The John Marshall Journal of Information Technology & Privacy Law

Volume 26
Issue 1 *Journal of Computer & Information Law - Fall 2008*
Article 1

Fall 2008

The Future of Privacy Policies: A Privacy Nutrition Label Filled with Fair Information Practices, 26 J. Marshall J. Computer & Info. L. 1 (2008)

Corey A. Ciocchetti

ARTICLES

THE FUTURE OF PRIVACY POLICIES: A PRIVACY NUTRITION LABEL FILLED WITH FAIR INFORMATION PRACTICES

COREY A. CIOCCHETTI*

I. INTRODUCTION

E-commerce is here to stay.[1] Since the late twentieth century, the World Wide Web has proven a profitable conduit for businesses to sell almost anything to almost anyone located almost anywhere across the globe. In the United States alone, online retail sales exceeded $33 billion for the first quarter in 2008.[2] Although this figure represents just over three percent of national retail sales, the ratio of e-commerce sales to total sales continues to rise steadily.[3] Despite the tendency of the financial community to look askance at economic figures in this range, it is important to remember that $33 billion changing hands is still *$33 billion changing hands*. Experts predict that online retail sales will top a non-trivial $300 billion per year within the next five years.[4] Additionally, the major players in the sector, companies such as Amazon.com and E-Bay are well-known, global entities that provide valuable services effi-

* Corey Ciocchetti (J.D. Duke 2002, M.A. 1999 University of Denver) is an Assistant Professor of Business Law and Ethics at Daniels College of Business, Univeristy of Denver. Please feel free to contact Professor Ciocchetti at cciocche@du.edu.

1. *See, e.g.*, Jody Yen, *E-Commerce is Here to Stay*, FORBES, Aug. 16, 2002, *available at* http://www.forbes.com/2002/08/16/0816sf.html.

2. *See Quarterly Retail E-Commerce Sales: 1st Quarter 2008*, U.S. CENSUS BUREAU NEWS, May 15, 2008, *available at* http://www.census.gov/mrts/www/data/pdf/08Q1.pdf (providing a chart which places the ratio of e-commerce retail sales to total retail sales (adjusted for seasonal and holiday variations) at approximately .07% in the first quarter of 2000 and approximately 3.4 % in the third quarter of 2007 with steady growth in between).

3. *Id.*

4. *See* Linda Rosencrance, *Online Retail Sales in the U.S. to Hit $204 Billion in '08*, COMPUTERWORLD, Apr. 8, 2008, *available at* http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9075759 (stating that "[o]nline retail sales are projected to hit $204 billion in 2008, up from $175 billion in 2007, and should top $300 billion over the next five years, according to a Shop.org study conducted by Forrester Research Inc.").

ciently via the click of a mouse.[5]

Businesses tap this growing market by enhancing e-transaction capabilities and offering a diverse array of products and services online.[6] In the process, e-commerce websites collect vast amounts of information from their visitors.[7] Much of the collected data is non-identifying and merely discloses computer and network-specific information such as a visitor's Internet Protocol ("IP") address and browser type.[8] The remainder of the data collected, however, is more sensitive and includes personalized information such as names, addresses and phone numbers. This information – known as personally identifying information ("PII") – is rather innocuous in pieces but poses serious threats upon aggregation into a customer profile or "digital dossier."[9]

---

5. *See* Amazon.com, Inc., Quarterly Report (Form 10-Q), at 4, *available at* http://library.corporate-ir.net/library/97/976/97664/items/290167/AMA_10Q.pdf (showing net sales of $4.135 billion and net income of $143 million from January 2008 through March 2008). *See also* E-Bay Inc., Amended Quarterly Report (Form 10-Q/A), at 3, *available at* http://investor.ebay.com/secfiling.cfm?filingID=891618-08-231 (showing net revenues of $2.19 billion and net income of $459 million from January 2008 through March 2008).

6. *See, e.g.,* Kim Leonard, *Retailers In Step With Trend Shift Focus to Web Commerce*, PITTSBURGH TRIB. REV, June 29, 2008, *available at* http://www.pittsburghlive.com/x/pittsburghtrib/news/breaking/s_575113.html.

> Retailers struggling in a weak economy are looking to boost Internet sales. Sometimes, they're closing stores, delaying store openings or simply paying less attention to them. Some national chains, such as technology retailer CompUSA, have shuttered dozens of bricks-and-mortar outlets to cut overhead and refocus efforts online. Smaller, local retailers with special niche products are part of the trend.

Id.

7. *See, e.g.*, Google.com, Google Privacy Center, http://www.google.com/intl/en/privacypolicy.html (last visited Feb. 9, 2008) [hereinafter *Google Privacy Policy*]. *See also* Fed. Trade Comm'n, *History and Overview*, June 1998, *available at* http://www.ftc.gov/reports/privacy3/history.shtm [hereinafter *Privacy Online 1998*]. The World Wide Web is an exciting new marketplace for consumers. This information-rich medium also serves as a source of vast amounts of personal information about consumers. Commercial websites collect personal information explicitly through a variety of means, including registration pages, user surveys, and online contests, application forms, and order forms. Websites also collect personal information through means that are not obvious to consumers, such as "cookies.

8. This type of collection is referred to as "passive" information collection because a website collects this information on its own and a visitor does not enter this information via a web form or other information transaction. *See, e.g.*, Speedtowin.com,, Speed to Win Privacy Policy, http://www.speedtowin.com/privacy.htm (last visited Aug. 2, 2008). Discussing the company's policy on passive collection:

> As you navigate through this site, certain anonymous information may be passively collected (that is, gathered without your actively providing the information) using various technologies. . . For example, your Internet browser automatically transmits to this site some of this anonymous information, such as the URL of the Web site you just came from and the Internet Protocol (IP) address and the browser version your computer is currently using.

Id.

9. *See* DANIEL SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 1–3, (NYU 2004) [hereinafter DIGITAL PERSON] (discussing the idea of aggre-

Realistically, PII collection is essential for e-commerce to function efficiently. For example, a company's transaction fulfillment process must require at a minimum: (1) a customer's financial information to collect payment; and (2) a customer's physical address or e-mail address to deliver purchased items. PII collection also makes online shopping experiences more efficient. For example, frequent customers enter usernames and passwords to create secure online accounts and allow cookie files to store records of previous transactions and other personal information.[10] Companies have learned personal information is a valuable commodity for non-transactional purposes as well. For instance, some companies collect PII, mine it for trends, and tailor marketing campaigns.[11] Others sell collected PII to unrelated third parties. An entire industry of data brokers has emerged to take advantage of the profit potential of aggregating and selling PII profiles.[12] This type of external PII sharing poses serious threats to consumers as their information moves through cyberspace and into the hands of unknown entities with potentially malicious intentions.[13]

The e-commerce community – spurred by pressure from privacy advocacy groups – attempted to combat these serious threats via electronic privacy policies. A privacy policy is a statement detailing a company's practices regarding information gathered via its Web presence.[14] Con-

---

gated digital profiles, or "digital dossiers," and the threats posed when various pieces of PII are collected in one location).

10. *See* Microsoft.com, Description of Cookies, http://support.microsoft.com/kb/260971/en-us (last visited July 1, 2008) (explaining that a cookie file is a small text file, stored on a visitor's computer, which helps a particular website remember information from the visitor's previous visits).

11. *See, e.g.*, *Google Privacy Policy, supra* note 7 (stating that Google "may combine personal information collected from you with information from other Google services or third parties to provide a better user experience, including customizing content for you.").

12. *See, e.g.*, *Congress Revisits a Growing Threat*, SAN JOSE MERCURY NEWS, July 12, 2005, at OP1 (stating that the data broker industry includes firms such as ChoicePoint, Lexis Nexis, Acxiom and which "hold detailed dossiers on every American adult. . .They sell the information to other businesses, which in turn use it to do background checks and determine eligibility for employment, housing, travel and other activities.").

13. *See* Quincy Maquet, *A Company's Guide to an Effective Web Site Privacy Policy*, 2 CHI.-KENT J. INTELL. PROP. 1, 1 (2000). Maquet argues:

> The recent growth of the Internet has provided businesses new and exciting opportunities to expand their business capabilities by using commercial websites. This growth has not only benefited businesses, but also the consumer. The Internet now provides the consumer with a wide variety of goods and services all at the click of a mouse. *However, this convenience also has a very significant drawback for consumers: loss of privacy.*

Id. (emphasis added).

