Vanderbilt Journal of Entertainment & Technology Law

Volume 10
Issue 3 *Issue 3 - Spring 2008*

Article 6

2008

Just Click Submit: The Collection, Dissemination, and Tagging of Personally Identifying Information

Corey Ciocchetti

Just Click Submit: The Collection, Dissemination, and Tagging of Personally Identifying Information

*Corey Ciocchetti**

ABSTRACT

As the twenty-first century bustles forward, the e-commerce arena becomes an ever more dangerous place. On a daily basis, Web sites collect vast amounts of personally identifying information (PII) and mine it in sophisticated databases to discover consumer trends and desires. This process provides many benefits—such as tailored Web sites and relevant marketing—that few Web surfers would care to do without. However, serious threats lurk in cyberspace and are enhanced by consumers who continue to submit vast amounts of information in a state of relative unawareness. Not wanting to miss out on their Web surfing experience, visitors submit their personal information without glancing at a company's privacy policy. In 2008, for example, 100% of the most highly trafficked Web sites in the United States collect PII while just over sixty percent have privacy polices that clearly explain PII practices. Instead of offering explanations, e-commerce companies obfuscate and exacerbate the serious threats surrounding PII collection and dissemination. This occurs most often via inconspicuously posted privacy policies written in small font and filled with legalese and loopholes. The United States legal system allows such obfuscation unless a company breaks a privacy promise.

This article argues for a federal PII tagging law where companies face a choice, and must either: (1) post a clear and

* Assistant Professor, Business Ethics and Legal Studies, Daniels College of Business, University of Denver, Denver, Colorado. J.D., Duke University School of Law, 2002; M.A., Religious Studies, University of Denver, 1998; B.S.B.A., Finance, University of Denver, 1997; B.A., Economics, University of Denver, 1997. Professor Ciocchetti would like to thank his wife Jillian for her consistent support of his academic endeavors.

conspicuous privacy policy drafted in plain English; or (2) associate (tag) their name to each piece of data they disseminate. Over time, consumers will tire of solicitations beginning with the required phrase "Hi, I represent company X *and we purchased your telephone number, etc. from company* Y.*" Such social pressure will lead companies to take the simple and nearly costless step of drafting and posting better privacy policies. At the end of the day, tagging legislation represents a middle-ground solution that protects PII without excessively hindering e-commerce efficiency.*

TABLE OF CONTENTS

> [Psychological profiles] can be deduced from data mining any available information such as public records, behavior records, consumer activities, shopping habits, memberships in various organizations & clubs, court records, demographic data, internet search, property deeds, media, publicly available databases, blogs, social networking services, wikis, newsgroups, opinions, comments, words, voice, pictures, videos[,] . . . body language, forums, message boards including other methods such as statistical comparisons with peer groups, polling and information submitted by searcher, friends, co-workers, relatives.
>
> - Akiba.com[1]

Do you ever wonder whether a colleague, neighbor, or department chair has a shady past? Are you curious as to whom your significant other calls, text messages, or e-mails throughout the day? Have you found yourself in awe of the ability of telemarketers and

1. Psychological Profiles, http://www.abika.com/Reports/Samples/Psychologicalprofile.htm (last visited Apr. 4, 2008).

spammers to bombard your telephone and e-mail accounts with personalized messages offering mortgage refinancing options, Viagra, and hot stock tips? Do you realize that you are potentially contributing to your electronic, downloadable, psychological profile every time you surf the Web? These questions represent vastly different scenarios but have a common denominator linking them together—the ability of anyone, anywhere in the world, to obtain and analyze vast amounts of your personally identifying information (PII) that is available and up-for-sale in cyberspace.

In fact, anyone with a credit card and a novice understanding of the Internet can purchase bits and pieces of personal information and, in the process, learn a great deal about someone they desire to befriend, employ, or investigate. This scavenger hunt often results in the disclosure of some sensitive aspects of the target's personal and professional life. For instance, $100 and a name, address, and mobile phone number will allow you to track and obtain the cellular phone records of your significant other.[2] Another $180 will allow you to determine the psychological/behavioral profile of your next-door neighbor, supervisor, or department chair.[3] If you desire to spend a bit more money, you can purchase or rent the e-mail addresses of 5.6 million small business owners or 830,000 medical professionals and solicit their business.[4]

This flourishing data trade is made possible by the hundreds of millions of Web site visitors worldwide who continually submit vast amounts of personal information as they complete online transactions, create accounts, and query search engines. Companies collect this information with a smile and store it in sophisticated databases where it can: (1) fulfill a transaction; (2) supplement an internal marketing profile; (3) be mined to predict future purchases; and (4) be sold to

---

2. *See, e.g.*, Jonathan Krim, *Online Data Gets Personal: Cell Phone Records for Sale*, WASH. POST, July 8, 2005, at D1 ("For $110, Locatecell.com will provide you with the outgoing calls from [your significant other's] cell phone for the last billing cycle, up to 100 calls. All you need to supply is the name, address and the number for the phone you want to trace. Order online, and get results within hours.").

3. *See, e.g.*, Person to Person Search, https://www.abika.com/shopping/shopdisplayproducts.asp?id=1&cat=People (last visited Apr. 4, 2008). Also, this site sells separate and more specific psychological profiles for several categories, including unconventional behaviors, cheaters, doctors, lawyers, psychiatrists, teachers/professors, contractors, child-care providers, and pastors/ministers/priests. *See* Psychological & Behavior Profiles, http://www.abika.com/Reports/behaviors.htm (last visited Apr. 4, 2008).

4. *See info*USA Inc., Annual Report (Form 10-k), at 2 (March 12, 2007), *available at* http://sec.gov/Archives/edgar/data/879437/000103570407000213/d44577e10vk.htm (discussing each of the company's databases of PII, which include data on, among other things: 200 million consumers, 14 million new movers, 3.6 million new homeowners, 1.7 million bankruptcies, and 50 million consumer e-mail addresses).

unrelated third parties for a profit. Direct marketing firms across the globe salivate to collect not only phone numbers and e-mail addresses, but also information pertaining to family relationships, political affiliations, personal interests, and prior purchase histories in order to target future advertisements effectively. Larger data collection firms aggregate these scattered pieces of personal information located all over the Web to create detailed profiles of a person's life.[5] These "digital dossiers" are worth much more on the open market than bits and pieces of personal information are worth individually.[6]

As the twenty-first century Internet economy bustles forward, this type of information aggregation has become an increasingly prominent part of the e-commerce landscape. Surprisingly, however, the majority of today's PII collection and dissemination practices fall within the boundary lines of the United States legal system.[7] The primary problem lurking within this reality is the fact that Internet users do not fully understand the extent to which their PII is continually collected, stored, aggregated, and then sold on the open market. These same users fail to take into account the fact that providing an e-mail address to an online medical research Web site might lead to an increase in spam e-mails offering Viagra, for example, sometime in the near future. Without such an understanding, Web surfers have become accustomed to entering all sorts of PII into Web site forms when asked to do so, clicking submit,

---

5. Data aggregation firms will purchase all different types of PII in order to form a profile on an individual. For example, data aggregation firm Acxiom Corp.

> knows a lot about you. It has scoured public records for how many cars you own and what your house is worth. It has accumulated surveys that show if you are married and how many children you have. And for years Acxiom sold that information to marketers eager to use it to send mailings and make telephone pitches to consumers most likely to buy. Now . . . [the] company is putting those hundreds of millions of bits of data in the service of customizing which display ads to show people browsing the Web—a development that has raised red flags with some privacy advocates.

Kevin J. Delaney & Emily Steel, *Firm Mines Offline Data To Target Online Ads*, WALL ST. J., Oct. 17, 2007, at B1.

6. *See* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 1-10 (Jack M. Balkin & Beth Simone Noveck eds., 2004) (coining the use of the term "digital dossiers" in the context of information privacy).

7. *See, e.g.*, JOSEPH TUROW, PH.D., AMERICANS & ONLINE PRIVACY: THE SYSTEM IS BROKEN 5 (2003), *available at* http://www.asc.upenn.edu/usr/jturow/internet-privacy-report/36-page-turow-version-9.pdf ("[With limited exceptions,] online companies have virtually free reign to use individuals' data in the U.S. for business purpose without their knowledge or consent. They can take, utilize and share personally identifiable information—that is, information that they link to individuals' names and addresses. They can also create, package and sell detailed profiles of people whose names they do not know but whose interests and lifestyles they feel they can infer from their web-surfing activities.").

and moving on with their lives. This tendency to "just click submit and forget about it"[8] causes individuals unwittingly to place a multitude of PII into cyberspace, where it becomes virtually irretrievable. The United States legal system must respond, without overreacting and stifling e-commerce efficiency, by encouraging companies to provide visitors with an understandable privacy policy detailing a company's privacy terms and containing a choice regarding PII dissemination.

This article assesses this problem and proposes a solution in five parts. The first Part conceptualizes the "just click submit" phenomenon in the world of information privacy and identifies the primary benefits and threats operating within this environment. Part I also discusses current PII collection practices and the types of choices companies offer regarding the collection and sale of such data. Part II analyzes twenty-five high-traffic Web sites to determine the extent to which these major players adequately disclose their PII collection and sharing practices and offer a meaningful choice in the matter. This study demonstrates that the vast majority of the highest-trafficked Web sites do post privacy policies and do collect PII, but generally fail to state clearly whether such information will be shared with third parties. Part III summarizes the current legal regime in the United States as it relates to the collection and sale of PII. Part IV utilizes this background to propose a solution to the threats caused by current data collection practices by advocating for a new federal regulation. This law would require all distributors of PII in interstate commerce to have their name permanently tagged to the information upon each and every distribution (a concept referred to as PII tagging) they make while operating under a misleading or otherwise insufficient privacy policy. This tagging requirement will only apply to companies that do not clearly and accurately explain all external sharing of PII in their privacy policies. The fifth and concluding Part summarizes the argument and advocates PII tagging as a unique way to decrease the amount of PII sold into the open market without the informed consent of the individuals it identifies and, at the same time, without excessively hindering e-commerce efficiency.

8. This author has coined this phrase.

I. E-COMMERCE, INFORMATION PRIVACY, AND THE "JUST CLICK SUBMIT" PHENOMENON

> Getting started is easy and free. You are a few short steps away from getting your Google Analytics account so you can see how people find, navigate and convert on your website. Just follow these brief steps:
>
> 1. Choose your login and password by creating a Google account . . .
>
> 2. You will then get your Google Analytics code that needs to be added to your website
>
> 3. Start tracking!
>
> - Google Analytics—Sign Up[9]

Google Analytics' sign-up page presents a common Web site-to-consumer (W2C) interaction. Google Analytics' account-creation process is typical because it combines: (1) the formation of an online account; (2) the collection of PII in exchange for a service; and (3) privacy promises regarding the external uses of collected information. The sequence of activities in these standard e-commerce transactions is fairly consistent. First, visitors who desire to use Google Analytics' Web-traffic monitoring service must submit specific pieces of PII via an online form; this information serves as a prerequisite to account creation.[10] Although Google Analytics does not necessarily need a user's phone number or country of residence to provide this service, the company still requires this information as part of the transaction.[11] Second, the newly created account allows access to the desired service—in this case, to valuable technology that tracks activity on an account holder's personal or business Web site. The final part of the typical transaction—an aspect that many account creators skip and that some companies obfuscate—deals with privacy disclosures. Google Analytics posts a privacy policy for this service,

---

9. Google Analytics—Sign Up, http://www.google.com/analytics/sign_up.html (last visited June 30, 2007). Google has since changed this page, and it now reads:

> Google wants you to attract more of the traffic you are looking for, and help you turn more visitors into customers.
>
> Use Google Analytics to learn which online marketing initiatives are cost effective and see how visitors actually interact with your site. Make informed site design improvements, drive targeted traffic, and increase your conversions and profits.
>
> Sign up now, it's easy—and free!

Google Analytics—Sign Up, http://www.google.com/analytics/sign_up.html (last visited Apr. 28, 2008).

10. Google Analytics, https://www.google.com/analytics/home/provision?vid=1000 (last visited Apr. 4, 2008) (notably, one must be signed in as a Google user to create an Analytics account).

11. *Id.*

which discusses collection practices and uses of information obtained during the creation of a Google account.[12] In its policy, Google describes the types of PII it collects and promises to keep this information relatively confidential unless an account holder chooses to allow various secondary uses.[13]

From an information privacy perspective, the biggest problem with the typical e-commerce transaction is that internet users are not fully cognizant of what happens to their PII upon submission. Evidence shows that e-consumers do not fully understand the serious threats pertaining to: (1) their PII submissions and (2) a company's external uses of their information. Instead, individuals merely enter whatever pieces of PII are required by the Web site, click submit, and then forget about the process entirely. This Part conceptualizes this "just click submit" phenomenon and provides the primary reasons why users continually submit vast amounts of information without a full grasp of the privacy consequences. Additionally, this Part identifies the primary benefits and threats revolving around this phenomenon, and then concludes with an analysis of customer choice options regarding the collection and sale of PII. The concepts outlined here both set the table for the study of actual company PII practices that are detailed in Part III and, ultimately, serve as crucial background information underlying the need for a PII tagging requirement, as advocated in Part IV.

---

12. Unlike most highly trafficked Web sites, the Google homepage does not contain a link to its privacy policy. In fact, it takes two clicks from the Google homepage to retrieve the company's privacy policy. Google, http://www.google.com/ (last visited Apr. 4, 2008) (click "About Google" hyperlink, then click "Privacy Policy" hyperlink). From the Google homepage, a visitor must realize that the privacy policy is linked from within the "About Google" hyperlink. *See id.* It seems unlikely that a typical Web surfer would know to click on the "About Google" hyperlink in order to reach the privacy policy, as there is no indication that this is where the policy is located.

13. Google Privacy Policy, http://www.google.com/intl/en_ALL/privacypolicy.html (last visited Apr. 4, 2008). The diligent Web site visitor who takes the time to read this privacy policy will note that Google uses the PII it collects in the following ways:

- Providing our products and services to users, including that the display of customized content and advertising;
- Auditing, research and analysis in order to maintain, protect and improve our services;
- Ensuring the technical functioning of our network; and
- Developing new services.

Id. Additionally, the Privacy Policy provides that "Google processes personal information on our servers in the United States of America and in other countries. In some cases, we process personal information on a server outside your own country." *Id.*

A. The "Just Click Submit" Phenomenon

From the consumer perspective, the "just click submit" phenomenon is caused by the simple concepts of: (1) must, (2) rush, and (3) trust. Internet users interact with the World Wide Web on a daily basis as they visit intriguing Web sites, conduct desired transactions, and create beneficial online accounts. Similar to the Google Analytics sign-up requirements, the vast majority of these online transactions require individuals to disclose specific pieces of PII in order to complete a sale or gain access to a service to which users feel that they *must* take part. Any refusal to provide the required information will generally stop a Web session in its tracks and hinder any further meaningful use of a Web site. Therefore, Web surfers, desiring to avoid any clogs in their Internet pipeline, will generally just submit the personal information required rather than lose the desired Web site experience they seek. Because these users "must have" access to such services, they will enter the required PII. Second, the "just click submit" phenomenon is made more serious by the fact that these same visitors are usually in a *rush* to get to the fun part of their Web experience (e.g., shopping, gaming, or networking) and, therefore, just enter the required information without as much as a glance at the company's privacy policy. This rush mentality leads to a failure to obtain any knowledge as to how PII might be used by its collectors. Finally, the vast majority of Web users *trust* that the transaction they undertake will be taken care of by the company and that their PII will be relatively safe. Ironically, even those consumers that feel that their privacy might be infringed by certain Web sites still tend to enter PII during online transactions. At the end of the day, the "just click submit phenomenon" is caused primarily by these *must*, *rush*, and *trust* tendencies, and is responsible for millions of pieces of PII being added annually to millions of online profiles.[14]

From the company perspective, businesses understand how this "just click submit" phenomenon works and make good use of their superior bargaining position by continuing to require the submission of more and more personal information in exchange for providing valuable products and services. Instead of merely asking for a customer's first and last name, delivery address, credit card number, and expiration date to complete an online sale, companies often require customers to submit multiple phone numbers and e-mail addresses as additional parts of the transaction fulfillment process.

14. SOLOVE, *supra* note 6, at 1-10 (discussing the vast amount of PII located in an individual's digital dossier).

Customers who do not want to enter these final two pieces of unnecessary information find themselves unable to complete their intended purchase. In a similar fashion, e-commerce companies often require physical and e-mail addresses, phone numbers, zip codes, birthdays, gender identification, and other miscellaneous information merely to set up an online account. At the end of the day, companies understand that users will just submit their PII in lieu of losing the ability to use the companies' services and view this information collection as a tradeoff for the ability to access the Web site services they provide. This is especially true in cases where Web site accounts are free and allow account holders to view interesting or dramatic content or conduct other types of desired activities.

As evidenced above, the mantra of the twenty-first century e-commerce environment seems to be: "just click submit" and forget about it. Customers must have access to the products/services, do not want to be bothered with a bogged down Internet experience, and trust that all will be well with the PII. Therefore, they submit as much PII is required and move on with their Web experience. Companies prefer this arrangement because it allows them to collect more data, mine it to make predictions about customer interests and behavior, and then market more effectively to their current and past customers. Companies can also earn extra revenue from the sale of this information on the open market. As demonstrated in the next section, this information collection and sharing arrangement has many benefits but also poses some serious threats from an information privacy standpoint.

B. The Collection of PII: Benefits and Threats

Personal information is the lifeblood of e-commerce. As mentioned previously, companies collect PII to: (1) facilitate and process transactions; (2) conduct marketing campaigns; (3) mine for demographics, clickstream data, purchasing behavior, and customer interests; and (4) sell for a fee. Some of today's most popular Web sites proudly proclaim collection of only enough personal information to complete specific, user-initiated transactions (i.e., solely for purpose number one above).[15] This approach sits well with privacy advocates. Other popular Web sites view PII collection differently, however, and use collected information for each of the four purposes. These universal information-collection practices do not sit well with privacy advocates (or e-consumers in general), and tend to be disclosed

15. *See infra* Part II.

discretely or in legalese disclaiming liability.[16] Finally, a few highly trafficked Web sites make no mention at all of their PII practices. Problematically, the current United States legal regime does not prohibit the discrete, the incomprehensible, or the non-existent disclosure of PII collection practices—an issue addressed in Part IV of this article.[17]

Logistically, the majority of online PII collection occurs via Web forms.[18] The typical form resembles a paper-based questionnaire with blank spacess calling for various pieces of PII, such as names, addresses (physical and e-mail), phone numbers, usernames, passwords, gender, country of origin, job title, job responsibilities, and company size.[19] These forms are simple to create, program, and then post on a Web site.[20] Furthermore, such forms transfer the information electronically from the individual it identifies to its collector's databases in the blink of an eye.[21] Here, this information can be stored in perpetuity, organized, quickly mined for its predictive value, and then sold to purchasers thousands of miles away with a click of a mouse.[22] Once the information leaves the hands of the

16. *Id.*

17. *See infra* Part IV.

18. Although passive collection devices such as cookies and Web beacons can collect information about Web site visitors, such information is more general and not necessarily personally identifying information. *See infra* Part III.A.3.

19. *See, e.g.*, washingtonpost.com, Registration http://www.washingtonpost.com/ac2/wp-dyn?node=admin/registration/register&destination=register&nextstep=gather&application=reg30-globalnav&applicationURL=http://www.washingtonpost.com (last visited Apr. 4, 2008) (requiring visitors to enter a username, password, zip code, job title, job industry, primary job responsibility, and company size, along with gender, zip code, year of birth, and country of residence, in order to sign up for a Washington Post account). This registration page also gives new account holders the chance to have their PII disseminated to a few Washington Post "affiliates" merely by the user checking a particular box. *Id.*

20. *See, e.g.*, HTML Forms Can Be as Simple as "Copy and Paste," http://www.freedback.com/ (last visited Apr. 4, 2008) (discussing the ease with which a Web site owner is able to post an HTML form on his or her Web site, as well as the low cost—$9.00 per month—of creating such a form).

21. There are two sides to processing PII collection via Web forms: (1) client-side and (2) server-side. *See, e.g.*, Larisa Thomason, *Beginner Tip: Form Processing Basics*, NETMECHANIC.COM, Oct. 2002, http://www.netmechanic.com/news/vol5/beginner_no19.htm (stating that client-side processing deals with "the actual form that a visitor sees on your Web page" and server-side processing deals with the PII after it is submitted on the form); Online Form Builder—Services, http://www.formsite.com/services.html (last visited Apr. 4, 2008) (offering a simple way for companies to deal with server-side processing issues, and stating that "[f]orm results, which can be optionally emailed to you, are stored on our server and available for review in several different formats 24 hours a day").

22. Facebook, the popular social–networking Web site, has come under recent scrutiny for collecting information on the Web sites its users frequent and then selling this information to direct marketing firms. *See, e.g.*, Vauhini Vara, *Facebook's Tracking of User*

individual it identifies, it is virtually irretrievable and subject to abusive dissemination practices as well as security breaches.[23] Although the reasons for and the logistics of PII collection may seem sinister at this point, as with most aspects of information privacy, PII collection provides a plethora of benefits in addition to serious threats.[24]

1. The Primary Benefits of PII Collection

Any discussion of benefits and threats pertaining to the collection of personal information must recognize that the Web functions as the primary tool of e-commerce precisely because of such collection. The ability to collect PII from e-consumers allows this ever-expanding economic sector to operate effectively; serious restrictions on the ability to collect this information is akin to removing a plant from sunlight—e-commerce, as it exists today, would inevitably wither and die. For example, companies operating without the ability to collect payment and shipping information would find it difficult to

---

Activity Riles Privacy Advocates, Members, WALL ST. J., Nov. 21, 2007, at D8 ("[The] backlash [against Facebook] comes as online advertisers experiment with 'behavioral targeting,' or sending people ads based on personal information about them. A common type of behavioral targeting involves tracking the Web sites an Internet user visits in order to send them ads that are relevant to their interests."). Facebook's Chief Privacy Officer, Chris Kelly, responded to complaints by stating:

> Facebook is transparent in communicating to users what it is tracking. When a user visits an outside site and completes an action like buying a movie ticket, a box shows up in the corner of his Internet browser telling that person the outside Web site is sending that information to Facebook. The user can opt out by clicking on text that reads "No, thanks." If the user doesn't, the next time they visit Facebook, the user will see a message from Facebook asking for permission to show the information to their friends. If the user declines, the information won't be sent.

Id. (quoting Chris Kelley, Chief Privacy Officer, Facebook).

23. Even a seemingly unrelated issue—armed home invasions against wealthy individuals—might be somehow linked to the robber's access to personal information submitted online and then purchased or stolen. *See, e.g.*, M.P. McQueen, *Wave of Home Invasions Puts the Wealthy on Alert*, WALL ST. J., Nov. 15, 2007, at D1 ("Increasingly, wealthy and high-profile individuals must step up security at home and be vigilant in their cars to avoid becoming victims, security experts and police say. They may also need to reduce the amount of information they reveal about themselves on the Internet in places like Facebook, and in the media."). In addition, security experts are increasingly advising people to reduce the amount of personal information that can be found on the Web. *Id.*

24. *See, e.g.*, Gaia Bernstein, *The Paradoxes of Technological Diffusion: Genetic Discrimination and Internet Privacy*, 39 CONN. L. REV. 241, 272-73 (2006) ("[The public has perceived] the collection of personal information on the Internet as a privacy threat. Internet users overwhelmingly opposed the specific information collection practices, such as profiling, inter-site sharing, and merging of browsing habits with PII. At the same time, it appears that individuals are unaware of the scope and intricacy of personal information collection and use of such information by commercial entities on the Internet." (internal citations omitted)).

conduct transactions online. Similarly, companies operating without the ability to track individualized customer data would create Web sites that insufficiently serve the ever-evolving needs and desires of their customers. In fact, many of the benefits provided to today's e-consumer are predicated on a company's ability to collect PII. While such benefits are numerous, the following four stand out as the most prominent: (1) convenience, (2) efficiency, (3) tailored marketing, and (4) exchange for beneficial services.

a. Convenience

The World Wide Web epitomizes the concept of convenience. People go online from the comfort of their own homes—often in their pajamas—at all hours of the day to retrieve pertinent information on basically any subject imaginable. This physical convenience is buttressed by the economic convenience provided by the Internet. E-consumers can purchase anything from airline tickets to pet supplies online merely by placing items in an electronic shopping cart, entering payment information, and providing delivery instructions. These purchases take mere moments compared to the time they would take inside a typical brick and mortar establishment or over the telephone.

Purchases of goods and services are not the only convenience-based aspect of the Internet. In addition, Web sites can collect pieces of information in order to make navigation more convenient. For instance, "cookies" set on a user's hard drive can collect usernames, passwords, credit card numbers, and other pieces of personal information in order to make return trips to the Web site much easier. Upon the user's return to a specific Web page, cookies eliminate the dreaded search for account/log-in information or even a wallet and instead provide a customized homepage which recognizes the user's prior purchases and preferences.

Any reduction in a company's ability to collect, process, and store personal information would lessen or even remove the convenience aspect from Web-based transactions. For example, a restriction on the use of passive information collection technologies, such as cookies, would make Web sites more difficult to navigate. In this new reality, usernames and passwords would have to be tracked-down and re-entered, clickstream and purchase history would be erased after each session, and users would only see advertisements that interested them via a stroke of good luck. Web site visitors would quickly become frustrated as their late-night surfing missions were thwarted by the inconvenience of conducting a transaction that used to be so simple; in fact, they might even have to wait until morning to

reach a sales representative via telephone to make a payment or provide a delivery address. Requiring even the slightest inconvenience, such as a telephone call or a search for a long-forgotten password, is considered blasphemy in the Internet age.

b. Efficiency

Efficiency is different from convenience in that efficiency deals with transaction times—the speedier the successful e-commerce transaction, the more efficient and desirable the transaction.[25] From an efficiency standpoint, online PII collection allows users to initiate and complete an entire transaction within seconds at any time of the day.[26] There is no need to wait for businesses to open or for customer service representatives—potentially outsourced with personnel who are still learning English[27]—to answer a phone call to handle the transaction. The most efficient Web sites and Web surfers earn badges of honor from the Web community as they figure out ways to speed up their Internet activities,[28] including the speed of their

---

25. *See, e.g.*, *More People Are Paying Their Bills Online*, CHIC. TRIB., Oct. 9, 2003, at 10 (discussing the idea of efficiency and electronic bill payment, and stating that: "Most of us are now paying at least one of our bills online . . . . Of the 57 percent who went online to pay, most said they paid bank and credit card companies. Three years ago, the same survey found that only 17 percent of 500 people questioned paid one of their bills online. *Most people said speed* [(efficiency benefit)] *and the ability to pay at the last minute* [(convenience benefit)] *prompted their Internet payments*." (emphasis added)).

