTAIN NEWS, Feb. 10, 2000, at B-5 (discussing a new insurance product—"Internet insurance"—that covers businesses against various Internet dangers including security breaches).

137. *See Chronology of Privacy Breaches*, *supra* note 112; discussion *infra* Part V.C (detailing a proposed solution, in the form of a federal law, placing regulations on companies storing PII in interstate commerce).

138. Webopedia.com, *Phishing*, http://www.webopedia.com/TERM/ p/phishing.html (last visited July 30, 2007). In January 2006, "a record 17,877 phishing sites were reported . . . up 17% from [December 2005], according to a new report from the Anti-Phishing Working Group." Phyllis Furman, *Don't Get Hooked by Phishing Scam*, DAILY NEWS (New York), Mar. 30, 2006, at B-42. According to a recent survey, Americans lost nearly $1 billion from participating in phishing scams in 2005. *Id.* A related concept called pharming occurs when software programs and viruses are used to detour Internet users to dummy sites. Howard Pankratz, *Suthers Warns of E-mail, Web Scams*, DENV. POST, Feb. 7, 2006, at B-4. *See also* Gregory M. Lamb, *New Twist on "Phishing"*

Today's e-thieves send out random phishing e-mails and "take a shotgun approach, scattering bogus e-mails everywhere and to everyone. They're counting on fooling only a few because it costs next to nothing to mass-blast these phony communiqués to millions of people—and it takes only a handful of suckers to make it worth their while."[139] Even more problematic, contemporary phishing e-mails are becoming more sophisticated, personalized and enticing.[140] These updated e-mails might cause even the most privacy-conscious web-surfer to at least pause, especially if the message slithers through the spam filter and is personally addressed to the e-mail account owner, and consider responding.[141] These more personalized and directly-targeted attacks are referred to as "spearphising" and are becoming more common as regular e-mail users become wise to the old fashioned, generic phishing scams of a few years ago.[142] Regardless of the form the attack takes—phishing or

---

Scam—"Pharming," CHRISTIAN SCI. MONITOR, May 5, 2005, at 13 (discussing the details of some types of pharming attacks).

139. Don Oldenburg, *Hook, Line and Sucker: Personalized Phishing Scams Use Customers' Names to Attract Attention*, WASH. POST, Apr. 2, 2006, at F-5.

140. Some recent phishing e-mails offer a cash reward for taking a brief survey when the volunteer is asked to enter different forms of PII. *See, e.g.*, Furman, *supra* note 138 (discussing a phishing scam allegedly from Chase that offers its customers a chance to take a brief survey for a cash reward of $20).

141. *See* Oldenburg, *supra* note 139 (discussing a personalized phishing e-mail that requests the recipient dispute a fraudulent transaction and, in the process, attempts to collect the individual's "name, birth date, mother's maiden name, driver's license number and state, and credit card info—just about anything your average criminal needs for identity theft." The e-mail was generated from a web site in Russia and routed through Amsterdam before arriving in the reporter's inbox).

142. *Id.* Oldenburg describes spearphishing as:

> such narrowly targeted fraud, called "spearphishing," has previously focused more on employees from particular corporations or on faculty members at universities—but not on specific individuals. [One expert] speculates that the crooks probably "scraped" random names accompanied by e-mail addresses somewhere online or hacked a database, then sent out tens of thousands of the tailored [phishing e-mails allegedly from the company PayPal] figuring to hit a decent percentage of actual PayPal customers.

Id.; *see also* Jon Swartz, *Phishing Scams Aim to Bilk Smaller Prey*, USA TODAY, Mar. 13, 2006, at B-1. Swartz states that

> [a] surge in phishing e-mail scams targeting regional credit unions and local banks is the latest sign fraudsters are shifting to narrow attacks. Smaller is better, security experts say, because the scams escape the attention of law enforcement and because a smaller company's cyberdefenses often aren't as imposing as those of a major corporation.

spearphishing—web site customers should be on the lookout for e-mails requesting immediate action in lieu of account closure, requests to update or enter more information to "update" an account, or requests to follow a link within the e-mail to be taken to an account update page. Even if a customer does not "fall for" the phishing scam by submitting the additional PII, merely opening up a phishing e-mail may lead to spyware and adware being transferred to the recipient's computer.[143]

While legitimate businesses are currently conducting more and more of their activities online,[144] policies at these same businesses frown upon sending e-mails requesting that customers transmit PII via e-mail.[145] Problematically, although many businesses make efforts to prevent phishing attacks, they are concurrently failing to make such efforts clear to their customers.[146] This fact, combined with customer feelings that (1) they will be penalized by the company for not responding, (2) their accounts will be closed, (3) electronic information was required to create an account in the first place, and, therefore, subsequently entering further information electronically is no big deal, and (4) the mock web sites linked to the spam look eerily similar to the official company web site,[147] serve

---

Swartz, *supra*.

143. *See* Furman, *supra* note 138 (stating that "Just by clicking on to a criminal Web site, you could become vulnerable to spyware infecting your computer that will track your key strokes").

144. *See, e.g.*, U.S. Census Bureau, *E-Stats: Estimated Quarterly U.S. Retail Sales* (last revised Nov. 17, 2006), http://www.census.gov/mrts/www/data/html/06Q3.html (showing that the amount of retail sales conducted via e-commerce have increased from $5.3 billion in the fourth quarter of 1999 to over $27.5 billion in the third quarter of 2006).

145. *See e.g.*, Oldenburg, *supra* note 139 (reporting that "[c]ustomers should keep in mind [that] PayPal (and any legitimate financial service) will not ask you to follow a link to enter personal, financial or account information. You should always open a new Web browser or call the company directly to confirm or dispute a transaction"). In fact, major targets of phishing attacks, like PayPal, have created their own webpages warning customers of the e-threat and informing them on how to deal with such e-mails. *See, e.g.*, PayPal, *Protect Yourself from Fraudulent Emails*, PAYPAL.COM, https://www.paypal.com/cgi-bin/webscr?cmd=_vdc-security-spoof-outside (last visited July 30, 2007) (this page warns customers to watch out for generic greetings, a false sense of urgency and fake links when reading e-mails alleging to come from PayPal).

146. *See, e.g.*, Providian, *Your Security: E-mail Scams: Phishing*, http://www.providian.com/home/your_security.htm (describing how Providian makes an effort to describe phishing and to educate its customers on how to avoid such attacks. However, this warning is buried as the twenty-ninth item in its privacy policy).

147. The following is a phishing e-mail I received recently:

> We recently have determined that different computers have logged into your PayPal account, and multiple password failures were present before the login. One of our Customer Service employees has already tryed [sic] to telephonically reach you. As our employee did not manage to reach you, this email has been sent to your notice.

as the primary reasons why web users consistently fall for phishing tactics.[148] All of these factors combine to make phishing America's "fastest growing form of consumer theft . . ."[149]

> Therefore your account has been temporary suspended. We need you to confirm your identity in order to regain full privileges of your account. If this is not completed by *December 9, 2005*, we reserve the right to terminate all privileges of your account indefinitely [sic], as it may have been used for fraudulent purposes. We thank you for your cooperation in this manner. To confirm your identity please follow the link below:
>
> *https://www.paypal.com/cgi-bin/webscr?cmd=_login-run*. Thank you for your patience in this matter.
> PayPal—Customer Service
>
> Please do not reply to this e-mail as this is only a notification. Mail sent to this address cannot be answered.

E-mail to the author, received on Dec. 5, 2005 (emphasis in original).

148. *See* Oldenburg, *supra* note 139. Oldenburg argues that

> there isn't a day my spam filter isn't filthy with pesky e-mails that pretend to come from eBay, PayPal, Chase and other legitimate businesses warning that my account has been compromised, defrauded or whatever. From urgent warnings (verify your information or your account will be suspended within 24 hours!) to look-alike Web sites and logos, most phishing spams are a study in crude social engineering. They're designed to convince the naive, gullible or unthinking to do one thing—click that link and give up a password or other confidential info.

Id. Other reasons people fall for phishing attacks are: (1) failing to look at the address bar or security features in the fake webpages linked to the phishing e-mails, (2) failing to understand the syntax of domain names (believing that "www.ebay-members-security.com belongs to www.ebay.com") and (3) a failure to distinguish between legitimate and illegitimate e-mails. Will Sturgeon, *The Secret of Phishers' Success*, CNETNEWS.COM, Apr. 3, 2006, http://news.com.com/2102-7349_3-6057000.html?tag=st.util.print (citing Rachna Dhamija et al., *Why Phishing Works*, PROCEEDINGS OF THE SIGCHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS (2006), http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf (detailing the reasons why people fall for phishing attacks years after warnings to avoid such e-mails first appeared).

149. Matt Hines, *Phishing is Fastest Growing Form of Computer Theft*, SILICON.COM, June 16, 2004, http://software. silicon.com/malware/0,3800003100,39121396,00.htm (stating that phishing attacks "accounted for a staggering $2.4bn in fraud, or an average of $1,200 per victim, during the last 12 months [2004]"). *See also* Jason Turcotte, *New Yahoo Shield May Dry Up the Phishing Well*, APPLICATION DEV. TRENDS, Aug. 24, 2006, http://www.adtmag.com/article.aspx?id=19114 (stating that "Phishing is one of the fastest growing security threats today"); Walter S. Mossberg, *Some Safety Tips to Help You Avoid Latest Scams*, PITTSBURG POST-GAZETTE, July 27, 2006, http://www.post-gazette.com/pg/06208/709074-96.stm. Mossberg states that

> the fastest-growing computer-security problem isn't viruses or other traditional malicious programs, and it can't be entirely defeated by using security software

2. External Security Breaches

An external security breach is "an unauthorized acquisition of computerized data [initiated by someone unrelated to the company] that compromises the security, confidentiality, or integrity of personal information maintained by the . . . business."[150] Many external security breaches are committed by hackers[151] utilizing computers to practice their trade from locations across the globe.[152] These break-in attempts seek to compromise a company's network security via: (1) physical intrusions, (2) system intrusions, or (3) remote intrusions.[153]

A physical intrusion occurs when individuals are physically present in front of a computer and use the keyboard or physically remove the disk drive in order to gain access to the system.[154] A system intrusion occurs when an individual already has some access to a computer system and utilizes that access to fraudulently gain access to more comprehensive

---

> or by buying a Mac. It's called "social engineering," and it consists of tactics that try to fool users into giving up sensitive financial data that criminals can use to steal their money and even their identities. Social engineering is a broad term that includes "phishing," the practice by which crooks create emails and Web sites that look just like legitimate messages and sites from real banks and other financial companies.

Id.

150. CAL. CIV. CODE § 1798.82(d) (West 2006); California Department of Consumer Affairs, *Recommended Practices on Notice of Security Breach Involving Personal Information* (Rev. Feb. 2007), *available at* http://www.privacy.ca.gov/recommendations/secbreach.pdf.

151. A hacker is a person who attempts to gain access to a computer network or system. *See, e.g.*, Wilson, *supra* note 135, at 1. There are two types of hackers: (1) benign hackers (who attempt only to access into their own computer systems) and (2) malicious hackers (who attempt to access other people's computer systems). *Id.* at 1.

152. *See, e.g.*, Steve Liewer, *Sub Base Hacking Suspect Arrested, Student, 18, Caught in Southern Spain*, SAN DIEGO UNION TRIB., Jan. 26, 2006, at B (discussing the arrest of a hacker operating in Spain who broke into the computer system of a U.S. Navy submarine base located in San Diego); *Hacker Facing U.S. Extradition*, PITTSBURG POST-GAZETTE (Pennsylvania), May 11, 2006, at A-4 (discussing attempts by the U.S. government to have a hacker jailed in Britain extradited to the United States where he is accused of hacking into federal government computers). *See also Credit Unions*, *supra* note 106 (citing a study by SecureWorks—a network manager for over 1000 credit unions and banks—demonstrating that credit unions are attacked 67% more often than banks. SecureWorks claims that it blocks over 760 daily hacker attacks on each credit union it represents).

153. *See* LinuxSecurity.com, FAQ: Network Instrusion Deteciton Systems, at 1.3 (discussing the primary ways in which an intruder can break into a computer network), http://www.linuxsecurity.com/resource_files/intrustion_detection/network-intrusion-detection.html (last visited Dec. 18, 2007).