14. Businessdictionary.com, Privacy Policy, http://www.businessdictionary.com/definition/privacy-policy.html (last visited Aug. 1, 2008) (defining a privacy policy as a "[s]tatement that declares a firm's or website's policy on collecting and releasing information about a visitor. . . It usually declares what specific information is collected and

ceptually, the privacy policy movement began with good intentions. Companies were encouraged to create privacy-protective policies they could then translate into posted privacy statements. Armed with information on how companies collect, store, use, and disseminate PII, website visitors would carefully choose when, where, and how they would submit PII online.

It is an understatement to claim the privacy policy concept differs radically from reality. As e-commerce grows and commercial websites flourish, the idea of a privacy policy actually doing what it is supposed to do has become a common joke.[15] Although they are improving, today's privacy policies are: (1) inconspicuously posted; (2) poorly written; and (3) rarely read by website visitors. This article discusses the evolution of this problem and proposes a solution in the form of a privacy nutrition label. Part III demonstrates how privacy policies should work via an examination of key fair information practices ("FIPs"). Part IV proposes a solution via a standardized privacy nutrition label that incorporates key FIPs. This non-obtrusive label is capable of providing visitors with a quick and accurate understanding of how companies utilize their PII. Part V concludes with a request to Congress to require all businesses operating websites in interstate commerce to post a standardized privacy policy label conspicuously on their homepage.

II. PRIVACY POLICIES: THE BASICS

Businesses are habitual policy creators.[16] Typical corporate policies govern operational areas such as human resources, emergency management, or customer service. Policy terms bind specific audiences, most often employees and customers, as well as the company itself. E-com-

---

whether it is kept confidential or shared with or sold to other firms, researchers or sellers.").

15. *See* Donald Daly, *Perspective: Turning Online Privacy Into a Joke*, CNET NEWS, Mar. 29, 2004, http://news.cnet.com/Turning-online-privacy-into-a-joke/2010-1025_3-5180140.html [hereinafter *Perspective*].

> Why is it that some large corporations seem so out of tune with the deep-seated [privacy] concerns of some of their audience? The legalistic approach that some adopt when crafting their online privacy policy is both unfriendly and counter-productive. It serves only to foment anger and distrust while simultaneously perpetuating the 'us and them' culture so graphically exhibited by the major corporate scandals of recent years.

Id. See also Chet Dembeck, *Report Labels Internet Privacy Policies "A Joke,"* E-COMMERCE TIMES, Sept. 16, 1999, *available at* http://www.ecommercetimes.com/story/1243.html?welcome=1214953391.

16. There is an entire market niche dedicated to providing sample policies and helping business draft specific policies. *See, e.g.*, Bizmanualz.com, *Policies and Procedures Manuals & Training Courses*, http://www.bizmanualz.com/about_us/all.html?utm_source=business20&utm_medium=cpc&utm_term=company+policies (last visited July 1, 2008) (helping to provide policies and procedures manuals for businesses).

merce firms create policies similar to brick-and-mortar establishments and add supplemental policies to cover the unique aspects of online operations. Typical e-commerce-specific policies include: (1) *Terms of Use* – governing visitor conduct while surfing a company's website;[17] and (2) *Online Advertising* – governing third-party advertising on a firm's website.[18] Online privacy policies are descended from this administrative lineage.

As the information privacy movement gained momentum, companies faced pressure to protect PII.[19] Unsurprisingly, many turned for help to the familiar practice of policy creation.[20] Firms began to discuss their information practices via online privacy policies linked to their homepage. Instead of protecting an individual's PII, however, early privacy policies tended to create profound confusion – especially in terms of content, readability, and posting.[21] Although the concept of a privacy

---

17. *See, e.g.,* E-Bay.com, *Your User Agreement,* http://pages.ebay.com/help/policies/user-agreement.html (last visited July 1, 2008). *See also* Amazon.com, *Conditions of Use,* http://www.amazon.com/gp/help/customer/display.html?ie=UTF8&nodeId=508088 (last visited July 1, 2008).

18. *See, e.g.,* Amazon.com, *Advertise with Amazon*, http://www.amazon.com/Advertising/b/?node=276257011 (last visited July 1, 2008).

19. Privacy in the arena of PII is often referred to as information privacy. *See, e.g.,* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1205 (1998) (defining information privacy as "an individual's claim to control the terms under which personal information – information identifiable to the individual – is acquired, disclosed, and used.") (internal citations omitted).

20. For example, a law review article from 2000 by a well-known privacy scholar discussed the trend of corporations creating privacy policies in the following manner:

> [M]any companies are actively competing for customers by promoting their privacy policies and practices [via online privacy policies]. If enough consumers demand better privacy protection and back up that demand, if necessary, by withdrawing their patronage, virtually all competitive industry sectors are certain to respond to that market demand. In fact, consumer inquiries about, and response to, corporate privacy policies are an excellent measure of how much the society really values privacy. . . . These more flexible, more contextual, more specific tools often provide better privacy protection than broad laws, and that protection is achieved at potentially lower cost to consumers, businesses, and the society as a whole.

Fred H. Cate, *Commentary: Principles of Internet Privacy*, 32 CONN. L. REV. 877, 890-91 (2000) (internal citations omitted).

21. *See, e.g.,* Will Rodger*, Privacy Isn't Public Knowledge: Online Policies Spread Confusion with Legal Jargon*, USA TODAY, May 1, 2000, at 3D (discussing the problems consumers had with privacy policies). Also stating that:

> Most major Web sites now have privacy policies explaining how they collect and use personal information gathered from visitors. . . . But do big Web sites want you to understand what they tell you? Maybe not, suggests an analysis by an independent expert for USA TODAY of the privacy policies of 10 major sites. . . . [W]ithout exception, policies are ponderous, full of jargon or written so as to leave many surfers scratching their heads, says Mark Hochhauser, the psychologist and linguistics expert who analyzed the sites. Every policy studied is written at a college level or higher, he says. And in a nation in which most people read at the 10th-

policy remained simple,[22] low visitor comprehension and a company's vague privacy commitments[23] created skepticism in the information privacy arena.[24] Ever-developing technologies, sophisticated identity thieves, and the absence of a standardized privacy policy format magnified this problem.

At the same time, the United States legal system failed to provide clear regulatory guidance on information privacy practices.[25] Thus, this void forced companies to self-regulate their privacy policy content,[26] or to focus their administrative energy elsewhere and ignore the privacy implications of collecting PII.[27] While the legal system stumbled, the Fed-

---

> grade level or below, that means a minority will understand the policies. "If you really don't want people to understand, write it in legalese and have it run on for four or five pages. People will say, 'To hell with it,'" he says. Privacy policies began showing up on the Web four years ago, but many policies continue to be confusing because privacy is inherently complex.

Id.

22. *See, e.g.*, Scott Killingsworth, *Minding Your Own Business: Privacy Policies in Principle and Practice*, 7 J. INTELL. PROP. L. 57, 57 (1999) (stating that "[i]n principle, privacy policies are simple: if your website collects individually-identifying information about visitors or customers, tell them how and why you collect the information, how it is used and to whom it is disclosed, and give them some choice in the matter.").

23. *See, e.g.,* DIGITAL PERSON, *supra* note 9, at 83 ("Privacy policies tend to be self-indulgent, making vague promises such as the fact that company will be careful with data; that it will respect privacy; that privacy is its number one concern. . .These public relations statements are far from reliable.").

24. *See, e.g., Perspective*, *supra* note 15.

25. *See, e.g.,* Fred H. Cate, *The Failure of Fair Information Practice Principles* (included in CONSUMER PROTECTION IN THE AGE OF THE INFORMATION ECONOMY, 352 (2006)) [hereinafter CONSUMER PROTECTION]. "[B]eginning in the mid-1990s, the Federal Trade Commission and states attorneys general *encouraged* U.S. operators of commercial websites to adopt and publish online privacy policies. . . *Adoption of such policies was voluntary*; compliance with them was not." *Id.* (emphasis added).

26. *See, e.g.,* Stefanie Olsen, *Ad Firms Benefit from FTC Privacy Decision*, CNET NEWS, July 28, 2000, http://news.cnet.com/2100-1023-243822.html. The article stated that:

> [P]rivacy storm clouds [that had been] gathering above online advertising networks broke up quickly this week, following a government approved proposal to let the industry police itself when it comes to collecting and trading consumer data.. Yesterday's decision by the Federal Trade Commission is the first time the government has set rules on online consumer profiling. The move went a long way toward easing fears that the industry would be severely regulated any time soon.

Id.