26. *See, e.g.*, Saul Hansell, *Google Aims To Speed the Online Checkout Line*, N.Y. TIMES, June 29, 2006, at C1 (discussing e-commerce efficiency with Google's CEO, Eric Schmidt). Google is introducing a service

> that will allow users to make purchases from online stores using payment and shipping information they keep on file with Google. Google's aim . . . is to make it easier and faster for people to buy products advertised on Google—thus attracting more advertisers. [Schmidt commented that:] "The goal here is to make it be one nanosecond from the time the customer decides to buy to the time the transaction is complete and the product is on the way."

Id. (quoting Eric Schmidt, Chief Executive Officer, Google).

27. *See, e.g.*, Donald Greenlees, *Filipinos Are Taking More Calls in Outsourcing Boom*, N.Y. TIMES, Nov. 24, 2006, at C4 (discussing the outsourcing of customer service jobs to different parts of the world and the fact that most "call center employees receive intensive training to acquire the accent of the customers they will be talking to"); Bruce Weinstein, Ph.D., *The Ethics of Outsourcing Customer Service*, RELIABLEANSWERS.COM, http://reliableanswers.com/jobs/outsourcing_ethics.asp (last visited Apr. 4, 2008) (describing the frustrations that customers feel when they reach a company representative who does not speak English).

28. *See, e.g.*, Julie Bick, *When PayPal Becomes the Back Office, Too*, N.Y. TIMES Dec. 18, 2005, at 3.6 (discussing the rise of online payment-processing Web site PayPal, and interviewing a small business owner that uses the Web site, who said "he liked the feeling of security because he has always been paid for the items he has sold through PayPal. *He also appreciates the transaction speed that PayPal allows his business,* [stating:]

Internet connection.[29] This trend is evidenced by Orbitz's commercials depicting neighbors and co-workers hovering in front of their computers and vying for the quickest purchase of airline tickets, or by the fact that Google displays the total time it takes for each and every search to compute.[30]

Businesses lacking the ability to collect sensitive PII, such as names, credit card numbers, and bank account numbers, would be unable to complete even the simplest e-commerce transaction without implementing time-consuming offline processes. Under such circumstances, customers could browse for and select products and services online; they would then have to wait, however, for normal business hours to phone, mail, or physically deliver payment and delivery information. Over time, these same customers might even find a more efficient use of their time by walking into a brick and mortar establishment to experience the "one-stop" event that used to be the highlight of Web-based shopping. Customers who frequent online retailers, such as eBay and Amazon.com, and social networking sites, such as Facebook and MySpace, would find it particularly difficult to transact business and create individualized user profiles, as they have in the past.[31] Each of these highly successful companies requires the ability to collect and use personal information legally in order to operate normally, and is thriving under the current conditions allowing virtually unrestrained PII collection.[32]

"I can put something up for sale at 9:30 p.m. . . . [and] a buyer can pay for it that night from anywhere, and I can ship it out first thing in the morning." (emphasis added)).

29. *See, e.g.*, Bob Tedeschi, *High-Speed Internet Access Makes It Easy To Leaf Through Catalogs Online*, N.Y. TIMES, June 14, 2004, at C6 ("[High-speed Internet] connections are more than just a boon to Web surfers. Internet retailing executives love them, too. Now that most people have at least some access to high-speed Internet lines, online retailers can finally dust off features they had shelved, lest they alienate the click-and-wait set.").

30. For instance, a Google search for Corey Ciocchetti took 0.24 seconds to produce 2,560 results. Google, http://www.google.com/ (search "Google Search" for "Corey Ciocchetti") (last visited Apr. 4, 2008). Notably, these results will change daily, as content is added and removed from the Web.

31. Rest assured, however, that many Web sites could still operate but their functionality would be greatly diminished.

32. *See, e.g.*, Joel Dreyfuss, *Does Facebook Need a Privacy Cop?*, REDHERRING.COM, http://www.redherring.com/Home/23296 (last visited Apr. 4, 2008) (comparing the success of prominent e-commerce and social networking Web sites with the public's desire for increased information privacy, and promoting a Web site rating system that would alter the current self-regulatory system).

c. Tailored Marketing

The third important benefit of PII collection lies in a company's ability to aggregate and mine information for customer preferences and then tailor marketing efforts specifically towards the consumer's interests.[33] It is obvious that people would rather see marketing for the products and services they desire, and that they are far more likely to click on and view such advertisements.[34] For instance, a visitor to the National Football League's (NFL) Web site (www.nfl.com) can sign up to play fantasy football for free.[35] These extremely popular, mock football seasons are conducted online via the NFL's Web site, where the advertisements that participants see are tailored to each viewer.[36] Through its sign-up process, the NFL collects different forms of PII, mines this data to determine a user's age, location, interests, gender, etc., and then serves up advertisements based on the appropriate demographic.[37] PII

---

33. *See, e.g.*, Brad Stone, *MySpace Mining Members' Data To Tailor Ads Expressly for Them*, N.Y. TIMES, Sept. 18, 2007 (stating that MySpace says that it has technology that "can tailor ads to the personal information that its 110 million active users leave on their profile pages"); Christopher Wolf, *We Don't Need 'Do Not Track,'* BUS. WK., Nov. 12, 2007, *available at* http://www.businessweek.com/technology/content/nov2007/tc2007119_029422.htm ("[T]here are many new ways marketers can use personal information to tailor advertising messages. They're able to gather information about personal interests by tracking Internet use and digital media viewing habits, among other things, and then tailor messages accordingly. *Consumers benefit from the customization as they receive ads relevant to them instead of those intended for mass consumption that may have no utility for them at all.*" (emphasis added)).

34. *See, e.g.*, MySpace.com, Privacy Policy, http://www.myspace.com/index.cfm?fuseaction=misc.privacy (last visited Apr. 4, 2008) ("MySpace may use cookies and similar tools to customize the content and advertising you receive based on the Profile Information you have provided.").

35. NFL Events: Fantasy, http://www.nfl.com/fantasy (last visited Apr. 4, 2008).

36. *See, e.g.*, Paul R. La Monica, *Fantasy Football . . . Real Money*, CNNMONEY.COM, Aug. 11, 2006, http://money.cnn.com/2006/08/11/news/companies/fantasyfootball/ (discussing the popularity of fantasy football). The "sport" has

> become an increasingly popular pastime. According to figures from the Fantasy Sports Trade Association—yes, this is big enough of a market to warrant a real trade group—there are currently between 15 million and 18 million fantasy sports players in the U.S. The number of players has grown 7 percent to 10 percent a year for the past three years. About 85 percent of all fantasy sports participants play fantasy football, mainly online.

Id.

37. *See id.* (discussing an interview with the director of advertising from a direct marketing firm, and stating that "marketing research has shown the average fantasy football player to be predominantly male, married, in a high income bracket and more likely to do research or make purchases online"). As for PII collection, the NFL collects personal information in order to "customize" the advertising and other content seen by individual players. NFL.com, Privacy Policy, http://www.nfl.com/help/privacy (last visited Apr. 4, 2008).

collection, for this reason, benefits each user as advertisements for products and services of actual interest are served in lieu of advertisements likely to be ignored completely.

The newest trend in tailored marketing is called behavioral targeting—a concept where companies collect and monitor the external Web sites that their customers visit in order to tailor advertisements seen when customers return to the company's own homepage.[38] To make this happen, data aggregation companies contract with companies interested in implementing behavioral targeting, and also contract with

> Web sites that collect consumer addresses, such as online retailers and those offering sweepstakes and surveys. In a blink, [aggregation companies can look] up the people who provide their addresses in its database, [match] them with their demographic and lifestyle [categories and place] "cookies," or small pieces of tracking data, on their computer hard drives. When those people [return to a company's] Web sites in the future, [the data aggregation company] can read cluster codes embedded in the cookies and use them to pick which ads to show.[39]

Even though behavioral targeting has caused controversy among several privacy advocacy groups, some of the country's largest

---

38. *See, e.g.*, Steve Lohr, *Your Ad Here*, N.Y. TIMES, May 16, 2007, at H1 ("The most common technique for identifying an audience is called behavioral targeting, which tracks, analyzes and predicts online behavior based on where you (actually your browser software) have gone before on the Internet. The ad targeters cull vast quantities of Web-viewing behavior and other data, like the speed of your Internet connection, the time of day you visited a site, whether it was done from work or home and even associated ZIP codes. These defined audience clusters consist of people who share characteristics based on their behavior on the Internet, not personal information like names, ages, home addresses or telephone numbers. So, for example, a person who recently visited sports and auto Web sites and read global warming articles on news sites would most likely turn out to be an 18- to 45-year-old male. An algorithm would then determine that he would be a good candidate for an ad about Toyota's hybrid-electric Prius. Advertisers are willing to pay much higher rates to reach such screened audiences."); *see also, e.g.*, Delaney & Steel, *supra* note 5, at D1 (discussing the concept of behavioral targeting). Behavioral targeting generally has a split financial arrangement. *See, e.g.*, Lohr, *supra*, at H1 (discussing a marketing company called Tacoda which specializes in behavioral marketing).

> [Tacoda's] network has 125 million individuals (PCs with the Tacoda cookie). Its software tags are also on 4,000 Web sites; and it collects nine billion data items a day. *For every dollar it collects from an advertiser, Tacoda keeps 40 cents, gives 40 cents, as a broker, to the Web publisher displaying the ad and distributes 20 cents to the sites providing targeted data.*

Id. (emphasis added)).

39. Delaney & Steel, *supra* note 5 (referring to data aggregation firm Acxiom).

> The Company classifies each U.S. household into 70 clusters based . . . "on that household's specific consumer and demographic characteristics, including shopping, media, lifestyle and attitudinal information." Clusters range from "Married Sophisticates" to "Penny Pinchers." . . . That allows a company selling an expensive antiwrinkle cream, for example, to contract with Acxiom to display its ads to affluent women 40 years or older in the "Skyboxes and Suburbans" or "Summit Estates"' clusters.

Id.

companies—such as Yahoo! and Microsoft—continue to implement this technique in their marketing practices.[40] In fact, studies show that companies spent $575 million on behavioral targeting alone in 2007, and that such spending will increase to $3.8 billion by 2011.[41] This advanced form of tailored marketing can benefit users through the serving of advertisements that are continually more likely to pique the interest of specific visitors. The privacy-invasive nature of this practice will be discussed below in the subsection discussing the threats caused by PII collection.[42]

d. Exchange for Beneficial Services

Companies with a strong presence in today's e-commerce environment execute on unique value propositions. Most of these business concepts are difficult to replicate in the brick and mortar world.[43] In fact, social networking Web sites such as Facebook and MySpace have found their ever-expanding niche precisely because of this e-commerce advantage.[44] For instance, it would be awkward,

---

40. *See, e.g.*, Anick Jesdanun, *Portals Mining Behavior on Web To Target Advertising*, CHI. TRIB., Dec. 2, 2007, at C16 (discussing the privacy controversy surrounding behavioral targeting). The author discusses how

> [major companies] are stepping up their educational efforts in response to privacy concerns [in response to behavioral targeting], trying to sell Internet users on the idea that if they are to see advertising to support free services, a targeted, relevant ad is far less annoying. They also stress that they aren't capturing sensitive information like names and e-mail addresses, and in many cases consumers can take steps to decline targeted ads. Indeed, companies aren't going as far as they could. "At the end of the day, if behavioral targeting is being used and consumers get annoyed, they are going to take it out on the advertiser or the publisher that placed the ad," said Michael Cassidy, chief executive of Undertone Networks, which contracts with a network of third-party sites to run ads.

Id.

41. DAVID HALLERMAN, EMARKETER, BEHAVIORAL TARGETING: ADVERTISING GETS PERSONAL (June 2007), http://www.emarketer.com/reports/all/emarketer_2000415.aspx?src=report_head_info_sitesearch.

42. *See infra* Part II.B.

43. *See, e.g.*, Steve Strauss, *Ask An Expert: To Boost Web Presence, Make These Basic Concepts Click*, USATODAY, *available at* http://www.usatoday.com/money/smallbusiness/columnist/strauss/2007-03-19-web_N.htm (last visited Apr. 4, 2008) (discussing Amazon.com founder Jeff Bezos's thoughts on what gives a company a strong web presence via Bezos's query: "*Does the website harness the unique characteristics of the Internet to create a strong value proposition for customers, one that could not be easily duplicated in the physical world*?").

44. Three popular social networking Web sites are designed for

> [t]he 35-and-under crowd . . . which together have more than 18 million members . . . . New members spend time filling out forms with personal information, from marital status and favorite movies to educational background and resume details. Some even have space for photos. Then, they set out to create a network, searching the site for friends, colleagues and peers. As personal networks grow,

cost-prohibitive, and incomprehensible for these companies to spend the resources necessary to create, post, and store millions of individualized profiles in hard copy. The Web, however, is an ideal environment for such a project, as users update their own customizable profiles, search for others with similar interests, and have their pages accessible to all members in real-time. Tens of millions of people find this type of online service extremely beneficial and spend a great deal of time tailoring their profiles and surfing the network.[45] As is the case with social networking Web sites, companies in various economic sectors offer a plethora of beneficial services online free of charge or at a very low price.[46] A Google search for the phrase "what the Web offers for free" buttresses this point by returning over 25 million hits.[47]

These beneficial services do come at a cost, however, as companies tend to predicate participation upon an exchange for an individual's PII.[48] As mentioned above when discussing the Google

---

> members can voyeuristically browse the profiles of friends-of-friends-of-friends; if a stranger catches their eye, they usually can find someone in their own network to broker an introduction.

Jessica Mintz, *Social Networking Sites Catch Employers' Eyes*, COLLEGEJOURNAL FROM THE WALL ST. J., http://www.collegejournal.com/columnists/thejungle/20050331-jungle.html (last visited Apr. 4, 2008).

45. *Id.*

46. *See, e.g.*, John Holusha, *Disney To Offer Some ABC Shows Free on the Web*, N.Y. TIMES, Apr. 10, 2006, *available at* http://www.nytimes.com/2006/04/10/business/media/10cnd-disney.html (discussing a recent trend in free Web services—free television programs—and stating that "[i]n an effort to extend its broadcast economic model to the Internet, the Walt Disney Company said today that it would offer some of its most popular ABC television shows free on its Web sites but with commercials that cannot be eliminated").

47. Google, http://www.google.com/ (search "Google Search" for "what the Web offers for free") (last visited Apr. 4, 2008). Notably, this entire search took all of 0.27 seconds. *Id.*

48. *See, e.g.*, La Monica, *supra* note 36 (discussing the dilemma a company faces when deciding whether to charge for an online service—like fantasy football—and stating that "several media companies are recognizing that it is more lucrative to not charge fantasy players since free games draw more traffic . . . and hence, more advertising revenue"). If a company does not desire to offer a free service, it can create rewards and discount programs that provide incentives for every dollar/hour spent on the company's products or services as another incentive for people to provide their PII. For instance,

> [t]he computer can attempt to use the stored data to ease the user's burden while they surf the web. When a person decides to purchase a book, for instance, a personal computer can communicate with a website to prepare to purchase the book, have suggestions for other products in which the user might be interested, and offer discounts for those goods. The current day version of R2-D2 would not only offer Luke Skywalker his lightsaber, but also suggest alternate brands and maybe a discount on an accompanying blaster.

Analytics program, only some of the information collected is actually necessary for the program's operation. Interestingly enough, it turns out that even privacy-sensitive e-consumers appreciate the value these services provide and concede that most of the PII collection is a small price to pay in return for the benefits provided.[49] In fact, e-consumers who decline to take advantage of such services end up paying more for the things they purchase and find themselves unable to utilize the Web sites they frequent as efficiently as otherwise possible.[50]

2. The Primary Threats from PII Collection

The benefits of PII collection, from the standpoints of convenience, efficiency, tailored marketing, and exchange for beneficial services, are extraordinary. Such collection is also necessary for e-commerce to function and flourish. However, these positive aspects should not cause e-consumers to ignore the many threats lurking whenever and wherever PII is collected. Although submitting information is simple and allows for a complete Internet experience, Web surfers must understand that the threats involved can bring about rather minor injuries, such as unwanted solicitations,[51] more serious injuries such as identity theft,[52] or, in the

---

David Goldman, *I Always Feel Like Someone Is Watching Me: A Technological Solution for Online Privacy*, 28 HASTINGS COMM. & ENT. L.J. 353, 354 (2006) [hereinafter *Someone Is Watching Me*] (internal citations omitted).

49. *Selling Your Personal Data*, CNET NEWS.COM, Sept. 1, 2003, http://news.com.com/2030-1069_3-5068504.html (discussing an interview with Harvard Business School professor John Deighton, who argues for market regulation of PII). Professor Deighton appreciates some of the benefits of PII collection and states:

> I want Amazon to know my identity, in particular my taste in books and music. I know that they respect the value of that knowledge so that the issue of sharing the data won't ever come up. I want American Airlines to know my flying habits and preferences because I want them to keep giving me the best service they can deliver in exchange for my commitment to fly them whenever I can.

Id. (quoting John Deignton, Professor, Harvard Business School).

50. *Id.* ("Consumers can achieve anonymity today by declining to join supermarket frequent-shopper programs, but by so doing, the average household pays $200 a year more for products. The points awarded by airline frequent flyer and hotel frequent guest programs, if redeemed, amount to discounts of 1 percent to 5 percent over the prices paid by nonsubscribers. They also lose out on a variety of nonmonetary benefits like recognition and preferential service that may matter more than money.").

51. *See, e.g.*, Eileen Ambrose, *Turn Off Spigot of Information About You*, CHI. TRIB., Sept. 2, 2007, at C5 ("[P]ersonal information seems more at risk than ever, and it is often not our fault. We shred credit card offers and hunch over ATMs so no one sees our personal identification number. . . . Of course, you can't stem the flow of all information about you. But you can control enough to make a difference. . . . Identity theft isn't the only reason to do this. Companies make big bucks selling details about you. And what do you get?

worst case, murder.[53] Of all the potential threats stemming from the collection of PII, the following two merit attention: (1) the power and sophistication of today's computer and database technology, and (2) the sensitive nature of aggregated PII.[54]

a. Powerful and Sophisticated Technology

Today's ever-advancing computer technology[55] enables Web sites to collect PII both actively from user inputs and passively from

---

Nettlesome sales calls and a mailbox stuffed with *unwanted solicitations.* (emphasis added)).

52. *See, e.g.*, Tom Zeller, Jr., *To Catch a Thief*, N.Y. TIMES, June 25, 2005, at C1 ("[E]very day, waves of criminals from around the globe, armed with stolen account information (or new accounts they have created in other people's names) poke and prod at the gates [of e-commerce], looking for weak spots. Blink, many merchants say, and your defenses are compromised.").

53. For example, Amy Boyer was murdered by a criminal who obtained her PII from an online information broker for $150. *See* Holly Ramer, *Slain Woman's Parents Target Internet Brokers; Stalker Purchased Her Personal Data*, CHI. TRIB., Dec. 30, 2002, at 8. Boyer's killer, Liam Youens

> paid Docusearch Inc. of Boca Raton, Fla. [(an Internet information broker)], about $150 to get Boyer's Social Security number and other information, including her work address. "Docusearch pulled through 'amazingly' it's like a dream," Youens wrote on his Web site. A few weeks later, Youens pulled alongside Boyer's car after she left her job at a dental office and shot her 11 times before killing himself.

Id.

54. An interesting point is that data collection companies are shying away from collecting PII from offline sources, such as public records, because they can collect all of the PII they need from online sources. *See, e.g.*, Delaney & Steel, *supra* note 5, at D1 ("[T]he more prominent digital ad firms that specialize in behavioral targeting shy away from using the reams of data collected about people offline to target online ads. These firms say they already collect enough anonymous information based on people's online activities and would rather not tackle the privacy issues that come along with gathering offline data.").

55. *See, e.g.*, Jerry Berman & Paula Bruening, *Is Privacy Still Possible in the Twenty-First Century?*, CTR. FOR DEMOCRACY & TECH., http://www.cdt.org/publications/privacystill.shtml (last visited Dec. 20, 2007) ("[Advances] in communications technologies over the last half century significantly challenge individual privacy. Deployment of rapid and powerful computing technologies has vastly enhanced the ability to collect, store, link, and share personal information. This ability to manipulate information has played a critical role in reshaping the American economy, making it possible to predict consumer demand, manage inventories, serve individual consumer requirements, and tailor marketing techniques. But to do this successfully, businesses require and use information about individuals, which means that the demand for personal information, and business efforts to acquire it from customers, constantly increase. Undoubtedly, the Internet has made this kind of data collection and analysis easier and more efficient.); Sylvia W. Gaines & Warren W. Gaines, *Future Trends in Computer Applications*, 45(3) AM. ANTIQUITY 462-71, 462 (1980) ("[C]omputer technology itself has advanced. Today, many sophisticated and powerful tools . . . exist for managing data.").

devices such as cookies and Web beacons.[56] Upon collection, company computers are able to store vast amounts of this information in sophisticated databases, which can mine it in the blink of an eye to predict customer interests.[57] These results are highly sought after on the open market and an entire industry of data brokers has formed to aggregate and then sell specific lists of common profiles.[58] As a result

---

56. Cookies are text files placed on the user's hard drive that are able to collect information. *See* About Cookies, http://www.allaboutcookies.org/cookies/ (last visited Apr. 4, 2008). Typically, cookies will

> contain the name of the domain from which the cookie has come, the "lifetime" of the cookie, and a value, usually a randomly generated unique number. Two types of cookies are used on this website-session cookies, which are temporary cookies that remain in the cookie file of your browser until you leave the site, and persistent cookies, which remain in the cookie file of your browser for much longer (though how long will depend on the lifetime of the specific cookie).
>
> Cookies can help a website to arrange content to match your preferred interests more quickly. Most major websites use cookies. Cookies cannot be used by themselves to identify you.

Id. Web beacons are small, invisible graphic images placed on Web pages that are able to collect information. *See* Web Beacons and Other Tools, http://www.allaboutcookies.org/web-beacons/ (last visited Mar. 29, 2008). When a user's browser requests information from a Web site containing a web beacon, many types of information can be gathered, including:

> the IP address of your computer; time the material was viewed; the type of browser that retrieved the image; and the existence of cookies previously set by that server. This is information that is available to any web server you visit. Web beacons do not give any "extra" information away. They are simply a convenient way of gathering the simplest of statistics and managing cookies.

Id.

57. An Introduction to Data Mining, http://www.thearling.com/text/dmwhite/dmwhite.htm (last visited Apr. 4, 2008). Data mining is

> a powerful new technology with great potential to help companies focus on the most important information in their data warehouses. Data mining tools predict future trends and behaviors, allowing businesses to make proactive, knowledge-driven decisions. The automated, prospective analyses offered by data mining move beyond the analyses of past events provided by retrospective tools typical of decision support systems. Data mining tools can answer business questions that traditionally were too time consuming to resolve. They scour databases for hidden patterns, finding predictive information that experts may miss because it lies outside their expectations.
>
> Most companies already collect and refine massive quantities of data. Data mining techniques can be implemented rapidly on existing software and hardware platforms to enhance the value of existing information resources, and can be integrated with new products and systems as they are brought on-line. When implemented on high performance client/server or parallel processing computers, data mining tools can analyze massive databases to deliver answers to questions such as, "Which clients are most likely to respond to my next promotional mailing, and why?"

Id.

58. *See, e.g.*, Tom Zeller, Jr., *The Scramble To Protect Personal Information*, N.Y. TIMES, June 9, 2005, http://www.nytimes.com/2005/06/09/business/09data.html?pagewanted=2 (quoting Senator Charles Schumer, who stated that the "world has changed and this kind of information [(PII)] is as valuable as cash and any institution dealing with it ought to treat it that way"); Online Data Vendors and Information Brokers:

of PII collection, organizations oftentimes possess billions of pieces of PII on hundreds of millions of Americans.[59] For example, one of the largest data brokers, ChoicePoint, has over 50,000 clients[60] and a market value of over $3 billion.[61] It is doubtful that the average Web site visitor understands the power and sophistication of this technology or the fact that it is being implemented to analyze submitted personal information in great detail.[62]

b. The Sensitivity of Aggregated PII

Individuals with only a few pieces of PII floating around in cyberspace are not particularly vulnerable.[63] For instance, even an identity thief would find it difficult to work with only an individual's phone number or e-mail address. When a few of these pieces of

---

How To Opt-Out, http://www.privacyrights.org/ar/infobrokers.htm (last visited Apr. 4, 2008) (providing two lists of data brokers, with one list detailing data brokers that allow individuals to opt-out of having their PII non-public disseminated and those that do not offer an opt-out policy).

59. Robert O'Harrow, Jr., *In Age of Security, Firm Mines Wealth of Personal Data*, WASH. POST, Jan. 20, 2005, at A1 (discussing the data broker ChoicePoint Inc. and the idea that the company has "billions of details about [Americans and] their homes, cars, relatives, criminal records and other aspects of their lives").

60. *See* ChoicePoint Inc., Annual Report (Form 10-K), at 3 (Feb. 26, 2007), *available at* http://www.sec.gov/Archives/edgar/data/1040596/000119312507042820/d10k.htm [hereinafter ChoicePoint 2007 Annual Report] (stating that, as of February 21, 2007, ChoicePoint had over 50,000 clients, including "substantially all domestic insurance companies, many of the nation's largest employers, non-profit organizations, small businesses, financial institutions, consumers and certain local, state and federal government agencies").

61. On February 21, 2007, the closing price of ChoicePoint stock was $39.35, and the company had 76.6 million shares outstanding, providing evidence of a market capitalization of over $3 billion. *See* Stock Quotes, Stock Highs and Lows for NASDAQ, NYSE, AMEX and OTC-BB—CNBC.com, http://www.cnbc.com/id/15837290?q=CPS (last visited Jan. 31, 2008) (showing ChoicePoint's closing stock price on February 21, 2007 at $49.35); ChoicePoint 2007 Annual Report, *supra* note 60, at cover page (showing that 76,566,461 shares of ChoicePoint common stock outstanding on Feb. 21, 2007).

62. Privacy advocates point to this threat as it relates to the concept of behavioral targeting mentioned previously. *See, e.g.*, Delaney & Steel, *supra* note 5. For example,

> [s]ome privacy advocates say they are concerned that [data aggregation firms risk] going too far with [their] Internet ad targeting. "You're potentially seeing a link between very sophisticated offline databases being used to target online advertising," says Jeff Chester, executive director of the Center for Digital Democracy, a nonprofit consumer-advocacy group focused on digital media.

Id. In addition, executives at one data aggregation firm admitted that Internet users do not understand the sophistication of the technology involved in PII collection and data mining. *See id.* (interviewing Acxiom's Chief Marketing and Strategy Officer, who opined that the majority of consumers submitting PII do not know a great deal about how the information they submit may be used by third parties for behavioral targeting purposes).