154. *Id.* (stating that a stolen disk drive can then be read on another machine).

privileges.[155] Finally, remote intrusions occur when unauthorized access is attempted from afar—basically, from a remote location physically unassociated from the company.[156]

Each form of these attacks is made possible primarily because of software vulnerabilities[157] and the acquisition of passwords.[158] Although software programming is much better today than in the past, there will always be vulnerabilities—such as situations where hackers overload an input field with extra characters or otherwise try to crash the software program in order to gain access.[159] Additionally, because people—including system administrations—do not take the process of password creation seriously, hackers are able to access sensitive data merely by guessing simple passwords such as "admin."[160] Once inside a company's network, hackers most often: (1) commit reconnaissance (i.e., browse through data files searching for valuable PII), (2) deface web pages with web-graffiti, (3) establish a foothold on the network allowing for easy future access,[161] and (4) otherwise exploit the network through denial-of-service attacks or by using the network to institute future attacks.[162]

Aside from hackers accessing company systems to gain PII, other security breaches occur when thieves unassociated with a company con employees into giving out PII (a practice referred to as social engineering), pose as legitimate entities and request the data (a form of social engineering called pretexting),[163] or actually break into a physical location

155. Because system intrusions generally indicate at least some form of access they are more appropriately categorized as internal security breaches and are listed under the external breach section merely because they are a form of hacking.

156. Wilson, *supra* note 135, at 2.

157. *Id.* (stating that "[s]oftware always has bugs. System administrators and programmers can never track down and eliminate all possible software vulnerabilities, and attackers have only to find one hole in order to break in").

158. *Id.* at 2-4 (stating that "passwords are possibly the single weakest link in the security chain").

159. *Id.* at 3 (stating that situations where hackers try and overload a program by entering more characters than the program can take are called "buffer attacks.").

160. *Id.* at 4 (stating that a "surprising number of machines are configured with an empty or easy-to-guess root/administrator password" and that one "of the first things an attacker will do on a network is to scan all machines for empty or commonly used passwords").

161. Wilson, *supra* note 135, at 7 (discussing the idea that, at this point, hackers attempt to cover up their tracks by altering log files and audit trails while, at the same time, making sure that future access is obtainable).

162. *Id.* at 8 (stating that a denial-of-service attack occurs when a hacker attempts to prevent proper use of a computer, network, or web site by implementing tactics meant to temporarily crash the system).

163. *See, e.g.*, Rodney Gedda, *Hacker Mitnick Preaches Social Engineering Awareness*, CIO, July 26, 2005, http://www.cio-asia.com/ShowPage.aspx?pagetype=2&articleid=2141&pubid=5&issueid=55. Famous hacker, turned security consultant, Kevin Mitnick and states

to steal computer equipment containing PII records.[164] At the end of the day, regardless of the kind of external security breach perpetrated, stored PII should never be considered completely secure.[165] Company networks always will have holes, uninformed and negligent employees will constantly be tempted to give out sensitive information to unauthorized parties posing as legitimate entities and diligent e-thieves will generally find ways to infiltrate digital and physical structures to obtain information.

> "Social engineering attacks [of which pretexting is one type] can be simple or complex and take from minutes to years," [Mitnik] said, adding that surveys have revealed that nine out of 10 people will give their password in exchange for a chocolate Easter egg. Mitnick spoke of how social engineering has been used to extract millions of dollars from banks and how he used the technique to siphon source code for a mobile phone out of Motorola by posing as an employee in its own R&D department. Mitnick also mentioned how he is not immune to the social engineering scourge and was sent an e-mail "phishing" for information from his PayPal account earlier this year.

Id.; *see also* discussion, *supra* Part III.B.1 (discussing pretexting as a front-door e-threat).

164. *See, e.g.*, Bill Brenner, *Data Theft Roundup: More Laptops Stolen, Roughly 300,000 at Risk*, SEARCHSECURITY.COM, June 5, 2006, http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1192241,00.html (stating that "instead of hacking into company databases, thieves are making off with personal data on hundreds of thousands of people the old-fashioned way—by stealing machines from cargo holds, cars and offices").

165. *See, e.g.*, Wes Miller, *Reduce Your Risk: 10 Security Rules to Live By*, TECHNET MAG., May/June 2006, http://www.microsoft.com/technet/technetmag/issues/2006/05/ReduceRisk/default.aspx (explaining that computer data will never be 100% secure: "1. Because people are involved. 2. Because users make mistakes. 3. Because administrators also make mistakes. 4. Because systems don't always get updated when they should. 5. Because software itself is never completely secure"). *See also* Michael W. Hawkins, *Guidelines for Building a Secure IT Infrastructure*, informit.com, Jan. 25, 2002, http://www.informit.com/articles/article.asp?p=25065&seqNum=3&rl=1. Hawkins states that:

> It's impossible for any organization to completely eliminate all security risks. An organization can never be completely secure because all security technologies have weaknesses and limitations. While many organizations may acknowledge this fact, they often fail to manage the corresponding risks. For example, well-known penetration systems fail to explore many security technology issues, and completely disregard policies, processes, and facilities, among others. Virus-protection programs are always out of date. Firewalls are directed at outsiders, but do nothing to protect against malicious inside attacks. Most companies still rely on simple user ID and password controls that are ineffective for sensitive systems. And of course all security technologies are subject to human error, failure, and disaster.

Id.

Today's popular press is filled with stories reporting the types external security breaches just described.[166] Ironically, one of the most infamous recent external security breaches occurred at ChoicePoint—a prominent member of the data broker community conducting business by compiling and selling vast amounts of PII for a profit.[167] Through this breach,

166. *See, e.g.*. Ellen Nakashima, *AT&T Sues, Alleging Fraudulent Access to Consumer Accounts*, WASH. POST, Aug. 24, 2006, at D-3. Nakashima discusses a recent social engineering attack on AT&T Corp. whereby twenty-five people:

> [A]llegedly posed as customers to gain unauthorized online access to private phone records. Some 2,500 customers' records were stolen [and the] individuals gained access to the records by "pretexting" or fooling AT&T's computer or interactive voice response phone system into believing they were real customers. This was done by providing the customer's telephone number and the last four digits of the customer's Social Security number or the three-digit customer code associated with the customer's account . . . The [pretexters] also sometimes used "spoofing" software to make it appear that they were calling from the customer's telephone.

Id.; *see also Hackers Hit AT&T's Online Store*, SAN ANTONIO EXPRESS-NEWS, Aug. 30, 2006, at E-6 (discussing a recent instance of a remote intrusion through which hackers broker into AT&T Corp.'s computer system and stole over 19,000 pieces of PII collected from customers who purchased products from the company's online store). Aside from companies, even American colleges are experiencing a rash of external security breaches. *See, e.g.*, Mary Beth Marklein, *Colleges are Textbook Cases of Cybersecurity Breaches*, USA TODAY, Aug. 2, 2006, at A-1 (discussing over a dozen external security breaches occurring during the summer of 2006). Additionally, a different type of external security breach—loss of PII by an unrelated delivery service—is frequently reported in the popular press. *See e.g.*, Susan E. Peterson, *Borrowers Warned of Possible Security Breach*, STAR TRIB. (Minneapolis), Aug. 1, 2006, at D-2 (discussing a security breach that occurred when the U.S. Postal Service lost tapes containing the PII (including social security numbers, names, and student loan account numbers) of 188,000 individuals); Lazarus, *supra* note 125 (discussing a data tape containing PII on over 300,000 certified public accountants that was lost in transit by FedEx).

167. *See, e.g.*, David Litterick, *Thousands Hit by U.S. Identity Theft*, DAILY TELEGRAPH (London), Feb. 24, 2005, at 35. Litterick details the ChoicePoint security breach in the following manner:

> ChoicePoint, a data warehousing company, is facing a raft of lawsuits after it admitted that thieves, apparently using identities already stolen, created what appeared to be legitimate debt-collecting and cheque-cashing businesses seeking ChoicePoint's services. They then opened 50 accounts and received volumes of data on consumers, including names, addresses, social security numbers and credit reports.

Id. ChoicePoint is a data broker, "founded in 1997 as part of a spin-off of Equifax Inc. [that] has 19 billion public records in its database, including motor-vehicle registrations, license and deed transfers, military records, names, addresses, credit records and Social Security numbers." *ChoicePoint Breach Worse than First Reported*, CONSUMERAFFAIRS.COM, Feb. 22, 2005,

ChoicePoint lost control of the driver's license and social security numbers of more than 145,000 individuals nationwide as e-thieves, posing as small business owners, requested and obtained this information directly from the company.[168] Aside from the headline cases such as ChoicePoint, many smaller instances of external security breaches are common and each passing year is lamented as being more dangerous for e-commerce participants than the previous twelve month period.[169]

C. *U.S. Law Operating Inside the Company*

The U.S. legal system is trying to catch up to the e-threats targeting PII at the inside-the-company stage. For instance, some states prohibit phishing[170] while others require companies to promptly notify affected

---

http://www.consumeraffairs.com/news04/2005/choicepoint_worse. html. *See also Press Release: ChoicePoint Reports Revenue of $241 Million for the Second Quarter Reflecting Continued Strong Customer Demand*, ChoicePoint.com, July 20, 2006, http://www.choicepointasia.com/choicepoint/news.nsf/printview/920949876e82da3f852571a70077ec8a?Open Document. Press Release reports that:

> Legal expenses and other professional fees related to the previously disclosed fraudulent data access of $1.0 million ($0.6 million net of taxes) were incurred by the Company during the second quarter of 2006. The Company continues to estimate a total pretax expense of between $2 and $4 million for the full year 2006, exclusive of any potential settlements.

Id.

168. *See* Bill Husted, *ChoicePoint's Recovery*, ATLANTA J.-CONST., Feb. 12, 2006, at Q1 (discussing the security breach and the remedies implemented by ChoicePoint after the breach).

169. *See, e.g.*, Jon Swartz, *2005 Worst Year for Breaches of Computer Security*, USA TODAY, Dec. 29, 2005 (stating that "[a]t least 130 reported breaches have exposed more than 55 million Americans to potential ID theft [in 2005]. Security experts warn that wayward personal data, such as Social Security and credit card numbers, could end up in the hands of criminals and feed a growing problem").

170. *See, e.g.*, New York Anti-Phishing Act of 2006, N.Y. CLS Gen. Bus. § 390-b(3) (2007) (prohibiting e-mails that deceptively solicit PII from New York residents). *See also N.Y. Laws Turn Privacy Triple Play*, CONSUMER FIN. SERVICES L. REP., June 28, 2006, at 3 (discussing three consumer privacy laws enacted by the New York state legislature, including the Anti-Phishing Act of 2006). Additionally, some Internet Service Providers are suing people operating phishing web sites on their networks. *See, e.g.*, AOL, Cyota Partner in Anti-Phishing Campaign, Globes (online)—Israel's Business Area, Apr. 20, 2005.

> America Online today announced a major new initiative to combat "phishing"—the practice of using fraudulent e-mail and fake web sites to solicit sensitive personal information from users. As part of the campaign, America Online has partnered with Cytoa to help identify and block access to suspected phishing sites through a 24-hour-a-day, 7-day-a-week monitoring process. AOL and Cytoa are also working to evaluate and deploy other joint technologies and

residents when such companies experience serious security breaches.[171] Little synergy stems from these regulations, however, as most are narrowly-targeted at individual e-threats and provide gaping holes through which different e-threats can cause problems. Although some of these holes are filled with industry self-regulation efforts and other industry initiatives, other gaps remain uncovered allowing companies to ignore the e-threats if protecting against them becomes too expensive or too tedious. Unsurprisingly, because they are not forced to do so, contemporary e-commerce companies are not rapidly jumping on the self-regulatory bandwagon or drafting comprehensive security policies to protect PII they obtain, process and store. Finally, the provisions contained in the laws that do exist vary widely from state to state. This patchwork regulatory framework makes it more difficult for companies to comply with the law and for the public to fully understand the implication of these regulations on their PII once they have submitted such information online.

This current regulatory framework governing inside the company e-threats can be improved by creating a national standard via a federal statute directly targeting each of the major e-threats at this stage. To make this happen, the federal law introduced in Part III of this Article should be drafted to contain a second substantive section designed to protect valuable PII once it is out of the hands of the individuals it identifies and into the hands of its collectors—at the inside of the company stage. Requiring the mandatory posting of an electronic, multilayered, standardized, and readable privacy policy is a fair compromise between businesses' commercial interests and an individual's information privacy interests when PII has yet to be submitted into cyberspace. However, a privacy policy requirement, in and of itself, is insufficient to protect PII once it changes hands and travels into a company's databases. Once inside the

---

> share information in order to better detect and respond to phishing attacks. . . . AOL stated that it is also working internally and with other partners to identify and block phishing sites.

Id.