27. *See, e.g.,* Joel R. Reidenberg, *Symposium: Data Protection Law and the European Union's Directive: The Challenge for the United States: Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 507-08 (1995). Reidenberg discusses the United States information privacy regime and states:

> As a corollary to minimal state regulation of information flows, the American [information privacy] system values a dispersion of standards for fair information practice. There are no universal rules and there is no discrete source, such as one sectoral rule or one industry norm or practice, to provide all the standards for a particular context. Fair treatment of personal information relies on the aggregation of standards from various sources. This diversity promotes the goal that no

eral Trade Commission ("FTC") attempted to bridge the gap by bringing several high profile cases against companies operating under misleading privacy policy statements.[28] The threat of similar enforcement actions combined with a lack of meaningful governmental regulation sent an ironic message to the e-commerce community. The message said, "create a clear privacy policy and be careful or avoid having a policy and breathe easy." Since companies worried their privacy policies would be next in line to make negative national news, policy drafters (i.e., corporate counsel) could protect their clients by advocating that they operate: (1) without a privacy policy; or (2) under a privacy policy filled with legalese and loopholes, subject to amendment at any time. Either option seemed better than creating a clear and understandable privacy policy. Doing so would run the risk of misleading website visitors as PII practices evolved and subject the company to a potentially embarrassing and expensive FTC enforcement action.[29]

Congress could have improved this situation a decade ago by taking the threats surrounding PII seriously enough to pass legislation.[30] Al-

---

> single actor, whether it be the government through its power to make legal rules or a private firm through market power and contractual relationships, should control information flows.

Id.

See also Thomas T. Reith, *Consumer Confidence: The Key to Successful E-Commerce in the Global Marketplace*, 24 SUFFOLK TRANSNAT'L L. REV. 467, 477 (2001) (stating the "United States has adopted a lassiez-faire position in regulating the on-line industry concerning the retention of consumer information assembled through on-line transactions. . .An established system of privacy protection does not currently exist in the United States.") (internal citations omitted).

28. *See* Fed. Trade Comm'n, Privacy Initiatives: Unfairness & Deception: Enforcement, http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html (last visited Aug. 8, 2008) (discussing the FTC's online privacy cases and linking to the complaints and settlement documents). The FTC's website shows that the Commission began brining actions in the late 1990s with a complaint against GeoCities for violating the terms of its privacy policy. *Id. See also* Press Release, Fed. Trade Comm'n, Internet Site Agrees to Settle FTC Charges of Deceptively Collecting Personal Information in Agency's First Internet Privacy Case (Aug. 13, 1998) *available at* http://www.ftc.gov/opa/1998/08/geocitie.shtm.

29. *See* Robert J. Batson, III, *Personal Privacy on the Internet: Issues and Guidelines for Practicing Attorneys*, 2 TRANSACTIONS 9, 22 (2001). Batson discusses this conundrum and states:

> Internet companies are not required to post a privacy policy on their website under current U.S. law. However, if an online business elects to have a privacy policy, it must not violate it—or it risks an FTC enforcement action. Corporate clients and their counsel should carefully consider how they plan to use any personal information and determine whether or not to create and post a privacy policy that strictly follows such a plan. They must then monitor their business practices to ensure compliance.

Id.

30. There are many threats targeting PII at all stages of an e-commerce transaction. For example, PII can be targeted: (1) upon collection when unnecessary data is required to proceed with a transaction; (2) during storage via a data breach; (3) in possession of its

though the federal government was aware of the threats targeting PII, and the FTC monitored the situation, the lack of national legislation created a free for all in PII collection, storage and dissemination practices.[31] In hindsight, allowing self-regulation to operate unabated by meaningful regulatory guidance was a mistake.[32]

Without over-regulating and replacing self-regulation with a burdensome comprehensive PII regime, Congress can help solve this problem by harnessing the power of privacy policies. This solution must require companies to, at the very least, discuss key fair information practices ("FIPs") in a clearly drafted and conspicuously posted privacy policy.[33]

III. FAIR INFORMATION PRACTICES

The data trade involves the exchange of information from a party who should care a great deal about its protection, to another party who is not interested in the protection of such data. Unfortunately, exchanging sensitive personal information is crucial for the efficiencies of e-commerce to flourish. Fair information practices are guidelines, many of which have international support, which cover the most important as-

---

collectors when PII is used for undisclosed purposes; and (4) upon dissemination to unrelated parties when such parties are bad actors disguised as innocent purchasers. *See generally* Corey Ciocchetti, *The Privacy Matrix*, 12 J. TECH. L. & POL'Y 245 (2007) (discussing the major threats facing PII that is collected, utilized, stored and disseminated by its collector).

31. *See, e.g., Privacy Online 1998*, *supra* note 7. *See also* Fed. Trade Comm'n, *Self-Regulation and Privacy Online: A Report to Congress*, June 1999, *available at* http://www.doncio.navy.mil/privacyprotection/resources/docs/reports/FTC-SelfRegulation-Privacy.html [hereinafter *Privacy Online 1999*] (describing the privacy-invasive issues surrounding the collection of PII).

32. *See, e.g.,* Allyson. W. Haynes, *Online Privacy Policies: Contracting Away Control Over Personal Information?*, 111 PENN. ST. L. REV. 587, 606 (2007). "The focus of FTC and state enforcement is primarily on the website's adherence to its promises, not a general standard of fairness. If the website follows its own policy and provides reasonable security, it is free to do what it wants with a user's personal information." *Id.*

33. *See, e.g.,* Major R. Ken Pippin, *Consumer Privacy on the Internet: It's Surfer* Beware, 47 A.F. L. REV. 125, 136 (1999). Pippin discusses the state of information privacy law in the late 1990s and states:

> [T]he overall self-regulation endorsement by the [Federal Trade] Commission has generally staved off most Congressional action so far, but the potential exists for significant change . . . Numerous Internet privacy bills are currently awaiting action by Congress, most notably, the Online Privacy Protection Act of 1999 [OPPA] and the Consumer Internet Privacy Protection Act of 1999 ("CIPPA"). However, Congress is divided on the issue.

Id.(internal citations omitted). Years later, the significant change has not occurred, neither the OPPA nor the CIPPA are land Congress continues its piecemeal approach to information privacy. *Id.* Federal laws of this type were proposed but continually stalled in Congress. *Id.*

pects of PII collection, use, storage, and dissemination.[34] FIPs protect data subjects, regulate data collectors, and attempt to ensure companies reasonably protect the information they obtain.[35] There are many FIPs in existence across the globe,[36] but five deserve particular attention be-

34. *See Privacy Online 1998*, *supra* note 7. The report discusses FIPs and states that:

> [O]ver the past quarter century, government agencies in the United States, Canada, and Europe have studied the manner in which entities collect and use personal information — their "information practices" — and the safeguards required to assure those practices are fair and provide adequate privacy protection. The result has been a series of reports, guidelines, and model codes that represent widely-accepted principles concerning fair information practices.

Id. (internal citations omitted). The first FIPs were created by the United States government in 1973 via a report issued by the Department of Health, Education and Welfare. *Id. See also* U.S. Dep't of Health, Educ. & Welfare, Secretary's Advisory Comm'n, *On Automated Personal Data Systems, Records, Computers and the Rights of Citizens* (1973), *available at* http://aspe.os.dhhs.gov/datacncl/1973privacy/tocprefacemembers.htm [hereinafter *HEW Report*]. This report was issued by the Secretary of Health, Education and Welfare's Advisory Committee on Automated Personal Data Systems which was charged with looking into the data collection procedures of public and private organizations. *Id.* "In the twenty-five years that have elapsed since the HEW Report, a canon of fair information practice principles has been developed by a variety of governmental and inter-governmental agencies." *Id.* (citing important FIP documents created in the twenty-five years since the issuance of the *HEW Report*). Another important international document of FIPs originated with the Organisation for Economic Cooperation and Development (OECD) in 1980 and has taken the name: *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. See* Oecd.org, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, http://www.oecd.org/document/18/0,3343,en_2649_201185_1815186_1_1_1_1,00.html (last visited July 6, 2008) [hereinafter *OECD Guidelines*].The United States is a member of OECD but the *OECD Guidelines* are not binding on the United States. *Id.*

35. *See Online Privacy 1998*, *supra* note 7. The policy states that FIPs:

> Can be either procedural or substantive. Procedural principles address how personal information is collected and used by governing the methods by which data collectors and data providers interact. These principles ensure that consumers have notice of, and consent to, an entity's information practices. Substantive principles, by contrast, impose substantive limitations on the collection and use of personal information, regardless of consumer consent, by requiring that only certain information be collected and that such information only be used in certain ways. Most of the principles . . . are procedural in nature. One substantive principle widely adopted by the fair information practice codes . . . is the collection limitation principle, which states that entities should only collect personal information necessary for a legitimate business purpose.