63. This is obviously not the case with some pieces of PII, such as a Social Security Number, a credit card number, or a bank account number.

information are aggregated together, however, the total package becomes much more sensitive and the individual becomes much more vulnerable.[64] For instance, if the same identity thief that discovered your e-mail address could also discover your Social Security number or mother's maiden name, she could potentially hack into your credit card Web-account or pose as you over the phone and access your account. Therefore, online customers must keep in mind that the bits and pieces of personal information submitted online can be, and often are, aggregated into digital profiles. If these profiles are sold on the open market, any willing buyer will potentially have access to key accounts. Finally, digital profiles become almost irretrievable once they leave the hands of the company that created them.

C. The Dissemination of PII: Benefits and Threats

PII is valuable in part because it can be commoditized and disseminated efficiently and electronically. Companies are incentivized to sell the information they collect because, with a few mouse clicks and a plethora of available buyers, they generate additional revenue streams. Buyers are incentivized to purchase PII because such information arrives prepackaged—collected, mined, and correlated into categorized lists—and ready to use.[65] Purchasers find it much easier and more efficient to buy prepackaged PII than to gather and aggregate the same information independently. In the end, parties on both sides of a PII transaction benefit from today's high supply/high demand environment.

---

64. *See, e.g.*, Hampton Stephens, *Security Concerns Prompt Army To Review Web Sites, Access*, DEFENSE INFORMATION AND ELECTRONICS REPORT, Oct. 26, 2001, http://www.fas.org/sgp/news/2001/10/dier102601.html (discussing criticism of security on military Web sites). For instance,

> [t]he idea that the Web is a "potent instrument to obtain, correlate and evaluate an unprecedented volume of aggregated information regarding DOD capabilities," as Hamre wrote in 1998, is echoed in the recent [Paul] Wolfowitz memo. This notion—that unclassified, seemingly benign information becomes dangerous when aggregated—may account for recent concerns about the Internet, which is particularly suited to gathering large amounts of information quickly. "Unclassified information may likewise require protection because it can often be compiled to reveal sensitive conclusions."

Id.

65. *See, e.g.*, ChoicePoint, Market*View*, http://www.choicepoint.com/products/marketview.html (last visited Apr. 4, 2008) (discussing ChoicePoint's direct-marketing data containing pre-sorted PII on 210 million people); Guaranteed Lists: Consumer Mailing Lists—Consumer Telemarketing Lists, http://www.guaranteedlists.com/specialty.php (last visited Apr. 4, 2008) (offering for sale lists of, for example, gardening enthusiasts, automobile owners, motorcycle owners, new movers, and new homeowners).

However, studies show that the American public resents the idea of companies doing whatever they wish with personal information. For example, eighty-four percent of people responding to a Washington Post–ABC News poll stated that companies collecting their PII are not doing enough to protect this information from abuse.[66] In addition, other studies show that consumers are becoming more unwilling to spend money online due to a lack of trust,[67] and that consumers are uncomfortable providing the financial and personal information necessary to complete online transactions.[68] However, the population's actual information submission practices do not bear out

66. *See, e.g.*, *Washington Post–ABC News Poll, Social Security/Iraq*, Mar. 15, 2005, *available at* http://www.washingtonpost.com/wp-srv/politics/polls/polltrend_031405.html (telephoning 1,001 randomly-selected adults and asking forty-two questions—including the following question: "As you may know there are some companies that collect and sell information about people such as their Social Security number, credit card payment history, and public records such as drivers license, real estate, court and military service records. Do you think the companies that collect and sell this information are doing enough to protect your personal privacy, or not?"); *see also, e.g.*, Princeton Survey Research Associates International, *Leap of Faith: Using the Internet Despite the Dangers*, Oct. 26, 2005, at 2, *available at* http://www.consumerwebwatch.org/pdfs/princeton.pdf [hereinafter Princeton Survey] (showing that eighty-eight percent of the 1,501 people surveyed claimed that it was very important, when browsing the Web, that specific Web sites keep their PII safe and secure).

67. *See, e.g.*, Kalinda Basho, *The Licensing of Our Personal Information: Is It a Solution to Internet Privacy?*, 88 CAL. L. REV. 1507, 1509 (2000) (stating that a company's use of PII without the knowledge or consent of the person it identifies, and for purposes other than for which it was submitted, "leaves many Internet users feeling as if they have no privacy"); Thomas A. Hemphill, *The Federal Trade Commission and Electronic Commerce Security Policy: A Viable Solution?*, 106:2 BUS. & SOC. REV. 161, 161 (2001), *available at* http://www.blackwell-synergy.com.proxy.library.vanderbilt.edu/doi/pdf/10.1111/0045-3609.00108?cookieSet=1 (stating that consumers may be spending less online because of "an unwillingness to 'trust [collectors of PII] with private data.'"); Princeton Survey, *supra* note 66, at 1 ("[E]arly in this second decade of the Web, Internet users are more demanding of Web sites, less trusting and adjusting their behavior in response to what they see as very real threats in the online world").

68. *See, e.g.*, Thomas A. Hemphill, *DoubleClick and Consumer Online Privacy: An E-Commerce Lesson Learned*, 105:3 BUS. & SOC. REV. 361, 361 (2000) *available at* http://www.blackwell-synergy.com.proxy.library.vanderbilt.edu/doi/pdf/10.1111/0045-3609.00087 (citing a study by Louis Harris and Company for the National Consumers League that showed that seventy-three percent of consumers surveyed were uncomfortable providing credit card information, seventy-three percent were uncomfortable providing other financial information, and seventy percent were uncomfortable providing personal information online). The survey also found that "only 24 percent of Internet browsers actually engaged in purchasing online." *Id.*; *see also* Donna L. Hoffman et al., *Information Privacy in the Marketplace: Implications for the Commercial Uses of Anonymity on the Web*, 15 INFO. SOC'Y 129, 131 (1999) (citing articles claiming that consumers are worried that their PII will be sold to third parties "without their knowledge or permission," and noting that such worries comprise one of the two dimensions of an individual's information privacy concerns).

this frustration.[69] For instance, few Web site visitors read company privacy policies and understand that the information they enter online can be, and often is, sold on the open market without their knowledge or consent.[70] Many of these "secondary uses" make the information virtually irretrievable, as it is now completely outside of the hands of the person it identifies or the company that collected it in the first place. This PII may reappear in the hands of a direct marketing firm or, in the worst case scenario, in the hands of an identity thief or other criminal.

Dissemination of personally identifying information creates benefits and threats for online consumers. Unlike PII collection, however, the threats stemming from dissemination outweigh the benefits from the consumer perspective. This section compares the more miniscule benefits to the more serious threats of PII dissemination and helps bolster the argument made in Part IV that companies must provide some form of meaningful disclosure regarding onward transfers of PII before dissemination occurs.

1. The Primary Benefit of PII Dissemination: Efficient Marketing

Sales of PII to unrelated parties provide an indirect benefit to consumers in the form of more efficient marketing. For example, when a company purchases PII and mines the data for customer preferences and future interests, consumers receive advertisements better suited to their needs and desires.[71] In an era of mass marketing and oversaturated consumers, companies are better served when they spend more time and resources improving the quality, instead of the quantity, of their marketing efforts.[72] Company

---

69. *See, e.g., Privacy: Consumers Know Online Privacy Measures, but Lax in Taking Precautions, Survey Finds*, E-COM. LAW DAILY, Dec. 8, 2006, *available at* http://pubs.bna.com.proxy.library.vanderbilt.edu/NWSSTND/IP/BNA/ecd.nsf/SearchAllView/EF9873EC1B8C25F78525723D0080294D?Open&highlight=PRIVACY ("[Although] a majority of consumers believe they know how to protect their privacy when online, most do not actually implement the privacy and security measures available to them").

70. *Id.* (stating that a majority of respondents to a survey reported that they "do not read online privacy policies when providing their personal information for the first time on a Web site"). Twenty-eight percent of respondents claimed that they checked "most of the time to confirm that a Web site had a posted privacy policy" (with only 20 percent actually reading the policy), and only five percent of respondents claimed that they returned "frequently to a posted privacy policy to check for updates or revisions." *Id.*

71. *See, e.g.*, Basho, *supra* note 67, at 1508 ("By using your consumer profile, entities can determine how to effectively advertise to you and sell you more products.").

72. *See id.* at 1515 ("[Some] business uses of personal information benefit consumers. The more a business knows about an individual, the better it can customize Web pages to meet her interests [or] develop targeted emails that provide her with useful

revenues should increase as people see what they want to see advertised and purchase more products and services that pique their interest. Without a cost-effective way to procure and mine data for customer preferences, companies will continue their old approach of posting, en masse, the same advertisements to every demographic group, a practice destined to spark an interest with a very low percentage of recipients. In fact, the benefit of more efficient marketing would be drastically reduced if companies were not able to purchase disseminated PII.

2. The Primary Threats of PII Dissemination

As opposed to the important benefit of increased marketing efficiency, PII dissemination poses several privacy-invasive threats. Primary among this group are the threats of: (1) virtually irretrievable data, (2) lack of purchaser verification, and (3) efficient transfers of aggregated profiles. Each of these issues is exacerbated when PII is disseminated by entities unconcerned with the privacy of the individual it identifies to entities exhibiting the same lack of concern. This subsection demonstrates that these three threats are much more serious than the threats posed by PII collection.

a. Virtually Irretrievable Data

PII is not necessarily private information or the personal property of the individual it identifies. While there are strong arguments on both sides of this divide, pieces of personal data such as addresses (physical and e-mail), phone numbers, and mother's maiden name are all readily discoverable and are not created by the individual they identify.[73] Additionally, it is difficult to argue that these

information or discounts."). These types of benefits make the Internet "a more interactive and convenient medium for consumers." *Id.*

73. *See, e.g.*, Jerry Kang & Benedikt Buchner, *Privacy in Atlantis*, 18 HARV. J.L. & TECH. 229, 232 (2004) (discussing the various arguments for and against property rights in personally identifying information). Several key articles advocate for a property regime in personally identifying information. *See, e.g.*, Vera Bergelson, *It's Personal but Is It Mine? Toward Property Rights in Personal Information*, 37 U.C. DAVIS L. REV. 379, 442 (2003) (suggesting a legal regime classifying personally identifying information as property); Lawrence Lessig, *The Architecture of Privacy*, 1 VAND. J. ENT. L. & PRAC. 56, 63-65 (1999) (advocating for a market where personally identifying information is considered to be property); Patricia Mell, *Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness*, 11 BERKELEY TECH. L.J. 1 (1996) (arguing that personally identifying information is property); Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381 (1996) (arguing that personally identifying information is property). However, a few key articles advocate against a property right in personally identifying information. *See, e.g.*, Jessica Litman,

individual pieces of PII create a reasonable expectation of privacy, as many are specifically designed to increase a person's exposure to the outside world. This virtually eliminates the ability of an individual to sue a disseminator under a tort theory.

What should be considered more private, however, is the aggregation of such information into a digital profile. Suddenly, important pieces of an individual's educational, family, financial, and personal life are gathered together in one place.[74] With access to each of the major pieces of information companies use to authenticate customer accounts, digital profiles grant e-thieves a leg-up in impersonating specific individuals. These digital profiles are relatively secure in the hands of the company that collects the information initially. Individuals know that they submitted their information to a particular company for a particular purpose and know where to turn if something goes wrong. The more serious threats arise when such information leaves the hands of its collectors and enters the realm of cyberspace—a place where it is virtually irretrievable. In cyberspace, PII is often purchased anonymously and from anywhere around the world.[75] This information can then be resold multiple times until it is completely out of the control of the individual it identifies and its initial collectors. More importantly, purchasers can disappear quickly and utilize the information in any way they want without fear that law enforcement officials will have the resources and ability to track down their global operations.[76]

In addition, purchasers of such information have no legal obligation to disclose their purchases or the information that they purchased to the individual such information identifies. Making matters worse is the fact that customers rarely receive any promise that they will be notified of pending or conducted PII sales and will rarely know the identities of the parties that purchase their PII.[77]

Information Privacy/Information Property, 52 STAN. L. REV. 1283 (2000) (arguing against personally identifying information being classified as property); Pamela Samuelson, *Privacy as Intellectual Property*, 52 STAN. L. REV. 1125 (2000) (advocating against personally identifying information being classified as property).

74. For example, an online investigation of this author, Corey Ciocchetti, provided accurate pieces of information regarding my educational (schools attended), family (addresses of my relatives), financial (credit card accounts), and personal (home address) life. *See* Intelligent Investigations, http://www.intelligentinvestigations.com/upsellbefore2.php?referral=&src=&product=cm&upsell=a (report on file with the author).

75. *See, e.g.*, Jeanne Sahadi, *Your Identity . . . for Sale*, CNNMONEY.COM, May 9, 2005, http://money.cnn.com/2005/05/09/pf/info_profit/.

76. *See id.*

77. *See id.* ("[M]uch of your information is already bought and sold year-round. And you never know into whose hands it falls since identity thieves and company insiders have proven quite clever at obtaining records.").

This situation makes any recovery of a digital profile impossible. As stated previously, if the package of information falls into the wrong hands, a great deal of personal and financial damage can be done.

b. Lack of Purchaser Verification

Today's Internet is truly global in scope.[78] In 2008, data is purchased and disseminated in seconds to buyers who may anonymously request such information from at least five continents.[79] Sellers have virtually no legal obligation to verify the identity of buyers participating on the other side of these transactions, unless they promise verification in a privacy policy.[80] Although a blatant disregard for an individual's safety has led to liability in some cases,[81] companies generally have to follow privacy policy procedures in order to avoid legal trouble.

This PII dissemination threat is now more prominent thanks to ChoicePoint's failure to protect a vast amount of PII located in its databases adequately. In the ChoicePoint case, the company failed to verify the identities of parties who requested access to PII in the form of names, addresses, Social Security numbers, and dates of birth.[82]

---

78. *See, e.g.*, Stephen Labaton, *F.C.C. Takes on Oversight of Internet Phone Services*, N.Y. TIMES, Nov. 10, 2004, at C8 (citing a former Chairman of the Federal Communication Commission, Michael K. Powell, who was discussing the preemption of Internet phone service regulation when he said "that the Internet is global in scope").

79. *See, e.g.*, Internet Traffic Report, http://www.internettrafficreport.com/ (last visited Apr. 4, 2008) (cataloging recent Internet activity and connection reliability on five of the seven continents).

80. *See, e.g.*, Federal Trade Commission, Enforcing Privacy Promises: Section 5 of the FTC Act, http://www.ftc.gov/privacy/privacyinitiatives/promises.html (last visited Apr. 4, 2008) (discussing the role of the Federal Trade Commission in punishing companies that fail to abide by their privacy policy promises); PAUL N. OTTO, ANNIE I. ANTÓN & DAVID L. BAUMER, THE CHOICEPOINT DILEMMA: HOW DATA BROKERS SHOULD HANDLE THE PRIVACY OF PERSONAL INFORMATION, N.C. St. Univ. Tech.Report TR-2006-18, 2 (2006), *available at* http://theprivacyplace.org/wp-content/uploads/2007/07/tr-2006-18u.pdf [hereinafter CHOICEPOINT DILEMMA] ("[D]ata brokers exist in a largely unregulated market space and thus structure their operations to avoid privacy protection laws that restrict information gathering and sharing by government agencies and credit bureaus").

81. *See, e.g.*, Amy Boyer, http://epic.org/privacy/boyer/ (last visited Apr. 4, 2008) (discussing the Amy Boyer murder case and the New Hampshire Supreme Court ruling that information brokers may be held responsible for selling PII with a blatant disregard for purchaser verification).

82. *See, e.g.*, Tom Zeller, Jr., *U.S. Settles with Company on Leak of Consumers' Data*, N.Y. TIMES, Jan. 27, 2006, at C3 (discussing the ChoicePoint case and the company's settlement with the Federal Trade Commission); CHOICEPOINT DILEMMA, *supra* note 80 ("[The] massive security breach at ChoicePoint seems to be a tipping point. Ever since the ChoicePoint news, the data broker industry as well as the privacy and security of personally identifiable information . . . have been subject to increasing public and congressional attention.").

These bad actors, posing as legitimate businesses, were allowed to conduct over 17,000 searches within ChoicePoint databases and purchase data on over 163,000 individuals from the company before the scam was discovered.[83] In January 2006, the company settled the case with the Federal Trade Commission (FTC) by agreeing to pay $15 million, with $10 million designated as a fine and $5 million designated to compensate injured consumers.[84] In settling the case, the FTC proclaimed that companies must put "reasonable" safeguards in place to hinder the sale of PII of criminals.[85] This proclamation does not have the force of a federal law passed by Congress, and the FTC has limited resources with which to pursue violators of its reasonable safeguards standard.[86] Therefore, the threat of a lack of purchaser verification upon PII dissemination remains serious.

c. Efficient Transfer of Aggregated Profiles

Sophisticated database technology, in combination with e-mail and file transfer software, allows for the efficient transfer of large

---

83. Zeller, Jr., *supra* note 82; *see also* CHOICEPOINT DILEMMA, *supra* note 80, at 5 (discussing the number of searches conducted by the criminals (17,000) and the number of people who data was potentially misappropriated (163,000)).

84. Zeller, Jr., *supra* note 82 (stating that the $10 million fine represents the largest "civil penalty ever imposed by the [Federal Trade Commission]"). In addition, ChoicePoint agreed to "overhaul its security program . . . and submit to independent audits of its procedures every two years for the next 20 years." *Id.*

85. *Id.* In its complaint against ChoicePoint, the FTC

> claimed that the company did not have "reasonable procedures" in place to screen would-be subscribers to its databases and that in this case, the applications for access made by the fake businesses should have raised "obvious red flags." The company did not, for instance, raise questions when an apartment number or a commercial mail drop was given as a business address, or when cellphone numbers were provided as a "business's sole telephone number," according to the agency's complaint. Multiple applications from nominally different businesses arriving from the same commercial fax number also did not prevent the applications from the fake companies from being approved, the commission charged.

Id.

86. *See, e.g.*, FTC Bureau of Consumer Protection—Business Information, http://www.ftc.gov/bcp/business.shtm (last visited Mar. 29, 2008) (admitting that the FTC has limited resources). "The FTC's information for businesses can enhance compliance with the law. To leverage limited resources, the FTC often partners with industry associations, advocacy organizations, and other government agencies." *Id.*; *see also* Kevin E. Gronberg, *FTC ChoicePoint Settlement: A Turning Point for Data Integrity*, 2(6) CYBER SECURITY INDUSTRY ALLIANCE NEWSLETTER, Feb. 2006, *available at* https://www.csialliance.org/news/newsletters/feb2006/feb_choicepoint.html (urging Congress to act to assist in protecting PII, because "the FTC has limited resources its disposal to attempt to prosecute each organization that fails to properly protect consumer information").

quantities of aggregated PII.[87] In fact, it is amazing to consider how times have changed drastically in the world of PII collection and dissemination:

> Before advanced computerized techniques for aggregating, analyzing, and disseminating data came into widespread use, personal information contained in paper-based public records at courthouses or other government offices was relatively difficult to obtain, usually requiring a personal visit to inspect the records. Nonpublic information, such as personal information contained in product registrations, insurance applications, and other business records, was also generally inaccessible. In recent years, however, advances in technology have spawned information reseller businesses that systematically collect extensive amounts of personal information from a wide variety of sources and make it available electronically over the Internet and by other means to customers in both government and the private sector. This automation of the collection and aggregation of multiple-source data, combined with the ease and speed of its retrieval, have dramatically reduced the time and effort needed to obtain information of this type.[88]

Today, a seller of PII located in Denver, Colorado can transfer millions of aggregated digital profiles in real-time to a buyer as far as 6,000 miles away or as close as the nearest United States government official.[89] Such a transfer does not require any physical mailing, postage, or packaging, and the transit time is minutes on average.[90]

---

87. *See, e.g.*, CHOICEPOINT DILEMMA, *supra* note 80, at 3 (discussing the storage capacity of data brokers, and stating that ChoicePoint alone has accumulated "over 19 billion public records, equaling over 250 terabytes of data in its databases").

88. *See, e.g.*, UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE, REPORT TO CONGRESSIONAL COMMITTEES: PERSONAL INFORMATION: AGENCY AND RESELLER ADHERENCE TO KEY PRIVACY PRINCIPLES 7 (Apr. 2006), *available at* http://www.gao.gov/new.items/d06421.pdf.

89. *See id.* at 19 (reporting on the amounts of PII purchased by the United States government from data brokers).

> Primarily through governmentwide contracts, [the Justice Department (Justice), Department of Homeland Security (DHS), State Department (State), and the Social Security Administration (SSA)] reported using personal information obtained from resellers [a category of which data brokers are a part] for a variety of purposes, including law enforcement, counterterrorism, fraud detection/prevention, and debt collection. Most uses by Justice were for law enforcement and counterterrorism, such as investigations of fugitives and obtaining information on witnesses and assets held by individuals of interest. DHS also used reseller information primarily for law enforcement and counterterrorism, such as screening vehicles entering the United States. State and SSA reported acquiring personal information from information resellers for fraud detection and investigation, identity verification, and benefit eligibility determination. The four agencies reported approximately $30 million in contractual arrangements with information resellers in fiscal year 2005.

Id.

90. *See, e.g.*, *Japanese Company Claims Fibre-Optic Data Transfer Record*, ABC NEWS ONLINE, Oct. 27, 2005, http://www.abc.net.au/news/newsitems/200510/s1492314.htm (discussing the ever-increasing speed of data transfers). The article discusses how

> [a] Japanese company has developed technology to transmit a two-hour movie in 0.5 seconds, the world's fastest speed achieved with fibre-optic [sic] cables in the field . . . . Kansai Electric used fibre-optic cables on power-transmitting steel

This efficient transfer of aggregated profiles removes pressure from the decision to disseminate personal information as companies do not have to undertake a substantial cost/benefit analysis in terms of time and resources. The low cost and effort involved, combined with the lack of consumer awareness of contemporary data transfers (and the resulting lack of social pressure marshaled against dissemination), makes the profit gained a win–win for the disseminator.[91]

II. CONTEMPORARY COLLECTION AND SALE OF PII: A STUDY OF TWENTY-FIVE HIGH-TRAFFIC WEB SITES

Part I established that companies are incentivized to collect PII and then sell the information on the open market. The discussion demonstrated that the benefits and threats surrounding PII collection are balanced, but that the threats surrounding PII dissemination far outweigh the benefits. Before proposing a legal regime better tailored to govern PII practices, it is important to verify whether e-commerce companies are actually collecting and selling personally identifying information to the extent feared by privacy advocates.[92] The following study addresses this issue by analyzing the twenty-five most highly trafficked Web sites in the United States (the Top 25).[93] The rankings are recent—posted for the month of November 2007—and provide insight into the privacy policies governing hundreds of millions of Web

---

towers to achieve the speed of one terabit per second, which is more than 100 times faster than inter-city data transmissions currently in use.

Id.

91. Because consumers are generally unaware of security breaches and data sales, Congress and state legislatures have passed or are considering notification laws that would have the effect of raising social pressure against companies that act cavalierly with PII. *See, e.g., Senate Vote on Data Brokers Likely This Week*, CONSUMERAFFAIRS.COM, Sept. 26, 2005, http://www.consumeraffairs.com/news04/2005/senate_data_privacy.html (discussing proposals in Congress for a national data breach notification law).

92. *See, e.g., Data Brokers Violating Basic Privacy Laws, Privacy Group Charges*, CONSUMERAFFAIRS.COM, July 11, 2005, http://www.consumeraffairs.com/news04/2005/epic.html ("A privacy watchdog group charges that some data brokers are offering to sell phone calling records [and other particular pieces of PII]. The Electronic Privacy Information Center (EPIC) has filed a complaint with the Federal Trade Commission, asking that these companies be investigated. The group charges the information being offered for sale cannot be obtained without federal laws or regulations."); Patricia Jacobus, *Privacy Advocates Wary of Data-Sharing Standard*, CNET NEWS.COM, Dec. 7, 2000, http://www.news.com/2100-1023-249570.html (discussing new technological standards that help facilitate quick and efficient data transfers, and the fears of privacy advocates about the ability to safeguard PII transferred by such technology).

93. *See* Press Release, comScore, comScore Media Matrix Releases Top 50 Web Rankings for November, at tbl. 3 (Dec. 19, 2007), *available at* http://www.comscore.com/press/release.asp?press=1974.

surfers each month.[94] In conducting the study, each Web site was analyzed to answer the following questions:

1. Does the company post a conspicuously linked privacy policy;

2. Does the company actively collect PII;

3. Does the company passively collect PII;

4. Does the company sell, distribute, or otherwise transfer PII to unrelated third parties or reserve the right to do so (i.e., what are the company's onward transfer practices);

5. What type of choice, if any, does the company provide to consumers; and

6. Does the company grant itself the right to amend its choice options without the consent of its customers and/or without notice?[95]

The results provide a snapshot of contemporary privacy practices as they relate to the collection and dissemination of PII. If the results demonstrate that the major players currently collect and disseminate PII without providing conspicuous and understandable notices to their visitors, the American legal system must react. On the other hand, if companies adequately inform visitors of their PII practices, the legal system should avoid excessive interference with the benefits provided by PII collection and dissemination, and mandate that visitors take some form of personal responsibility and recognize the implications of their PII submissions.

A. Elements of the Study—The Details

Each element of this study pinpoints the current PII practices of each of the twenty-five most visited e-commerce Web sites in America.[96] These companies set an important precedent for the rest of the Internet world because:

1. Smaller e-commerce companies are prone to follow their lead in the information privacy arena;

---

94. *Id.* (showing that hundreds of millions of visitors clicked on these Top 25 Web sites in November 2007).

95. These questions were formulated by this author.

96. There are other information privacy–related elements, such as a company's data security practices or a company's stated values regarding PII, that this study could have examined. The data on these additional categories would be easy to locate, as each category is generally contained in a company's privacy policy. *See, e.g.*, AT&T Privacy Policy, effective June 16, 2006, http://www.att.com/gen/privacy-policy?pid=7666#17 (discussing both of these issues, and how AT&T deals with PII in general). However, the six elements chosen here represent the best way to drill down to a company's PII collection and dissemination practices.

2. Such companies have the potential to collect millions of pieces of PII from their customers every month and then disseminate the information on the open market; and

3. These large companies have the resources and competence to lobby lawmakers regarding PII regulations.[97]

Because data brokers and mass marketers salivate over the vast amounts of PII stored in the Top 25's databases, these prominent companies surely face pressure to part with the data they collect. The results of this study help indicate whether these companies resist this pressure in their privacy policies or whether they succumb to it and currently share, or reserve the right to share, their treasure troves of PII.