171. *See, e.g.*, Pennsylvania Breach of Personal Information Notification Act, PA. CONS. STAT. § 712 (2005) (requiring companies to notify Pennsylvania residents if their PII has been lost or stolen). As for PII security policies, the law does not require companies to create any type of security policy. In fact, "[t]he vast majority of companies issue a security policy only because their lawyers tell them to . . . It typically gets buried in an employee handbook and is never seen again." *See* Lazarus, *supra* note 125 (quoting a Silicon Valley privacy consultant). It took the Department of Veterans Affairs three weeks from the date of the laptop theft to disclose the security breach to the public. *Id.* To combat this trend, current laws in thirty-four states require companies and public institutions to report on security breaches. *See* Marklein, *supra* note 166 (stating that "[b]usinesses, non-profits and public institutions in 34 states are required to notify consumers when personal data have been compromised.").

company, even the most diligent consumer cannot control whether the company experiences a security snafu or a rouge company employee stealing and selling PII on the open market. Therefore, this second section of the proposed federal law needs to be more comprehensive and require more of covered companies than the section dealing with front door e-threats.

The additional provisions that are necessary at this stage should be specifically designed to protect against the e-threats of data mining, security breaches (both internally- and externally-created), and phishing. Similar to the front door regulatory policy, all regulations in this section must be designed as regulatory ceilings. This preemption of state and local laws will create a needed national standard that eliminates state-by-state variations, helps e-commerce companies comply, and increases the chances that the American public can better understand the law and its privacy implications.

At this stage, a regulatory ceiling is a fair compromise between e-commerce efficiency and information privacy because PII is partially within the control of the person it identifies (submitters may have the opportunity to opt-out, amend, or delete their PII from company databases) and partially in the hands of the company (submitters have their PII stored in inaccessible company databases that are subject to use and sale). Therefore, individuals are able to take a bit of personal responsibility over their Internet activities if they feel that a company is mishandling their PII. On the other hand, individuals can only exercise this responsibility if the company allows them to opt-out or amend and delete their PII before it is sold on the open market or otherwise distributed. Therefore, effective regulations at this stage of the PII processing cycle must require more than the mere posting of a compliant, multilayered, standardized and readable privacy policy. More specifically, this section of the proposed law will deal with the inside-the-company e-threats, in the following manner.

1. Data Mining & Phishing

This sub-section of the proposed law will require companies to disclose two things in their privacy policies and on all customer account registration pages: (1) whether they will ever seek to obtain account or personal information electronically and (2) their data mining practices. Therefore, web site visitors will have two places to familiarize themselves with such practices and these notifications will help users understand the implications of submitting their PII as well as combat the effectiveness of phishing attacks because of this increased consumer awareness.

More specifically, companies should be required to state whether they will ask a visitor to add or amend PII through an e-mail correspondence and, if so, what visitors should look for to ensure that the request is authentic. They also should be required to detail the data mining procedures they utilize and how the end results of such data mining are implemented into their business strategy. If a company elicits PII via electronic correspondence or if a company conducts data mining then it must accurately disclose this information in the PERSONAL INFORMATION SECURITY (phishing policies) PERSONAL INFORMATION USES (data mining policies) required heading in its privacy policy.

2. Security Breaches

On the security breach front, this section of the proposed law will set a national standard requiring companies experiencing a major security breach to notify affected customers within a certain period of time. Under these provisions, companies will be required to notify any visitor who had PII compromised through an internal or external security breach that specific pieces of PII were compromised and how the visitor can begin to rectify the situation. Today, residents in thirty-four states[172] are required to receive such notifications while residents in non-covered states remain unprotected. Some states require the compromise of the specific information to put the individual it identifies at some sort of risk before notification is mandatory,[173] while others require notification upon breach alone, regardless of the risk presented by the breach.[174] Risk-based statutes protect less privacy but also allow companies some ability to remedy the problem before spending financial and political capital on a breach notification. However, a national standard will remedy this problem and

172. *See State PIRG Summary of State Security Freeze and Security Breach Notification Laws*, STATE PIRG CONSUMER PROTECTION, http://www.pirg.org/consumer/credit/statelaws.htm (last visited July 30, 2007) (demonstrating that thirty-four states had enacted security beach notification legislation as of July 18, 2006).

173. *See, e.g.*, ARK. CODE ANN. § 4-110-105(d) (2006) (requiring notification only after a reasonable investigation and determination that no "reasonable likelihood of harm" is posed to customers whose PII was compromised).

174. *See, e.g.*, DEL. CODE ANN. tit. 6, § 12-B-102 (2006). Companies conducting business in Delaware and owning or licensing PII

> shall give notice to a resident of Delaware of any breach of the security of the system immediately following the discovery of a breach in the security of personal information of the Delaware resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Id.

make it easier for companies to comply—there being only one regulation on this area instead of thirty-four. E-consumers also will benefit from these provisions because a national standard, and the corresponding consistency, will make it easier for all Americans to understand the events that will occur once a security breach occurs—rather than just the consumers in the states where notification laws exist. Additionally, customers will be able to rest assured that the company will take their information privacy more seriously than it has in the past.[175]

---

175. The following are suggestions companies can implement to better protect against security breaches, according to Mark Melodia, an attorney working in the area of information privacy:

1. Review customer and investor communications and don't overpromise on privacy. Businesses that promise too much are setting themselves up for a breach of contract lawsuit;
2. Inventory the personal information you keep and share;
3. Assign responsibility for data security to the highest levels. Make data security a priority for the board and senior management;
4. Consider the widest practical use of encryption. State security breach laws don't require disclosure of stolen data if it is encrypted;
5. Destroy documents with no remaining business use;
6. Train and certify employees on data security;
7. Restrict access to personal information, especially Social Security numbers; secure electronic devices;
8. Implement an incident response plan. If someone loses a company laptop, who takes action?;
9. Audit compliance regularly; and
10. Review security breach insurance coverage.

Patricia Sabatini, *New State Law Will Require Companies to Notify Customers of Data Security Breaches*, PITTSBURG POST-GAZETTE, June 13, 2006, at D-1 (discussing the advisement of companies on dealing with the new Pennsylvania security breach notification law. This advice would also be applicable to similar federal security breach legislation). With this federal security breach notification law in place companies will be encouraged to take PII protection more seriously to avoid the unpleasant notification requirements. In fact, protection lessons may be gleaned from the practices of company HR departments which are undertaking effective measures to protect the PII of their employees. Some of these tactics encompass the: (1) creation of a PII-protection policy, (2) limitation on the amount of people with access to PII (3) creation of an environment with PII is physically protected by a locked file cabinet or a password-protected database, (4) encryption of PII when it is stored and transmitted either internally or externally and (5) limitation of the amount of PII on company documents (i.e., truncate a social security number on a customer invoice or marketing list). *See, e.g.*, *How HR is Coping*, *supra* note 123 (citing a HRfocus Employee Privacy survey finding that over 96% percent of the companies surveyed limited the number of people with access to employees' PII and also locked file cabinets and office doors where such information is stored, but only half of the respondents had a formal PII-protection policy and just over 30% encrypted stored data).

More specifically, companies experiencing an internal or external security breach where any piece of PII is compromised—lost or stolen—and cannot be recovered within a 48-hour period must notify the affected customer(s) via e-mail or postal mail if the company has a reasonable belief that customers will experience a financial loss or injury.[176] This notification must occur within fifteen business days from the date the security breach was discovered and detail exactly what pieces of PII were compromised and how the customer should protect against various e-threats such as identity theft.[177]

Specifically excluded are any requirements for a company to implement any type of security policy.[178] However, companies will pay, both from a financial and a goodwill standpoint, by choosing to ignore this type of policy implementation. Additionally, companies will not be required to provide credit monitoring services to affected customers because the very early notification requirements—fifteen business days from the date of breach discovery—will give individuals enough time to monitor their accounts.

In addition to the thirty-four state security breach notification laws, numerous security breach laws have been floating around the U.S. Capitol, but none has materialized into a serious candidate to become a successfully-enacted bill.[179] Five Congressional committees—two in the House of Representatives and three in the Senate—have recently discussed

176. If more than 100,000 people are affected or if the notification would cost more than $100,000, then all notifications may occur via e-mail and the posting of the breach on the company's homepage for thirty days and announced in the national media periodically over the same period. If the breach affects more than 500 people, the company would also have to notify the national credit bureaus. This type of notice is referred to as substitute notice and is common in state security breach notification laws. *See, e.g.*, ARK. CODE ANN. § 4-110-105(e)(3)(A) (2006) (providing for substitute notice if notification costs exceed $250,000, over 500,000 individuals would need to be notified or the company does not possess sufficient contact information).

177. Companies will not be forced to provide credit monitoring services to affected customers in notification situations as the early notification requirements (fifteen days from the date of breach discovery) will give the customers enough time to monitor their account activities.

178. Contrary to the federal law proposed in this Article, Arkansas requires companies to implement and maintain "reasonable security procedures and practices appropriate to the nature of the information to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." ARK. CODE ANN. § 4-110-104(b) (2005).

179. *See, e.g.*, *Washington Wire*, WALL ST. J. ABSTRACTS, Aug. 12, 2005, at A-4 (stating that the "Senate Commerce Committee approved bill before recess requiring companies to inform consumers of security breaches, but Senate Banking and Judiciary Committees are also vying for jurisdiction over identity-theft legislation.").

such legislation[180] and approximately twenty bills were introduced with none coming to a floor vote.[181] The four most prominent bills would all preempt conflicting state laws[182] but differ in their definitions of what constitutes a security breach,[183] which customers must be notified,[184] the timing of such notice[185] and their enforcement options.[186]

The third substantive section of this proposed federal law will deal with the serious e-threats attacking PII at a company's back door. Before delving into these final provisions, however, the beginning sections of Part V will identify both the internally- and externally-created e-threats at this final stage of the PII processing cycle.

V. E-THREATS AT THE BACK DOOR (PII DISSEMINATION)

Companies that obtained PII for the purpose of executing transactions and creating internal marketing profiles recently have discovered the value

180. *See, e.g.*, Kirk Nahra, *Federal Security Breach Legislation Progresses (But Slowly)*, WILEY REIN AND FIELDING, LLP: NEWSLETTERS, Nov. 2005, http://www.wileyrein.com/publication_newsletters.cfm?id=10&publication_ID=12393.

181. *See* Financial Data Protection Act, H.R. 3997, 109th Cong. (1st Sess. 2005) [hereinafter H.R. 3997], Data Accountability and Trust Act, H.R. 4127, 109th Cong. (1st Sess. 2005) [hereinafter H.R. 4127], Identity Theft Protection Act, S. 1408, 109th Cong. (1st Sess. 2005) [hereinafter S. 1408]; Personal Data Privacy and Security Act of 2005, S. 1789, 109th Cong. (1st Sess. 2005) [hereinafter S. 1789]. *See also* Satish M. Kini & James T. Shreve, *Notice Requirements: Common Themes and Differences in the Regulatory and Legislative Responses to Data Security Breaches*, 10 N.C. BANKING INST. 87, 103 (Mar. 2006) (discussing each of these bills).

182. H.R. 3997, *supra* note 181, § 2, H.R. 4127, *supra* note 181, § 6, S. 1408, *supra* note 181, § 7; S. 1789, *supra* note 181, § 404.

183. For example, the Financial Data Protection Act of 2005 considers a security breach to have occurred when personal information has been acquired and can be used to commit a financial fraud. H.R. 3997, *supra* note 181, § 2. However, the Data Accountability and Trust Act defines as security breach as an unauthorized acquisition of personal information providing a "reasonable basis to conclude that there is a significant risk of identity theft to the individual to whom the personal information relates." H.R. 4127, *supra* note 181, § 5(1).

184. For example, the Financial Data Protection Act of 2005 requires that the Secret Service be notified in addition to the affected customers. H.R. 3997, *supra* note 181, § 2. The Identity Theft Protection Act, on the other hand, requires notice to affected customers, the FTC and the most prominent consumer reporting agencies (as long as over 1,000 customers are affected). S. 1408, *supra* note 181, § 3(a)(1) & 3(b).

185. The Personal Data Privacy and Security Act of 2005 requires some forms of notice to be made within thirty days. S. 1789, *supra* note 181, § 421(d)(2).

186. The Data Accountability and Trust Act assigns the FTC as the major enforcer of its provisions while the Personal Data Privacy and Security Act of 2005 assigns this role to the U.S. Attorney General. H.R. 4127, *supra* note 181, § 4; S. 1789, *supra* note 181, § 428.

of this information on the open market.[187] In fact, the PII data trade has spawned entire industries comprised of commercial data brokers devoted to the compilation and fee-based dissemination of PII.[188] For under $50, virtually anyone can buy a comprehensive and accurate PII profile pertaining to virtually anyone else. The typical purchasers of this information range from business entities to individuals such as private investigators to governmental agencies.[189] Surrounded by this flourishing personal data economy, today's e-commerce companies are faced with a serious operational dilemma. They can either: (1) destroy PII, (2) retain PII for internal purposes only and risk the loss of a cutting-edge profit stream and raising the ire of shareholders seeking higher earnings, or (3) disseminate the PII records into the marketplace for a fee, generate revenue and lose control of valuable information entrusted to the company by its customers.[190]

---

187. *See, e.g.*, Jeanne Sahadi, *Your Identity... For Sale: From Credit Bureaus to Grocers to Unscrupulous Brokers, There's a Healthy Trade in Your Good Name*, CNNMONEY.COM, May 9, 2005, http://money.cnn.com/2005/05/09/pf/security_info_profit/index.htm (stating that the data trade is a multi-billion-dollar industry and that "there's a lot of money to be made off of your good name").