Id. (internal citations omitted).

36. *HEW Report*, *supra* note 34. The *HEW Report* discussed the following FIPs as follows:

> Safeguards for personal privacy based on our concept of mutuality in record-keeping would require adherence by record-keeping organizations to certain fundamental principles of fair information practice.
>
> - There must be no personal-data record-keeping systems whose very existence is secret [**The Openness Principle**].
> - There must be a way for an individual, to find out what information about him is in a record and how it is used [**The Disclosure Principle**].

- There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent [**The Secondary Use Principle**].
- There must be a way for an individual to correct or amend a record of identifiable information about him [**The Correction Principle**].
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data [**The Security Principle**].

These principles should govern the conduct of all personal-data record-keeping systems. Deviations from them should be permitted only if it is clear that some significant interest of the individual data subject, will be served or if some paramount societal interest can be clearly demonstrated; no deviation should be permitted except as specifically provided by law.

Id. See also Privacila.org, Privacy and Business: OECD Guidelines, http://www.privacilla.org/business/oecdguidelines.html (last visited July 6, 2008). The OECD's FIPs include the:

1. **Collection Limitation Principle**: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
2. **Data Quality Principle**: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, compete and kept up-to-date.
3. **Purpose Specification Principle**: The purposes for which personal data are collected should be specified not later than at the time of collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
4. **Use Limitation Principle**: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Principle 3 except [under certain circumstances]. . .
5. **Security Safeguards Principle**: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.
6. **Openness Principle**: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
7. **Individual Participation Principle**: An individual should have the right:
   - to obtain from the a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
   - to have communicated to him, data relating to him . . .
8. **Accountability Principle**: A data controller should be accountable for complying with measures which give effect to the principles stated above.

Id. See also OECD Guidelines, supra note 34 (discussing each of the *OECD Guidelines* in more detail). Importantly, the European Union has adopted a list of FIPs in its comprehensive 1995 Data Protection Directive. *See* Parliament and Council Directive 95/46EC of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data, 1995 O.J. (L 281), *available at* http://www.cdt.org/privacy/guide/basic/fips.html [hereinafter *EU Directive*]. "The [EU] Directive granted data subjects a number of important rights including the right of access to personal data, the right to know where the data originated (if such information is available), the right to have inaccurate data rectified, a right of recourse in the event of unlawful processing, and the right to withhold permission to use data in certain circumstances — for example, individuals have the right to opt-out free of charge from being sent direct market-

cause of their recognition by United States law[37] and the FTC.[38] These key FIPs are: (1) Notice; (2) Choice; (3) Access; (4) Integrity; and (5) Enforcement ("Key FIPs").[39] Although privacy advocates claim the list is incomplete and other fair information practices merit similar attention,[40] the FTC calls these five FIPs the "core principles of privacy protection."[41] Regardless of which principles actually constitute the heart of

---

ing material." Center for Democracy and Technology, CDT's Guide to Online Privacy: Privacy Basics: Fair Information Practices, http://www.cdt.org/privacy/guide/basic/fips.html (last visited July 6, 2008).

37. *See* 5 U.S.C. §552a (2000). Federal law implemented the FIPs mentioned in the *HEW Report* via the Privacy Act of 1974 – a law that applies only to federal agencies. *See also* U.S. Dep't. of Justice, Overview of the Privacy Act of 1974, 2004 Ed. (May 2004), http://www.usdoj.gov/oip/1974intro.htm (last visited July 7, 2008). "The Privacy Act of 1974 . . . in effect since September 27, 1975, can generally be characterized as an omnibus 'code of fair information practices' that attempts to regulate the collection, maintenance, use, and dissemination of personal information by federal executive branch agencies." *Id.*

38. *See Privacy Online 1998*, *supra* note 7.

39. *See id.* It is interesting to note that the FTC placed Enforcement in its list of FIPs in its 1998 report to Congress and then took Enforcement out of a similar report in 2000. *See* Fed. Trade Comm'n, *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress*, 12-20 (2000), *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf [hereinafter *Privacy Online 2000*] (reiterating the importance of enforcement by stating: "[i]n addition to the substantive fair information practice principles of Notice, Choice, Access, and Security, a fifth principle is essential to ensuring consumer protection: Enforcement."). However, the FTC does not title Enforcement as a FIP in its 2000 report to Congress. *Id.*

40. *See, e.g., Final Report of the FTC Advisory Committee on Online Access and Security: Online Access*, ABACUS-MS.COM, May 15, 2000, *available at* http://www.abacus-ms.com/acoas/papers/finalreport.htm (discussing the FTC's FIPS [except for enforcement] and stating that as "the Committee's deliberations revealed, this principle of the FTC's Fair Information Practices . . . can be complicated — and controversial.") (emphasis added). *See also* Robert Gellman, *The FTC Saws Off the Privacy Flagpole*, DIRECT MARKETING NEWS, at 14, July 20, 1998, *available at* http://www.anu.edu.au/people/Roger.Clarke/DV/SLCCPteSupp.html. Gellman writes:

> [T]he FTC is guilty of privacy revisionism. Trade associations have for years played the game of redefining fair information practices to suit themselves. Their privacy policies simply omit any inconvenient requirements. The Direct Marketing Association privacy policy is a good example. Much of the content of fair information practices has simply been left out of the DMA policy. The FTC did the same thing, although not to the same degree. . . . This is a better list than you will find in most industry codes, but it is still not complete. . . . Privacy does not mean that anything goes as long as the consumer has not objected. We should not lose sight of the importance of the word fair in fair information practices. Some uses of data and some collection activities are simply inappropriate. Privacy is not just a game of wheedling consumers so they do not object to anything that industry wants to do with data.)

Id. (emphasis added).

41. *Privacy Online 1998*, *supra* note 7. This paper will refer to them as "Key fair information practices" or "Key FIPs."

PII protection.[42] Professor Mary Culnan sums up the argument to use FIPs to govern information privacy in the following manner:

> Fair information practices represent good public policy for both consumers and business. . . . Assuming that the firm's practices are consistent with what it discloses, fair information practices signal to the consumer that the firm will abide by a set of rules that most consumers perceive as fair and will not behave opportunistically. Because fair information practices minimize the risk of disclosure, they help build trust and promote the disclosure of the personal information needed for relationship marketing. Therefore, observing fair information practices is good for business.[43]

At the end of the day, the Key FIPs represent the best place to start building a privacy-protective regulatory regime that does not excessively interfere with e-commerce efficiency. If Congress is going to break its deadlock and actually pass legislation in this area, any extended list of FIPs or overly comprehensive regime proposal will likely face insurmountable opposition. These Key FIPs have gained acceptance by the federal government and provide adequate guidance when utilized in unison. The next five sections analyze each Key FIP and propose the best practices for addressing each in a company's privacy policy.[44]

A. Notice of PII Practices Via Conspicuous Posting

Notice is "the most fundamental" fair information practice.[45] Conceptually, notice requires companies to post their privacy practices clearly and conspicuously for visitors to discover and comprehend before submitting PII.[46] However, such enlightenment cannot occur when com-

---

42. *See, e.g.,* Consumer Protection, *supra* note 25, at 355. The Initial problem of basing a data protection regime on [FIPs] is determining which set of [FIPs] to apply. *Id.* The OECD Guidelines provide eight, the EU data protection directive eleven, and the FTC principles only five (or four). *Id.* The differences are often quite substantive. *Id.*

43. Mary J. Culnan, *Protecting Privacy Online: Is Self-Regulation Working?,* 19(1) J. of Pub. Pol'y & Mktg. 20, 20-26 (2000) [hereinafter *Is Self-Regulation Working?*] (internal citations omitted).

44. *See, e.g.,* Maxine Lans Retsky, *Equip Yourself with Good Privacy Policy*, Am. Mktg. Ass'n: Mktg. News, Feb. 12, 2001, at 9 [hereinafter *Equip Yourself*]. The author states that:

> According to the Better Business Bureau, a good privacy policy says what you do does what you say and verifies that it has been done. The first step in developing such a policy is to figure out what you want to do with the data you collect or decide that you are not going to share the data. Then, draft a policy that is easy to read; for example, create section headings for [certain key elements], and make sure the policy does not contain legalese and jargon.

Id.

45. *See Privacy Online 1998, supra* note 7.