1. Conspicuously Linked Privacy Policies

The vast majority of e-commerce companies post privacy policies on their Web sites.[98] However, few companies actually place the full text of their privacy policy on their homepage. This is understandable, as homepages are meant to catch the eye and provide key information about a company's products or services. On the other hand, privacy policies contain important pieces of information and should be readily accessible to any Web site visitor. Because Web users are becoming more comfortable scanning a Web page for content and links to content, it is not privacy-invasive for a company to link its privacy policy to its homepage instead of posting the full text on its

---

97. Large e-commerce companies have the resources to help lobby Congress and state legislatures to go easy on regulating the PII data trade. *See, e.g.*, Dante Chinni, *The Anti-Privacy Lobby*, MOTHER JONES, Jan. 13, 1998, *available at* http://www.motherjones.com/news/feature/1998/01/privacy.html ("[The Direct Marketing association (DMA) is] one of the corporate giants that make up what can best be called America's anti-privacy lobby. Together with information clearinghouses and insurance companies, DMA is making its presence felt on Capitol Hill as Congress deals with the stickiest issue of the electronic age: deciding what personal information is truly personal and what is for sale to the public."). This lobbying power makes it likely that smaller e-commerce companies will follow the guidance of larger companies that have the resources to not only understand the current law and its loopholes but also to set a legal precedent with their lobbying and courtroom practices. *See, e.g.*, Katherine Noyes, *Data Liability, Part 1: Size Doesn't Matter*, E-COMMERCE TIMES, July 27, 2007, http://www.ecommercetimes.com/story/58485.html?welcome=1200179558 (discussing the idea that small e-commerce companies are often subject to legal liability for data mismanagement and that this liability is likely to result in bankruptcy).

98. Karim Jamal et al., *Privacy in E-Commerce: Development of Reporting Standards, Disclosure, and Assurance Services in an Unregulated Market*, 41(2) J. ACCOUNTING RES. 285, 296 (2003), *available at* http://www.blackwell-synergy.com/doi/pdf/10.1111/1475-679X.00104 (discussing a study of 100 high-traffic websites, and stating that ninety-seven of them posted a privacy policy).

homepage. In the end, this study looked for a conspicuously linked privacy policy.

For the purposes of this study, a "conspicuously linked privacy policy" is: (1) any link to a company's privacy policy, (2) containing the word "privacy," (3) appearing somewhere on a company's homepage, (4) published in a font at least as large as any other links in the same vicinity, and (5) likely to appear to a Web site visitor upon first glance. For example, a privacy policy is not conspicuously linked when a visitor is required to click on more than one link to get to the full-text version, when the name of the link does not indicate that privacy information is attached, or when small and discreet links at the very bottom of a Web page must be scanned diligently in order to find the link to the privacy policy. This study analyzed each company's homepage and allowed no more than one minute in an attempt to locate and analyze each company's privacy policy link. The content of the policy was not analyzed for this first step.

2. Active PII Collection

Active PII collection occurs when Web sites ask or require visitors to enter pieces of PII to complete a transaction, create an account, or otherwise navigate the Web site. This information is generally collected via online forms and sent directly to a company database or e-mail account. Active PII collection, unlike the passive form of PII collection discussed below, allows Web site visitors to determine which pieces of personal information they will part with in order to partake in the Web site experience they desire. If a visitor does not wish to enter a credit card number or an address, for instance, she can merely navigate elsewhere on the Web site or end the Web session without completing the intended transaction.

It is a rather simple task to discover whether a company actively collects PII. A quick glance at company Web pages will show the existence of online forms, and company privacy policies will generally disclose such collection. On this note, some companies take a plain English approach and place their active collection policy under a simple privacy policy heading entitled "How We Collect PII" or something similar.[99] Less forthcoming companies, however, mask

99. *See, e.g.*, BREG Inc., Privacy Statement, http://www.breg.com/privacy_statement/default.html (last visited Apr. 4, 2008) ("BREG can actively collect Personal Information on the Site in many different ways, including when you send BREG an e-mail or submit a reply form, request an online newsletter or other materials or literature, submit information to inquire about the purchase of products or services, or submit a resume or other information in connection with a job opportunity.").

active collection in legalese or fail to mention the practice altogether.[100]

Studies show that active PII collection is being widely implemented in the e-commerce community, and the study contained in this article attempts to verify this hypothesis.[101] To categorize this element, each company's homepage and privacy policy was analyzed to determine if the company reserves the right to collect PII actively. Policies obfuscating the practice or discussing it in any manner other than through plain English terminology were labeled as "unclear." The plain English standard adopted in this study tracks closely the "plain English" rules drafted by the United States Securities and Exchange Commission (SEC).[102] According to these standards, a sentence is in plain English if it "uses words economically and at a level the audience can understand. Its sentence structure is tight. Its tone is welcoming and direct. Its design is visually appealing. A plain English document is easy to read and looks like it's meant to be read."[103]

---

100. In some sectors, such as Web sites targeting children under the age of thirteen, Web sites cannot take this approach and must disclose in their privacy policy whether they collect PII actively or passively. *See* Children's Online Privacy Protection Rule, 16 C.F.R. § 312.4(b)(2)(i) (West 2008).

101. *See, e.g.*, FEDERAL TRADE COMMISSION, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE 9 (May 2000), *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf [hereinafter PRIVACY ONLINE] ("Web sites collect a vast amount of personal information from and about consumers. This information is routinely collected from consumers through registration forms, order forms, surveys, contests, and other means, and includes personal identifying information, which can be used to locate or identify an individual." (internal citation omitted)); *see also* Danielle J. Garber, Comment, *COPPA: Protecting Children's Personal Information on the Internet*, 10 J.L. & POL'Y 129, 138 (2001) (citing the FTC's *Privacy Online* study and stating that "[i]nformation collection online, through both active and passive methods, is so widespread that nearly all Web sites routinely collect personal information from consumers" (internal citation omitted)); Eric J. Sinrod & Barak D. Jolish, *Controlling Chaos: The Emerging Law of Privacy and Speech in Cyberspace*, 1999 STAN. TECH. L. REV. 1, 4 (1999) (stating that Web sites commonly collect PII actively from "online registration forms, mailing lists, surveys, user profiles, and order fulfillment forms").

102. *See, e.g.*, OFFICE OF INVESTOR EDUCATION AND ASSISTANCE, U.S. SECURITIES AND EXCHANGE COMMISSION, A PLAIN ENGLISH HANDBOOK: HOW TO CREATE CLEAR SEC DISCLOSURE DOCUMENTS 15-36 (Aug. 1998), *available at* http://www.sec.gov/pdf/handbook.pdf [hereinafter SEC PLAIN ENGLISH HANDBOOK] (discussing the SEC's plain English rules and providing guidance on drafting documents in plain English).

103. *Id.* at 5 (clarifying that the SEC's Plain English standard does not mean a dumbed-down document). There is

> a common misconception about plain English writing. It does not mean deleting complex information to make the document easier to understand. For investors to make informed decisions, disclosure documents must impart complex information. Using plain English assures the orderly and clear presentation of complex information so that investors have the best possible chance of understanding it.

Privacy policies suffer from many of the problems associated with old SEC documents filed prior to the plain English rule and often contain "long sentences, passive voice, weak verbs, superfluous words, legal and financial jargon, numerous defined terms, abstract words, unnecessary details [and] unreadable design and layout."[104] Finally, it is important to note that companies face few legal obligations banning active PII collection or requiring disclosure of active PII collection practices.[105]

3. Passive PII Collection

Unlike active collection, passive PII collection occurs automatically and discreetly, and generally without the knowledge or consent of the Web site visitor.[106] The most common passive PII collection devices are cookies and Web beacons.[107] Both devices are

---

Id.

104. *Id.* at 17 (listing common problems and offering solutions to avoid them throughout the document drafting process).

105. *See, e.g.*, Matthew C. Keck, *Cookies, the Constitution, and the Common Law: A Framework for the Right of Privacy on the Internet*, 13 ALB. L.J. SCI. & TECH. 83, 92-93 (2002) ("In the past, Congress has taken a step-by-step, sector-by-sector approach to encouraging better privacy protections. Hence, American citizens enjoy a strong right of privacy in their video rental records, but a lesser right of privacy in their medical and financial records. As a practical matter, however, the boundary-less Internet and its continually emerging architecture will not allow comprehensive detailed regulations to succeed over the long-term. Congress' inability to enact comprehensive Internet privacy legislation is clear from its history. Further, sector-by-sector regulations leave many gaps and loopholes for information hungry businesses. There is insufficient market motivation for companies to stop collecting information." (internal citations omitted)).

106. *See, e.g.*, Michelle Z. Hall, Comment, *Internet Privacy or Information Piracy: Spinning Lies on the World Wide Web*, 18 N.Y.L. SCH. J. HUM. RTS. 609, 615 (2002) (discussing privacy-invasive aspects of passive PII collection). Hall notes that

> [p]rivacy advocates urge that even when computer users do not actively agree to store cookies, there is a strong possibility for privacy violations, because every time a user logs onto a web site, significant information is given away—including an individual's unique web address and what web site that user visited last. Advocates' contentions are based on the critical point that most user agreements are made passively; in other words, a majority of users are not even aware that they are permitting cookies to be stored. Websites might give the user the choice to "opt-out," but that typically involves "wading through a convoluted process to curb third-party use of data on personal tastes and behavior." If there is no active "opt-out" by the user, the computer typically accepts the cookie without the user's knowledge.

Id. (internal citations omitted).

107. Netscape created the first cookies in 1994. *See* Gaia Bernstein, *The Paradoxes of Technological Diffusion: Genetic Discrimination and Internet Privacy*, 39 CONN. L. REV. 241, 265 (2006). As Bernstein notes,

> [i]n the early days of the Internet, every time a person clicked on a link, their computer's browser entered the new site as a clean slate. No references were left of previous surfing activities. This changed in 1994, however, when Netscape created cookies to facilitate web surfing. Cookies operate by identifying the

small programs set into Web pages that are able to collect information such as Internet protocol (IP) addresses,[108] browser types, and Web sites/Web pages viewed.[109] While cookies and Web beacons are

---

> individual and highlighting trails already taken; for example, by storing passwords or coloring links. Yet, by creating individual trails, cookies eliminated the newly-discovered anonymity enabled by the Internet. *Furthermore, as time went by, cookies became a tool in the hands of commercial profiling companies who used them to collect personal information about Internet users in order to target advertisements. Cookies became one of many new tools that enabled private companies to collect information on the Internet.*

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

108. Keck, *supra* note 105, at 86-87 ("Each separate component of the Internet, such as the computer, router, or network, must have a unique numeric 'address.' A unique identifier is required to enable one connected computer or network to identify and send information to another connected computer or network. A protocol system was developed to designate these numbers, which are known as Internet Protocol addresses or 'IP addresses.'" (internal citations omitted) (internal quotation marks omitted)).

109. A cookie is a

> piece of text that a Web server can store on a user's hard disk. Cookies allow a Web site to store information on a user's machine and later retrieve it. The pieces of information are stored as name-value pairs. For example, a Web site might generate a unique ID number for each visitor and store the ID number on each user's machine using a cookie file.

Marshall Brain, *How Internet Cookies Work*, HOW STUFF WORKS, http://computer.howstuffworks.com/cookie1.htm (last visited Apr. 4, 2008). Notably,

> [t]he vast majority of sites store just one piece of information—a user ID—on your machine. But a site can store many name-value pairs if it wants to. A name-value pair is simply a named piece of data. It is not a program, and it cannot "do" anything. A Web site can retrieve only the information that it has placed on your machine. It cannot retrieve information from other cookie files [or] any other information from your machine.

Id. Web beacons are

> used in combination with cookies to help people running websites to understand the behaviour [sic] of their customers. A web beacon is typically a transparent graphic image (usually 1 pixel x 1 pixel) that is placed on a site or in an email. The use of a web beacon allows the site to record the simple actions of the user opening the page that contains the beacon. The beacon is one of the ingredients of the page, just like other images and text except it is so small and clear that it is effectively invisible. . . . Web beacons are retrieved in the same way and the action of calling the material from another server allows the event to be counted.
>
> When a user's browser requests information from a website in this way certain simple information can also be gathered, such as: the IP address of your computer; time the material was viewed; the type of browser that retrieved the image; and the existence of cookies previously set by that server. This is information that is available to any web server you visit. Web beacons do not give any "extra" information away. They are simply a convenient way of gathering the simplest of statistics and managing cookies.

Web Beacons and Other Tools, *supra* note 56 (providing examples of how companies might use web beacons). One example would be

> a company owning a network of sites may use web beacons in order to count and recognise [sic] users travelling around its network. Rather than gathering statistics and managing cookies on all their servers separately, they can use web beacons to keep them all together. Being able to recognise [sic] you enables the site owner to personalise [sic] your visit and make it more user friendly.

unlikely to collect more sensitive forms of PII—such as addresses and credit card numbers—without the consent of the visitor, it is important for visitors to understand that various pieces of information are being collected discretely and likely without their knowledge.

Similar to active PII collection, a company's passive PII collection is easy to discover if the practice is disclosed in its privacy policy. Some companies take a plain English approach to this disclosure as well and place their passive PII collection policies under a heading entitled "Our Use of Cookies" or something similar. Studies show that passive PII collection is implemented widely in the e-commerce community, and the study discussed in this article attempts to verify this hypothesis.[110] To categorize this element, each company's homepage and privacy policy was analyzed to determine if the company reserves the right to collect PII passively. Policies obfuscating the practice or discussing it in any manner other than through plain English terminology were labeled as "unclear." Finally, it is important to note that companies face few legal obligations to ban passive PII collection or to disclose passive PII collection practices.[111]

4. External PII Sharing

External PII sharing constitutes any distribution of personally identifying information to unrelated third parties. Many instances of PII sharing take the form of sales of PII disseminated in exchange for money.[112] In addition to external sharing, many companies share PII internally with their marketing departments or with their affiliated

---

Id.

110. *See, e.g.*, Lawrence Lessig, *Law Regulating Code Regulating Law*, 35 LOY. U. CHI. L.J. 1, 5 (2003) ("As cookies became more prevalent, however, they had a more general effect on the Internet. Now it was easier for information about users of the Internet to become known. And this in turn meant it was easier to track who did what on the Internet. Thus, as the ability to track increased, this meant that privacy on the Internet decreased. This decrease came not from law. This decrease came from a change in technology.").

111. *See, e.g.*, Keck, *supra* note 105, at 92-93.

112. *See, e.g.*, James P. Nehf, *Shopping for Privacy Online: Consumer Decision-Making Strategies and the Emerging Market for Information Privacy*, 2005 U. ILL. J.L. TECH. & POL'Y 1, 10-11 (2005) ("The collection and trading of personal information is viewed as part of a voluntary undertaking and exchange between consumers who give businesses their personal information and businesses that use or sell the information. The model is under increasing scrutiny, however. Many consumers feel wronged if a firm collects information without their express knowledge and agreement, if the firm sells or rents that information to a third party without permission, or if a consumer's desire to revoke consent is not heeded (for instance, if a consumer is not given the opportunity to remove personal information from the database or restrict its use). (internal citations omitted)).

entities—a practice referred to as "internal sharing."[113] With internal sharing, PII stays within the confines of the company and its affiliates and never reaches the open market and many of the threats lurking outside the collector's confines. While there are threats related to internal PII sharing—such as having aggregated digital profiles outside of the control of the people they identify and subject to data breaches—such threats are not as serious as the threats stemming from external PII sharing. To better understand the seriousness of these threats, recall the discussion in Part I defining the most serious threats from PII dissemination as: (1) the difficulty in verifying the identity of purchasers; (2) the fact that aggregated profiles are efficiently transferred with the click of a mouse; and (3) the idea that information sold into cyberspace is virtually irretrievable.[114]

This study tracks external PII sharing in a similar fashion to active and passive PII collection. Each company's privacy policy was searched for stipulations concerning the sale and/or other form of external sharing of PII. Policies that obfuscated the practice or discussed it in any manner other than through the use of plain English terminology were labeled as "unclear."

5. Type of Customer Choice Offered Regarding PII Sharing

The serious threats posed by the collection and sale of PII have led many privacy advocates to call for mandatory consumer choice pertaining to all uses of collected PII.[115] Although claiming that an individual should be able to exercise complete legal control over all future uses of submitted PII seems a bit of a stretch, companies should, at the very least, be required to provide a conspicuous and comprehensive notice about when, how, and to what extent an individual's personal information is collected and shared externally.

---

113. *See, e.g.*, Key Privacy Policy, https://www.key.com/kfh/privacyPages/PagePrivacyPolicy.jsp?policy=PRVX (last visited Apr. 4, 2008) ("[Key Corp.] engages in several businesses (e.g., banking, mortgage lending, brokerage and investment services, trust administration, asset management and insurance). We may share Personal Private, Transaction and Experience, as well as Identification Information internally to prevent fraud, enhance services, and tailor products and services. Employees are only authorized to share information when a 'business need to know' exists.").

114. See *supra* Part I.C.2 for a discussion of the three most serious threats facing PII upon dissemination.

115. *See* Christine A. Varney, Commissioner, Fed. Trade Comm'n, Address at the Privacy & American Business National Conference: Consumer Privacy in the Information Age: A View From the United States (Oct. 9, 1996), *available at* http://www.ftc.gov/speeches/varney/priv&ame.shtm ("As part of [the FTC's] Privacy Initiative, the FTC held a two-day workshop in June of 1996 to provide industry, privacy advocates and consumer groups a forum to express their ideas for self-regulation and the use of technology to ensure consumer choice.").

Providing a customer with too much power in making such a determination will hinder e-commerce efficiency and may cause companies to conduct less business online or to stop offering Web site services and accounts for free. On the other hand, providing companies too much power to determine the manner in which they collect and sell PII is likely to impact a customer's privacy negatively by exacerbating the threats described in Part I.

There are two primary choice options that companies provide regarding the collection, use, and sharing of PII: (1) an Opt-in Policy and (2) an Opt-out Policy. Neither of these methods is required by law for the average e-commerce company, and the only legal requirement regarding this choice is that a company must honor the pledges it makes in a privacy policy. Unsurprisingly, privacy advocates prefer opt-in policies that create the broadest form of customer choice, while businesses prefer the flexibility provided by opt-out policies.[116] This part of the study attempts to decipher which form each of the Top 25 companies utilizes. Generally, companies list the method of choice under a separate privacy policy subheading titled "Your Privacy Choices." If a company does not offer any choice, this fact was noted in the study. Additionally, privacy policies that obfuscated the practice or discussed it in any manner other than through Plain English terminology were labeled as "unclear." The following two subsections describe these options in more detail.

6. Opt-In Choice for PII Dissemination

Opt-in policies require customers to consent affirmatively before a company can share any PII with unrelated third parties. More specifically, under a typical opt-in policy, a company must provide some form of notice to its customers detailing any proposed use(s) of collected PII and then await explicit permission from such customers before utilizing the information for the purposes specified in the notice.

Opt-in policies are particularly unpopular with the business community because they require more effort, time, and resources than opt-out policies.[117] Because opt-in policies require customers to consent before PII is used externally, companies are forced to locate current and previous customers, draft a notice specifying the intended uses of PII, provide notice, and await customer permission. Under these policies, companies are stuck with their opt-in policy unless and

116. *See, e.g.*, Martha Rogers, *Solving the Opt-in/Opt-out Debate*, INC.COM, Oct. 2002, http://www.inc.com/articles/2002/10/24718.html.

117. *See id.*

until they issue an additional notice memorializing any change to an opt-out or no-choice policy. Additionally, studies show that people generally remain with the information-sharing option first offered by the companies that collect their information.[118] Therefore, if customers submit PII to a company whose policy allows sharing without consent or if a company operates under an opt-out system, customers will not take the time to request that their information remain private or to opt-out. This allows companies that do not need consent to share information to share information more efficiently and change their policies at their own discretion. On the other hand, opt-in policies are especially popular among privacy advocates because no information is shared without the explicit, informed consent of the individuals it identifies.[119]

7. Opt-Out Choice

Opt-out policies require customers to request affirmatively that a company not share any PII with unrelated third parties. More specifically, under a typical opt-out policy, a company must provide some channel for its customers to stop some or all of the instances of external PII sharing. Opt-out policies are the preferred method of choice among companies because they remain free to collect and share, externally, any information they desire. Businesses also make the argument that PII belongs not to the individual it identifies, but to the companies that collect it, mine it, and then offer it for sale.[120] On the other hand, privacy advocates prefer opt-in policies to opt-out policies because of the potential for businesses to disseminate vast amounts of PII without really informing the person it identifies.[121] Companies appear to honor their pledges not to share information when customers opt-out of such disclosure.[122]

---

118. Robert Gellman, *Privacy: Finding a Balanced Approach to Consumer Options*, *in* CONSIDERING CONSUMER PRIVACY: A RESOURCE FOR POLICYMAKERS AND PRACTITIONERS 33-37 (Paula J. Bruening ed., 2003), *available at* http://www.cdt.org/privacy/ccp/consentchoice4.shtml.

119. Yvenne M. King, *From Subway Stations to the Information Superhighway: Compliance Strategies for Musicians To Avoid the Worldwide Entanglement of Privacy Laws*, 4 VAND. J. ENT. L. & PRAC. 129, 135 (2002) ("Although privacy advocates strongly favor the use of opt-in controls, most websites use variations of the opt-out mechanism for marketing purposes.").

120. *See Selling Your Personal Data*, *supra* note 49 (discussing Professor Deighton's belief that companies are the rightful owners of this property and that individuals and the market can come up with the best solution to the problem of PII abuse).

121. *See* King, *supra* note 119, at 135.

122. Jamal et al., *supra* note 98, at 301 ("[T]he opt-out regime works surprisingly well. A user can avoid virtually all the junk e-mail by using an opt-out option.").

8. Privacy Policy Amendments

No company wants to be bound by a decades-old privacy policy. As preferences, technological standards, and laws change, companies are prone to amend their privacy policies to adapt to the times.[123] Therefore, the final element of this study analyzes privacy policy amendments and the choice options given to customers operating under previous policies. In general, a company's privacy policy amendments come in three forms: (1) amendments that are binding on all past, current, and future visitors regardless of consent; (2) amendments that are binding on past customers who transacted with the Web site under an old policy, unless such customers consent to the amendment; and (3) amendments that are binding only on current and future customers, but not on past customers. This part of the study analyzed the Top 25 Web sites to determine the terms governing privacy policy amendments, if any. Again, policies that obfuscated the practice or discussed it in any manner other than through plain English terminology were labeled as "unclear."

123. *See, e.g.*, Morse, Barnes-Brown & Pendleton, PC, *Privacy Rights and Policies Evolve*, IP NEWS 2 (May 2006), *available at* http://www.mbbp.com/resources/iptech/newsletters/pdfs/IPNEWS-privacy.pdf (providing tips to companies creating privacy policies, and giving the following advice: "Check these [privacy] policies periodically against your actual practices to be sure you do what you say you do, that your policies allow for actual *and predictable* uses of collected data, and that your security features are up-to-date and effective").

B. The Results

CHART I—The Results

Company Name	Conspicuous Privacy Policy	Collect Actively	Collect Passively	Share PII Externally	Type of Choice	Binding Amendments (N) = w/ notice
Yahoo! Sites	Yes	Yes	Yes	Unclear	Opt-In	Unclear (N)
Google Sites	No	Yes	Yes	Yes	Opt-In	No (N)
Microsoft Sites (MSN)	Yes	Yes	Yes	Yes	Opt-In	Unclear (N)
Time Warner Network	Yes	Yes	Yes	Unclear	Unclear	No Mention
Fox Interactive Media[124]	Yes	Yes	Yes	Unclear	Unclear	Unclear
eBay	No	Yes	Yes	Yes	Opt-In	Unclear (N)
Amazon Sites	No	Yes	Yes	Unclear	Opt-Out	No (N)
Wikipedia Sites	No	Yes	Yes	Yes	Opt-In	Unclear
Ask Network	No	Yes	Yes	Unclear	Unclear	Unclear (N)
New York Times	Yes	Yes	Yes	Yes	Opt-In	Unclear (N)
Apple Computer	Yes	Yes	Yes	No	N/A	Unclear (N)
Viacom Digital	Yes	Yes	Yes	Unclear	Unclear	No (N)
Wal-Mart	No	Yes	Yes	Yes	Opt-In	Unclear
Target Corporation	Yes	Yes	Yes	Yes	Opt-Out	Unclear (N)

124. *See* News Corporation, http://www.newscorp.com/management/fim.html (last visited Apr. 30, 2008) ("A division of News Corporation . . . , Fox Interactive Media (FIM) is a portfolio of leading social networking, entertainment, sports and information sites that offer a platform and tools for consumers to express themselves, communicate with each other, and engage with media. The company's worldwide network includes such category leaders as MySpace, Photobucket, IGN, FOXSports.com, RottenTomatoes, AskMen, Flektor and more . . . .").

CNET NETWORKS	YES	YES	YES	YES	OPT-IN	YES (N)
THE WEATHER CHANNEL	NO	YES	YES	YES	OPT-IN	YES (N)
FACEBOOK.COM	YES	YES	YES	YES	OPT-IN	YES (N)
ADOBE SITES	YES	YES	YES	YES	OPT-OUT	YES (N)
AT&T, INC.	YES	YES	YES	YES	OPT-IN	YES (N)
VERIZON COMMUNICATIONS	YES	YES	YES	YES	OPT-IN	YES (N)
CBS CORPORATION	NO	YES	YES	YES	OPT-IN	NO
GORILLA NATION MEDIA	YES	YES	YES	UNCLEAR	OPT-OUT	NO MENTION
COMCAST CORPORATION	YES	YES	YES	UNCLEAR	UNCLEAR	UNCLEAR (N)
SUPREPAGES.COM NETWORK	YES	YES	YES	YES	OPT-IN	NO (N)
GLAM MEDIA	YES	YES	YES	YES	OPT-IN	UNCLEAR (N)

Although this study was relatively easy to conduct in terms of cost, effort, and time, actually reading the twenty-five privacy policies was mind numbing. Not all companies drafted their policies in plain English, many obfuscated important privacy options, and some ignored reader-friendly devices, such as subheadings and short paragraphs. If a researcher/privacy scholar writing a paper on the topic found it difficult to sort through this information, it is highly doubtful that even the most privacy-conscious visitor would be willing to make the effort to read these policies and make an informed decision before submitting PII. Most importantly, the results of the study show that many of the fears of privacy advocates regarding PII collection and dissemination are accurate as the vast majority of the Top 25 reserve the right to collect PII and disseminate the information to unrelated third parties. The following analysis probes into each element more deeply and leads into a discussion of the current United States legal regime governing PII.