188. Some of the largest commercial data brokers are: ChoicePoint, http://www.choicepoint.com (last visited May 28, 2006), Acxiom, http://www.acxiom.com (last visited May 28, 2006) and Lexis/Nexis, http://www.lexisnexis.com (last visited May 28, 2006). To show the profit potential of the major commercial data brokers, Acxiom earned $44.6 million of off revenue of $344 million. Acxiom, *Acxiom Reports Fourth-Quarter, Fiscal-Year Results*, May 17, 2006, http://www.acxiom.com/default.aspx?ID=2946.

189. *See, e.g.*, Nancy Libin, *Perspective: The Anxious New Dawn of Cybersnooping*, CNET NEWS.COM, May 3, 2006, http://news.com.com/The+anxious+new+dawn+of+cybersnooping/2010-1028_3-6067598.html?tag=item (stating that federal government agencies, such as the Social Security Administration, the Justice Department, the Department of Homeland Security and the State Department, have collectively purchased over $30 million worth of PII on American citizens that was collected by private entities). These agencies have found a loophole in the Privacy Act of 1974 that requires governmental agencies to follow strict protocols when collecting and storing PII on American citizens but not if they merely purchase this same information from private entities. *Id.*

190. *See, e.g.*, Robert Gellman, *Privacy: Finding a Balanced Approach to Consumer Options*, Center for Democracy & Technology, http://www.cdt.org/privacy/ccp/consentchoice4.shtml (last visited July 30, 2007) (discussing the importance of finding the appropriate balance between record-keepers and record-subjects whereby certain circumstances—such as "law enforcement, national security, public health and economic growth"—record-keepers to put PII to secondary uses regardless of consumer consent while other circumstances require record-subjects to control dissemination of PII for secondary uses), Pricilla Regan, *The Role of Consent in Information Privacy Protection*, CENTER FOR DEMOCRACY AND TECHNOLOGY, http://www.cdt.org/privacy/ccp/consentchoice2.pdf (last visited July 31, 2007) (arguing that secondary uses of PII have created a slippery slope where PII is now used for purposes close enough to the original purpose of its collection and this practice is inconsistent with fair information practice principles) and Larry Ponemon, *The Seven Deadly Sins of Identity Management*, COMPUTERWORLD.COM, May 20, 2005,

If a company chooses the dissemination option—exchanging PII for money through its back door—it has two primary alternatives. First, PII may be disseminated to third parties with restrictions on its future use and its further dissemination.[191] This arrangement may, for instance, allow for the purchaser to utilize the PII to market to the person the PII identifies but not to sell the information to anyone else. The second alternative would allow for the purchased PII to be disseminated to third parties unrelated to the initial purchaser and with no restrictions on any future use and further dissemination of the information. Under this second option, the PII is released into a digital environment where it becomes virtually irretrievable.[192]

Today, state and federal law does not restrict companies from disseminating the PII they have collected. The law is also silent as to whether companies must restrict the future uses of the PII if they choose dissemination. This silence strengthens e-threats targeting PII at the back door as companies set their own dissemination policies that may or may not revolve around PII security.[193] As may be expected, the most serious e-threats arise when PII is released without restrictions and to unrelated entities. At this point, the data is outside of the control of the individual it identifies as well as the company that likely promised to protect it. Available now to anyone armed with only a modem, computer (or a computerized device such as a cellular phone) and a small amount of cash, this information may be snatched up and utilized for sinister purposes such as criminal acts, identity theft and/or spam. Because the law does not adequately protect consumers from these back door e-threats, people find

---

http://www.computerworld.com/securitytopics/security/story/0,10801,101893,00.html?source=x73 (arguing that companies face a dilemma between the desire to collect vast amounts of PII and the expectations that customers do not expect that their information will be put to secondary purposes).

191. *See, e.g.*, Editorial, *Wells Fargo and Privacy*, S.F. CHRON., Dec. 23, 2002, at A-20 (stating that the Chairman and CEO of Wells Fargo "would support legislation to offer consumers more control over the secondary use of their personal financial information" as long as the legislation is made on the federal, rather than the state, level).

192. *See, e.g.*, SoccerTutor.com, Terms and Conditions—Does Soccertutor.com, Ltd. Sell my Personal Information to Other Companies, http://www.soccertutor.com/termsandconditions.asp (last visited July 31, 2007) (stating, in the privacy policy for this company, that PII collected may be used for secondary uses such as marketing conducted by unrelated third parties unless the consumer affirmatively opts-out of such secondary uses).

193. Electronic Privacy Information Center, *In the Matter* of Intelligent e-Commerce, Inc., Complaint and Request for Injunction, Investigation and for Other Relief, http://www.epic.org/privacy/iei/ftccomplaint.html (last visited July 31, 2007) (stating that "the release of [PII] without a consumer's knowledge can lead to devastating results, including identity theft and fraud." This statement was made in a complaint against Intelligent E-Commerce, Inc. (an Internet investigative service/PII provider) that was filed with the FTC by the Electronic Privacy Information Center or EPIC).

themselves trying to restore their identity and protect their personal information after an attack has occurred. Although the media plays down this restoration process as a mere annoyance where the credit card companies take on most of the risk, in actuality, adequate recovery from the ill effects of back door e-threats often becomes a major hardship and costs precious money and time.

This part discusses three primary e-threats targeting PII at this back door stage: (1) unverified information requests, (2) identity theft, and (3) spam. It argues that the federal law proposed previously must be supplemented by a third substantive section. This third section must be designed as a regulatory floor instead of a regulatory ceiling, and it must place tight restrictions on the dissemination of PII via a company's back door. As with the other two categories of e-threats, some of the most prominent back door threats are created internally while others are created externally.

A. *Internally-Created "Back Door" Threats*

Unless stored PII is compromised and disseminated by criminals during a network hack or other form of security breach,[194] companies are the disseminators of personal information into cyberspace. This is problematic because companies across the United States possess hundreds of millions of pieces of personal information in powerful customer and marketing databases. These databases allow for the efficient and simple transfer of such information to third parties. These third parties can then download the information directly into their powerful databases in an instant.

Although companies may not realize it at the time of sale (or may not care in the first place), disseminated PII is extremely vulnerable as the information is irretrievable and can be instantaneously transferred to anyone, anywhere across the globe. Although the initial purchaser may intend to use the information legally, a secondary or tertiary purchaser may utilize this information for malicious purposes. All the while, the person the PII identifies will have no idea that her PII is even in circulation. Such uninhibited dissemination also allows a wide variety of entities and individuals to create digital dossiers on the vast majority of the public. These dossiers are then sold on the open market and more information surfaces in cyberspace. To help protect against such vulnerabilities, companies must be required to guard against back door e-threats targeting information that they disseminate; the most prominent e-threat of this nature occurs in the form of backdoor pretexting.

194. *See supra* Parts IV.A.2, IV.B.2 (discussing both internal and security threats occurring at the inside-the-company stage).

Back-door pretexting occurs when a company official or employee, either negligently or knowingly, disseminates PII to someone assuming an identity or otherwise seeking to obtain the information for improper purposes. Back-door pretexting is similar to front-door pretexting in the sense that an individual utilizes fraudulent means to obtain PII.[195] The difference is that with front-door pretexting the thief obtains the information from the consumer while back-door pretexting involves obtaining the information from a company that has collected and stored such information. Back-door pretexters are looking to obtain pieces of PII in order to complete an investigation, serve a summons or locate an individual. The problem is that the pretexter does not reveal his true identity or the true reasons for such information requests. Back door pretexting is a bit different from identity theft because an individual's identity is not stolen by the pretexter; rather, pretexters look to obtain a key piece of PII for some specific reason unrelated to identity theft. An easy way to remember this distinction is that pretexters generally lie to obtain PII to complete a pre-assigned task more often than they steal such information for their own aggrandizement while identity thieves generally steal PII for their own aggrandizement more often than they lie to obtain such information to complete a pre-assigned task.

An infamous example of back-door pretexting occurred in the Rebecca Schaeffer murder case. Schaeffer, a twenty-one year old actress, was shot several times at her apartment by a stalker who located her home address by retaining a private investigator. The investigator obtained her address by paying a fee to California's motor vehicles agency—an organization that did not make an effort to determine why the information was being requested.[196] Regardless, the information was obtained for an improper purpose and should not have been released in the first place. In response to this back-door pretexting, Congress passed the Driver's Privacy Protection Act (DPPA).[197] The DPPA subsequently was challenged on federalism grounds based on the idea that individual states have the

195. Back-door pretexting is similar to front-door pretexting in the sense that an individual utilizes fraudulent means to obtain PII. The difference is that with front-door pretexting the thief obtains the information from the consumer while back-door pretexting involves obtaining the information from a company that has collected and stored the information. *See supra* Part III.B.1 (discussing the e-threat of front-door pretexting).

196. *See* Steve Lash, *Court Upholds Law that Protects Privacy of Driver's License Data*, HOUSTON CHRON., Jan. 13, 2000, at A-6 (reporting that states were selling PII to the public before the enactment of the Driver's Privacy Protection Act).

197. DRIVER'S PRIVACY PROTECTION ACT OF 1994, 18 U.S.C. § 2721 (2000) [hereinafter DPPA]. The law forbids a state to disclose driver's information such as a name, address, telephone number, or photograph although states may still disclose accident information and other driving history.

authority to regulate issues intrastate commerce such as state driving licenses.[198] The U.S. Supreme Court, however, unanimously upheld the law and it is still in force today.[199] Unfortunately, the protections of the DPPA only apply to state motor vehicle agencies and not to private entities disseminating PII, leaving the major source of PII dissemination unregulated.[200]

As demonstrated above, this internally created e-threat of disseminating PII for improper uses can be deadly serious. Although the real bad actors are the people requesting the information by posing as someone else or by disguising their proper purpose, companies are at fault for not at least verifying the identity of such requestors. Once this information is purposefully disseminated outside of its control, the company has subjected an individual's sense of security—both financial security and personal security—to potential problems. The next section will discuss externally-created e-threats that stem directly from the dissemination of PII through a company's back door.

B. *Externally-Created "Back Door" Threats*

It is important to note that the two major externally-created e-threats—identity theft and spam—primarily occur only after a company disseminates PII into the open market. If companies chose not to disseminate PII for a fee then the primary way that such information would be available to identity thieves and spammers would be from some type of internal or external security breach. For better or worse, companies today do disseminate PII into cyberspace making the discussion of these two external back door e-threats very important.

1. Identity Theft

Identity theft occurs when PII is obtained and utilized for unlawful purposes without permission from the individual the information identifies.[201] These unlawful purposes can range between applying for a

198. *See* Reno v. Condon, 528 U.S. 141 (2000) (arguing, in the unanimous decision written by Chief Justice Rehnquist, that the law was constitutional in that it only required state employees to refrain from selling PII and not to participate in a large federal program). *See also* Lash, *supra* note 196 (reiterating the argument of the states that the federal government could not constitutionally require state employees "to participate in a federal privacy program.").

199. *See Reno*, 528 U.S. at 141 (stating that the DPPA was upheld over a state federalism challenge).

200. 18 U.S.C. § 2721(a) (limiting coverage to "a State department of motor vehicles, and any officer, employee, or contractor thereof.").