46. *Id*. (stating that consumers "should be given notice of an entity's information practices before any personal information is collected from them. .Without notice, a consumer cannot make an informed decision as to whether and to what extent to disclose personal

panies obfuscate privacy policy links and draft policies in legalese.[47] This remainder of this section analyzes what proper notice means by discussing best practices for privacy policy: (1) posting; (2) drafting; and (3) content.

(1) *Privacy Policy Posting*

The placement of a company's privacy policy is of utmost importance in today's e–commerce environment.[48] Two key factors make this fact abundantly clear. First, a company cannot fulfill its FIP promises if website visitors cannot first locate its privacy statement. Web surfers – accustomed to finding information rapidly on the Internet – will not take the time to track down an inconspicuously posted privacy policy link. Instead, these potential customers generally leave a company's site without entering PII[49] or making a purchase.[50] Second, the majority of major e-commerce companies in the United States currently place a link to their privacy policy on their homepage without any legal obligation to

information."). *See also Is Self-Regulation Working?, supra* note 43, at 20 (describing this FIP as constituting notice "of the firm's information practices regarding what personal information it collects and how the information is used.").

47. *See, e.g.*, George R. Milne, Mary J. Culnan & Henry Greene, *A Longitudinal Assessment of Online Privacy Readability*, 25(2) J. PUB. POL'Y & MKTG. 238, 238-49 (2006) [hereinafter *Longitudinal Assessment*] (stating that "[i]nformation disclosure by marketers has a long history in marketing as a way to improve consumer decision making and choice and to reduce risk. . .For disclosures to be useful in addition to being complete, consumers need to be motivated to read the disclosure, and they must have the ability to comprehend its content.") *Id.* (internal citations omitted).

48. *See Equip Yourself, supra* note 44 (discussing the proper placement of a privacy policy and stating that next, make the privacy policy easy to find by including a prominent link to it on the home page, and especially on the pages where you collect information).

49. *See, e.g.*, George R. Milne & Mary J. Culnan, *Strategies for Reducing Online Privacy Risks: Why Consumers Read (Or Don't Read) Online Privacy Notices*, 18(3) J. OF INTERACTIVE MKTG. 15, 24 (2004) [hereinafter *Privacy Risks*] (discussing a study of 2,468 adult Internet users to determine the extent to which each read privacy policies and finding "that privacy notices are used as one part of an overall strategy to manage the risks of disclosing personal information and that consumers tend to read notices to manage risk."). This study indicates that e-consumers are not prone to enter any PII if they are skeptical of a company's privacy commitments. *Id*. at 25. "[I]f consumers perceive privacy notices as being irrelevant because of format [including policy posting] issues, they may balk at even attempting to read them as some of the open ended comments illustrate." *Id.* (internal citations omitted).

50. In fact, it is unlikely that a consumer will make a purchase if suspicious of a company's privacy policy. *See, e.g.*, *Longitudinal Assessment, supra* note 47, at 238 (stating "[w]hen business is conducted online, there are fewer signaling opportunities for marketers than in the offline world; thus, the notice is a critical contact point with consumers. . .If consumers perceive the online environment as overly risky, they will be less motivated to purchase online.").

do so.[51] Since such a link draws attention – both from customers looking to understand policy terms and from the FTC and various state agencies looking for violations – voluntary policy posting indicates the importance companies place on providing notice of their privacy practices.[52]

Although it is awkward to post the full text of a privacy policy on a homepage, the current best practice is to provide notice that a policy exists via a conspicuous homepage hyperlink.[53] A conspicuous link: (1) contains only the words "Privacy Policy";[54] (2) is placed in a easily discoverable location on a homepage (not buried at the bottom surrounded

---

51. Corey Ciocchetti, *Just Click Submit: The Collection, Dissemination, and Tagging of Personally Identifying Information*, 10 VAND. J. ENT. & TECH. L. 553, 597-98 (2008) (discussing a study of the top twenty-five e-commerce companies which found that 68% placed a conspicuous link to their privacy policy on their homepage).

52. The major outlier is Google. Until July 2008, the company resisted massive public pressure to adhere to the FIP of notice and refused link its privacy policy to its homepage. *See, e.g.,* Saul Hansell, *Google Changes Home Page, Adding Link To Privacy* Policy, N.Y. TIMES, July 4, 2008, http://bits.blogs.nytimes.com/2008/07/04/google-changes-home-page-adding-link-to-privacy-policy/ [hereinafter *Google Changes Homepage*] (stating that the "word 'privacy' now appears on Google's home page, with a link to the company's privacy policy."). A Google executive discussed the change to its purposefully-simplistic homepage on an official Google blog. *See* Posting of Marissa Mayer to The Official Google Blog, *What Comes Next In This Series? 13, 33, 53, 61, 37, 28 . . .*, http://googleblog.blogspot.com/2008/07/what-comes-next-in-this-series-13-33-53.html (July 3, 2008, 01:36 EST). The Google VP stated that Google values information privacy and therefore:

> [W]e are making a homepage change by adding a link to our privacy overview and policies. Google values our users' privacy first and foremost. Trust is the basis of everything we do, so we want you to be familiar and comfortable with the integrity and care we give your personal data. We added this link both to our homepage and to our results page to make it easier for you to find information about our privacy principles. The new "Privacy" link goes to our Privacy Center, which was revamped earlier this year to be more straightforward and approachable, with videos and a non-legalese overview to make sure you understand in basic terms what Google does, does not, will, and won't, do in regard to your personal information.

Id. Problematically, only California requires conspicuous posting of a privacy policy link on a company's homepage and even in the face of this state regulation, Google believed that omitting any mention of privacy on its homepage complied. *See Google Changes Homepage, supra* note 52 (stating that Google "did not believe [the company] was required to put a link on its home page. . . The company said that its privacy policy was easy enough to find."). An official from California's Office of Privacy Protection disagreed and stated that, in her opinion, Google was legally required to post a privacy policy link on its homepage. *Id.*

53. Company policy posting is improving although many links are still difficult to find. *See, e.g.,* Michael Beaudet & Josh Duberman, *Privacy Perspectives for Online Searchers; Internet/Web/Online Service Information*, SEARCHER, 32, July 1, 2000, (stating that "[a]lthough some Web sites still lack a posted privacy policy, an increasing number of sites have them — though they may require some searching to find.").

54. This consistency in terminology is important to encourage website visitors to become comfortable looking for and analyzing a company's privacy policy.

by links visitors tend to ignore such as *Terms of Use* or *Site Feedback*);[55] and (3) appears in a font size similar to surrounding links.[56] Part IV of this article argues that this best practice should evolve to include a privacy nutrition label capable of improving notice of PII practices.

(2) *Privacy Policy Drafting*

Even conspicuous policy posting is only effective if a visitor can comprehend a company's privacy practices. To this end, a recent study showed that if a privacy notice "is not perceived as comprehensible, then it will be less likely to be read. . . . Alternatively, when consumers perceive they can comprehend privacy notices, the more likely they are to both read notices across an array of situations and to trust the notices."[57] Facilitating this understanding and earning visitor trust that a company will keep its word encapsulate what the FIP of notice means. An added benefit stems from the idea that clear policies allow individuals to take ownership for responsibly submitting PII.

Problematically, and for the reasons detailed above, companies have historically struggled to make their policies comprehensible. Part IV discusses some of the major struggles associated with policy drafting such as incomprehensible legalese, excessive length and privacy-invasive loopholes. This section focuses instead on drafting best practices and discusses the benefits that both companies and customers reap when policies are comprehensible. If even lawyers dislike reading legalese, it is easy to imagine how the typical web surfer regards the practice. Even so, today's privacy policies are filled with legalese, loopholes and confusing statements.[58] Even if a diligent website visitor took the time to sort through this document, true and meaningful comprehension would rarely be possible. Additionally:

---

55. *See, e.g.,* Monster.com, http://www.monster.com (last visited July 19, 2008) (providing an example of a privacy policy link buried at the bottom of a prominent company's homepage near links that visitors are likely to ignore).

56. Companies have minimized the impact and discoverability of their privacy policy link by decreasing its font size on their homepage. *See, e.g.,* Comcast.com, http://www.comcast.com/ (last visited July 19, 2008). Links in this format send the message to website visitors that information privacy is less important than the information contained in the larger links.

57. *Privacy Risks*, *supra* note 49, at 24 (continuing by stating that some of the survey comments "also suggested that notices that are perceived by consumers to be obfuscated or excessively legalistic can contribute to skepticism.").