Chart II—Summary of Study Results[125]

Study Element	Results		Comments
	Yes	No	
Conspicuously Linked Privacy Policy	68%	42%	100% of Web sites posted privacy policies, but eight policies were inconspicuously linked
Active PII Collection	100%	0%	
Passive PII Collection	100%	0%	
External PII Sharing	64%	4%	32% of policies were unclear as to PII sharing practices 96% of companies either share information or obfuscate the practice in their policies Only Apple Computer was clear in its promise never to share PII externally
Binding Privacy Policy Amendments	24%	20%	48% of policies were unclear as to whether amendments are binding 8% of companies made no mention of amendments 72% of policy amendments are either binding or unclear as to the status of policy amendments 24% of policies stated that amendments are binding, but that visitors will receive notice of most changes
	Opt-In	Opt-Out	
Visitor Have A Choice Regarding PII Sharing	60%	16%	20% of policies were unclear as to visitor choice regarding PII sharing 36% of the Top 25 require visitors to request that the company stop sharing PII or are unclear as to how to stop the company from sharing PII

125. *Id.*

1. Conspicuously Linked Privacy Policies

The study shows that only sixty-eight percent of the most highly trafficked Web sites contain a conspicuous privacy policy link. Although each of the remaining eight companies did post a privacy policy, links to such policies were inconspicuously placed on the homepage[126] or placed on Web pages beyond the homepage and required more than one click to reach.[127] Of note, the results revealed that Google, the second-most-visited Web site in the Top 25, and a company currently taking heat for its privacy practices, failed to post a conspicuous link to its privacy policy.[128] In order to find Google's privacy statement, a visitor must click a link titled "About Google"[129] and then look to the bottom of that secondary Web page to find a link to the company's policy.[130] Google's privacy policy text is located three Web pages removed from its homepage and lurks behind a combination of clicks that is not readily decipherable from the homepage itself. As discussed in Part III, however, the failures of Google and the other six companies (of the Top 25) to post conspicuous links are not legally significant. Currently, the United States legal system does not require most e-commerce companies to create a privacy policy, much less provide a conspicuous link to a privacy policy. Therefore, the forty-two of companies failing this test are not

126. *See, e.g.*, National and Local Weather Forecast, Radar, Map and Report, http://www.weather.com/ (last visited Apr. 4, 2008) (posting the link to the company's "privacy statement" at the very bottom of a large homepage and in a font smaller than most of the similar links).

127. *See, e.g.*, Google, *supra* note 12 (failing to post a link to the company's privacy policy on the homepage, and requiring more than one click from the homepage in order to reach the company's privacy policy).

128. *See* Peter Swire, *Google and Privacy: Merger with DoubleClick Prompts New Privacy Guidelines*, CTR. FOR AMER. PROGRESS, Dec. 20, 2007, http://www.americanprogress.org/issues/2007/12/google.html (discussing the Google/DoubleClick merger and arguing that the privacy practices of both companies should be a consideration in antitrust decisions before such mergers are approved); *see also* Justin Mann, *Google Faces Privacy Concerns Over Google Reader*, TECHSPOT.COM, Dec. 27, 2007, http://www.techspot.com/news/28391-google-faces-privacy-concerns-over-google-reader.html (describing a Google program—Google Reader—whose default setting is to share information instead of keeping it private).

129. *See* Google, *supra* note 12.

130. *See* About Google, http://www.google.com/intl/en/about.html (last visited Apr. 4, 2008). An even worse situation occurs on the website Ask.com. *See* Ask.com, www.ask.com (last visited Apr. 4, 2008). Here, visitors must try to determine where to click to find a privacy policy because, similar to the Google homepage, the link is not present on the company's homepage. *See id.* (providing visitors with various choices, such as "MyStuff," "Options," "Advanced," "Skins," "About," "Advertise," and "Careers"). If a visitor guesses correctly and chooses the "About" link, then a second link titled "Site Policies" must be clicked to get to a third page containing a link to the company's privacy policy. *See id.* (click "About" hyperlink, then click "Site Policies" hyperlink).

in violation of the law and may continue to operate their Web sites in this fashion for the foreseeable future, despite growing pressure from the press and privacy advocates.[131]

At the end of the day, a conspicuously linked privacy policy demonstrates that a company is serious about its visitors' understanding of how their personal information will be handled. In addition to visitor comprehension, the following four statements provide ample evidence as to why companies should not hesitate to post such a link:

> 1. A well-written privacy policy need not be long and drawn out, and drafting a privacy statement is not an intellectual feat for the highly educated lawyers and executives working for companies within the Top 25;[132]
>
> 2. Hyperlinks to privacy policies are nearly effortless to insert into the Web page code and do not detract from the appearance of a homepage;[133]
>
> 3. Companies operating at the Top 25 level surely know that privacy advocates and Web site visitors desire to understand company privacy practices; and[134]
>
> 4. Web site visitors have not historically taken the time to read privacy documents drafted and, with this behavior in mind, companies must realize that visitors are

---

131. *See, e.g.*, Grant Gross, *Online Privacy Policies Don't Do Their Job, Critics Say*, PCWORLD, Nov. 4, 2007, http://www.pcworld.com/article/id,139238-c,onlineprivacy/article.html ("More standardization of privacy notices is needed [according to a computer science professor at Oregon State University]. . . . Web users don't want to wade through multiple Web sites with different privacy notices in different locations.").

132. Companies have created the position of Chief Privacy Officer (CPO) to help draft privacy policies and protect visitors' PII. *See, e.g.*, Edward Hurley, *Companies Creating More Chief Privacy Officer Jobs*, SEARCHSECURITY.COM, Jan. 15, 2003, http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci874297,00.html ("CPOs are the public point people for a company's privacy initiatives. In other words, they function as the human face that is responsible for protecting the customer data that's collected and stored by companies."). As for the power of the CPO position, experts claim that a CPO should be at the same level as a company's Chief Information Officer (CIO), and should report to the company's Chief Executive Officer (CEO). *See id.* ("To be truly effective, a CPO shouldn't answer to the CIO . . . . Such an arrangement would lessen the CPO's value because the CIO's main concern is business operations, not privacy. A model arrangement would entail the CPO, CIO and CSO [(Chief Security Officer)] all being on about the same level.).

133. *See, e.g.*, Tryit Editor v1.4, http://www.w3schools.com/html/tryit.asp?filename=tryhtml_links (last visited Apr. 4, 2008) (demonstrating the simplicity of inserting a hyperlink into a Web page).

134. *See, e.g.*, *Fox News/Opinion Dynamics Poll*, July 25, 2006, http://www.foxnews.com/projects/pdf/FOX_229_privacy_web.pdf (showing that, on average, eighty-four percent of respondents were concerned about keeping their PII, especially their medical and financial records, confidential online).

not likely to take the time to determine where a company's policy is posted if it is not obvious.[135]

This evidence leads to the conclusion that companies that fail to post a conspicuous privacy policy link do so deliberately because (1) they are not comfortable with their current privacy policies, and/or (2) they do not want visitors to understand how they collect, store, and disseminate PII. Part IV will discuss how the United States legal system should react to this evidence and ensure 100% compliance with this important element.

2. Active and Passive PII Collection

The study revealed that each of the Top 25 Web sites collects PII actively and passively. These results come as no surprise, as a similar study, conducted during the summer of 2001, found that ninety-eight of the top 100 most-highly-trafficked Web sites implemented cookies to track visitor information and that seventy-eight of these companies allowed third parties to track their visitors' information.[136] Each of these findings show, in dramatic fashion, that e-commerce companies are collecting all types of information—personally identifying information and non-identifying information alike—from their visitors.

On a positive note, each Web site took the time to discuss its active and passive information collection practices in its privacy policy. However, some descriptions were unclear and obfuscated by the lack of a subheading, use of legalese, and inclusion in combination with other, non-privacy-related company policies. For example, compare and contrast the information collection disclosures made by two of the Top 25's most well known companies—Facebook and TimeWarner. Facebook clearly discusses its collection practices under a subheading entitled "The Information We Collect":

> When you enter Facebook, we collect your browser type and IP address. This information is gathered for all Facebook visitors. In addition, we store certain information from your browser using "cookies." A cookie is a piece of data stored on the user's computer tied to information about the user. We use session ID cookies to confirm that users are logged in. These cookies terminate once the user closes the browser. By default, we use a persistent cookie that stores your login ID

135. *See* Gross, *supra* note 131 ("Online privacy policies need to be easier to understand and more conspicuous because few people now actually read them, said panelists at a U.S. Federal Trade Commission workshop on targeted online advertising.").

136. Jamal et al., *supra* note 98, at 295 (discussing the methodology of the experiment and revealing that seventy-nine of the 100 high-traffic Web sites implemented third-party cookies; the study also found that only sixty percent of the 100 companies disclosed the fact that they allowed third-party cookies, and only thirty-nine percent provided a link to the third party's privacy policy).

> (but not your password) to make it easier for you to login when you come back to Facebook. You can remove or block this cookie using the settings in your browser if you want to disable this convenience feature.[137]

Facebook's statement about its passive collection practices is in plain English and the language and concepts are understandable.[138] Facebook clearly explains to its visitors: (1) when their PII is collected (upon entering the Web site); (2) what type of PII is collected (browser type, IP address, and login ID); (3) how the information is collected (via session and persistent cookies); (4) how users can stop collection (disable the cookies via their own browser); and (5) why Facebook collects the information (to make it easier to navigate the company's Web site).[139]

TimeWarner, on the other hand, combines its legal disclaimers with its privacy policy in a link titled "Legal & Privacy."[140] Legal disclaimers and privacy policies are never a good combination if a company wants its visitors to actually click on, read, and understand what happens to their PII. This is especially true if the company places the legal disclaimers before its privacy policy statement.[141] In addition, Time Warner's privacy policy does not present clearly identified subheadings, employs legalese by defining terms in quotes and parentheses, uses unnecessary and legal-sounding words such as "herein" and "therein," and contains convoluted statements, such as:

> As a general policy, no personal information is automatically collected from visitors to this site. However, certain non-personal information of visitors is recorded by the standard operation of Time Warner's Internet servers. . . . By having this

---

137. Facebook, Privacy Policy, effective Dec. 6, 2007, http://www.facebook.com/policy.php (stating the company's privacy policy in plain English and via a conspicuous link from the homepage).

138. This easily understood example stands in stark contrast to most privacy policies where readers "often need 'college-level reading skills' to understand them." Gross, *supra* note 131 (quoting Lorrie Faith Cranor, a Carnegie Mellon University computer science professor who has done research on privacy policies).

139. Keep in mind that, although Facebook's privacy policy is clearly written and laid-out, the company still faces criticism from privacy advocates. *See, e.g.*, Ari Melber, *Facebook: The New Look of Surveillance*, ALTERNET, Jan. 16, 2008, http://www.alternet.org/story/72556/ (discussing Facebook's "news-feed" option and the lack of privacy protection provided by the company when user activities were disseminated via the feed).

140. TimeWarner, Legal & Privacy, http://www.timewarner.com/corp/legal_and_privacy.html (last visited Apr. 4, 2008) [hereinafter TimeWarner Privacy Policy] (stating both the company's legal and privacy policies through one link and on the same template).

141. Dominic Jones, *Proof No One Reads Disclaimers*, IRWEBREPORT, May 3, 2007, http://www.irwebreport.com/daily/2007/05/03/proof-no-one-reads-disclaimers/ (discussing legal disclaimers and the idea that people do not read them—potentially not even the companies that post them—as one company was caught using Washington Mutual's disclaimers for its unrelated products).

> information, Web pages optimized for a particular visitor's computer are automatically made available to that visitor.[142]

These few sentences are worded awkwardly, contain the passive voice, hedge against any concrete commitments, and do not present a clear picture of the company's privacy practices (even when viewed in the context of the entire privacy policy). In addition, the statements do not define what it means when a Web page is "optimized" for a particular user's computer or why it is necessary to refer to the "standard operation" of the company's Internet servers.

3. External PII Sharing

Only one of the Top 25 Web sites—Apple Computer (Apple)—states that the company will not share PII with unrelated third parties.[143] Apple's privacy policy states that the company "takes your privacy very seriously [and that] Apple does not sell or rent your contact information to other marketers."[144] This statement comprises the first two sentences under the subheading "When we disclose your information," and emphasizes the weight Apple places on its no-external-sharing policy.[145]

---

142. TimeWarner Privacy Policy, *supra* note 140. The following preamble to CBS Corporation's privacy policy is filled with even more legalese, and must certainly be perplexing to visitors:

> This Privacy Policy applies to certain Web sites which are owned and/or operated by or on behalf of CBS Corporation and other affiliated entities controlled by, or under common control with, such parties (each such web site being individually referred to herein as the "Web Site"). If you have arrived at this Privacy Policy by "clicking" on an authorized link from a Web Site, then this Privacy Policy applies to such Web Site, and the individual entity which owns and/or operates the particular Web Site from which you "clicked" to this Privacy Policy via an authorized link shall be referred to herein as "Sponsor," "we" or "us." Sponsor respects the privacy of its users, and this Privacy Policy explains what information we collect on our Web Site and how we use such information. Please read this Privacy Policy carefully. In addition, please review the Terms of Use posted at the Web Site, which governs your use of the Web Site. Your use of our Web Site indicates to us that you have read and accepted our privacy practices, as outlined in this Privacy Policy and our Terms of Use.

CBS Corporation, Privacy Policy, http://www.cbscorporation.com/privacy/index.php [hereinafter CBS Privacy Policy] (last visited Apr. 4, 2008).

143. Apple Customer Privacy Policy, http://www.apple.com/legal/privacy/ (last visited Apr. 4, 2008) (stating that the company reserves the right to share PII internally and with its "service providers, vendors, and strategic partners"). Each of the Top 25 Web sites reserves the right to share PII internally and with the company's vendors and/or strategic partners. Without the ability to share internally in this fashion, companies would have a hard time delivering their products and services to customers.

144. *Id.*

145. *Id.*

On the other hand, fifteen of the Top 25 companies reserved the right to share PII externally.[146] Most of the companies in this classification require visitors to opt-in before sharing PII. For instance, The New York Times posts a privacy policy stating: "If you have registered online to one of our sites, The New York Times will not sell, rent, swap or authorize any third party to use your e-mail address without your permission."[147] A few of the companies in this classification explicitly reserve the right to share PII externally unless visitors affirmatively opt-out. For instance, Target Corporation—ranked number fourteen on the Top 25 list—states in its privacy policy that the company "may share information with carefully selected vendors, business partners and other organizations, which are not part of the Target family. These companies and organizations may use the information we share to provide special opportunities and offers to you."[148]

The remaining nine companies posted privacy policies that were unclear about the practice of external PII sharing.[149] For example, the Ask Networks (particularly the brand Ask.com) post a privacy policy with a subheading discussing how the company uses PII.[150] This section, however, states that Ask.com does "not share your personally identifiable information with third parties for the purpose of enabling them to send you information about their products."[151] However, a few sections below, the policy vaguely discusses the idea that Ask.com may share a visitor's search queries, which may contain PII, to third parties for advertising purposes.[152]

---

146. *See supra* Chart I.

147. The New York Times Privacy Policy Highlights, http://www.nytimes.com/ref/membercenter/help/privacysummary.html (last visited Apr. 4, 2008). Additionally, CBS's privacy policy states that it "does not rent, sell or otherwise disclose your PII to third parties unless disclosed to you at the time such information is collected or unless you otherwise give consent." CBS Privacy Policy, *supra* note 142.

148. Target, Privacy Policy, http://sites.target.com/site/en/spot/page.jsp?title=privacy%5Fpolicy (last visited Apr. 4, 2008) (stating that visitors who do not desire this external PII sharing must opt out: "If you do not want us to share information you provide to our website with vendors, business partners and other organizations that are not part of the Target family, please click here").

149. A subject for future research would entail discovering whether the companies with the unclear external sharing policies actually are selling PII on the open market.

150. Privacy Policy for Ask.com, effective Feb. 25, 2008, http://about.ask.com/en/docs/about /privacy.shtml.

151. *Id.*

152. *Id.* Ask.com's Privacy Policy states:

> Some elements on the [Ask.com] Sites, such as news content, our Smart Answers, or the sponsored links advertising on our search results pages, are supplied to us by third parties under contract. We may supply some information we gather from you to those third parties so that they can provide those elements for display on the Sites. We may share the following information with third

Similarly, Yahoo! states that it "does not rent, sell, or share personal information about you with other people or non-affiliated companies except to provide products or services you've requested, when we have your permission, or under the following circumstances," and then lists some vague circumstances.[153] For example, Yahoo! is allowed to share PII if:

> We have a parent's permission to share the information [from] a child under age 13. Parents have the option of allowing Yahoo! to collect and use their child's information without consenting to Yahoo! sharing of this information with people and companies who may use this information for their own purposes.[154]

Such statements make it difficult for visitors to determine if and when a company is allowed to share its PII with unrelated third parties. These results point to the conclusion that companies are purposefully obfuscating their external sharing practices so that they maintain the ability to share PII as they desire without facing the repercussions that follow from a statement that clearly reserves this right. Otherwise, their privacy policy statements would capitalize on the social gain that comes with a clearly written statement like "this Corporation promises *never* to share your PII externally!"

4. Type of Customer Choice Offered Regarding PII Sharing

Only Apple Computer, the sole company that promises not to share PII, is relieved from discussing how visitors can stop the company from sharing PII. The remaining companies should disclose how visitors choose what happens to the PII they submit, if they have any choice in the matter. Of the twenty-four companies in this classification, four require visitors to opt-out of PII sharing (sixteen percent), fifteen require visitors to opt-in (sixty percent), and six are unclear as to a visitor's choice options (twenty-four percent).

Similar to the findings above, a recent study found that customers choosing to receive external marketing messages (or customers who fail to opt-out) can quickly become overwhelmed.[155] The study group registered accounts with sixty-nine Web sites and chose to opt-in to external sharing of their PII; over a twenty-six-week period, the opt-in e-mail addresses received over 15,000 e-mail

---

> parties . . . the search queries you submit. For example, when you submit a query we transmit it . . . to our paid listing providers in order to obtain relevant advertising to display in response to your query.

Id.

153. Yahoo! Privacy Policy, effective Nov. 22, 2006, http://info.yahoo.com/privacy/us/yahoo/details.html.

154. *Id.*

155. *See* Jamal et al., *supra* note 98, at 300-01.

messages, or over eighteen percent of the average volume of e-mail that such accounts received on average before the registrations.[156] In the end, the study concluded that "once an e-mail address is sold to third-party marketers, the amount of junk e-mail received increases steadily over time, and there appears to be no way to recoup the privacy of the sold addresses."[157] The huge increase in solicitations combined with the fact that ninety-six percent of the Top 25 reserve the right to share PII indicates the seriousness of this issue. Web site visitors deserve a clear description of how a company shares PII and whether the company provides a way to stop such sharing.

5. Privacy Policy Amendments

In all, ninety-two percent of the Top 25 discussed amendments in their privacy policies.[158] Five companies promised that amendments would not take the place of past policies under which customers submitted PII (i.e., the amendments are not binding on past customers).[159] Four of these five companies stated that they provide visitors with notice of amendments. For example, CBS Corporation binds visitors to its current privacy policy as soon as they utilize the Web site, but policy amendments changing PII uses are not binding:

> [CBS] reserves the right to modify, alter or otherwise update this Privacy Policy at any time in its sole discretion. We will post any changes here, so be sure to check back from time to time. *However, we will only use the PII you provide to the Web Site in a manner consistent with this [current] Privacy Policy, unless you give us your consent.*[160]

---

156. *Id.* at tbl. 3 (showing that the stream of e-mail advertisements grew in size over time as the companies sold more and more PII). Interestingly, very few marketing phone calls were made to either the opt-in or the opt-out accounts causing the authors to state "independent of opt-in or opt-out, junk phone calls are not an important consequence of e-commerce registrations." *Id.* at 302 (stating that only twenty-two phones calls in total were made to the phone numbers on the accounts forming the study; this finding is in stark contrast to the nearly 16,000 e-mail solicitations resulting from the experiment). The same results hold true for postal mail as very few postal mail solicitations were received at the addresses for the 100 accounts. *Id.* (finding that only "27 pieces of postal mail, of which 15 came from a single registration," were delivered to the addresses in the study).

157. *Id.* at 300 (discussing one Web site that accounted for over fifty-six percent of all the e-mail solicitations—over 8,000 e-mail messages—during the twenty-six-week period. This suggests that individual Web sites are able to sell PII many times to many different purchasers, all of whom have the ability to flood the customer's account with marketing e-mails.). Problematically, the typical customer will have no way of determining which Web sites will be the direct cause of the e-mail flood.

158. *See supra* Chart II.

159. *See id.*

160. CBS Privacy Policy, *supra* note 142 (emphasis added); *see also* Amazon.com Privacy Notice, http://www.amazon.com/gp/help/customer/display.html?ie=UTF8&nodeId=468496 (last visited Apr. 4, 2008) ("Our business changes constantly, and our Privacy

From a different perspective, six companies stated that privacy policy amendments are binding on visitors regardless of the version under which they submitted PII, and another twelve are unclear about their policies in this area.[161]

Another major difference between companies in the Top 25 lies in whether Web site visitors will be notified of PII policy changes or be forced to discover the changes on their own. Yahoo! takes the most common approach among the Top 25 and reserves the right to modify its privacy policy at any time and only promises notice of "significant" changes: "Yahoo! may update this policy. We will notify you about significant changes in the way we treat personal information by sending a notice to the primary email address specified in your Yahoo! account or by placing a prominent notice on our site."[162] Yahoo!'s policy does not define which changes the company considers significant enough to trigger this notice requirement. On a similar note, the company neglects to mention when a visitor will receive an e-mail notice as opposed to merely a prominent notice on the Yahoo! Web site. These issues are simple enough to clarify, and visitors deserve to know the answers before they submit PII. Finally, no company was bold enough to make privacy policy amendments binding on visitors without providing at least some form of notice.

The discussion, to this point, makes it clear that many of the fears of privacy advocates have come to life in the twenty-first century e-commerce environment. Large, highly trafficked company Web sites collect PII from visitors, both actively and passively. The vast majority of these companies also reserve the right, either expressly or via a lack of clear privacy policies, to share the information externally. Although visitors generally have a choice in the matter, a few policies require individuals to opt-out of external sharing—an action that few visitors actually undertake. The next Part describes the current United States legal regime as it pertains to PII collection and dissemination, and the final Part discusses a way to tailor the current system to protect PII more thoroughly in this mass-collection environment.

Notice and the Conditions of Use will change also. . . . *Unless stated otherwise, our current Privacy Notice applies to all information that we have about you and your account.* We stand behind the promises we make, however, and will never materially change our policies and practices to make them less protective of customer information collected in the past without the consent of affected customers." (emphasis added)).

161. *See supra* Chart II.

162. Yahoo! Privacy Policy, *supra* note 153.

III. CURRENT LAW GOVERNING THE COLLECTION AND EXTERNAL SHARING OF PII

Part II identified the serious threats from the collection and dissemination of PII. Part II demonstrated that 100% of today's most visited Web sites collect PII, and that ninety-six percent of such companies either reserve the right to share this information externally or obfuscate their policy on PII dissemination. These results emphasize that the laws governing information privacy must adequately address these threats or they will leave the interests of Internet users across the country relatively unprotected. Part II also provided evidence that much of responsibility for such protection should fall on the collectors and sharers of PII because the information rests primarily within their control at the point at which these threats are most serious: after collection and during the selection of dissemination partners.[163] This Part, divided into two sections, discusses the idea that the United States legal system and its sectoral approach to information privacy is ill-prepared to deal with the reality of today's massive PII collection and dissemination. This analysis will lead into the final Part of the article, proposing a solution by tweaking the law to protect PII without excessively hindering e-commerce efficiency.

Unlike the European Union, the United States legal system does not govern information privacy in any comprehensive manner.[164]

---

163. Although the most serious threats target PII after dissemination, companies that collect information can hinder such threats tremendously by taking the privacy of their visitors' information more seriously.

164. In 1995, the European Union (EU) passed Directive 95/46 to protect EU citizens' fundamental right to privacy in their PII while at the same time attempting to ensure that PII is able to flow freely between each of the EU's member states. *See* Council Directive 95/46, 1995 O.J. (L 281) (EC). The EU Privacy Directive created a comprehensive legal regime, requiring each EU member state to enact substantial regulations covering eight data protection principles:

1. *Purpose Limitation Principle*: PII should only be used for a specific purpose;

2. *Data Quality & Proportionality Principle*: PII collected should be accurate and up-to-date;

3. *Transparency Principle*: individuals should be notified of the PII uses and as to who controls the information;

4. *Access, Rectification and Opposition Principle*: individuals should have access to collected PII, be able to rectify inaccurate information and oppose particular PII uses;

5. *Security Principle*: PII collectors should take technical and organizational precautions to protect stored PII;

6. *Restriction on Onward Transfers Principle*: PII collectors should not externally transfer any PII to countries that do not have adequate data protection regulations;

In fact, the American approach at the federal level is sectoral in nature,[165] and protects only certain individuals in certain economic sectors against certain privacy-invading threats.[166] For instance, the

---

7. *Sensitive Data Principle*: PII collectors must take extra precautions with sensitive PII; and

8. *Enforcement and Remedies Principle*: Individuals should be able to enforce these regulations and should be entitled to a remedy upon a violation.

Virginia Boyd, *Financial Privacy in the United States and the European Union: A Path to Transatlantic Regulatory Harmonization*, 24 BERKELEY J. INT'L L. 939, 958-59 (2006); *see* Edward C. Harris, *Personal Data Privacy Tradeoffs and How a Swedish Church Lady, Austrian Public Radio Employees, and Transatlantic Air Carriers Show that Europe Does Not Have the Answers*, 22 AM. U. INT'L L. REV. 745, 750-60, 798-800 (2007) (discussing the similarities and differences between the United States information privacy regime and the EU Privacy Directive, and concluding that a comprehensive statute may not be the best choice for the United States Congress); Marsha Cope Huie et al., *The Right to Privacy in Personal Data: The EU Prods the U.S. and Controversy Continues*, 9 TULSA J. COMP. & INT'L L. 391, 403-07 (2002) (comparing the United States regulatory regime with the EU Privacy Directive, stating that the EU is far ahead of the United States in protecting PII and providing ways to strengthen the United States system).

165. *See, e.g.*, The Business Roundtable: Digital Economy Task Force, *Information Privacy: The Current Legal Regime* 2 (July 2001), *available at* http://www.businessroundtable.org/pdf/617.pdf [hereinafter Business Roundtable Report] ("Privacy protection is currently governed by a sectoral system of laws, regulations and industry-imposed guidelines.").