201. FTC, About Identity Theft, http://ftc.gov/hcp/edu/ microsites/idtheft/consumers/about-identity-theft.html [hereinafter FTC, *Identity Theft Web Site*] (last visited July 31, 2007) (defining

credit card under an assumed identity to posing as someone else to gain an employment opportunity.[202] The idea is that another person's identity allows the thief easy access to money or to a clean police record. The fallout from these activities may cause the identity theft victim to incur a monetary loss, negative credit reputation and, potentially, criminal record.[203] Although this e-threat preceded the Internet in offline forms such

---

identity theft and providing comprehensive information intended to keep consumers from becoming victimized by identity theft). Other definitions of identity theft are expressed a bit differently; for instance, the e-threat has been defined as "the appropriation of someone else's personal or financial identity to commit fraud or theft." George R. Milne et al., *Consumers' Protection of Online Privacy and Identity*, 38 J. CONSUMER AFF. 2, 217 (2004). This definition is incomplete, in my opinion, because it omits the concept of the identity being compromised without the permission of the person the information identifies; this knowledge aspect is crucial to the definition because complicity in the identity theft would omit the victimization aspect of the crime. Sometimes PII is stolen offline by fraudulently obtaining paper records (pretexting) or household mail, through an electronic phishing attach, via a fraudulent scanning device attached to an ATM machine (skimming) or in the trash (dumpster diving). FTC, Identity Theft Web Site, *About Identity Theft*, http://www.consumer.gov/idtheft/con_about. htm (last visited May 29, 2006). This is in contrast to identity fraud which includes identity theft as defined above as well as cases where a fictitious identity is created to commit unlawful activities. *See, e.g.*, David Lacey & Suresh Cuganesan, *The Role of Organizations in Identity Theft Response: The Organization-Individual Victim Dynamic*, 38 J. CONSUMER AFF. 2, 245 (2004) (demonstrating that customers are injured only by identity theft while companies can be injured by both identity theft and identity fraud). Therefore, "identity theft is a narrower subset of identity fraud." *Id.*

202. *See* FTC, *Consumer Fraud and Identity Theft Complaint Data: January—December 2005*, 3 (Jan. 2006) [hereinafter *Consumer Fraud and Identity Theft Complaint Data*]. According to FTC data from 2005,

> [c]redit card fraud (26%) was the most common form of reported identity theft followed by phone or utilities fraud (18%), bank fraud (17%) [generally in the form of an electronic funds transfer to a fraudulent account], and employment fraud (12%). Other significant categories of identity theft reported by victims were government documents/benefits fraud (9%) and loan fraud (5%).

Id.

203. *See, e.g.*, Lacey & Cuganesan, *supra* note 201, at 244. Lacey & Cuganesan argue that other consequences are the

> ability to secure employment, obtain goods and services on credit, travel freely, and participate in the wider society in a generally unencumbered fashion. In fact, merely seeking to reestablish an identity can result in ongoing denial of services for the victim, such as access to existing accounts and execution of existing contracts.

Id. Many of these negative consequences occur when the identity thief fails to pay for the charges incurred under the false identity and the creditors send the accounts to collections where collection agencies then notify credit agencies. *See, e.g.*, George R. Milne, *How Well Do Consumers Protect Themselves from Identity Theft?*, 37 J. CONSUMER AFF. 2, 388 (2003) (stating that "[t]he billing

as "opening new credit card accounts, taking out loans in the victim's name, and stealing funds from existing checking, savings, or investment accounts . . . the latest vehicle for perpetrating identity theft can be found on the 'Information Highway.'"[204] In 2005, more than 250,000 complaints of Identity Theft were logged by the FTC's Consumer Sentinel database, a number only slightly higher than the nearly 247,000 complaints received in 2004[205]–leading some commentators to discredit identity theft as a true threat.[206] Complaints filed with the FTC alone, however, may not paint a

---

statement is often diverted to another billing address so that the victim is not aware charges have been made and payment is overdue, which results in a bad credit rating."). Identity thieves have been known to utilize the stolen identity during an arrest and, subsequently miss the court date, causing an arrest warrant to be issued in the victim's name. *See* FTC, *ID Theft: What It's All About*, 4 (June 2005) [hereinafter *What It's All About*].

204. Hemphill, *supra* note 65, at 51. Hemphill quotes the chief executive officer of an institute studying economic crime stating that the Internet has

> allowed the identity thief to obtain personal identifiers of multiple persons quicker; to access higher quality fake identification tools (driver's licenses, birth certificates, Social Security cards, etc.) and, through e-commerce, to render the credit transaction completely impersonal. The potential harm caused by an identity thief using the Internet is exponential.

Id.; see also Milne et al., *supra* note 201, at 219 (stating that "[w]hile identity theft has traditionally occurred through offline methods, online data collection of stolen identities can be easier and more efficient for thieves, with new approaches and scams being created and implemented under the cloak of electronic anonymity.") (internal citations omitted).

205. *See* FTC, *Identity Theft Victim Complaint Data: Figures and Trends 1*, Dec. 31, 2005 [hereinafter FTC, *Identity Theft Data 2005*], http://ftc.gov/bcp/edu/microsites/idtheft/downloads/clearinghouse_2005.pdf (presenting detailed figures and statistics on the number and type of identity theft complaints received as well as a state-by-state analysis from January 1 through December 31, 2005); *Consumer Fraud and Identity Theft Complaint Data*, *supra* note 202, at 3 (reporting that the FTC received "over 685,000 . . . complaints during calendar year 2005—63% [or 431,550] represented [general online or offline] fraud and 37% [or 253,450] were identity theft complaints."). In 2005, "[c]onsumers reported losses from [general fraud and identity theft] of more than $680 million." *Id.* at 2. This data is stored with and correlated by the Consumer Sentinel—a complaint database that is "developed and maintained by the FTC" that collects consumer fraud and identity theft from the FTC and 150 other organizations and "makes it available to law enforcement partners across the nation and throughout the world for use in their investigations." *Id.* Complaints to the FTC can be anonymously filed either online (at http://www.ftc.gov) or via a toll-free phone number (1-877-FTC-HELP). Press Release, FTC, Press Release: FTC Releases Top 10 Consumer Fraud Complaint Categories (Jan. 25, 2006). The online complaint form is five pages in length and allows victims to describe their complaint, including a chance to describe the identity thief! FTC, ID Theft Complaint Input Form, https://rn.ftc.gov/pls/dod/widtpubl$.startup?Z_ORG_CODE=PU03.

206. *See* Lacey & Cuganesan, *supra* note 201, at 244 (lamenting that "evidence indicates that identity theft is becoming increasingly attractive for perpetrators vis-à-vis other forms of crime. In the United States, for example, identity theft is described as growing at a rate of 30% per year, with

complete picture of identity theft as a 2003 FTC report found that more than 9.9 million people were victims of identity theft in a twelve-month period.[207] Other sources claim that more than 7 million people became victims of identity theft between July 2002 and July 2003.[208] If accurate, a victim's list hovering near 10 million people would place identity theft into the category of a serious e-threat.[209]

In the twenty-first-century Internet environment, identity thieves have a much easier time—oftentimes operating online from the comfort of their own homes across the globe—piecing together false identities because of the easy access to PII from data broker entities,[210] companies selling such

---

its losses estimated at reaching $8 billion by 2005 [according to a report issued by the Florida Supreme Court (*see Statewide Grand Jury Report: Identity Theft in Florida, First Interim Report of the 16th Statewide Grand Jury, Case No.: SC 01-1095* (2002)].").

207. FTC, *Identity Theft Survey Report*, 2003, http://www.ftc.gov/os/2003/09/synovatereport.pdf [hereinafter *Identity Theft Survey*] (finding, in a report by Synovate that was commissioned by the FTC, that the loss to consumers from these 9.9 million cases of identity theft was estimated around five billion dollars).

208. *See* National Online Consumer Protection Association, *Identity Theft: Fact [sic] and Statistics*, http://www.nocpa.org/identitytheft/facts.html (last visited July 31, 2007) (citing a Gartner Research and Harris Interactive study on identity theft and claims that, as of July 2003, identity theft was occurring 19,178 times per day, 799 times per hour, and 13.3 times per minute).

209. *See, e.g.*, Jeff Sovern, *Stopping Identity Theft*, 38 J. CONSUMER AFF. 2, 233-43 (2004) (stating that "Identity theft . . . is a serious consumer problem."), Milne et al., *supra* note 201, at 217 (stating that "[I]dentity theft . . . is one of the fastest growing crimes in the United States and is increasingly affecting customers' online transactions.") (internal citations omitted); Milne, *supra* note 203, at 388 (citing *Stealing People is Wrong; White-Collar Crime; the Identity-Theft Industry*, Economist, Mar. 8, 2001, at 28-29 (stating that "identity theft . . . is one of the fastest-growing white-collar crimes in the United States.").

210. The identity thief would need only the victim's first and last name, physical address, and social security number in order to run a background check through a commercial data broker with such reports revealing even more PII such as the victim's: (1) employment information, (2) credit accounts listing creditor and account balances, (3) criminal record, and (4) motor vehicle record including driver's license number. *See, e.g.*, ChoicePoint: *ScreenNow: Combined Report*, http://www.employment.screennow.com/hdocs/sample_combined.html (last visited May 29, 2006). Names are easily obtainable either online or offline through dumpster diving or stealing of mail. Physical addresses are also easily obtained online through web sites such as www.secret-info.com where an individual's name and state of residence is enough information to locate address information. *See* Secret-Info.com, Property Ownership Information, http://www.secret-info.com/searchcosts.html (last visited May 29, 2006). Additionally, social security numbers may be obtained online through web sites such as www.secret-info.com (this site offers to "locate a social security number" for $20-45 if the seeker provides merely a name or address). Secret-info.com, *Locate a Social Security Number*, http://www.secret-info.com/searchcosts.html (last visited May 29, 2006). *See also Social Security Numbers are for Sale Online*, NEWSMAX.COM WIRES, Apr. 5, 2005, http://archive.newsmax.com/archives/articles/2005/4/4/155759.shtml (discussing the idea that social security numbers are still easily obtainable and relatively inexpensive to purchase even after the security breaches of such information at major commercial data brokers over the past few years); Milne et al., *supra* note 201, at 217 (stating that "[b]ecause of its ability to accumulate and

information, as well as the lax application standards in a world of instant credit and account approval.[211] Companies collecting PII substantially increase the amount of information available to identity thieves when they disseminate this information into cyberspace.[212] While credit card companies and other financial institutions bear most of the financial brunt from identity theft,[213] victimized consumers spend, on average, thirty hours "trying to resolve the consequences associated with the theft"[214] and some victims deal with fallout of a much more serious nature.[215]

---

disseminate vast amounts of information electronically, the Internet may make theft of personal or financial identity easier.").

211. In fact, customers resent having to show many forms of identification when applying for credit and companies, not wanting to lose the business, concede, and continue the application process making identity theft even easier. *See, e.g.*, Sovern, *supra* note 209, at 237.

212. Aside from the dissemination of PII through a company's back door, there are three other primary ways in which the PII of an online consumer may be obtained by identity thieves: (1) PII on consumers' personal computers is vulnerable to various e-threats and may be compromised, (2) the collection of PII by e-commerce companies may be compromised in transit, and (3) PII stored by companies after collection may be compromised by various e-threats. *See* Milne et al., *supra* note 201, at 219. *See infra* Part V.C (discussing a way to increase the accountability of businesses to people about whom they collect PII).

213. *See, e.g.*, Sovern, *supra* note 209, at 234 (stating that "lenders may suffer losses because they cannot recover the amounts loaned to thieves. The credit industry seems willing to absorb these losses, however, because of the benefits that flow from easily available credit.").

214. *See* Marla Royne Stafford, *Editorial Prelude: Identity Theft: Laws, Crimes, and Victims*, 38 J. CONSUMER AFF. 2, 202 (2004).

215. *See, e.g., Identity Theft Survey*, *supra* note 207. *See also* Milne, *supra* note 203, at 388 (stating that "reclaiming one's identity is a lengthy and costly experience."). The story of Stacy Sullivan reveals the travails of an identity theft victim. *See* Stacy Sullivan, *How I Lost My Good Name*, N.Y. TIMES, Apr. 17, 2000, at A-19. In 1996 a male identity thief utilized Sullivan's Social Security number to obtain phone service in her name in a city where she had never even visited and subsequently racked-up thousands of dollars in phone bills. *Id.* The bills went unpaid and the phone company sent the account to collections where the collection agency informed the three major credit bureaus of the delinquency. *Id.* The resulting negative credit history emerged in a credit check run on an apartment lease application and Sullivan was turned away. *Id.* Four years later, in 2000, the negative credit items still appeared in her credit report further hindering her efforts to rent an apartment. *Id.* (quoting Sullivan who subsequently stated that "[t]he most maddening aspect of all this is that it could have been prevented had the phone companies simply checked the identity of the person who established phone service in my name."). Other ways in which victims of identity theft are harmed include: "(1) having their privacy invaded, (2) suffering the psychological trauma of having their reputation ruined . . . and (4) undergoing tremendous transaction costs to restore their names." Milne, *supra* note 203, at 392. The FTC's identity theft online complaint form allows a victim to detail any problems with companies, credit bureaus, or organizations in remedying the problems caused by the theft. *See* FTC, ID Theft Complaint Input Form, *supra* note 205.

Identity theft was first criminalized in 1998 when Congress passed the Identity Theft and Assumption Deterrence Act (the ITADA).[216] This Act labels identity theft as a federal offense with a maximum sentence of fifteen years in addition to a potential fine of up to $250,000 and the "forfeiture . . . of [A]ny personal property used or intended to be used to commit the offense . . ."[217] for anyone who "knowingly transfers . . . or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet . . . any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law."[218] The ITADA also created a mandate for the FTC to become the primary clearinghouse for identity theft prevention in the United States.[219] More recently, in 2003, Congress passed the Fair and Accurate Credit Transactions Act (FACTA) at least partially designed to remedy identity theft as companies are required to truncate social security numbers and names of individuals, through a system of nationwide fraud alerts, granting a greater ability to detect identity theft and prevent some of its repercussions. Under the Fair Credit Reporting Act (FCRA),[220] individuals also may obtain a free annual credit report.[221]

---

216. 18 U.S.C. § 1028 (2000). *See also* Stafford, *supra* note 214, at 201 (discussing identity theft and pertinent regulations designed to hinder its effectiveness) and General Accounting Office, Identity Theft: Prevalence and Cost Appear to be Growing (2002).