58. *See, e.g.,* Frank Davies, *FTC Reviews Ads Shaped By Online Use*, SAN JOSE MERCURY NEWS, Nov. 2, 2007, at Science and Tech (citing Jon Leibowitz of the Federal Trade Commission stating, "Consumers need better information and more meaningful choices."). Leibowitz complained that too many online privacy policies "are posted inconspicuously, with fine-print legalese and techno-talk." *Id.*

> [T]he growing use of such policies is far from reassuring to privacy advocates. They say that few Web surfers actually bother to read the policies, and that the policies can be hard to understand, misleading, or openly hostile to consumer privacy. "There's a general perception that the presence of a privacy statement implies that your privacy is being protected, which is not true. The privacy statement can say anything," said Lance Cottrell, founder of Anonymizer.com, a site that lets users Web-surf and send e-mail without divulging personal information. "It really takes several years of college education to even understand most privacy policies," he said.[59]

Unclear privacy policies fail to apprise visitors of PII uses that may pose serious privacy violations.[60] "For consumers, there is no silver bullet to solving these privacy issues because each web site shares information differently. So right now the onus is on individuals to protect themselves by painstakingly visiting each site to change their settings."[61] However, the lack of clarity makes self-protection a tough task and leads to visitor neglect of privacy policies.

The concepts discussed in the typical privacy policy require pondering but are by no means rocket science. With this in mind, policy drafters must strive to organize policy content effectively and use words and sentence structure that facilitate comprehension. The best way to guide such drafters is to require the use of plain English. Borrowed from the realm of securities regulation, plain English is a concept designed to eliminate writing styles and phrasing that the average citizen struggles to understand.[62] This is important in a country where hundreds of millions of people (approximately 72% of the United States population) from all different ages and educational/technological backgrounds have Internet access.[63] A plain English document "uses words economically and at a level the audience can understand. Its sentence structure is tight. Its tone is welcoming and direct. Its design is visually appealing. A plain English document is easy to read and looks like it's meant to be read."[64]

---

59. Reid Kanaley, *Web Site Privacy Policies Don't Guarantee Safety*, AUGUSTA CHRON., Oct. 25, 2000, at B8 [hereinafter *Guarantee Safety*].

60. *See, e.g., Web Sites Let Others See Users' Personal Data*, WALL ST. J., Feb. 10, 2008, *available at* http://www.pittsburghlive.com/x/pittsburghtrib/s_551469.html (discussing a controversial policy whereby Facebook.com, Sears.com, and Google News allowed users access to its customers' personal information, sometimes without their knowledge).

61. *Id.*

62. *See* SECURITIES & EXCHANGE COMMISSION, A PLAIN ENGLISH HANDBOOK: HOW TO CREATE CLEAR SEC DISCLOSURE DOCUMENTS (1998), *available at* http://www.sec.gov/pdf/handbook.pdf [hereinafter PLAIN ENGLISH HANDBOOK].

63. Internet World Stats, Usage and Population Statistics, http://www.internetworldstats.com/am/us.htm (last visited July 22, 2008) (showing that the United States had 219,537,606 Internet users as of May 2008 out of a total population of just over 300 million).

64. PLAIN ENGLISH HANDBOOK, *supra* note 62, at 5.

Plain English documents should avoid long sentences, passive voice, weak verbs, superfluous words, legal and financial jargon, numerous defined terms, abstract words, unnecessary details, and unreadable design and layout. As stated above, the Securities and Exchange Commission requires plain English in certain areas of securities documents. The FTC would be able to apply similar plain English standards to privacy policy language.

Privacy policies drafted in plain English provide benefits to both businesses and consumers. From a business perspective, clearly drafted privacy statements provide a continual reminder to company personnel as to the privacy promises they must keep. Clarity of language and distinct promises provide a solid foundation for employees to question privacy-invasive PII collections or to inform customers of current policy honestly and accurately. Properly drafted policies also serve as a quasi compliance checklist to consult every time a company feels pressure to collect more PII, collect different forms of PII, or share more information on the open market. A policy that is not complicated by legalese and loopholes makes the decision as to whether company policy allows additional PII usage much easier. Additionally, the deliberate thought process involved when companies take the time to create privacy terms and draft them clearly is valuable because it forces executives to analyze the desires of their visitors, the ways in which they handle sensitive data, and whether current PII collection/dissemination efforts are worthwhile.

Second, from the consumer perspective, properly drafted privacy policies allow website visitors to comprehend how a company will collect and use their PII *before* they choose to submit any information online. Such knowledge provides consumers with the information they need to have confidence in privacy-protective websites and distrust in privacy-invasive websites. Additionally, studies show that website visitors desire such information and will take company privacy policy into consideration while surfing the Web.[65] Visitors are fed up with the problems mentioned above and retaliate by ignoring a company's privacy policy entirely.[66] Studies show that this neglect stems directly from the fact that visitors tire of the endless legalese placed in privacy statements.[67]

65. *Privacy Risks*, *supra* note 49, at 24 (stating the results of a recent study "suggest that privacy notices are used as one part of an overall strategy to manage the risks of disclosing personal information and that consumers tend to read notices to manage risk.").

66. *See, e.g.,* A. Barton Hinkle, *Government Invades Privacy in Unseen Ways*, RICHMOND TIMES DISPATCH, Nov. 19, 2002, at A11 (discussing a privacy poll by Jupiter Research showing that although 73% of Web surfers worry about their privacy online, 97% claimed they did not read electronic privacy policies carefully and 64% gave such policies even a "cursory glance").

67. *See, e.g., Reduce Legalese in Customer Privacy Policy Language*, 22 HOSPITALITY LAW 8, Aug. 1, 2007 (discussing a study of privacy policies created by companies in the hospitality industry and interviewing the study's author who stated:

The problem with this willful ignorance is that visitors ignore privacy policies and yet continue to submit vast amounts of PII online.[68] This represents the worst of both worlds.

(3) *Privacy Policy Content*

Privacy policies must cover a company's practices regarding the Key FIPs of choice, access, integrity and enforcement to reap the benefits provided by the Key FIP of notice (conspicuous posting and plain English drafting),[69] However, companies must be able to maintain flexibility in their PII practices to operate efficiently in the e-commerce world. Over-regulation and mandated boilerplate terms would hinder executives whose decisions depend on changing technology and trends. This article therefore argues in Part IV for an effective, middle-ground regulatory approach that is stricter than the current self-regulatory regime but less restrictive than a European-style comprehensive regime. Therefore, best practices require that companies accurately cover choice, access, integrity and enforcement. However, policies need not contain any specific

---

> [T]hat almost no one reads privacy policies, Wagner said. "One reason is that most policies are written in impenetrable legalese, and many customers can't be bothered. Instead, we suggest that hospitality firms make a straightforward statement of how personal data will be used up front and then move into the more nuanced points – and that statement should be based on an ethical stance of acting in a trustworthy fashion. The basic principles that we suggest are to minimize harm, offer respect and operate consistently. Doing so will likely manage reputation risk and build customer loyalty over the long term".

Id.

68. Michael W. Lynch, *Privacy at STAKE*, CHIEF EXECUTIVE, Nov. 2008, at 58 (stating that, "[a]ccording to recent surveys, most Internet users describe privacy as one of their major concerns, yet a majority readily provide personal data on a regular basis.").

69. There is no Rosetta stone indicating what types of information to include to maximize privacy policy effectiveness. For instance, the FTC states that:

> Notice of some or all of the following have been recognized as essential to ensuring that consumers are properly informed before divulging personal information:
> - identification of the entity collecting the data [Notice];
> - identification of the uses to which the data will be put [Choice];
> - identification of any potential recipients of the data [Choice];
> - the nature of the data collected and the means by which it is collected if not obvious (passively, by means of electronic monitoring, or actively, by asking the consumer to provide the information) [Choice];
> - whether the provision of the requested data is voluntary or required, and the consequences of a refusal to provide the requested information [Choice]; and
> - the steps taken by the data collector to ensure the confidentiality, integrity and quality of the data [Integrity].

Privacy Online 1998, *supra* note 7 (internal citations omitted). Each of these pieces of information is contained within the remaining four FIPs of choice, access, integrity and enforcement as labeled with the bracketed terms above and are discussed in the relevant sections of this article. *Id.* This article makes the argument that adequately covering choice, access, integrity and enforcement will cover most of the information people claim should be included in proper notice. A more controversial position taken by this article occurs with the privacy policy content provisions detailed later.

PII practices as these remain at the discretion of company executives operating within the ever-evolving industry environment.