166. *See* Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506 (2000) (authorizing the Federal Trade Commission to promulgate regulations governing companies with Web sites targeting children under the age of thirteen); Cable Communications Policy Act of 1984, Pub. L. No. 98-549, 98 Stat. 2794 (codified as amended at 47 U.S.C.A. §§ 521-560 (West 2008)) (regulating cable television providers' use of certain customer PII by state driver's license agencies); Driver's Privacy Protection Act of 1994, Pub. L. No., 103-322, 108 Stat. 2099 (codified as amended at 18 U.S.C.A. §§ 2721-2725 (West 2008)) (regulating the disclosure of PII); Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.A. (West 2008)) (regulating the disclosure of certain PII by electronic communications service providers and certain interceptions of electronic information); Electronic Fund Transfer Act of 1978, 15 U.S.C. §§ 1693-1693r (2000) (requiring the notification of customers when third parties access certain pieces of PII during electronic funds transfers); Fair and Accurate Credit Transactions Act of 2003, 15 U.S.C.A. §§ 1681-1681x (West 2008) (amending the Fair Credit Reporting Act of 1970, *infra*, to "prevent identity theft, improve resolution of consumer disputes, improve the accuracy of consumer records"); Fair Credit Reporting Act of 1970, Pub. L. No. 91-508, 84 Stat. 1128 (codified as amended at 15 U.S.C. §§ 1681-1681x (2000)) (regulating the disclosure of certain pieces of PII used in credit decisions); Family Educational Rights and Privacy Act of 1974, Pub. L. No. 93-380, 88 Stat. 484 (codified as amended at 20 U.S.C.A. § 1232g (West 2008)) (regulating access to and disclosure of student records); Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended primarily in scattered sections of 18, 29, and 42 U.S.C.A. (West 2008)) (regulating the use of medical PII by health care providers and heath insurance providers); Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (codified as amended in relevant part at 15 U.S.C. §§ 6801-6809, 6821-6827 (2000)) (regulating the use of financial PII by certain financial services providers); Identity Theft Assumption Deterrence Act of 1998, Pub. L. No. 105-318, 112 Stat. 3007 (codified as amended at 18 U.S.C.A. §§ 1001-1028 (West 2008)) (regulating the unauthorized possessing, procuring or transferring of certain

federal Children's Online Privacy Protection Act (COPPA) protects only a small segment of Americans—children under the age of thirteen who surf the Web—against certain PII submissions by requiring companies targeting such children to post a privacy policy.[167] Similarly, the federal Gramm-Leach-Bliley Act (GLBA) requires certain companies—those significantly engaged in financial activities—to provide privacy policies detailing PII collection and distribution practices, and include an opt-out choice before sharing PII externally.[168] These laws were never designed to protect the average consumer against the serious threats looming over a multi-billion dollar e-commerce world filled with millions upon millions of online retail transactions.[169]

This sectoral structure exposes giant regulatory gaps regarding the collection and dissemination of PII.[170] For example, federal law does not require the vast majority of companies conducting e-commerce to (1) create a comprehensible and succinct privacy policy detailing their PII practices;[171] (2) post a conspicuous link to any

---

forms of PII to commit an unlawful activity); Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified as amended at 5 U.S.C.A. § 552a (West 2008)) (regulating certain governmental uses of PII); Privacy Protection Act of 1980, Pub. L. No. 96-440, 94 Stat. 1879 (codified as amended at 42 U.S.C. § 2000aa (2000)) (regulating government access to media work product); Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, 92 Stat. 3641 (codified as amended at 12 U.S.C. §§ 3401-3420 (2000)) (regulating outside access to PII collected by financial institutions); Telephone Consumer Protection Act of 1991, Pub. L. No. 102-243, 105 Stat. 2394 (codified at 47 U.S.C.A. § 227 (West 2008)) (regulating the use of PII by telemarketers); Video Privacy Protection Act of 1988, Pub. L. No. 100-618, 102 Stat. 3195 (codified as amended at 18 U.S.C.A. §§ 2701-2712 (West 2008)) (regulating the use of PII in video rental transactions).

167. 15 U.S.C. § 6502(b)(1) (2000) (requiring Web site operators that collect PII from children under thirteen to, among other things, provide notice as to what types of PII are collected as well as how such information is used and disclosed).

168. Gramm-Leach-Bliley Act of 1999, 15 U.S.C. § 6802(a)-(b) (2000) (banning covered financial institutions from disclosing non-public PII to unrelated third parties without providing a clear and conspicuous, written or electronic, privacy policy which provides customers with a chance to opt-out of any PII disclosure); *see* 15 U.S.C. § 6803(a)-(c) (2000) (discussing more specifically the legally required privacy policy).

169. *See, e.g.*, Enid Burns, *Online Retail Revenues to Reach $200 Billion*, CLICKZ NETWORK, June 5, 2006, http://www.clickz.com/showPage.html?page=3611181 ("[Online] retail is expected to hit $211.4 billion in 2006, a 20 percent gain over revenues of $176.4 last year.").

170. *See, e.g.*, Steven Labaton, *U.S. Is Said To Seek New Law To Bolster Privacy on the Internet*, N.Y. TIMES, May 20, 2000, at A1 ("'The bottom line is that the privacy gap between the safeguards in place and the intrusions seems to be growing not narrowing, and that has as much as anything to do with the lack of enforcement at the F.T.C. . . . There is little indication that self-regulation is working'" (quoting Marc Rotenberg, privacy advocate).

171. Industry self-regulation is the only national "enforcement" mechanism available to require companies outside of United States sectoral regulations to post privacy policies. *See, e.g.*, Jeri Clausing, *Group Proposes Voluntary Guidelines for Internet Privacy*, N.Y.

privacy statement; (3) disclose the external uses of PII (either collected actively or passively); (4) disclose visitor consent options regarding PII collection and dissemination or regarding privacy policy amendments; or (5) refrain from widely disseminating PII to the highest bidder on the open market.[172]

Congress's inaction leaves each of these issues in the hands of the e-commerce industry to self-regulate.[173] To date, and as the results of the study in Part II help demonstrate, industry efforts have failed even to require e-commerce companies to link their privacy policies conspicuously or to provide adequate protection of PII against the serious threats targeting its collection and distribution. At the local level, a few state legislatures have recognized the seriousness of this issue as well as Congress's inaction, and have enacted their own regulations regarding the collection and sale of PII.[174] Problematically, however, these local laws are insufficient to solve what has become a national problem.[175]

TIMES, July 21, 1988, at D4 ("[In 1988, t]he F.T.C. . . . surveyed 1,400 Web sites and issued a report that found private-sector initiatives seriously lagging, especially regarding information collected from and about children."). Privacy advocates have claimed for decades that self-regulation is not enough to properly protect PII. *See* Jeri Clausing, *Report Rings Alarm Bells About Privacy on the Internet,* N.Y. TIMES, Feb. 7, 2000, at C10. As an interview with a privacy advocate revealed:

> [B]aseline laws were needed to spell out for companies what they can and cannot do with private information they collect online and to allow consumers to take civil action when they think their rights have been violated. "At the moment . . . saying self-regulation is the way we are going to go, that basically says, 'Do whatever you want or do as little as you want' . . . . That's exactly the wrong message to send to companies that have strong economic incentives to collect and use personal information."

Id. See discussion *infra* Part IV(A) for a more in-depth discussion of the law, or lack thereof, surrounding company privacy policies as it relates to PII collection and external sharing.

172. *See, e.g.*, Goldman, *supra* note 48, at 355 ("[U]nder the current regulatory model (or absence thereof) for online information, there is almost no way for a user to prevent the collection of . . . personal information."). Again, a few sector-based federal laws regulate a company's collection and external use of PII. *See, e.g.*, Fair Credit Reporting Act of 1970, Pub. L. No. 91-508, 84 Stat. 1128 (codified as amended at 15 U.S.C. §§ 1681-1681x, 1681s-3 (2000)) (prohibiting certain uses of PII within a consumer report for external marketing purposes).

173. *See, e.g.*, William S. Challis & Ann Cavoukian, *The Case for a U.S. Privacy Commissioner: A Canadian Commissioner's Perspective*, 19 J. MARSHALL J. COMP. & INFO. L. 1, n.3 (2000) ("Privacy protection on the Internet has largely been left to industry self-regulation, which has received strong encouragement and support from the Federal Trade Commission, the U.S. Department of Commerce and the White House." (citation omitted)).

174. See *infra* Part III(A)-(B) for a detailed discussion of the various state laws in play in this area.

175. *See, e.g.*, Business Roundtable Report, *supra* note 165, at 3 ("Many states have undertaken their own laws and regulations concerning the confidentiality of certain information about its [sic] citizens. If states continue to deal with the privacy issue

The few federal or state laws that actually touch upon the collection and sale of PII generally fall into one of two classifications: (1) privacy policy regulations or (2) external dissemination regulations. The remainder of this Part shows where the law stands today regarding these two classifications and how this regime inadequately protects individuals from the various threats targeting PII collection and dissemination.

A. Federal and State Privacy Policy Regulations

A privacy policy represents a company's commitment regarding the collection, storage, and use of an individual's PII. The creation and posting of a privacy policy is an inexpensive and straightforward way for a company to disclose its privacy standards to all Web site visitors. If individuals are able to locate and understand a company's collection and external use policies, they will be able to make informed decisions before submitting their PII online. Aside from a few sectoral state and federal laws, California is the only jurisdiction that has mandated that most companies doing business with its residents post an electronic privacy policy.[176]

At the federal level, Congress has chosen not to mandate the posting of privacy policies for most companies operating Web sites in interstate commerce.[177] The federal sectoral-based laws mentioned above deal with broader information privacy issues, and only indirectly touch on privacy policies. As discussed above, currently, only companies targeting children under thirteen,[178] certain financial

---

individually through laws and regulations, they risk worsening this patchwork of rules [i.e., federal sectoral regulations]. This will create considerable confusion as well as direct and indirect costs to businesses to comply—costs that will inevitably be borne by consumers.").

176. CAL. BUS. & PROF. CODE § 22575 (West 2008).

177. *See, e.g.*, Corey A. Ciocchetti, *E-Commerce and Information Privacy: Privacy Policies As Personal Information Protectors*, 44 AM. BUS. L.J. 55, 72-73 (2007) ("In the United States today, a handful of federal and state laws combine with private-sector self-regulation to govern the content and use of electronic privacy policies. *Within this environment, the relevant regulations are targeted toward a few specific economic sectors, leaving the majority of e-commerce operations outside of their reach.* The only recompense available to Web site visitors suffering injuries stemming from information privacy violations rests on the small chance of an enforcement action brought by the FTC or by a state attorney general." (emphasis added) (internal citations omitted)).

178. 15 U.S.C. § 6502(b)(1)(A)(i) (2000). The statute states:

> [T]he operator of any website or online service directed to children that collects personal information from children or the operator of a website or online service that has actual knowledge that it is collecting personal information from a child [must] provide notice [i.e., a privacy policy] on the website of what information is collected from children by the operator, how the operator uses such information, and the operator's disclosure practices for such information.

services companies,[179] and certain healthcare providers[180] are required to create and post an electronic privacy policy. The vast majority of e-commerce companies that fall outside of these specific industry sectors face only weak self-regulatory pressure from companies and industry groups that choose to take information privacy seriously. As an example, IBM threatened to pull all of its advertising from Web sites that failed to post a privacy policy.[181] While this social pressure to

---

Id.

179. 15 U.S.C. § 6802 (2000) ("Except as otherwise provided in this subchapter, a financial institution may not, directly or through any affiliate, disclose to a nonaffiliated third party any nonpublic personal information, unless such financial institution provides or has provided to the consumer a notice [i.e., a privacy policy] that complies with [this title]"); *see also* Xinguang Sheng & Lorrie Faith Cranor, *An Evaluation of the Effect of US Financial Privacy Legislation Through the Analysis of Privacy Policies*, 2 I/S: J.L. & POL'Y INFO. SOC'Y 943, 946 (2006) (discussing the history and composition of the Gramm-Leach-Bliley Act). Sheng and Cranor summarized the law as follows:

> The Financial Modernization Act of 1999, also known as the "Gramm-Leach-Bliley Act" ("GLB") was signed into law on November 12, 1999 and became effective on July 1, 2001. The law modified previous federal laws and "allow[ed] for the creation of a financial holding company. . . . Such companies may include a commercial bank and subsidiaries that conduct financial activities or activities incidental to financial activities." In other words, GLB enables banks to engage in a whole line of financial activities. Late in the legislative process, legislators were concerned at the prospect that the consolidation of the financial industry would lead to privacy invasions. As a result of this concern, Title V was added to GLB. Title V requires financial institutions to provide an initial "clear and conspicuous notice of privacy policies and practices to all customers," an annual notice of their privacy policies, and an opportunity for consumers to opt out of disclosing protected financial information to nonaffiliated third parties. The FTC's final rule specifies the minimum information that should be included in the privacy notices and provides examples of GLB-compliant privacy policies.

Id. (internal citations omitted).

180. *See* Notice of Privacy Practices for Protected Health Information, 45 C.F.R. § 164.520(a)(1) (West 2008) (stating, in relevant part, that "an individual has a right to adequate notice of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information"). The Notice of Privacy Practices for Protected Health Information provides that "the covered entity [various health care providers, heath insurance companies and health care clearinghouses] must provide a notice [(i.e., a privacy policy)] that is written in plain language and that contains" various information regarding the uses and external sharing of the personally identifying health information and the individual's rights regarding this information once collected. *Id.* § 164.520(b)(1)(i)-(viii).

181. *See* Jeri Clausing, *I.B.M. Vows To Pull Ads from Web Sites That Lack Clear Policies on Protecting Consumer Privacy*, N.Y. TIMES, Apr. 1, 1999, at C4. In 1999, I.B.M. vowed that it

> would pull its ads from Web sites that lacked clear privacy policies. In a letter sent to 350 Web sites it advertises with in the United States and Canada, I.B.M. said that as of June 1 it would advertise only on sites that posted such policies. The announcement, thought to be the first by a United States company, comes as the Federal Trade Commission, Congress and the European Union are closely monitoring the effectiveness of efforts by on-line businesses to police themselves on the issue of buying and selling personal data they gather.

protect PII is admirable, it is toothless from a mandatory compliance perspective.

The federal government has stepped in, however, if a company makes privacy promises that it subsequently breaks.[182] At that point in the process, the FTC may bring a complaint against a company under its unfair and deceptive practices enforcement authority stemming from the Federal Trade Commission Act.[183] To date, the FTC has brought nearly twenty high-profile cases against companies with alleged unfair or deceptive PII practices.[184] Therefore, an individual unhappy with the PII collection practices of a particular company and desiring legal action would be forced to wait until the company breaks a privacy promise in relation to such information, and then hope that the FTC, with its rather limited resources, steps in to halt the practice. This lack of targeted federal regulations combined

---

Id. At the time, I.B.M. claimed that "its own recent survey had found that only 30 percent of the 800 sites worldwide from which it buys ads had privacy policies posted." *Id.*

182. *See, e.g.*, Business Roundtable Report, *supra* note 165, at 3 ("[The] U.S. federal government's involvement in privacy also extends to the Federal Trade Commission (FTC), the agency responsible for ensuring customer protection and market competition. The FTC has sanctioned companies that have violated their own privacy policies, on the basis of those companies having thereby engaged in unfair or deceptive practices, and they will continue to do so under their mandate.").

183. 15 U.S.C. § 45(a)(1), (n) (2000). The FTC describes its consumer protection enforcement powers as follows:

> The basic consumer protection statute enforced by the Commission is Section 5(a) of the [Federal Trade Commission] Act, which provides that "unfair or deceptive acts or practices in or affecting commerce are declared unlawful."
>
> "Unfair" practices are defined to mean those that "cause[] or [are] likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."

FED. TRADE COMM'N, OFFICE OF THE GENERAL COUNSEL, A BRIEF OVERVIEW OF THE FEDERAL TRADE COMMISSION'S INVESTIGATIVE AND LAW ENFORCEMENT AUTHORITY: ENFORCEMENT AUTHORITY II.A, Sept. 2002, *available at* http://www.ftc.gov/ogc/brfovrvw.shtm (internal citations omitted). The FTC considers a broken privacy policy promise to be an unfair or a deceptive trade practice "in or affecting commerce." *See, e.g.*, First Amended Complaint for Permanent Injunction and Other Equitable Relief, Fed. Trade Comm'n v. Toysmart.com, LCC, Civ. Action No. 00-11341-RGS, 2000 WL 1523287 (D. Mass. Aug. 21, 2000) (charging Toysmart.com with a deceptive practice in violation of the Federal Trade Commission Act when it sold a PII database as an asset in bankruptcy after the company's privacy policy promised that no PII would be sold).

184. *See, e.g.*, Privacy Initiatives, http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html (last visited Apr. 4, 2008) (listing links to cases brought by the FTC under its unfairness and deception regulatory authority). A typical FTC complaint in this area locates a company's privacy policy and then demonstrates how certain company actions violate the policy. *See, e.g.*, In Re Gateway Learning Corp., Decision & Order No. C-4120 (FTC 2004), *available at* http://www.ftc.gov/os/caselist/0423047/040917do0423047.pdf (stipulating that Gateway Learning Corp. rented its customers' PII to outside entities in violation of its posted privacy policy and instituting various penalties for its violation of the Federal Trade Commission Act).

with the threat of FTC scrutiny on broken privacy promises provides incentives for companies (1) to fail to post a privacy policy at all; or (2) to create a privacy policy filled with legalese and loopholes designed specifically to avoid breaking any promises.[185]

At the state level, various state legislatures have attempted to bridge the gap between the emerging threats to PII and the sectoral approach to information privacy taken under federal law. As mentioned previously, California's Online Privacy Protection Act[186]—the first law of its type in the nation—requires that anyone collecting PII from a California resident must:

1. Create and post a privacy policy;[187]

2. Identify the types of PII collected;[188]

3. Identify the categories of external parties to whom the company may disclose the information;[189]

---

185. *See, e.g.*, Business Roundtable Report, *supra* note 165, at 4. A recent study of FTC enforcement actions

> makes it clear that once a business has communicated its privacy policy to its consumers, any deviation from that policy will most likely be considered a misrepresentation constituting an unfair or deceptive act or practice. Accordingly, any business (online or offline) . . . must strictly adhere to the collection, use, access and storage practices that are described to consumers in the business' privacy notice.

Id. (emphasis in original); *see also, e.g.*, Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control Over Personal Information?*, 111 PENN. ST. L. REV. 587, 612 (2007) ("In the meantime, there is a distinct possibility that as website operators grow savvier with respect to the law, they will respond to the lack of substantive privacy protection (and lack of consumer awareness) by including in privacy policies terms that are not favorable to consumers. Thus, operators will make the cost-benefit calculation that allowing themselves the option of sharing such information in their privacy policies will outweigh any risk that such a provision will prevent consumers from sharing their information in the first place. (internal citations omitted)).

186. CAL. BUS. & PROF. CODE § 22575 (West 2008) ("An operator of a commercial Web site or online service that collects personally identifiable information through the Internet about individual consumers residing in California who use or visit its commercial Web site or online service shall conspicuously post its privacy policy on its Web site."); *see also,* Margaret Betzel, *2005-2006 Privacy Year in Review Special Topic: Privacy Law Developments in California*, 2 I/S: J.L. & POL'Y INFO. SOC'Y, 831, 865 (2006) ("The California Online Privacy Protection Act . . . became operative on July 1, 2004. California was the first state in the nation to enact a law of this kind governing online privacy policies. This statute says that operators of commercial web sites and online services 'that collects personally identifiable information through the Internet about individual consumers residing in California' must conspicuously post the website's privacy policy." (internal citations omitted)).

187. CAL. BUS. & PROF. CODE § 22575(a).

188. *Id.* § 22575(b)(1) (stating that privacy policies of covered companies must "[i]dentify the categories of personally identifiable information that the operator collects through the Web site . . . about individual consumers who use or visit its commercial Web site").

4. Describe any policy allowing individuals to review or request changes to submitted PII, if applicable;[190]

5. Notify individuals about how the company may alter its policy;[191] and

6. Identify the effective date of the policy.[192]

This state law is beneficial to Web site visitors, at least those surfing on Web sites targeting California residents, as it requires companies to be transparent about their PII collection practices.

Beyond California, other states have passed regulations that indirectly touch upon the issue of privacy policies without mandating their posting. The following chart briefly discusses each of these state laws and shows the impact on the collection of PII. This is not an exclusive list, but merely a categorization of the typical types of regulations found in the states. It is important to note that, as was true with federal law in this area, the vast majority of these state laws are sector specific, covering insurance, state agencies, etc. For example, both the Nebraska and the Pennsylvania laws only mandate that companies tell the truth in their privacy policies—a practice that may only encourage companies to fail to post a privacy policy rather than face the scrutiny of the state law. To compensate for this lack of regulation, state attorneys general have brought unfair and deceptive trade practices complaints against companies that violate their privacy policy promises.[193] Similar to the FTC actions, these complaints are filed after-the-fact, while this article is more concerned

189. *Id.* (stating that covered companies must "[i]dentify the . . . categories of third-party persons or entities with whom the operator may share that personally identifiable information").

190. *Id.* § 22575(b)(2) ("If the operator maintains a process for an individual consumer who uses or visits its commercial Web site . . . [the privacy policy must provide a customer with an opportunity] to review and request changes to any of his or her personally identifiable information that is collected through the Web site . . . , [and must] provide a description of that process.").

191. *Id.* § 22575(b)(3) (stating that the privacy policies of covered companies must "[d]escribe the process by which the operator notifies consumers who use or visit its commercial Web site . . . of material changes to the operator's privacy policy for that Web site.").

192. *Id.* § 22575(b)(4) (stating that the privacy policies of covered companies must "identify" an effective date.).

193. *See, e.g.*, New York v. Gratis Internet, Inc., No. 401210/06, 2006 WL 777061 (N.Y. Sup. Ct. Mar. 22, 2006) (discussing the facts of the case brought by then New York Attorney General Elliot Spitzer under the New York deceptive acts and practice statue alleging that Gratis promised to keep collected PII confidential and then sold such information to email marketing companies); *see also Internet Company Sued For Selling Consumer Info, Violating Its Privacy Policy*, 2(9) MEALEY'S PRIVACY REP. 1 (2006) (providing details of the case and discussing a previous deceptive acts and practices case).

with before-the-fact preventions of PII misuse than it is with post-violation remedies.

Chart III—A Sample of State Laws Indirectly Targeting PII Collection

STATE	STATUTORY COVERAGE
CONNECTICUT	Requires insurance institutions or agents to provide notice of PII practices in relationship to insurance transactions.[194]
GEORGIA	The General Assembly found that "the privacy and financial security of individuals in increasingly at risk due to the ever more widespread collection of personal information by both the private and public sectors."[195] However, Georgia has not passed any significant law regulating the collection of PII based on this legislative finding.[196]

194. CONN. GEN. STAT. § 38a-979(a) (West 2008). The notice must disclose:

> (1) Whether personal information may be collected from persons other than the individual proposed for coverage;
>
> (2) The types of personal information that may be collected, the kinds of investigative techniques that may be used to collect such information and the sources from which such information may be collected;
>
> (3) The types of disclosures . . . and the circumstances under which such disclosures may be made without prior authorization; provided only those circumstances need be described which occur with such frequency as to indicate a general business practice;
>
> (4) A description of the rights established under [various state statutes] and the manner in which these rights may be exercised; and
>
> (5) That information obtained from a report prepared by an insurance-support organization may be retained by the organization and disclosed to other persons.

Id. § 38a-979(b).

195. GA. CODE ANN. § 10-1-910(1) (West 2007).

196. Georgia did pass a data breach notification statute to protect PII from security breaches. *Id.* § 10-1-912 (West 2007). The Georgia Data Breach Statute defines personal information as follows:

> [A]n individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:
>
> (A) Social security number;
>
> (B) Driver's license number or state identification card number;
>
> (C) Account number, credit card number, or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes, or passwords;
>
> (D) Account passwords or personal identification numbers or other access codes; or
>
> (E) Any of the items contained in subparagraphs [1 through 5] of this paragraph when not in connection with the individual's first name or first initial and last name, if the information compromised would be sufficient to perform or attempt to perform identity theft against the person whose information was compromised.

INDIANA	Any state agency maintaining a personal information system must follow certain fair collection practices regarding the collection of PII.[197]
MARYLAND	State agencies are required to post privacy policies on their Web sites regarding the collection of PII.[198]
MICHIGAN	Anyone who obtains one or more social security number(s) in the ordinary course of business must create a privacy policy that secures such PII.[199]
NEBRASKA	Nebraska's deceptive trade practice statute was amended in 2003 to ban companies from knowingly making false or misleading statements in their privacy policies.[200]

Id. § 10-1-911(5) (West 2007).

197. IND. CODE § 4-1-6-2(e) (West 2008). The Indiana statute requires, among other things, that a PII collector

> [i]nform any individual requested to disclose personal information whether that disclosure is mandatory or voluntary, by what statutory authority it is solicited, what uses the agency will make of it, what penalties and specific consequences for the individual, which are known to the agency, are likely to result from nondisclosure, whether the information will be treated as a matter of public record or as confidential information, and what rules of confidentiality will govern the information.

Id. Every year, state agencies that maintain personal information must issue an annual report detailing, among other things:

- The categories of sources of such personal information;
- The agency's policies and practices regarding . . . information storage, duration of retention of information, and elimination of information from the system; and
- The uses made by the agency of personal information contained in the system.

Id. at § 4-1-6-7(b)(6)-(8).

198. MD. CODE ANN. STATE GOV'T § 10-624(c)(4) (West 2008). For examples of other states that have passed similar statutes requiring state agencies to post privacy policies, see ARIZ. REV. STAT. ANN. §§ 41-4151, 41-4152 (West 2008); ARK. CODE ANN. § 25-1-114 (West 2008); CAL. GOV'T CODE § 11019.9 (West 2008); COLO. REV. STAT. §§ 24-72-501, 24-72-502 (West 2008); DEL. CODE ANN. tit. 29, §§ 9017C, 9018C (West 2008); 5 ILL. COMP. STAT. 177/10(b)(2) (West 2008); IOWA CODE ANN. § 22.11 (West 2008); ME. REV. STAT. ANN. tit. 1, §§ 541, 542 (West 2008); MICH. COMP. LAWS SERV. § 205.827 (West 2008); MINN. STAT. ANN. § 13.15 (West 2008); MONT. CODE ANN. §§ 2-17-550, -553 (West 2007); N.Y. STATE TECH. LAW §§ 201, 207 (McKinney 2008); S.C. CODE ANN. § 30-2-40 (West 2007); TEX. GOV'T CODE ANN. § 2054.126 (Vernon 2008); and VA. CODE ANN. §§ 2.2-3800 to -3803 (West 2008).

199. MICH. COMP. LAWS SERV. § 445.84 (West 2008).

200. NEB. REV. STAT. § 87-302(a)(14) (West 2007) (considering it a deceptive trade practice when a person or entity "makes a false or misleading statement in a privacy policy, published on the Internet or otherwise distributed or published, regarding the use of personal information submitted by members of the public").