217. 18 U.S.C. § 1028 (b)(5).

218. 18 U.S.C § 1028(a)(7). *See also* Hemphill, *supra* note 65, at 55. Hemphill states that the means of identification identified under this law can come in the form of a:

> [N]ame, Social Security number, date of birth, driver's license or other government issued identification number . . . employer or taxpayer identification number, biometric data, e.g., fingerprint, voice print, retina, or iris image, unique electronic identification number, address, or routing code, and telecommunication identifying information or access device.

Id.

219. *Id.*

220. 15 U.S.C. § 1681 (2000).

221. 15 U.S.C. § 1681(j)(a). The FCRA requires each of the three major credit reporting agencies to provide a free credit report—upon an individual's request—once during every twelve month period. *Id. See also What It's All About*, *supra* note 203, at 6 (On September 1, 2005, consumers nationwide were eligible to access this free report by accessing the web site http://www.annualcreditreport.com, by calling 1-877-322-8228, or by mailing in a request as the three major credit reporting agencies need not honor a request made directly to them). Some clever companies created their own domain names utilizing the free report concept to entice users to request a report that generally comes with strings attached—such as fee-based credit monitoring attached to the free report. *See* FTC, *Your Access to Free Credit Reports*, Sept. 2005, http://www.ftc.gov/bcp/conline/pubs/credit/freereports.htm. The danger of these imposter web sites as follows:

Consumers also may place fraud alerts in their credit report if they feel they are, or could become, the victim of an identity thief.[222] An initial alert is valid for ninety days while an extended alert exists on a credit report for seven years.[223] Any fraud alert requires a creditor to verify the identity of

---

> Only one web site is authorized to fill orders for the free annual credit report you are entitled to under law—*annualcreditreport.com.* Other web sites that claim to offer "free credit reports," "free credit scores," or "free credit monitoring" are not part of the legally mandated free annual credit report program. In some cases, the "free" product comes with strings attached. For example, some sites sign you up for a supposedly "free" service that converts to one you have to pay for after a trial period. If you don't cancel during the trial period, you may be unwittingly agreeing to let the company start charging fees to your credit card. Some "imposter" sites use terms like "free report" in their names; others have URLs that purposely misspell *annualcreditreport.com* in the hope that you will mistype the name of the official site. Some of these "imposter" sites direct you to other sites that try to sell you something or collect your personal information.

Id. A few states also allow access to free credit reports aside from the requirements of the FCRA. *See, e.g.*, COLO. REV. STAT. § 12-14.3-104(2)(e) (2006). The Colorado statute states that

> [e]ach consumer reporting agency shall, upon request of a consumer, provide the consumer with one disclosure copy of his or her file per year at no charge . . . If the consumer requests more than one disclosure copy of his or her file per year . . . the consumer reporting agency may charge the consumer up to eight dollars for each additional disclosure copy.

Id.; VT. STAT. ANN. tit. 9, § 2480b(c)(1) (2006) (stating that "[u]nder Vermont law, you are allowed to receive one free copy of your credit report every 12 months from each credit reporting agency."). A few other states have statutorily created a reduced price for obtaining a credit report. *See, e.g.*, MINN. STAT. § 13C.01(1)(a) (2006) (stating that "[a] consumer who is the subject of a consumer report maintained by a consumer reporting agency is entitled to request and receive by mail, for a charge not to exceed $3, a copy of the consumer report once in any 12-month period.").

222. 15 U.S.C. § 1681c-1 (stating that individuals with a "good faith" suspicion that they have been or are about "to become a victim of fraud or related crime, including identity theft" may request a fraud alert be placed in their credit file). According to the FTC, placing a fraud alert is appropriate, for instance, if a person has lost a wallet or purse or been fooled by a phishing or pretexting scam. *See What It's All About, supra* note 203, at 19. Placing this alert entitles an individual to one free credit report from each of the three major credit reporting agencies. *Id.*

223. 15 U.S.C. § 1681c-1(a)(1)(A) (providing for the ninety-day initial fraud alert). *See What It's All About, supra* note 203, at 19. In order to file an extended report, an individual must provide a credit reporting company with an "identity theft report" and this extended alert entitles the victim to two free credit reports per year from the three major credit reporting agencies. 15 U.S.C. § 1681c-1(b)(1) and (2) and *What It's All About, supra* note 203, at 19. An identity theft report may consist of two parts: (1) a copy of a filed police report and (2) additional information as requested by the credit reporting agency from which the fraud alert was requested. *Id.* at 20 (demonstrating that credit reporting agencies are entitled to make this request within 15 days of the alert request and fifteen additional days to complete the alert implementation). Additionally, the credit reporting agency initially receiving the fraud alert request must notify the other major agencies of such

the person requesting the credit before issuance.[224] Finally, consumer reporting agencies are required to block the transmission of credit information that a consumer identifies as "information that resulted from an alleged identity theft[.]"[225] Willful noncompliance with the FCRA can lead to civil penalties in favor of the injured consumer of up to $1,000, any punitive damages "as the court may allow" and, potentially, attorney fees.[226]

These laws are not working as initially planned as identity thieves are hard to catch and nationwide fraud alerts are not necessarily stopping thieves from accessing PII—even PII under a fraud alert![227] In fact, current law does not allow consumers to sue a credit reporting agency for reporting false information unless the agency acted negligently—a situation that is difficult when the agency is accurately reporting the negative credit information caused by identity thieves.[228] However, this negative information will make the clean-up and move-on processes much

---

request. 15 U.S.C. § 1681c-1(a)(1)(B). An "active duty alert" is a special kind of fraud alert existing for twelve months and is designed to protect the identity of troops currently serving in the U.S. military. 15 U.S.C. § 1681c-1(c). Interestingly, a reseller of a credit report is also required to include the fraud alert in the transaction. 15 U.S.C. § 1681c-1(f).

224. 15 U.S.C. § 1681c-1(h). Potential credit issuers must not issue credit to a consumer with a ninety-day fraud alert unless the issuer "utilizes reasonable policies and procedures to form a reasonable belief that the [issuer] knows the identity of the person making the request." 15 U.S.C. § 1681c-1(h)(1)(B)(i). If a consumer has an extended fraud alert, a potential issuer of credit must contact the consumer in person "to confirm that the application for a new credit plan . . . is not the result of identity theft." *Id.* § 1681c-1(h)(2). *See also What It's All About, supra* note 203, at 19 (stating that "[a]s part of this verification process, the business may try to contact [the person under whose name the credit is being requested] directly. This may cause some delays [to the process].").

225. 15 U.S.C. § 1681c-2 (this block must occur "not later than 4 business days after the date" the agency receives: (1) appropriate proof of the consumer's identity, (2) a copy of the identity theft report, (3) the identification of the fraudulent information by the consumer, and (4) "a statement by the consumer that the information is not information relating to any [legitimate] transaction by the consumer.").

226. 15 U.S.C. § 1681n (Additionally any "person who obtains a consumer report from a consumer reporting agency under false pretenses or knowingly without a permissible purpose shall be liable to the consumer reporting agency for actual damages" up to $1,000). Negligent violations of the FCRA may result in actual damages being paid to the consumer-victim. 15 U.S.C. § 1681o. The knowing and willing obtaining of PII on a consumer from a credit reporting agency under false pretenses can be fined and imprisoned for up to two years. 15 U.S.C. § 1681q. Knowing and willful unauthorized disclosures of consumer PII by a credit reporting agency employee or officer can also lead to a fine and up to two years imprisonment. 15 U.S.C. § 1681r.

227. *See, e.g.*, Sovern, *supra* note 209, at 233 (stating that "[c]onsumers complain that even after they place fraud alerts in their credit files, identity thieves are still able to borrow in their names.").

228. *See id.* at 234 (discussing this negligence standard and comparing it with other legal standards in offline cases of impersonation such as forged checks).

more difficult as injured consumers attempt to open new accounts and lines of credit.[229]

2. Spam

Spam is:

> Electronic junk mail or junk newsgroup postings. Some people define spam even more generally as any unsolicited e-mail. However, if a long-lost brother finds your e-mail address and sends you a message, this could hardly be called spam, even though it's unsolicited. Real spam is generally e-mail advertising for some product sent to a mailing list or newsgroup.[230]

---

229. Evidence suggests that companies dealing with consumers alleging identity theft are often non-responsive. *See id.* at 235 (citing congressional hearings at which identity theft victims detailed accounts of their treatment by companies—particularly lenders and credit reporting agencies—while trying to reclaim their identities). *See also Identity Theft: How to Protect and Restore Your Good Name: Hearing Before the Senate Comm. on the Judiciary, Subcomm. on Technology, Terrorism, and Gov't Info.*, 106th Cong. (2000) (statement of Michelle Brown); *Identity Theft: Hearing Before the House Comm. on Banking and Fin. Services*, 106th Cong. (2000) (statement of Shon Boulden). Credit reporting agencies have little incentive to be responsive to identity theft victims because such agencies are not in business to buy or sell from these individuals and have little financial incentive to help. Sovern, *supra* note 209, at 235. Sovern states that:

> Credit bureaus do not appear to suffer any losses when identity thefts occur . . . Moreover, credit bureaus need not fear losing business if they alienate consumers because credit bureaus typically do not engage in transactions directly with consumers beyond supplying consumers with their own credit reports or credit monitoring services—products that victims of identity theft are likely to buy no matter how angry they may be at credit bureaus. Accordingly, the only incentive credit reporting agencies have to prevent identity theft is altruism, and that appears not to be a sufficient motivation.

Id. Lenders also possess little incentive to notify a credit agency that a recent default was the result of identity theft and not a result of the person identified in the report. *Id.* at 236.

> In contrast to credit bureaus, lenders incur losses because of identity theft. They may provide goods and services for which they are not paid. . . . But, because [a lender has already suffered a loss at the time it would inform the credit agency of the identity theft] the lender has little to gain by [such reporting]. . . . Consequently, like credit reporting agencies, lenders have a chance to reduce the damages suffered by consumer-victims of identity theft at a time when their chief motivation for doing so is altruism.

Id. (internal citations omitted)).

230. Webopedia.com, *Spam*, http://www.webopedia.com/TERM/s/spam.html (last visited July 31, 2007). Spam is no longer made up of merely text messages; today's spam is increasingly made

Spam is one of the oldest e-threats and today, forty percent of all e-mail sent can be classified as spam.[231] Once a spammer locates a working e-mail address, topics as diverse as pornography and real estate may be sent to millions of people instantaneously, and at a cost much reduced from other forms of direct marketing, via the click of a mouse.[232] Some spam is sent when hackers break into a computer and utilize PII stored within to send spam without the knowledge of the computer's owner; this process turns the computer into a "zombie" machine under the hacker's control.[233] It also is possible for spammers to send spam messages to e-mail addresses purchased from data brokers.[234]

Spam devotes resources from more productive tasks—such as working—as the recipient spends time eliminating the unsolicited e-mails and cleaning-up the computer system.[235] Even more threatening is the fact

---

up of pictures as well as text in an attempt to bypass spam filters and to encourage people to interact with the message. *See* Jon Swartz, *Picture This: A Sneakier Kind of Spam.*, USA TODAY, July 24, 2006, at A-1 (stating that "[i]mage-based spam [now] accounts for 21% of all spam, almost double what it was at the start of [2006][.]").

231. Don Evett, *Spam Filter Review: Spam Statistics 2006*, TOPTENREVIEWS.COM, http://spam-filter-review.toptenreviews.com/spam-statistics.html (last visited July 31, 2007) (claiming that 12.4 billion e-mails sent per day can be classified as spam and the average person receives 2,200 spam e-mail messages per year). Interestingly, the United States also leads the world as the country relaying the most spam and is the "source of 23.2 per cent of the world's spam." *U.S. Heads Spam List,* ADVERTISER (Australia), July 29, 2006, at 96 (stating that China and South Korea are the two countries that most closely trail the United States in the relaying of spam). Some studies from 2004 show that spam represented 65% of all e-mail. *See* Saul Hansell, *Junk E-Mail and Fraud are Focus of Crackdown*, N.Y. TIMES, Aug. 25, 2004, at C-1.