Under these content regulations, website visitors can discover a company's privacy policy, comprehend its terms and make decisions before submitting PII. Once web surfers read and understand policy terms, companies with privacy-protective policies will flourish while companies with privacy-invasive practices will likely find themselves without the PII they need to conduct even the most basic e-commerce transaction. For example, it is crucial that companies discuss policy amendment processes. Visitors need to understand when and how their PII will be used differently from the uses they agreed to upon submission. However, it is not necessary to require companies to adopt a policy of "zero policy amendments" without first gaining the consent of each customer. This mandate would please privacy advocates and be very protective of privacy, but it would also hinder a company's ability to change course in an ever-evolving marketplace. Instead, this articles argues that visitors be given the opportunity to judge for themselves whether a company's policy amendment processes adequately protect their PII. These types of decisions cannot occur unless companies are required to discuss choice, access, integrity and enforcement in a standardized manner. Part IV will illustrate how the privacy nutrition label can facilitate this process.

B. Visitor *Choice* Regarding PII Dissemination

As mentioned, companies embrace notice as a fair information practice by discussing the remaining Key FIPs – choice, access, integrity and enforcement – conspicuously and clearly. The FIP of choice deals with visitor control over the collection, use and dissemination of their PII.[70] This discussion must include a discussion of control over PII utilized in a manner different then promised upon collection. Describing choice-related privacy provisions is important because visitors are less likely to perceive PII practices negatively when they can "control future use of [their personal] information."[71] This section elaborates on this FIP by analyzing: (1) PII collection methods; (2) the ways companies utilize and disseminate PII; and (3) various types of visitor choice.

---

70. *See Privacy Online 1998*, *supra* note 7 (stating that "[a]t its simplest, choice means giving consumers options as to how any personal information collected from them may be used."). It is important to remember that this type of choice occurs after an individual has made the initial decision to submit PII online. *Id.* The choice to submit PII (other than passively collected information such as IP addresses and Web browser type) always rests with the individual Web surfer. *Id.*

71. Mary Culnan & Pamela K. Armstrong, *Information Privacy Concerns, Procedural Fairness and Impersonal Trust: An Empirical Investigation*, 10 Org. Science 104, 106 (1999) [hereinafter *Information Privacy Concerns*].

(1) *PII Collection Methods*

There are two ways that companies gather information online – active collection and passive collection.[72] Active collection captures PII when visitors manually submit data to a company's website via a Web form or an e-mail request.[73] Active collection requires an individual to act and cannot occur without visitor consent. Passive collection, on the other hand, occurs as websites collect data without visitor submission or explicit permission.[74] Companies generally collect information passively through devices called cookies or web beacons (i.e., small files/programs embedded into a company's website that do not require a visitor to submit data intentionally).[75] It is important to note that passive collection generally does not involve PII and is less privacy-invasive than active collection.[76] Again, this article does not advocate for a law requiring any

72. *See, e.g.,* Easyonlineclosing.com, Privacy Policy, http://www.easyonlineclosing.com/about/privacypolicy.html (last visited Aug. 1, 2008) (providing an example of a privacy policy that discusses both active and passive PII collection and the methods of such collection) [hereinafter *PII Collection Example*].

73. A typical privacy policy statement regarding active PII collection by states "[w]e will ask you when we need to collect PII . . . PII which we collect may vary depending on the benefits and/or services you select, and may include one or more of the following categories of information: name, company name, physical address, email address, phone number, and credit card information including credit card number, expiration date, and billing address." *Id*.

74. A typical privacy policy statement regarding passive information collection states:

> As you navigate through this site, certain anonymous information may be passively collected (that is, gathered without your actively providing the information) using various technologies, such as cookies, Internet tags or web beacons, and navigational data collection (log files, server logs, clickstream). For example, as explained in more detail below, your Internet browser automatically transmits to this site some of this anonymous information, such as the URL of the website you just came from and the Internet Protocol (IP) address and the browser version your computer is currently using. This site may also collect anonymous information from your computer through cookies and Internet tags or web beacons. You may set your browser to notify you when a cookie is sent or to refuse cookies altogether, but certain features of this site might not work without cookies.

Id.

75. *See PII Collection Example, supra* note 72(discussing PII collection practices). The policy states that:

> [A] privacy policy is a written statement telling users how personal information is collected and used. In some cases, the information is gathered overtly, such as when questionnaires ask for the user's age, address and interests. Sometimes the information gathered is not as obvious; technology can determine what site the user came from, the user's e-mail address, what other sites the user has visited, how long the user stays at a particular Web page and more.

Id. *Guarantee Safety*, *supra* note 59 (discussing passive PII collection). Cookies are "small text files that Web sites place onto visitors' hard drives. *Id.* Cookies tell Web sites and advertising companies where a visitor has been online, and what he or she has viewed. *Id.* Advertisers can use the information to target ads to presumably receptive viewers." *Id*.

76. *See PII Collection Example*, *supra* note 72 (showing that this company does not categorize the information it collects passively as PII because the collection does not in-

particular form of visitor choice regarding the methods by which companies collect information. Instead, best practices require a company to discuss both active and passive information collection practices and specifically define how they collect information under both methods.

(2) *Choice Regarding PII Utilization & Dissemination*

Companies typically use the information they collect in three ways: (1) transaction-related uses; (2) internal uses; and (3) external uses. A transactional use occurs when companies utilize PII to complete an online transaction. For example, an e-commerce retailer such as Amazon.com needs a customer's credit card information and physical address to ship the products from its warehouse to its customer's doorstep. Without such information, the transaction cannot occur.

An internal use involves utilization of PII to market to website visitors, conduct a sweepstakes, communicate, or improve a company's business model.[77] For example, a company may mine home addresses and job titles to tailor a marketing campaign directed at a particular market niche such as upper-middle class homeowners working in sales. Other internal uses include sharing PII with a company's subsidiaries or business partners (often called affiliates) to retool product lines or allocate spending priorities.[78]

An external use occurs whenever a company sells or shares PII with unrelated third parties. Here, the information leaves the relatively safe confines of the company that collected it and enters cyberspace. Once disseminated, the information is irretrievable and may fall into the

---

volve the "collection of personally identifiable information that may personally identify you or allow us to contact you.").

77. *See, e.g.,* Arby's, Privacy Policy, http://www.arbys.com/privacy/ (last visited July 22, 2008). The policy states:

> We may use PII in sweepstakes, contests or promotional activity (i) to register you for those activities, to verify that you comply with the published rules and to notify you if you are a winner, (ii) for coupon, premium or prize delivery, (iii) for notification of special offers; and (iv) to ensure that we comply with applicable laws. The PII you disclose for these and similar activities may be shared with third parties, such as those who may administer the activity for us, and shipping companies who may deliver a prize or premium. . . . We may also use your PII for the following purposes: (v) to personalize and enhance our site and your web site experience; (vi) to send you personalized information about our site via email, (vii) to send you advertising or promotional material from us, our advertisers or business partners; and (viii) to contact you for feedback regarding us, our advertisers or business partners. . . . Your PII will only be shared with administrators, business partners or advertisers for a particular purpose and they will not be permitted to use it for any unauthorized purpose.

Id.

78. This type of use is not PII dissemination because these affiliates generally sign privacy agreements with a company to protect this information, abide by the company's privacy policy and avoid disseminating the information externally.

hands of nefarious e-thieves or other bad actors. For these reasons, external PII dissemination is resoundingly unpopular among Web surfers.[79] External uses represent the greatest threat to PII and companies should make an effort to direct visitor attention to this area.[80]

(3) *Visitor Choice Options*

There are two types of visitor choice options: opt-in choice and opt-out choice.[81] The opt-in choice is privacy-protective and requires the affirmative consent of a visitor before certain PII uses. Some companies require visitors to opt-in to any non-transaction-based uses while others reserve opt-in choice for uses of PII not described in the privacy policy.[82] Companies obtain visitor consent via online registration forms, via specific Web pages, or through an e-mail. Companies operating under an opt-in regime must keep accurate visitor consent records to avoid scrutiny. The opt-out choice, on the other hand, requires that visitors affirmatively request for a company not to use their PII in specific ways. In other words, "[o]pt-out is simply a mechanism where the default is set expressly to allow sharing for [certain PII] uses."[83] Companies prefer the

79. *See, e.g.,* KRISTIN MOAG, AARP PUBLIC POLICY INSTITUTE, AARP MEMBERS' CONCERNS ABOUT INFORMATION PRIVACY (1999), *available at* http://www.aarp.org/research/reference/publicopinions/aresearch-import-180-DD39.html. The report discusses a survey of over 500 AARP members regarding PII uses and finds that the "survey revealed a high level of aversion to businesses, government agencies, or websites selling information about customers to other businesses." *Id.* Moreover, "[i]n each case, at least 87% of respondents reported that it would bother them if their personal information was sold in this manner." *Id.*

80. Many companies explicitly state that they will not share PII with unrelated third parties. *See, e.g.*, The Western Reserve Group, Privacy Policy, http://www.wrg-ins.com/images/privacy_policy.pdf (last visited July 22, 2008) (stating emphatically – in bold and underlined text – the fact that the company does "not sell your personal information to anyone").