NEW YORK	The Personal Privacy Protection Law is a fair information practices statute that prevents state agencies from collecting more PII than is necessary, requires such PII to be collected directly from the data subject whenever possible, and requires the agency to distribute a privacy policy upon any collection.[201] Individual victims can file civil actions against a state agency collecting PII in violation of this statute.[202] New York's deceptive practices and false advertising statute has been used to require companies to honor their privacy policy promises.[203]
PENNSYLVANIA	Pennsylvania's statute considers it a deceptive or fraudulent business practice when a person or entity "knowingly makes a false or misleading statement in a privacy policy, published on the Internet or otherwise distributed or published, regarding the use of personal information submitted by members of the public."[204]
WASHINGTON	State agencies and local governments must attempt to gain consent before collecting PII if information will be widely accessible to the public.[205]

B. Federal and State PII Dissemination Regulations

Aside from the sectoral regulations described above, federal law does not prohibit any dissemination of PII to third parties.[206] This means that a company like Google may sell the information it collects from its Analytics customers during registration or from its visitors' search queries. Google would suffer legal repercussions only if the

201. N.Y. PUB. OFF. LAW §§ 92, 94 (McKinney 2008). The N.Y. Privacy Act defines personal information as "any information concerning a data subject which, because of name, number, symbol, mark or other identifier, can be used to identify that data subject." *Id.* § 92(7).

202. *Id.* § 97(1) ("[Any] data subject aggrieved by any action taken under this article may seek judicial review and relief pursuant to article seventy-eight of the [New York] civil practice law and rules.").

203. N.Y. GEN. BUS. LAW § 349(a) (McKinney 2008) ("Deceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state are hereby declared unlawful.").

204. 18 PA. CONS. STAT. ANN. § 4107(a)(10) (West 2008).

205. WASH. REV. CODE ANN. § 43.105.310 (West 2008).

206. *See, e.g.*, Haynes, *supra* note 185, at 597-98 ("No law prevents a website operator from sharing or selling personal information it has lawfully been given, although a website can be held liable for failing to notify its customers of its practice of selling or sharing such information. As long as they comply with the disclosure requirement, websites are free to state in their privacy policies that they will treat a visitor's personal information virtually any way they wish, arguably immunizing themselves from liability for such treatment." (internal citations omitted)).

company promised in its privacy policy that it would not sell the information and subsequently broke that promise. This breach could trigger an FTC investigation under the FTC's unfair practices authority.[207]

At the state level, California has taken the lead in regulating a company's PII dissemination practices.[208] On January 1, 2005, companies doing business with California residents became required to disclose (upon customer request): (1) the types of PII they share for direct marketing purposes and (2) the names of each purchaser.[209]

---

207. *See id.* at 599-600 ("[The] FTC has also applied Section 5 [of the Federal Trade Commission Act] to websites' misuse of personal information in the absence of a posted privacy policy pursuant to the 'unfair' rather than 'deceptive' prong of the statute." (internal citations omitted)).

208. California has passed the nation's most stringent information privacy laws relating to PII dissemination. *See, e.g.*, Anthony D. Milewski, Jr., *Compliance with California Privacy Laws: Federal Law Also Provides Guidance to Businesses Nationwide*, 2 SHIDLER J. L. COM. & TECH. 19, para. 2 (2006), *available at* http://www.lctjournal.washington.edu/Vol2/a019Milewski.html ("The State of California has taken the lead by adopting new privacy laws with the country's most stringent requirements."). Laws coming out of California are powerful from a nationwide standpoint as well because, "[a]s the tenth largest economy in the world, nearly all of the nation's largest businesses work within the state and are therefore bound by its laws to some extent." *Id.* at para. 3 (footnote omitted). Milewski argues that privacy laws in California are also important because many privacy-based California laws "are the first of their kind in the United States, several states, including New York, are considering similar measures. . . . Thus, understanding how to comply with California law may help businesses satisfy future compliance requirements elsewhere in the United States." (footnotes omitted)). See *infra* Part IV for a discussion of reasons why Congress should pass a federal law that relieves California from its efforts to set national policy.

209. CAL. CIV. CODE § 1798.83 (West 2008). California's statute provides:

> (a) [I]f a business has an established business relationship with a customer and has within the immediately preceding calendar year disclosed personal information that corresponds to any of the categories of personal information set forth [in this statute] to third parties, and if the business knows or reasonably should know that the third parties used the personal information for the third parties' direct marketing purposes, that business shall, after the receipt of a written or electronic mail request, or, if the business chooses to receive requests by toll-free telephone or facsimile numbers, a telephone or facsimile request from the customer, provide all of the following information to the customer free of charge:
>
> > (1) In writing or by electronic mail, a list of the categories set forth [in this statute] that correspond to the personal information disclosed by the business to third parties for the third parties' direct marketing purposes during the immediately preceding calendar year.
> >
> > (2) In writing or by electronic mail, the names and addresses of all of the third parties that received personal information from the business for the third parties' direct marketing purposes during the preceding calendar year and, if the nature of the third parties' business cannot reasonably be determined from the third parties' name, examples of the products or services marketed, if known to the business, sufficient to give the customer a reasonable indication of the nature of the third parties' business.

Id. Additionally, businesses must place a section in their privacy policies describing the requirements of this California law. *Id.* § 1798.83(b). This law only applies to business with

The groundbreaking California Online Privacy Protection Act (CAL-OPPA) covers twenty-seven different types of PII—representing the types of information businesses are inclined to sell and which unrelated businesses are inclined to purchase.[210] This state law also broadly defines a "direct marketing purpose" to include "the use of personal information to solicit or induce a purchase, rental, lease, or exchange of products, goods, property, or services directly to individuals by means of the mail, telephone, or electronic mail for

---

California residents as customers and who employ twenty or more employees. *Id.* § 1798.83(c)(1), (e)(1). Additionally, this California law only allows one PII dissemination request per customer per year. *Id.* § 1798.83(c).

210. *Id.* § 1798.83(e)(6). California's law states broadly the categories of PII required to be disclosed under the PII dissemination law:

> (i) Name and address.
>
> (ii) Electronic mail address.
>
> (iii) Age or date of birth.
>
> (iv) Names of children.
>
> (v) Electronic mail or other addresses of children.
>
> (vi) Number of children.
>
> (vii) The age or gender of children.
>
> (viii) Height.
>
> (ix) Weight.
>
> (x) Race.
>
> (xi) Religion.
>
> (xii) Occupation.
>
> (xiii) Telephone number.
>
> (xiv) Education.
>
> (xv) Political party affiliation.
>
> (xvi) Medical condition.
>
> (xvii) Drugs, therapies, or medical products or equipment used.
>
> (xviii) The kind of product the customer purchased, leased, or rented.
>
> (xix) Real property purchased, leased, or rented.
>
> (xx) The kind of service provided.
>
> (xxi) Social security number.
>
> (xxii) Bank account number.
>
> (xxiii) Credit card number.
>
> (xxiv) Debit card number.
>
> (xxv) Bank or investment account, debit card, or credit card balance.
>
> (xxvi) Payment history.
>
> (xxvii) Information pertaining to the customer's creditworthiness, assets, income, or liabilities.

Id. § 1798.83(e)(6)(A).

their personal, family, or household purposes."[211] Companies may only avoid this disclosure if:

> 1. A visitor to the company's Web site discloses personal information but is not considered an established customer—a legal term of art requiring an ongoing business relationship or, requiring that a previous customer purchased a product or service from the company within the past eighteen months;[212]
>
> 2. Customers do not request information about dissemination of their PII;[213]
>
> 3. The company's privacy policy provides a clear opt-in or opt-out policy for PII dissemination and provides a free way for customers to opt-in or opt-out;[214] or
>
> 4. If the company conducts business with non-California residents and a non-California resident makes the request.[215]

Waivers of rights by an individual covered under this statute are void and against public policy.[216] Any violations may result in "damages, civil penalties, injunctive relief and attorneys' fees arising

---

211. *Id.* § 1798.83(e)(2) (stating that PII sold to religious and other charitable organizations does not count as being sold for direct marketing purposes and such sales are not covered by this law).

212. *See id.* § 1798.83(e)(5). In California, "established business relationship" is defined as

> a relationship formed by a voluntary, two-way communication between a business and a customer . . . for the purpose of . . . obtaining a product or service from the business, if the relationship is ongoing and has not been expressly terminated by the business or the customer, or if the relationship is not ongoing, but is solely established by the . . . purchase of a product or service, and no more than 18 months have elapsed from the date of the purchase.

Id.

213. *Id.* § 1798.83(a) (requiring a customer to request this disclosure via written letter, e-mail, or via telephone, if the company authorizes telephonic requests).

214. *Id.* § 1798.83(c)(2). California's opt-in/opt-out exemption provides:

> If a business that is required to comply with this section adopts and discloses to the public, in its privacy policy, a policy of not disclosing personal information of customers to third parties for the third parties' direct marketing purposes unless the customer first affirmatively agrees to that disclosure, or of not disclosing the personal information of customers to third parties for the third parties' direct marketing purposes if the customer has exercised an option that prevents that information from being disclosed to third parties for those purposes, as long as the business maintains and discloses the policies, the business may comply . . . by notifying the customer of his or her right to prevent disclosure of personal information, and providing the customer with a cost-free means to exercise that right.

Id.

215. *Id.* § 1798.83(a), (e)(1) (requiring disclosure only to companies that conduct business with California residents). *See generally* BINGHAM MCCUTCHEN LLP, CALIFORNIA CONSUMER PRIVACY BILL TAKES EFFECT JANUARY 1, 2005, 1 (Oct. 2004), *available at* http://www.bingham.com/Media.aspx?MediaID=1417 [hereinafter CALIFORNIA PRIVACY BILL REPORT] (discussing this statute in detail).

216. CAL. CIV. CODE § 1798.84(a) (West 2008).

from private rights of action by California consumers."[217] A study of the effects of this California law, polling thirty-two large United States e-commerce companies, found that fifty-six percent were limiting the amount of PII they disseminate and forty-one percent considered implementing "do not share" policies in response to the CAL-OPPA.[218] Also important was the fact that businesses were not complaining of excessive expenses to comply with the new law.[219]

Beyond California, other states have passed regulations that touch indirectly upon the issue of PII dissemination. The following chart briefly discusses each of these state laws and shows the impact on the collection and dissemination of PII. This is not an exclusive list, but merely a categorization of the typical types of regulations found in the states. It is important to note that, as was true with federal law in this area, the vast majority of these state laws are sector specific covering insurance, state agencies, etc. It is also important to note that none of these laws are designed to protect the general e-commerce consumer from the serious threats facing personal information dissemination.

Chart IV—A Sample of State Laws Indirectly Targeting PII Dissemination

STATE	STATUTORY COVERAGE
ARIZONA	It is unlawful to knowingly distribute the PII of certain government officials if such dissemination poses an imminent and serious threat to that person's safety.[220]
COLORADO	It is unlawful to knowingly distribute the PII of peace officers if

217. *Id.* § 1798.84 (discussing remedies for violations which include a $3,000 civil penalty for each willful, intentional, or reckless violation, and a $500 fine for each unintentional violation); *see also* CALIFORNIA PRIVACY BILL REPORT, *supra* note 215, at 1 (briefly discussing remedies for violations). Companies with unintentional violations may cure by disclosing the appropriate information within ninety days. CAL. CIV. CODE § 1794.84(d).

218. *See* EPIC SB 27 Shine the Light Law, http://epic.org/privacy/profiling/sb27.html (last visited Apr. 4, 2008) (discussing a study by Dr. Larry Ponemon based on the California law that also showed that thirty-four percent of companies were revising their opt-in/opt-out policies, six percent were limiting personal information sharing with affiliates, and forty-four percent created new due diligence procedures with third parties before disseminating PII).

219. *Id.*

220. ARIZ. REV. STAT. § 13-2401(A) (West 2008) (stating that the threat may be to such person's immediate family as well). Personal information is defined under this statute as "a peace officer's, justice's, judge's, commissioner's, public defender's or prosecutor's home address, home telephone number, pager number, personal photograph, directions to the person's home or photographs of the person's home or vehicle." *Id.* § 13-2401(D)(5).

	such dissemination poses an imminent and serious threat to that person's safety.[221]
INDIANA	Prohibits state agencies from preparing lists of collected PII to share or sell for commercial and charitable purposes.[222]
MINNESOTA	Prevents ISPs from sharing or selling certain pieces of PII with unrelated third parties.[223]
NEVADA	Similar to the law in Minnesota, Nevada prevents ISPs from externally sharing or selling certain pieces of PII.[224]
NEW YORK	Prohibits state agencies from disclosing PII for commercial purposes and allows an individual victim to file a civil action for breach of this law.[225]
OHIO	Governmental agencies must use PII in a manner that is consistent with the reason for its collection.[226] In addition, a state statute created the Ohio Privacy/Public Record Access

221. COLO. REV. STAT. ANN. § 18-9-313(b) (West 2008) (defining PII similarly to the definition in the Arizona PII Statute); *id.* § 18-9-313(b)(2) (limiting the protection only to peace officers and stating that the threat may be to such peace officer's immediate family as well).

222. IND. CODE ANN. § 4-1-6-2(i) (West 2008) (requiring state agencies to "refrain from preparing lists of the names and addresses of individuals for commercial or charitable solicitation purposes except as expressly authorized by law").

223. MINN. STAT. ANN. §§ 325M.01-.09 (West 2008) (requiring ISPs to keep all pieces of customer PII private, including the web-surfing habits of its customers). Violations of the Minnesota statute may result in a fine of $500 or actual damages and the awarding of attorney fees. *Id.* § 325M.07.

224. NEV. REV. STAT. ANN. § 205.498(1)(a) (West 2008) (requiring ISPs to keep all pieces of customer PII, except for email addresses, private unless a customer opts-in to external disclosure). The Nevada law also requires ISPs to provide a privacy notice to customers concerning the requirements of this statute and customers can opt-out of having their e-mail addresses distributed externally. *Id.* § 205.498(1)(b), (2). Violations of the Nevada statute result in a misdemeanor and result in a fine ranging from $50 to $500. *Id.* § 205.498(3).

225. N.Y. PUB. OFF. LAW § 96 (McKinney 2008) (prohibiting commercial PII dissemination); N.Y. PUB. OFF. LAW § 97 (McKinney 2008) (allowing for victims to bring civil actions).

226. OHIO REV. CODE ANN. § 1347.01(E) (West 2008). This Ohio Privacy Statute defines personal information as

> any information that describes anything about a person, or that indicates actions done by or to a person, or that indicates that a person possesses certain personal characteristics, and that contains, and can be retrieved from a system by, a name, identifying number, symbol, or other identifier assigned to a person.

Id. The Ohio state courts have declared that the purpose of the Ohio Privacy Statute is "to limit the public dissemination of personal information collected by a state agency." *See* Doe v. Univ. of Cincinnati, 538 N.E.2d 419, 426 (Ohio Ct. App. 1988).

	Study Committee to study the dissemination of PII by governmental agencies.[227]
VERMONT	A Legislative Council study regarding the dissemination of PII by governmental agencies proposed the adoption of a state Fair Information Practices Law that enhances privacy by limiting most forms of PII dissemination.[228]
VIRGINIA	Establishes certain fair information practices for governmental agencies including a policy that there "shall be a clearly prescribed procedure to prevent personal information collected for one purpose from being used for another purpose."[229] However, this statute does not directly prohibit the dissemination of PII.[230]
WASHINGTON	Makes it unlawful to distribute the PII of certain government officials knowingly if such dissemination poses an imminent and serious threat to the safety of that person or that person's family.[231]

This discussion demonstrates that contemporary federal and state laws do little to protect PII submitted to a general e-commerce company. Although sector-specific and individual-specific laws are beginning to proliferate, such laws are not designed to solve the serious threats posed by the widespread collection and dissemination of PII in cyberspace. The next Part discusses PII tagging legislation as a balanced and cost-effective solution to the threats facing PII at the collection and dissemination stage. Properly drafted, PII tagging

227. H.B. 204, 125th Gen. Assem. § 5703.49(3)(B)(1) (Ohio 2005), *available at* http://www.legislature.state.oh.us/bills.cfm?ID=125_HB_204 (stating, in relevant part, that the Commission must study the "concerns associated with the dissemination of personal information contained in public records, including, but not limited to, identity theft, misuse, harassment, and fraud").

228. VERMONT LEGISLATIVE COUNCIL, STAFF REPORT ON PUBLIC RECORDS, PRIVACY, AND ELECTRONIC ACCESS IN VERMONT, 12-14, 16 (Jan. 2005), *available at* http://www.leg.state.vt.us/reports/05PublicRecords/Public_records_study_report.pdf (discussing the issue of PII dissemination by governmental entities, cataloging dissemination laws in other states and proposing various privacy-enhancing practices which the Vermont Legislature could adopt).

229. VA. CODE ANN. § 2.2-3800(C)(9) (West 2008).

230. *See, e.g.*, Hinderliter v. Humphries, 297 S.E.2d 684, 688 (Va. 1982) ("[The Virginia statute] does not generally prohibit the dissemination of information. Instead, the enactment requires certain procedural steps . . . to be taken in the collection, maintenance, use, and dissemination of [PII].").

231. WASH. REV. CODE § 4.24.680(1) (West 2008) (stating that the threat may be to such person's immediate family as well); *id.* § 4.24.680(3)(f) (defining PII similarly to the definition in the Arizona PII statute, discussed *supra* note 220).

legislation has the capability to solve these serious problems without excessively burdening e-commerce efficiency.

IV. PII TAGGING: TRACKING THE DISSEMINATION OF PII WHEN COMPANIES OBFUSCATE THEIR PRIVACY PRACTICES

Part I of this article demonstrated that web surfers leave a clear PII trail for companies to track and bad actors to exploit. E-commerce innovations exacerbate this threat and allow companies to collect PII more effectively and disseminate it more efficiently. Part I elaborated on these fears by conceptualizing the major benefits and serious threats facing PII upon collection and dissemination. However, these theories need real-world validity before lawmakers allocate resources and the public takes them seriously. Therefore, Part II established, through a study of the twenty-five most highly trafficked Web sites in the United States, that large e-commerce companies currently reserve the right to collect, store, and share personally identifying information with unrelated third parties. This study also found that the privacy policies of these same companies provide poor guidance about PII practices and fail to inform visitors of their options regarding PII sharing. In the end, this study provides ammunition for the argument that PII dissemination is extremely profitable and that companies are not willing to give up revenue streams generated by selling personal information. Unfortunately, however, it appears that informing visitors about this PII-dissemination business strategy is undesirable. Therefore, companies draft privacy policies in legalese, post them inconspicuously on their homepages, and hedge their positions on PII dissemination—all as a means to avoid public exposure of an unpopular practice.[232] Problematically, and as Part III described, the United States legal system permits companies to obfuscate their privacy policies in this manner as well as to collect and disseminate massive amounts of PII in a virtually unregulated environment, as long as they do not break one of their privacy policy promises. Businesses have taken advantage of this leniency, failed to self-regulate effectively, and, in the process, enhanced the serious threats facing today's e-commerce community.

---

232. *See, e.g., Business Week/Harris Poll: A Growing Threat*, BUS. WK. ONLINE, Mar. 20, 2000, http://www.businessweek.com/2000/00_12/b3673010.htm [hereinafter *Business Week Privacy Poll*] (showing the results of a poll where eighty-eight percent of respondents claimed that they would prefer that a company obtain their permission before sharing PII externally).

With this information as background, this Part proposes a solution in the form of federal PII tagging legislation. A tagging regulation requires covered companies to post a conspicuously linked privacy policy that accurately describes seven key PII practices in plain English. Companies failing to meet these simple requirements must tag their name to every piece of PII they disseminate under their non-compliant policy. Purchasers of tagged PII are then legally required to identify the seller whenever they solicit individuals identified by the purchased PII. The remainder of this article introduces the concept of PII tagging, explores the contents of a model tagging law, and discusses the implications of such legislation, including the compromise it should broker between adequately protecting PII and excessively hampering e-commerce efficiency.

A. The Concept of PII Tagging, and Triggering the New Federal Law

It is crucial for e-consumers to notice, read, and comprehend a company's PII practices, especially in an environment where 100% of the most-trafficked Web sites collect PII and where ninety-four percent reserve the right to disseminate collected information. Responsibility for obtaining this knowledge should lie with the company *and* with the visitors to its Web site. On the one hand, it is unfair for the government to require companies to spoon-feed privacy terms to visitors who can understand them but choose not to and, instead, blindly submit PII. On the other hand, it is unfair to consumers to allow companies to continue down a self-regulatory path where privacy policy structure and language actively encourage visitors to ignore a company's privacy practices. Therefore, effective PII tagging legislation must bridge this gap and apply only when a company's privacy policy fails to provide accurate, adequate, and clear notice of terms, or when a company posts its policy inconspicuously. The remainder of this Part discusses the concept of PII tagging and elaborates on the requirements of a model tagging law.

1. The Concept of PII Tagging

PII tagging associates or "tags" a company's name with the data it disseminates externally.[233] This is a simple and effective way

233. This idea of tagging personally identifiable information is relatively new; however, Internet users have been developing ways to tag information that they find interesting. *See, e.g.*, Heather Green & Robert D. Hof, *Picking Up Where Search Leaves Off: The Time-Saving Trend of Tagging Is Luring Legions of Web Surfers—and Yahoo!*, BUS. WK., Apr. 11, 2005, *available at* http://www.businessweek.com/magazine/content/05_15/b3928112_mz063.htm (discussing the idea of tagging interesting information found

to inform consumers that particular companies share their personal information.[234] Such information is crucial in cases where a company's privacy policy obfuscates PII sharing practices. In order to work effectively, tagging must involve both the buyer and the seller in an information transaction. More specifically, sellers tag PII by disseminating it in a file that includes the sellers' "doing business as" (DBA) name alongside each piece of personally identifying information sold.[235] After dissemination, the purchaser must keep the seller's name attached to the data and announce it during solicitations to individuals identified by the information. In a way, tagged PII is similar to a time stamp embedded in a video recording—whenever the video plays, the time stamp is exposed to the viewer. PII tagging is akin to stamping a seller's name to a piece of data and requiring the buyer to expose the name at certain times to certain people.

For example, imagine that Wells Fargo purchases a list of 10,000 phone numbers and e-mail addresses identifying new residents to the Denver, Colorado area. With this information, Wells Fargo desires to market its home mortgage services to potential home purchasers. Wells Fargo contacts ChoicePoint to obtain lists of relevant PII and purchases a "multiple prospect database [including] . . . credit, demographic, commercial . . . new mover and new parent databases" for the Denver area.[236] Two months earlier, ChoicePoint purchased the data for this database from EAgency, a Colorado-based employment agency that collects personal information and helps new residents find local jobs. At the time of the sale to ChoicePoint, however, EAgency failed to post a privacy policy of any kind on its Web site. As discussed below, a federal PII tagging law penalizes

---

on the Web to make future references simple). Although the "tagging" referred to in Green & Hof's article refers to associated words with specific pieces of information on the Web, the idea of PII is similar in that it associates company names with specific pieces of PII.

234. *See id.* (discussing a tagging Web site where Web content can be tagged for future reference).

> [P]eople are able to tag any link they choose for easy retrieval later. *What makes tags more powerful than a Web bookmark is that they can be shared easily with other people.* If someone tags a story on Iraq, for example, that link is added to a list on [the Web site] of other Iraq content. Anyone on the service who wants to read about Iraq can then find a list of stories that have been tagged and see who tagged them. *Today more than 85,000 people are using the free service.* "Tagging is about the most important tool of last year," says Clay Shirky, an adjunct professor at New York University's Interactive Telecommunications Program.

Id. (emphasis added).

235. This is a simple tweak to contemporary dissemination practices, as DBA names can be added as separate columns in the typical file emailed to purchasers.

236. CHOICEPOINT DIRECT*LINK*, THE COMPREHENSIVE DIRECT MARKETING SOLUTION FOR YOUR DISTRIBUTED SALES FORCE, *available at* http://www.cp-pm.com/media/pdf/CPDL%20Brochure%20-%20Oct2005.pdf (last visited Apr. 4, 2008).

companies exhibiting poor information privacy practices such as this and requires them to tag all disseminated data. Because of its non-compliance, EAgency must now tag its name to each piece of PII sold to ChoicePoint. ChoicePoint must then associate the EAgency name with this data every time it markets from this list or sells the information to another purchaser.[237] In this case, Wells Fargo—as the purchaser of tagged information—must state that EAgency supplied the individual's PII whenever it contacts new Denver residents from this database. During such solicitations, a representative from Wells Fargo must state something to the effect of: "Hello. This is Donna from Wells Fargo. We received your telephone number from EAgency and heard that you are new to town. We would like to speak with you about financing your next home."[238]

2. Key Elements of a Model PII Tagging Law

The following section discusses the key elements that any PII tagging legislation should contain. The purpose of this article is to advocate for a PII tagging regime on its merits and not to propose a specific PII tagging law. Therefore, the following discussion constitutes a more general analysis than Congress or a federal agency tasked with rulemaking should undertake when actually implementing a tagging system. The first, and most important, requirement for an effective law in this area is that it be passed by Congress and preempt similar and stricter state laws.

a. The Case for a Federal Law and Ceiling Preemption

As an initial matter, PII tagging legislation should originate from Congress instead of from various state legislatures,[239] and should contain a ceiling preemption clause preempting more stringent dissemination legislation at the state level.[240] Although states can

---

237. As an additional consideration, ChoicePoint will only have to tag its name to EAgency's data if ChoicePoint's privacy policy is also non-compliant.

238. The same type of disclosure must occur with written or electronic solicitations as well. However, in those cases, the representative from Wells Fargo would have to change the statement pertaining to the type of PII received to "we received your home address from EAgency" or "we received your e-mail address from EAgency."

239. *See, e.g.*, Ciocchetti, *supra* note 177, at 105-08 (discussing the issue of state versus federal legislation and explaining why federal legislation is more effective for protecting PII).

240. As this author previously noted:

> The idea of preemption in American law originates from the Supremacy Clause of the U.S. Constitution. The Supremacy Clause provides that the "Constitution, and the laws of the United States . . . shall be the supreme law of the land." This

and should serve as laboratories for experimentation in certain areas, the serious threats facing PII collection and dissemination represent a nationwide problem. Furthermore, transactions conducted via the World Wide Web are national—even international—in scope and require a federal solution. In a split second, a consumer working in Portland can transact business with a merchant in California and have bedroom furniture shipped directly from a factory in North Carolina to the buyer's residence in southern Washington. This situation represents a common e-commerce transaction involving four separate states and four potentially conflicting state PII laws.