232. *See* Alex Mindlin, *Seems Somebody is Clicking on that Spam*, N.Y. TIMES, July 3, 2006, at C-3 (stating that spam messages on the subject of pornography are the most successful in getting recipients to click on them followed by pharmacy drugs and then Rolex watches). "Spam is made possible by the architecture of email, which, while intended to make email free and accessible, has also created a structure of costs such that there is little difference between sending a thousand emails or one hundred million." Rebecca Bolin, Note: *Opting Out of Spam: A Domain Level Do-Not-Spam Registry*, 24 YALE L. & POL'Y REV. 399, 400 (2006).

233. *See Spam Poses Threat to Privacy*, BBC NEWS WORLD EDITION, Oct. 16, 2002, http://news.bbc.co.uk/2/hi/technology/2330823.stm (discussing the idea of a "zombie" computer and the idea that most of the world's spam is relayed in this fashion).

234. *See, e.g.*, Rick Whiting, Data Brokers Draw Increased Scrutiny, InformationWeek.com (July 10, 2006) (stating that "Some data brokers are getting the message that changes are needed. ChoicePoint last year brought a spotlight to the industry's practices when it revealed it had previously sold information on 145,000 consumers to identity thieves posing as a legitimate business."), www.informationweek.com/management/showArticle.jhtml?articleID=190301136&pgno=2&queryText.

235. *See id.* (claiming that 10% of the typical workday is spent dealing with spam e-mails and that this time has the obvious impact of decreasing business productivity). "While spam has been a nuisance since the earliest days of electronic mail, in recent years it has become a mission-critical problem that can take down entire companies' mail servers, spread viruses, compromise systems,

that spam e-mails may contain viruses that may harm a computer and completely destroy a hard drive.[236]

For the purposes of this Article, the most privacy-intrusive aspect of spam occurs when recipients respond to the messages and enter PII.[237] The process works as follows: companies employ sophisticated software—called spam bots—that surf the Web and "harvest"[238] e-mail addresses. These companies then sell such PII to spammers and other interested parties who send the spam to each of the e-mail addresses.[239] Such messages request that the recipient enter PII in order to receive more information or to purchase the product in question—which may or may not exist in reality. Once this information is received by the spammer, it is used to commit identity theft or sold on the open market for a quick profit. This tactic is similar to the e-threat of phishing where e-mails which appear authentic collect PII for improper purposes. The primary difference is that phishing e-mails are designed to appear as if they came from an account already created while spam e-mails are designed to entice you to learn more about or purchase a product or service.[240]

An example of a serious spam attack occurred when a company in Texas sent out over 25 million unsolicited e-mails per day offering mortgage refinancing, extensions of automobile warranties, health

---

and overwhelm frustrated users." Bolin, *supra* note 232, at 400. *See also* Vivek Arora, Note: *The CAN-SPAM Act: An Inadequate Attempt to Deal with a Growing Problem*, 39 COLUM. J.L. & SOC. PROBS. 299, 300 (stating that "Spam is a nuisance for e-mail users because it clogs up e-mail inboxes, imposes costs on Internet servers that run e-mail programs, and invades people's privacy.").

236. *See* Damien Henderson, *Scottish Hacker Among Three Arrested after Virus Sent in Spam E-Mails*, HERALD (Glasgow) June 28, 2006, at 3 (discussing the arrest of a hacker "alleged to be part of an international criminal gang that has infected thousands of computers worldwide with viruses."). Hackers such as these often place viruses on computers in an attempt to gain control and "target valuable personal data such as credit card and bank details." *Id.*

237. *See, e.g.*, *Hefty Fine on Spammers Serves as a Fair Warning*, SAN ANTONIO EXPRESS NEWS, June 9, 2006, at B-6 [hereinafter *Hefty Fine*] (discussing a lawsuit by the Texas Attorney General against three companies—Leadplex, Payperaction, and Eastmark Technology, Ltd.—under the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act), the Texas Electronic Mail Solicitation Act and the Texas Deceptive Trade Practices Act for sending millions of spam messages and the subsequent $10 million judgment issued by a federal court).

238. Harvesting is the scanning of the Internet for public e-mail addresses. *See* Bolin, *supra*, note 232, at 419 (discussing that harvesting is not prohibited by CAN-SPAM, although the use of a harvested address in connection with a CAN-SPAM violation may lead to harsher penalties).

239. *See id.* at 419 (stating that spam bot programs "quickly run through webpages looking for email addresses to harvest. Collectors then sell the addresses to spamming operations.").

240. *See, e.g.*, SonicWall.com, Anti-Phishing Protection (discussing the differences between phishing and spam), http://www.sonicwallproducts.com/emea/796.html (last visited Dec. 18, 2007).

insurance and burglar alarm installation.[241] In all, the "spam was sent out under 250 assumed names and set up with misleading [and individually tailored] subject lines to give recipients the false impression the e-mails contained information important to them."[242] When the recipients responded to the spam messages, they entered PII, which was then sold on the open market despite the fact that the messages promised privacy.[243]

Today, a federal law, the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM),[244] governs some senders of spam by requiring all sexually-oriented unsolicited commercial e-mails to be labeled, include the sender's physical address[245] and include a way for the recipient to opt-out.[246] Because the CAN-SPAM was intended to create a national standard governing spam, the law preempts all state laws that require labels on unsolicited commercial e-mails or prohibit such e-mails entirely.[247] Time has shown that this pre-emption has many loopholes and most state spam laws have not been preempted.[248] The FTC,[249] state attorneys general[250] as well as Internet Service Providers,[251] can all enforce CAN-SPAM's provisions.

---

241. *See Hefty Fine*, *supra* note 237 (stating that, before the judgment, the company charged was believed to have been the fourth largest spam producer in the world).

242. *See id.*

243. *See id. See also* L.A. Lorek, *Former Spam King Seen as Good Kid Gone Astray*, SAN ANTONIO EXPRESS NEWS, June 11, 2006, at A-1 (stating that the spammers would sell particular pieces of PII for up to $28 each); *Spam King Hit for $13m*, AUSTRALIAN (Australia), June 13, 2006, at 5 (discussing the same case and stating that one of the "repentant" defendants recently created an Internet security company that provides protection against spam messages).

244. 15 U.S.C. § 7701 (2003).

245. 15 U.S.C. § 7704(a)(5) (2003).

246. 15 U.S.C. § 7704(a)(5) (2003). Effective on January 1, 2004, CAN-SPAM also prohibits deceptive subject lines and provides for jail terms of up to five years. 15 U.S.C. § 7704(a)(2) (discussing deceptive subject headers).

247. 15 U.S.C. § 7707(b)(1). CAN-SPAM

> supersedes any statute, regulation, or rule of a State or political subdivision of a State that expressly regulates the use of electronic mail to send commercial messages, except to the extent that any such statute, regulation, or rule prohibits falsity or deception in any portion of a commercial electronic mail message or information attached thereto.

Id.

248. *See also* Bolin, *supra* note 232, at 421-22 (stating that "Congress assessed the preemption as 'minimal' since CAN-SPAM does not preempt most of the laws previously used against spammers. In particular, its preemption excludes laws related to 'fraud or computer crime,' which many states now have. In other words, most state spam laws are still in effect.").

249. 15 U.S.C. § 7706(d) (2003).

250. 15 U.S.C. § 7706(f) (2003).

251. 15 U.S.C. § 7706(g) (2003).

In addition to the CAN-SPAM, at least thirty-eight states have some form of anti-spam legislation.[252] While some state laws are being upheld, others are being invalidated as governing interstate activity rather than purely intrastate activity.[253] Maryland's Commercial Electronic Mail Act (MCEMA)—allowing private rights of action when receiving e-mails containing false information—was struck down by a Maryland appeals court while similar laws were upheld by California and Washington state courts.[254]

C. *U.S. Law Operating at the Back Door*

Because the e-threats located at a company's back door pose the most serious risks to an individual's privacy, the law proposed in this Article must contain a stand-alone section that poses strict requirements for data dissemination. Differing from the sections covering e-threats at the front door and inside the company—both structured as regulatory ceilings—this

252. *See, e.g.*, ALASKA STAT. § 45.50.479 (2003) (requiring a label at the beginning of the subject line of any unsolicited commercial e-mail if the sender knows that the recipient is a resident of Alaska); ARIZ. REV. STAT. § 44-1372.01 (2003) (prohibiting false routing information and requiring a subject line label and an opt-out provision); ARK. CODE ANN. § 4-88-601~§ 4-88-603 (2003) (stating that all commercial and sexually explicit e-mails must contain a functioning reply e-mail address and instructions to opt out, while all unsolicited commercial and sexually explicit e-mails must include the sender's name, physical address and domain name); CAL. BUS. & PROF. CODE § 17529) (West 2003) (making it illegal to send unsolicited commercial e-mail from California or to a California e-mail address); Colorado Junk Email Law, COLO. REV. STAT. ANN. 6-2.5-101–103 (2003) (prohibiting, *inter alia*, unsolicited commercial e-mails to be sent from a third party's domain name or Internet address without permission); GA. CODE ANN. § 16-9-101 (2005) (prohibiting, *inter alia*, the sending of unsolicited commercial e-mail with false or misleading headers or that falsely represents that it is a solicited e-mail); MINN. STAT. ANN. § 325F.694 (2002) (expiring automatically when the federal CANSPAM Act became effective); NEV. REV. STAT. § 41.730 (1997 as amended in 2003) (enacting America's first anti-spam legislation and prohibiting, *inter alia*, the sending of unsolicited commercial e-mail unless it is labeled "ADV" or "ADVERTISEMENT" at the beginning of the subject line); TEX. BUS. & COM. CODE ANN. §§ 46.003-004 (2003) (requiring, *inter alia*, that all unsolicited commercial e-mail messages contain a functioning e-mail address for opt-out requests and that opt-out requests be honored).

253. *See, e.g.*, *Judge Overturns Law Against Junk E-Mail*, ST. PETERSBURG TIMES, Dec. 15, 2004, at A-4 [hereinafter *Junk E-Mail*] (discussing the invalidation of Maryland's 2002 Commercial Electronic Mail Act).

254. MO. CODE ANN., COM. LAW § 14-3002 (2006) (prohibiting the sending of unsolicited commercial e-mails containing false or misleading information about the sender, in the transmission path or in the subject line when such e-mail was sent either from a computer located within Maryland or to an e-mail address that the sender knew or should have known belonged to a Maryland resident). *See Junk E-Mail*, *supra* note 253 (discussing the decisions of a California appeals court and the Washington State Supreme Court). *See also* Washington v. Heckel, 24 P.3d 404, 405-05, 413 (Wash. 2001) (upholding the Washington anti-spam legislation against a dormant commerce clause attack).

section must be designated expressly as a regulatory floor. Regulatory floors are placed in legislation to set a minimum standard below which state laws regulating the same area cannot fall.[255] For instance, a federal law drafted as a regulatory floor, which defined spam as "any unsolicited commercial e-mail message sent to any individual," would prohibit a state from passing legislation defining spam merely as "any unsolicited commercial e-mail message dealing with the subject of pornography and sent to any individual." In this example, the regulatory floor would render the state law void because the provisions of the state are less strict than the federal provision's broader definition of spam (it falls below the regulatory floor).

On the other hand, regulatory floors allow states to draft regulations that are stricter than the federal law at issue. This attribute allows states to become players in regulating certain areas of interest to their residents. Tougher regulations also can be beneficial when states—possessing a better understanding of the local conditions, customs and feelings of their residents than Congress—effectively experiment with different regulatory formulas. Former U.S. Supreme Court Justice Louis D. Brandeis explained this concept eloquently when he stated: "[I]t is one of the happy incidents of the federal system that a single courageous state may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country."[256]

Although regulatory floors are commonly thought of as privacy-enhancing attributes of federal legislation, the downside, from a business perspective, revolves around two related issues: (1) the expense and other efforts surrounding compliance with as many as fifty-one[257] differing state regulations (and potentially many, many more local city and town regulations)[258] and (2) the ability of the state with the strictest regulations

255. *See* Daniel Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357, 381 (2006) (referring to the concept as "floor preemption" and stating that such preemption allows states "to innovate more comprehensive protections for individual rights.").

256. New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting). Keep in mind that this type of state experimentation is not permitted under regulatory ceilings, however, as states are banned from passing regulations that are stricter than the federal law at issue. *See* discussion, *supra* Parts III.C & IV.C.

257. The laws of Washington D.C. should be considered in this calculation as they are similar to state laws governing residents of the fifty states.

258. *See, e.g.*, Charity Scott, *Is Too Much Privacy Bad for Your Health? An Introduction to the Law, Ethics, and HIPAA Rule on Medical Privacy*, 17 GA. ST. U.L. REV. 481, 514 (2000) (referring to critics' arguments by stating that "being subjected to fifty states' extensive and inconsistent laws on privacy is costly and impractical."). The fifty-one differing regulations could come from fifty different state laws in addition to the federal law setting the regulatory floor in the first place.

to set a de facto national standard. For instance, assume that California becomes the first state in the nation to ban any company doing business with California residents from disseminating any PII to any third party, including a company's subsidiaries. With this strict privacy law on the books in California, it is possible that companies incorporated across the country, but that conduct business in California, may choose to comply with California's law on a national scale and cease their PII dissemination practices completely. This might cause them to cease any efforts to disseminate any PII in such a way that it is protected from back door e-threats (i.e., dissemination with restrictions of future use and subsequent dissemination). If this occurs, California legislators (elected only by California residents) have created a de facto national standard which businesses across the county feel compelled to comply with and which residents across the country (who did not vote for these legislators) are forced to deal with. While these consequences proved too burdensome during the PII-collection and utilization stages, they become a bit more acceptable at the back door stage where dissemination can cause tremendous damage.

The three back door e-threats described above initially stem from a company's dissemination of PII into cyberspace. For instance, back door pretexting would be ineffective if a company representative could sniff out the scam or refuse to give any PII over the phone without proper verification. Identity thieves would be frustrated if companies restricted access to the PII that they sell because less and less personal information would be for sale on the open market or merely floating around in cyberspace. Finally, spammers would need to find a different source of their e-mail addresses if companies better protected the PII they collect and store from their customers. With the source of many of these problems in the open, the third section of the proposed law singles out dissemination as its focus and forces companies to more carefully consider their dissemination practices.[259] Requiring businesses to be more careful with the PII they collect will be much more effective than trying to stop identity thieves and spammers located across the globe through the IDTDA and the CAN-SPAM. Even better, these practices can drastically reduce the instances of identity theft and spam without the identity thief and the spammer having any say in the matter—they will find themselves cut off from a major source of their information.

This section of the proposed law will require companies to consider the parties it commonly sells PII to and then make an educated decision as to which options concerning future dissemination of the PII it will provide to

259. *See, e.g.*, Bolin, *supra* note 232, at 419 (stating that "CAN-SPAM has made great progress toward actually suing and collecting damages from the worst spammers.").

the purchaser. More specifically, under its provisions, this section will require companies disseminating PII to unrelated parties to: (1) accurately describe any dissemination practices and restrictions on subsequent dissemination in its privacy policy, (2) attach its name to each piece of PII it disseminates for a secondary use (PII tagging) and (3) verify that the purchaser of any PII is a legitimate person or entity (legitimacy verification) and then place a responsibility on the seeker of the information to verify that it is being used for a proper purpose.

1. Privacy Policy Disclosure

Recall that the first section of the proposed law required all companies collecting, utilizing, storing, or disseminating PII in interstate commerce to post a standardized and readable e-commerce privacy policy.[260] As part of the required disclosure in such policies, companies will be forced to specifically discuss their policies concerning PII dissemination, if any.[261] If a company does sell or otherwise disseminate any PII to any party, this section of the privacy policy requires a statement as to: how the PII is disseminated, who receives the PII and for what consideration (in general terms) and, finally, any restrictions that the company places on subsequent sales and uses of the information. Because this proposed law requires privacy policies to be more readable and to be conspicuously linked to/located on homepages, customers will be more likely to read the dissemination section of the policy and determine whether they wish to continue on and submit PII. The idea is that: (1) better educated web site visitors will cause companies to carefully consider whether selling such data will lead to a loss of customers during the other two stages of the PII processing cycle, and (2) a requirement to disclose dissemination practices will cause companies to be more careful with the PII they collect.

2. PII Tagging

In addition to accurate disclosure in a company's privacy policy, the proposed law will require that every piece of PII disseminated to an unrelated third party be electronically associated—or tagged—with the seller's name. This identification tag must then be inputted into the purchaser's database and must remain associated with the PII for the entire time it is stored in the system. Upon any subsequent resale to another purchaser, the tag must be updated with the new seller's information to be

260. *See* discussion, *supra* Part III.C.

261. It is important to remember that companies will not be required to implement any particular PII dissemination policy, only to accurately disclose the actual policy they put in place. *See* discussion, *supra* Part III.C.

posted alongside the prior seller's information. This updated tag will then be stored in the second purchaser's database and updated in a similar fashion if ever resold.

For example, assume that Wells Fargo Home Mortgage (Wells Fargo) collects my home phone number in my loan application and later sells this PII to an unrelated mortgage insurance company such as Genworth Financial (Genworth). Further assume that Genworth calls me at home and attempts to sell me mortgage insurance. If this occurs, the caller from Genworth must state to me before proceeding with the pitch that my phone number was obtained from Wells Fargo. If Genworth then resells the same information to a local landscaping company, the landscaper must identify that it received my information from both Wells Fargo and Genworth.

Recipients of solicitations—whether via e-mail, postal mail or telephone—finally will be informed fully as to which party disseminated their PII and finally will be able to express their thoughts on this dissemination directly to the seller.[262] These thoughts may come in the form of a "thank you" for passing on the information to a desired service provider or in the form of a "how dare you" sell the information I disclosed to you. At the end of the day, this regulation will surely add an expense to the sale and secondary use of PII in the form of database configuration, updating, and organization. However, this added expense should help decrease the amount of PII floating in cyberspace vulnerable to a back door e-threat when companies uninterested in experiencing customer resentment from the sale of the PII choose limit their dissemination practices. Additionally, some companies will be able to frame the disseminations in a positive light such as on a flyer, delivered via regular mail, stating: "Your mortgage provider, Wells Fargo, thought you would appreciate this information about private mortgage insurance."

3. Legitimacy Verification

The final piece of the proposed law's back-door section will: (1) ban any company or individual to attempt to acquire PII from any business or individual via the utilization of a fraudulent identity, (2) require companies that disseminate PII to verify the identity of each recipient, and (3) require the recipient of such information to verify that the information is being requested for a legal purpose. In other words, any PII-disseminator covered by the proposed law must make an affirmative declaration that each purchaser of the information is actually the entity it claims to be (a "legitimate purchaser"). This declaration must be memorialized on some

262. This provision would not affect public information or situations where customers affirmatively consent—opt-in—to the secondary use of their PII.

type of PII Dissemination Verification Form, signed by an authorized corporate officer and retained for a period of five years. In addition, the recipient of any PII from a covered company must make a written declaration that the information is being requested for a legal purpose. This declaration must be made on some type of PII Receipt Verification Form, signed by an officer of the company or by any private individual receiving the information and kept on file for five years.

These requirements may not completely stop the back door e-threats, but it will make both disseminators and requestors of personal information take more time to determine whether releasing or obtaining the information is a business risk worth taking. For example, if the investigation company involved in the Amy Boyer case had been legally required to dig a little deeper into the reasons behind its client's request for Ms. Boyer's employment address, it is doubtful that the company would have provided such information to its client. Additionally, because this section of the proposed law makes back door pretexting illegal, the investigation company would have been deterred from deceiving Boyer into providing the information while pretending to be from her credit card company.

Logistically, this provision need not be excessively burdensome. Loyal to its principles of minimal intrusion into business decisions, the law will not specify the manner in which companies conduct verifications. In fact, companies remain free to experiment with verification techniques to determine which are the most effective—both from a compliance and cost perspective. The most cost effective way to determine legitimacy would likely occur via a webpage dedicated solely to PII requests. On this page, all requests would be submitted through an electronic form that can be instantaneously organized and then funneled through a company representative charged with verification matters. This representative must be satisfied that the requestor is part of the organization represented on the submittal form before any PII is transferred. Another option could be a facsimile request funneled through the same service representative. A low cost option that would not pass muster, however, would be the releasing of PII via a telephone request and a verbal confirmation by the requestor that she is who she claims to be.[263]

Again, if this provision was on the books when the ChoicePoint data security breach occurred, the fraud may have been caught as ChoicePoint would have been legally incentivized to investigate the background of the data requesters. This investigation should have led to the discovery that the

263. A telephone request could be honored if the service representative took the request, independently verified legitimacy, and then disseminated the PII. Here, the independent verification is the key.

requestors were illegitimate and to the extinguishment of the data transfer.[264] Although this requirement is more burdensome than the self-regulatory requirements in effect today, it is not overly burdensome and the benefits of preventing further ChoicePointesque scandals are well worth the cost.

VI. CONCLUSION

The twenty-first-century e-commerce environment can be a scary place. Hidden within its boundaries are technologically-sophisticated e-threats designed to compromise PII. These threats are lying in wait for inexperienced web-surfers and actively implemented by experienced e-thieves. At the same time, individuals continue to submit vast amounts of information into cyberspace without truly understanding these lurking dangers while, at the same time, businesses stumble to protect the information they collect. The Privacy Matrix is a conceptual model designed to identify the most prominent location of each major e-threat at the three different stages of the PII processing cycle. Categorizing such e-threats into these three stages—the front door, inside the company, and the back door—helps policy makers analyze which regulatory weapons, if any, will most effectively combat each threat while simultaneously minimizing the burden of such regulations on e-commerce efficiency.

The Privacy Matrix is helpful at this point in time because the U.S. legal system—currently a mixture of industry self-regulation and a patchwork of federal and state legislation—has proven itself unequipped to deal with these e-threats effectively. The Matrix demonstrates that a new federal law, with sliding-scale regulations specifically tailored to each stage of the PII processing cycle, can serve as a privacy-enhancing first-step in removing some of the bite from these e-threats. This legislation should serve as a regulatory ceiling at both the front door and inside the company stages and as a regulatory floor at the back door stage. The structure of this regulation will create an environment where individuals remain primarily liable for decisions concerning their PII when such information is within their control. This responsibility will shift to the businesses that collect PII once control of the information has shifted. Another benefit of the proposed legislation is that, during the early stages of the PII processing cycle, e-commerce companies will be governed by

264. As discussed previously, this provision will also help drive down the occurrences of pretexting. Because data sellers would be required to verify the identity of the requestor, a pretexter pretending to be someone else or someone from a company they are not associated with will have a more difficult time tricking a corporate representative into releasing personal information.

one federal statute—requiring a standardized privacy policy, security breach notification and conspicuous disclosure—and will not be forced to comply with widely-differing state laws or with a de-facto national standard determined by a legislative body elected by the citizens of a state. Later in the cycle, once PII is completely outside of the control of the person it identifies, a statutory floor will allow states to experiment with creative solutions—such as PII tagging technology and legitimacy verification—designed to prevent potentially dangerous dissemination of PII through a company's back door.

EXHIBIT 2—*Sample Compliant Multilayered Electronic Privacy Policy: Layer One*[265]

OUR PRIVACY POLICY

TYPES OF PERSONAL INFORMATION COLLECTED:

- Active Collection: We may collect your name and email address in return for website access.
- Passive Collection: We collect information regarding your visit, including your browser type, once you enter to determine the popularity of our website and the number of visitors.

PERSONAL INFORMATION USES:

- We may use your information internally to process a transaction you initiate with us.
- We may give your information to our partners to process a transaction you initiate with us.
- We may use your information for internal purposes unrelated to any transaction.
- Your information will not be aggregated with data we collect from other visitors.
- We may sell your information to unrelated companies to market worthwhile services to you.
- We will not sell your information to anyone in the event of our bankruptcy.

YOUR CONSENT OPTIONS:

- Once you submit your information to us through our website we may use it for any of the purposes mentioned above without first obtaining your consent.
- You do not have the choice of opting-out, or requesting that we do not use your information, for of any of the purposes mentioned above once you submit it to us.

PERSONAL INFORMATION SECURITY:

- Collection Security: All information you submit is collected through an unencrypted form.
- Transmission Security: All information you submit to us is encrypted during transmission.
- Storage Security: Your information is not encrypted once transmitted to us but is stored in a password-protected database that is continuously monitored by our trained staff.

ACCESSING/CHANGING/REMOVING PERSONAL INFORMATION:

- You cannot access any information you submit to us once submitted.
- You may request that we change/remove any information you submit to us by clicking **here**.

PRIVACY POLICY CHANGES:

- We may change our policy any time.
- We will email you and post all changes online when this happens.

OTHER IMPORTANT INFORMATION:

- View our complete privacy policy **here**.
- We belong to TRUSTe and BBB*Online*.
- We abide by the US/EU Safe Harbor.

Questions/comments about your privacy – Please click **here** and we will respond within 24 hours.

EFFECTIVE DATE: MARCH 30, 2005

265. *See* Corey Ciocchetti, *E-Commerce and Information Privacy: Privacy Policies as Personal Information Protectors*, 44 AM. BUS. L.J. 55, 102 (2007).

EXHIBIT 3—*Sample Compliant Multilayered Electronic Privacy Policy: Layer Two*[266]

OUR PRIVACY POLICY

We collect your information to market to you and to service your account.

You may tell us not to do so.

View our complete privacy policy by calling (800) 555-5555 or at www.ourcompany.com.

266. *Id.* at 103.