More specifically, this type of transaction illustrates a major problem under state privacy regimes easily remedied by a federal law containing a ceiling preemption clause. Assume that the furniture seller in California posts a privacy policy that specifically states that each piece of PII collected will be sold externally. The buyer reads this policy, is pleased with the clear disclosure language in the privacy policy, accepts the seller's external sharing practices, and proceeds with the order. Assume further that the Oregon legislature has banned the collection of PII by companies that share such information externally but that the state of Washington has a law allowing PII dissemination if properly disclosed in a company's privacy policy. Additionally, assume that California has its CAL-OPPA law in place (requiring disclosure of disseminated customer PII and buyers of such information upon customer request) and that North Carolina has no PII collection law whatsoever. The results of this mishmash of state legislation would allow Oregon law to trump the laws in the other three states and block this sale. This result is problematic because it places the buyer is in an awkward position as Washington law (the law of the state where the buyer resides and requests delivery) allows such a transaction to proceed. Here, consumers in Oregon find themselves overprotected because they cannot even consent to PII collection in any case where their information may be sold. On the other hand, consumers in North Carolina are under-protected because the state does not regulate PII dissemination. Consumers in

---

clause indicates that the federal government, "in exercising any of the powers enumerated in the Constitution, must prevail over any conflicting or inconsistent state exercise of power." Preemption of state and local laws in the business arena generally occurs when Congress enacts legislation that directly conflicts with state legislation (express preemption) or when the federal government has chosen to occupy the field forming the basis of the state legislation (implied preemption). At this point the federal law will preempt the state law rendering the state law invalid. Congress has the authority to regulate businesses conducting interstate commerce under the Commerce Clause of the U.S. Constitution.

See id. at 105 n.205 (internal citations omitted).

Washington and California are caught somewhere in the middle of this regulatory spectrum.

Under such a plausible circumstance, a company conducting business in each of these four jurisdictions must create multiple privacy policies and tailor its PII practices and business strategy accordingly. This situation would grow more perplexing if all fifty states—and many local jurisdictions on top of that—decided to pass their own PII dissemination laws.[241] Such a large regulatory hurdle would hinder e-commerce efficiency without gaining the benefit of protecting consumers equally across the country from a national problem. Even worse, businesses operating under these multiple laws would have a strong incentive to comply with the most stringent state law on the books and ignore the others. This practice allows lawmakers in one state to serve as a de facto national legislature and set policy for a nationwide constituency to which they are not accountable. Therefore, in case of electronic PII privacy, a federal law is better suited to protect Web site visitors from the serious national threats targeting the collection and dissemination of PII.

Before leaving the area of legislative origination, it is important to discuss the scope of a federal PII tagging law. The United States Constitution does not allow Congress to govern the operation of all businesses operating within the United States—only those businesses operating in interstate commerce.[242] Therefore, covered companies include only businesses conducting e-commerce (i.e., providing a product or service online) between one or more states. This jurisdictional limit would not hinder the national effect of a federal tagging law, however, because few contemporary e-commerce businesses operate solely in intrastate commerce. Therefore, this interstate commerce requirement would keep a tagging regulation free from constitutional scrutiny on federalism grounds without hindering the effectiveness of its nationwide protection.

b. Legal Requirements

The goal of PII tagging legislation is for companies to draft and post policies that consumers can actually locate and understand. This type of law must not remove personal responsibility from consumers by allowing the government to dictate particular terms of a company's privacy practices. Instead, businesses should maintain the ability to

241. Again, without preemption, local jurisdictions like cities and counties may choose to regulate PII in different and conflicting ways.

242. The United States Constitution allows Congress to regulate businesses operating in interstate commerce. *See* U.S. CONST. art. I, § 8, cl. 3.

strategize about their privacy policies and innovate new ways to protect information. Therefore, a PII tagging law should not require companies to create specific policy terms. To keep companies from obfuscating their practices as they have been doing recently, PII tagging legislation must require companies (1) to draft privacy policies in plain English, (2) to cover important privacy topics, and (3) to link their privacy policies to their homepages conspicuously.

i. Plain English

The plain English requirement stems directly from the Securities and Exchange Commission's plain English rules.[243] In line with SEC guidance, companies covered under a PII tagging regime must draft their policies with the ultimate goals being clarity of drafting and visitor comprehension. To this end, companies can comply with this requirement by consulting the SEC's *Plain English Handbook* and avoiding long sentences, passive voice, weak verbs, superfluous words, legal and financial jargon, numerous defined terms, abstract words, unnecessary details, and unreadable design and layout.[244]

A company that even makes an attempt to draft its privacy policy using plain English principles will produce a document that is much easier to comprehend than many policies currently posted by the Top 25. The intelligent people working for e-commerce companies can certainly find a way to remove the legalese and other jargon, and replace it with simplified concepts that still get the idea across to the reader. Additionally, these drafters can easily add subheadings, simplify the wording, explain key concepts, and increase the font size of the text of the privacy policies. This plain English requirement provides great benefits without sacrificing the important concepts that companies must get across in their privacy statements.

ii. Mandatory Privacy Topics

PII tagging legislation should mandate that companies discuss their privacy practices as they relate to the following seven areas:

1. Types and Manner of Personal Information Collected (both active and passive);

2. Internal Personal Information Uses;

3. External Personal Information Uses;

---

243. *See* 17 C.F.R. §§ 228-230, 239, 274 (West 2008).

244. SEC PLAIN ENGLISH HANDBOOK, *supra* note 102, at 17.

4. Visitor Choice Options (including how to Access/Change/Remove Personal Information);

5. Personal Information Security;

6. Privacy Policy Amendments; and

7. Other Important Information (including privacy officer contact information and effective dates).[245]

Companies should be free to create additional subheadings as long as the subject matter is privacy-related. In addition, companies should not be able to include their legal disclaimers in the same link as their privacy policy. At the end of the day, these seven areas represent the meat of any company's privacy practices. Therefore, each area must be explained clearly to Web site visitors. As stated earlier, companies should remain free to formulate any type of PII practice they desire. As long as such terms are clearly disclosed, visitors will quickly figure out which companies are not taking the protection of their personal information seriously.

iii. Conspicuous Posting

Covered companies must place a conspicuous link to their privacy policies on their homepage. Conspicuous linking is the simplest requirement in a tagging regime and merely requires companies to (1) place a link to their privacy policy on their homepage; (2) place only the title "Privacy Policy" in the link text; (3) link only to the privacy policy; and (4) place this privacy policy link in the same font type and size as each of the surrounding links.

As an example, companies should no longer be able to place their ten-point font links to a "Site Map" or "Press Room" at the bottom of a homepage and then hide the privacy policy link directly below in a seven-point font.[246] Additionally, companies should not be permitted to include both their legal disclaimers and their privacy policies in the same link under a title such as "Legal & Privacy," as TimeWarner does.[247] This type of inconspicuous and confusing posting

245. *See, e.g.*, Ciocchetti, *supra* note 177, at 111 (discussing different proposed privacy legislation and describing, in detail, the types of information companies should include in these same seven sections).

246. *See, e.g.*, National and Local Weather Forecast, Radar, Map and Report, *supra* note 126 (showing links to the following pages—"Home," "Site Map," "Video Site Map," "Customer Service," "Feedback," "About Us," "Press Room," "Careers," and "Advertise"—at the bottom of its homepage, and then placing the privacy policy link in the smallest font in the lower right corner below these links).

247. *See* TimeWarner.com, http://www.timewarner.com/corp/ (last visited Apr. 4, 2008).

is a serious problem, as Part II's study shows that only sixty-eight percent of the Top 25 currently meet this simple posting requirement.[248] The remaining thirty-two percent are non-compliant and, under the tagging regime envisioned in this Part, would be required to tag every piece of PII they disseminate externally.

3. Non-Compliance, Enforcement, and Penalties

Companies violate a PII tagging rule by avoiding plain English principles, failing to cover the required topic areas, or failing to post a conspicuous link. Companies should receive a grace period, perhaps up to six months from enactment of a tagging law, to sort through their current PII practices and then come into compliance with the new legislation. By the end of the grace period, all non-compliant privacy policies should immediately trigger the PII tagging legislation. Once triggered, the tagging requirements should apply and both sellers and buyers of PII must comply.

On the enforcement front, the Federal Trade Commission should receive the authority to promulgate rules to enforce the specific requirements of this legislation.[249] The FTC is the appropriate entity for this purpose,[250] as the FTC is already familiar with federal privacy regulations, such as the Children's Online Privacy Protection Act,[251]

---

248. *See supra* Part II.

249. Congress may grant the FTC the power to enforce a specific federal law. *See, e.g.*, Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act), 15 U.S.C. §§ 7701-7713 (2000 & Supp. III 2003) (providing that the CAN-SPAM Act "shall be enforced by the Commission as if the violation of this Act were an unfair or deceptive act or practice proscribed under [the Federal Trade Commission Act]" (citation omitted)). In addition, the Federal Trade Commission Act states that "unfair or deceptive acts or practices" that affect interstate commerce are unlawful. *See* 15 U.S.C.A. § 45(a)(1) (West 2008). Acts or practices considered unfair under the Federal Trade Commission Act "cause or [are] likely to cause substantial injury to consumers which [injury] is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n) (2000).

250. Nonetheless, some privacy advocates believe that the FTC is not the appropriate entity to protect information privacy. *See, e.g.*, Jeffrey Benner, *FTC Powerless To Protect Privacy*, WIRED.COM, May 31, 2001, http://www.wired.com/politics/security/news/2001/05/44173 ("Because there are few laws that address what companies can and cannot do with information collected online, much of the burden for protecting online privacy has fallen to the FTC. Advocates of stronger privacy laws said that, while the agency could do a little more, it doesn't actually have the power to really protect our privacy online."). However, the FTC is the most appropriate entity in existence at this point in time with the power, know-how, and mission to protect consumers from online privacy threats.

251. Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506 (2000) (protecting personal information of children under the age of thirteen).

the Gramm-Leach-Bliley Act,[252] and the Health Insurance Portability and Accountability Act.[253] Additionally, the FTC possesses the institutional knowledge to work with privacy legislation such as a tagging regime, and already proclaims that privacy is a "central element" of its consumer protection mission.[254] The enforcement costs should be low if Congress considers implementing the citizen-monitoring process described below and businesses respond as anticipated to the social pressures applied after violating a tagging law.

A citizen-monitoring program would allow concerned citizens and privacy advocate groups to monitor the e-commerce community for violations. Because a tagging law is simple to understand and non-compliant policies are easy to identify, it is likely that effective monitoring can and will take place. This type of citizen policing has already assisted in the enforcement of other privacy laws. For example, a group of law students took on a project where they requested PII dissemination disclosures under the CAL-OPPA and then informed companies of their non-compliance.[255] Pertaining to a tagging law, these monitors can provide comments and notice of potential violations to the companies themselves and/or to the FTC via

---

252. Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (codified as amended in scattered sections of 12 and 15 U.S.C. (2000)) (protecting personal information collected by covered financial institutions).

253. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 29, and 42 U.S.C. (2000)) (protecting health-related personal information).

254. Federal Trade Commission, Privacy Initiatives, http://www.ftc.gov/privacy/index.html (last visited Apr. 4, 2008) (discussing the FTC's role in federal information privacy law). The FTC has stated:

> Under the FTC Act, the Commission guards against unfairness and deception by enforcing companies' privacy promises about how they collect, use and secure consumers' personal information. Under the Gramm-Leach-Bliley Act, the Commission has implemented rules concerning financial privacy notices and the administrative, technical and physical safeguarding of personal information, and it aggressively enforces against pretexting. The Commission also protects consumer privacy under the Fair Credit Reporting Act and the Children's Online Privacy Protection Act.

Id.

255. *See* Chris Jay Hoofnagle & Jennifer King, *Consumer Information Sharing: Where The Sun Still Don't Shine* 9-11, Technology & Public Policy Clinic, University of California-Berkeley School of Law (2007), *available at* http://www.truststc.org/pubs/323/sb27report.pdf ("Students working the Samuelson Law, Technology & Public Policy Clinic during Summer 2007 each chose businesses with which they had a relationship to send [CAL-OPPA] requests. . . . Requests were sent on June 14, 2007. [CAL-OPPA] requires a response to a request within 30 days. In order to account for mailing delays, we waited 40 days for responses. On day 41 (July 25, 2007), we sent replies to responses that were inadequate, and sent reminder letters to companies that did not respond at all." (alteration in original) (on file with author)).

the "Consumer Complaint Form" link that already exists on the FTC's Web site.[256] Upon receiving a complaint, the FTC can investigate the allegations on their merit.[257] It would also be important for the FTC to create a monitoring scheme of its own to supplement citizen monitoring if insufficient violations are reported or if reported violations are inaccurate or prove to not to be actual violations. As for the tagging requirement prong, the FTC would likely be more involved in the discovery of companies that intentionally or negligently avoid tagging their PII as required.

From an enforcement perspective, Congress should grant the FTC the power to file an administrative complaint[258] and/or bring a civil action against non-compliant companies.[259] The enforcement remedies should be set on a sliding scale, depending upon the number of violations a particular company incurs and the seriousness of each violation. For example, companies with non-compliant privacy policies after the expiration of the grace period may be punished by a cease and desist order and/or a fine for the first offense.[260] Future offenses by the same company may be punished by a cease and desist order, a progressively larger fine structure, and injunctions on their e-

256. Complaint Form, *available at* https://rn.ftc.gov/pls/dod/wsolcq$.startup?Z_ORG_CODE=PU01 (last visited Apr. 4, 2008). The FTC could also create a separate complaint link on its homepage, its Consumer Protection page, or its Privacy Initiatives page. *See* Federal Trade Commission Homepage, http://www.ftc.gov/ (last visited Apr. 4, 2008); FTC Bureau of Consumer Protection, http://www.ftc.gov/bcp/index.shtml (last visited Apr. 4, 2008) (showing the FTC's Consumer Protection Web page, which includes many links relevant to the Commission's consumer protection mission); Federal Trade Commission, Privacy Initiatives, *supra* note 254. A "Tagging Report Card" link could appear along with these links or on the Privacy Policy page, accessible by a link on the bottom-right side of the FTC's Consumer Protection page.

257. *See* 15 U.S.C.A. § 46(a) (West 2008) (providing the FTC with the power "[t]o gather and compile information concerning, and to investigate from time to time the organization, business, conduct, practices, and management of any person, partnership, or corporation engaged in or whose business affects commerce").

258. *See* 15 U.S.C.A. § 45(b) (West 2008) (providing the FTC with the power to file an administrative complaint when it has "reason to believe" that a violation of the FTC Act has occurred).

259. *See id.* § 45(m)(1) (providing the FTC with the power to obtain civil penalties under certain circumstances for violations of the FTC Act).

260. The FTC has the power to levy fines as remedies in its administrative proceedings. *See id.* § 45(b). In a recent case, the FTC issued a cease-and-desist order, but not a fine, to a company that promised to keep collected PII secure and then violated its promise. *See* In re Life is Good, Inc., Order No. 072-346, at 3 (FTC Nov. 2007). In the ChoicePoint case, the FTC issued a cease and desist order along with $15 million in fines. *See* Press Release, Fed. Trade Comm'n, ChoicePoint Settles Data Security Breach Charges; To Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress (Jan. 26, 2006), *available at* http://www.ftc.gov/opa/2006/01/choicepoint.shtm.

commerce operations until compliance occurs.[261] Companies that attempt to skirt the tagging requirement and disseminate data without their name attached as required and purchasers of PII who fail to tag the information as required should be punished in the same manner. The reality of a tagging scheme is that it is not excessively demanding and most companies will choose to expend the minimal resources necessary to come into compliance with the regulations rather than face these increasingly burdensome punishments, especially an injunction that grinds their business to a halt. As for specific enforcement options, Congress should allow the FTC to decide how best to implement them via the FTC's rule-making process.[262]

Chart V—Model PII Tagging Law Requirement

REQUIREMENT	DISCUSSION
COVERED COMPANIES MUST CREATE COMPLIANT PRIVACY POLICIES	The entire privacy policy must comply with the plain English rules promulgated by the SEC; and The required privacy policy sections must describe the: Types and Manner of Personal Information Collected (both actively and passively); Internal Personal Information Uses; External Personal Information Uses; Visitor Choice Options (including how to access, change, and remove Personal Information); Personal Information Security; Privacy Policy Amendments; and Other Important Information (including contact information for privacy officers and effective dates).
COVERED COMPANIES MUST POST A CONSPICUOUS LINK TO THEIR PRIVACY POLICY	Privacy links must be located on a company's homepage; Privacy links must be in the same font and size as surrounding links; Privacy links must contain only the company's privacy policy; and Privacy links must contain only the title "Privacy Policy."

261. The FTC has the power to request a court to issue preliminary and permanent injunctions for violations of the laws it enforces. *See* 15 U.S.C. § 53(b) (2000).

262. Congress should grant the FTC this rulemaking authority in the text of the tagging legislation.

Chart VI—Key Steps in the PII Tagging Process

STEP	DESCRIPTION
(1)	A company's privacy policy triggers the PII tagging law. This may occur via inaccurate, inadequate, or unclear disclosures, or via an inconspicuous link. Enforcement may stem from diligent e-consumers and privacy advocates who report violations to the FTC or from an independent FTC investigation.
(2)	Immediately upon triggering, PII sellers must now disseminate information with their DBA name attached. This is a simple step and can occur as a separate column in the PII file transferred to the buyer.
(3)(A)	Whenever the buyer subsequently utilizes purchased PII to contact customers identified by the information it must disclose the seller's name. Additionally, the buyer is required to keep the seller's name attached to each piece of purchased PII for as long as it keeps the information in its databases.
(3)(B)	If the buyer sells the PII instead of marketing with it, the DBA name of the initial seller must stay attached to the information. Additionally, if the initial buyer's privacy policy also triggers the PII tagging law, then the initial buyer must also tag its name to the information along with the seller's name. This tagging requirement then burdens any purchaser of the information that operates under an insufficient privacy policy. Subsequent sellers must keep the tagging active for as long as they keep the information in their databases.
(4)	If a company improves its privacy policy to the point of compliance, each subsequent piece of PII disseminated is free from the tagging requirement. Previously disseminated pieces of PII, however, remain burdened. Coming into compliance is relatively easy because the requirements of a tagging regime are clear and simple. Additionally, required privacy policy changes are neither expensive nor complicated.

B. PII Tagging Legislation: Important Implications

Consumers are unhappy with contemporary PII practices and desire some form of regulation governing the collection and dissemination of their personal information.[263] In response to this dissatisfaction, a few e-commerce entities have bowed to public pressure and stopped selling certain pieces of PII, though generally

263. *See, e.g.*, *Business Week Privacy Poll*, *supra* note 232 (showing that fifty-seven percent of individuals in a March 2000 poll believed that "[t]he government should pass laws now for how personal information can be collected and used on the Internet").

only in the form of Social Security numbers.[264] However, Part II's study showed that this type of self-regulation is not working on a large scale, and that companies are bucking efforts to limit PII dissemination.[265] Federal tagging legislation would supplant this ineffective self-regulation and, at the same time, provide consumers with the regulatory security they desire without placing excessive limits or costs on e-commerce companies. The federal tagging regime outlined in this article presents a better option than the CAL-OPPA because of its (1) national scope, (2) conspicuous notice requirement, (3) increased clarity of privacy disclosures, (4) lack of a consumer-request requirement, and (5) ability to educate Web site visitors about PII practices.

PII tagging is not designed to force companies to stop PII dissemination completely. Rather, its intent is to provide the typical Web site visitor with knowledge about which companies disseminate personal information and how such information might be sold to unrelated third parties.[266] A tagging law will at least ensure that consumers have the opportunity to obtain this knowledge from mandatory privacy policies that are clear and conspicuous *or* when non-compliant privacy policies force buyers to reveal a seller's name during solicitations. At this point, it is up to consumers to take advantage of this clarity and make smarter decisions with their PII.

Under a tagging regime, consumers upset that their information has been disseminated via an unclear privacy policy or without their permission will now be able to associate a name with a seller and take action. Individuals are likely to respond initially by complaining to the seller's customer service department, informing their friends and families, and taking their business elsewhere. Injured consumers may also attempt to discover contradictions in unclear privacy policies and alert the FTC of such broken privacy promises. Additionally, it is foreseeable that angry customers and privacy advocacy groups will place social pressure on companies to

264. *See, e.g.*, Jonathan Krim, *Broker To Limit Sale of Personal Data*, WASH. POST, Mar. 18, 2005, at E1 (discussing the fact that corporate clients of the information broker Westlaw will no longer have access to Social Security numbers, and that government offices other than law-enforcement agencies will only have access to partial Social Security numbers).

265. *See, e.g.*, *Business Week Privacy Poll*, *supra* note 232 (showing that only fifteen percent of individuals in a March 2000 poll believed that the government should allow self-regulation to continue).

266. There is less of a concern with PII sharing among a company's affiliates and partners (internal PII sharing) because companies can require these entities to adhere to certain privacy practices as a condition of doing business. A subsequent study detailing the actual effects of internal PII sharing presents an interesting area for further research.

comply with the new tagging law.[267] The potential for such a social backlash, combined with the threat of future tagging requirements, will force companies to analyze their privacy practices in more detail and provide the clarity and simplicity needed to encourage consumers to take responsibility for their actions online.[268]

From a fairness perspective, companies that comply with the new law and adequately disclose their privacy practices face no burden from a PII tagging requirement. For instance, if a company plainly discloses that it shares or sells PII freely with unrelated third parties, it should be free to do so. However, upon gaining this knowledge, a Web site visitor should make a conscientious decision before submitting any information to that company online. Compliant privacy policies present a much easier decision for the typical Web surfer than policies that obfuscate secondary uses of PII and hinder informed decisions. Tagging presents a fair compromise because, as noted previously, individuals also bear responsibility for protecting their PII from the dangerous threats lurking on the Web.

From an enforcement perspective, the FTC, as monitor of the tagging regime, will not have to expend substantial resources to police violations. This is because diligent consumers and privacy advocates will be encouraged to help monitor privacy policies and report companies that fail to meet the requirements of the law. As stated previously, such citizen policing has already assisted in the enforcement of other privacy laws.[269] Additionally, the FTC's current consumer complaint form or a separate reporting link on the FTC's Consumer Protection homepage would provide an appropriate outlet for the FTC to receive comments from concerned citizens.[270]

---

267. Privacy advocacy groups already place tremendous pressure on companies to improve their PII practices. For example, the Electronic Privacy Information Center (EPIC), a well-known privacy advocacy group, testifies before Congress, issues reports, holds press conferences, and files legal briefs in cases involving information privacy. *See* Press Releases, Elec. Privacy Info. Ctr., http://epic.org/press/ (last visited Apr. 2, 2008) (providing a list of hyperlinks to various press releases demonstrating EPIC's most recent efforts to place social pressure on companies with privacy-invasive information practices).

268. Seventy-five percent of respondents to a *Business Week* privacy poll claimed that it is "absolutely essential" or "very important" that the websites they visit contain a privacy policy that explains how their PII will be used. *See Business Week Privacy Poll*, *supra* note 232. It is likely that these same people will take the time to read policies that they can find and understand—the type of policies required under a tagging law.

269. *See supra* note 255 and accompanying text.

270. *See supra* note 256 and accompanying text.

V. CONCLUSION

As the twenty-first century advances, information technology becomes increasingly efficient.[271] Each innovation tailored to the World Wide Web improves the interaction of people from many nations; this is especially true as the worldwide e-commerce community grows.[272] Companies benefit from technological advancements, collect vast quantities of data from online visitors, and store the information in sophisticated databases. These same companies also posses the ability to transfer the information across the globe in a matter of seconds. This collection and movement of personal information allows the Web to serve as an effective e-commerce conduit, and it is difficult to imagine a world without Amazon.com and Google only one click away.

Along with the many benefits, however, comes the fact that companies are now able to generate revenue streams not only from the sale of goods and services over the Web, but also from the personally identifying information they collect. This financial incentive to disseminate PII can have a negative impact on e-consumers if abused. Problematically, it appears that American e-commerce companies do not always put their best foot forward when it comes to their privacy policies, especially in their disclosure of PII dissemination practices. Even worse, the current United States legal regime creates no obligation for these companies to be more forthcoming. This reality leaves Web site visitors in the dark as to how their PII is used and, instead of demanding more protection, Web site visitors continue to enter information whenever necessary to move on with their Web experience. This nationwide problem cries out for a national solution as more and more PII finds its way into cyberspace where it is virtually irretrievable and subject to serious threats.

---

271. *See, e.g.*, *New NIST Effort Seeks To Improve Utility of Property Data*, NIST UPDATE, Jan. 18, 2000, *available at* http://www.nist.gov/public_affairs/update/upd000118.htm#Materials ("Much of science and technology owe their progress to the careful collection, logging and interpretation of data. And as information technology becomes more efficient, so do the methods scientists use for sorting and accessing data."). In fact, until recently, the idea that technology increasingly becomes efficient was typified by the fact that microchip capacity seemed to double every two years—a theory referred to as Moore's Law. *See, e.g.*, Manek Dubash, *Moore's Law Is Dead, Says Gordon Moore*, TECHWORLD, Apr. 13, 2005, http://www.techworld.com/opsys/news/ index.cfm?newsid=3477 (describing Moore's law and claiming that some advances in technology might now take a bit longer to double because of the results of this advancing efficiency).

272. *See, e.g.*, World Internet Usage Statistics News and Population Stats, http://www.internetworldstats.com/stats.htm (last visited Apr. 4, 2008) (showing that over 1.3 trillion people worldwide use the Internet, representing a growth rate of 265.6% in the last seven years).

PII tagging is an appropriate middle ground solution to this nationwide problem. A national tagging regime places the onus of protecting PII on businesses and on individual web surfers. This legislation protects individuals by requiring companies to post privacy policies conspicuously and to draft them in plain English. Each of these mandatory policies must contain important information about a company's privacy practices. At the same time, this legislation encourages individuals to notice, read, and comprehend these simpler statements. From a business perspective, a tagging regime only minimally burdens e-commerce operations because covered companies are neither required to adopt any particular privacy practices nor refrain from collecting and disseminating PII. Non-compliance brings a penalty of mandatory tagging, a situation that will create increased and undesired social scrutiny of a company's PII practices. At the end of the day, self-regulation struggles and a European-style, comprehensive information privacy regime is not likely to pass through Congress.[273] PII tagging provides a compromise solution with the power to create a more privacy-protective environment without excessively hampering e-commerce efficiency.

---

273. *See, e.g.*, Shane Ham, *Internet Privacy: The Case for Preemption*, PROGRESSIVE POLICY INSTITUTE, *available at* http://www.cdt.org/privacy/ccp/statepreemption2.pdf (last visited Apr. 4, 2008) (discussing the differences between the European Union and American approaches to information privacy).

> *The battle over legislation to regulate privacy on the Internet has raged for years without resolution in Congress.* Privacy advocates, giving voice to consumer fears about the use of computers to track their online behavior, have argued for tight controls over what may be done with personal information with explicit permission from consumers. Internet companies and other businesses with a presence on the World Wide Web have argued for greater flexibility in using personal information and a presumption that those uses are allowed unless consumers specify otherwise. This stalemate has brought increasing pressure on state legislators to pass laws regulating Internet privacy.

Id. (emphasis added).