81. A third route a company can take is to provide no choice as to PII utilization and dissemination.

82. *See, e.g., Guarantee Safety*, *supra* note 59. In a discussion of the firestorm surrounding Amazon.com's recent amendment to its privacy policy allowing future dissemination of PII without customer consent the company stated that:

> In mid-September [2000], privacy proponents cried foul over Amazon.com's announcement that it had revised its privacy policy to allow future disclosures of user information. Some experts hailed Amazon for being upfront with the change. "I thought, 'Thank you for clarifying,'" said Miller of the information technology association. Others saw it as a bellwether. "We have the leading e-tailer flip-flopping on its privacy policy because the winds have changed," said Evan Hendricks, editor of the Privacy Times newsletter. "I don't see how consumers can have confidence.

Id.

83. ARI SCHWARTZ & PAULA J. BRUENING, CENTER FOR DEMOCRACY AND TECHNOLOGY, ON CONSENT, CHOICE, AND CHECK BOXES: SORTING OUT THE OPT-IN V. OPT-OUT DEBATE, (July 22, 2007), *available at* http://www.cdt.org/publications/optin-optout.shtml [hereinaf-

opt-out choice because the onus rests on the visitor to: (1) understand potential PII uses; (2) understand how to opt-out of such uses; and (3) actually opt-out correctly.[84]

C. VISITOR *ACCESS* TO COLLECTED PII

The third Key FIP of access is the least intuitive of the group. A complete discussion includes four components. These components revolve around a visitor's ability to: (1) view collected PII ("Viewing"); (2) change collected PII ("Changing"); (3) remove collected PII ("Removal"); and (4) dispute the accuracy of collected PII ("Disputing"). The FTC addresses three of these variations in its definition of this FIP:

> Access . . . refers to an individual's ability both to access data about him or herself—*i.e.*, to view the data in an entity's files [VIEWING]—and to contest that data's accuracy and completeness [DISPUTING]. Both are essential to ensuring that data are accurate and complete. To be meaningful, access must encompass timely and inexpensive access to data, a simple means for contesting inaccurate or incomplete data, a mechanism by which the data collector can verify the information, and the means by which corrections [CHANGING] and/or consumer objections can be added to the data file and sent to all data recipients.[85]

The most obvious component is viewing collected PII. This permutation involves company policy regarding visitor access to individual-specific PII records.[86] Sophisticated databases facilitate visitor viewing and allow companies to craft an inexpensive and efficient viewing process.[87]

---

ter CHECK BOXES] (discussing the pros and cons of both opt-in and opt-out regimes from the perspective of a privacy advocacy group).

84. *See id.* (stating that the "incentive for companies selecting consent/choice mechanisms will be to choose the mechanism that will likely result in the greatest number of individuals sharing data for secondary purposes rather than the mechanism that provides the individual with the clearest choice."). Opting-out, however, is not as difficult as it used to be. *See Online Privacy 1998*, *supra* note 7 (stating that in "the online environment, choice easily can be exercised by simply clicking a box on the computer screen that indicates a user's decision with respect to the use and/or dissemination of the information being collected.").

85. *Privacy Online 1998*, *supra* note 7 (internal citations omitted). The only concept not explicitly mentioned by the FTC is removal of collected PII.

86. It is important to remember that this FIP refers to access by the submitter of PII and not by other individuals or entities.

87. In this vein, a typical privacy policy allowing access would read as follows: "You may contact us to access the personal information you provide to us [Viewing] and to ask us to update, correct, [Changing] or delete it from our databases [Removal]. You may also request that we cease using your personal information for marketing purposes or for sharing it with other Thomson Reuters affiliates for their marketing purposes." Thompson Reuters, Privacy Statement, http://www.thomsonreuters.com/business_units/financial/integration/privacy/ (last visited July 25, 2008) (disputing collected PII is the only access concept not allowed by this company). Today's databases are powerful and allow for almost instantaneous access to information. *See, e.g.*, The Database Company, Database Technol-

The biggest obstacle is ensuring that the individual requesting access is the same individual the PII identifies.[88] The other meanings of access are less obviously related, but just as important as viewing collected PII. Changing collected PII involves company policy regarding PII amendments made upon visitor request. Such amendments generally involve PII such as an e-mail address or credit card number that has changed. Similarly, removal of collected PII involves company policy allowing for removal of PII from company databases upon visitor request. Finally, the FIP of access contemplates visitor disputes over the accuracy of collected PII. Dispute provisions are most important when a company holds information that forms the basis of subsequent decisions. For instance, consumers should be able to dispute incorrect information held by a credit bureau as inaccuracies as these mistakes can lead to unjust denials of credit.[89]

D. *Integrity* of Collected, Stored and Disseminated PII

The recent ChoicePoint[90] and LexisNexis[91] security breaches, for example, demonstrate the importance of PII security in a world filled with

---

ogy Explained, http://www.the-database.co.nz/database-technology.html (last visited July 25, 2008) ("Extracting data has never been easier because of the powerful tools available that can help analyze and report your information. . .It's also much easier to access your database from spreadsheets and other software applications.").

88. Secure identity verification can occur via a secure login page with a username and password mailed to the e-mail address of the individual the PII identifies.

89. The Fair Credit Reporting Act ("FCRA") allows consumers to dispute errors in their credit report. *See* 15 U.S.C. § 1681 et seq. (2006). Section 1681(i)(a)(1)(A) states that:

> [I]f the completeness or accuracy of any item of information contained in a consumer's file at a consumer reporting agency is disputed by the consumer and the consumer notifies the agency directly . . . of such dispute, the agency shall, free of charge, conduct a reasonable reinvestigation to determine whether the disputed information is inaccurate and record the current status of the disputed information, or delete the item from the file . . . before the end of the 30-day period beginning on the date on which the agency receives the notice of the dispute from the consumer . . .

Id. See also Fed. Trade Comm'n, Facts For Consumers: How To Dispute Credit Report Errors, (Sept. 2008)http://www.ftc.gov/bcp/edu/pubs/consumer/credit/cre21.shtm (stating that "[u]nder the FCRA, both the consumer reporting company and the information provider (that is, the person, company, or organization that provides information about you to a consumer reporting company) are responsible for correcting inaccurate or incomplete information in your report. . .To take advantage of all your rights under this law, contact the consumer reporting company and the information provider.").

90. *See, e.g., ChoicePoint: Potentially 145,000 ID Victims,* FoxNews.com, Feb. 2, 2005, http://www.foxnews.com/story/0,2933,148259,00.html. The company "acknowledged . . . that thieves apparently used previously stolen identities to create what appeared to be legitimate businesses seeking ChoicePoint accounts." *Id.* "The bandits then opened up 50 accounts and received volumes of data on consumers, including names, addresses, Social Security numbers and credit reports." *Id.* The ID scam apparently accessed data on over 145,000 individuals. *Id.*

sophisticated e-thieves and lightening fast data movement.[92] Protecting personal information is a never-ending task and companies must invest in technology and expertise to stay ahead of current security breach strategies.[93] In doing so, companies must think about the following issues:

> Securing data is not a simple endeavor; a multi-discipline, defense-in-depth approach is necessary, as information can leak at any point in the communication process, from receipt, through storage, retrieval, transmission, and so on. Furthermore, each information system element is vulnerable to loss, including hardware, software, and personnel. Add to this the exceptional efforts made by those who want to acquire information through illicit means, whether for espionage, criminal, political, mischievous, or other intent. . .someone is always trying gain access to information they shouldn't have. Organizations, for the most part, have come to recognize the value of the operational and functional information they possess, and are taking pains to protect it accordingly.[94]

Best practices for the integrity FIP require a policy to describe the manner in which a company protects PII during the collection process and as the company stores PII in its databases. It is crucial that privacy policies clearly describe a company's security practices in *plain English* and without unnecessary details. It is also crucial that companies take the time to analyze their current data security practices and the types of

---

91. *See, e.g.,* Heather Timmons, *Security Breach at LexisNexis Now Appears Larger*, N.Y. TIMES, Apr. 13, 2005, at C7, *available at* http://www.nytimes.com/2005/04/13/technology/13theft.html. The "owner of the LexisNexis databases, said . . . that Social Security numbers, driver's license information and the addresses of 310,000 people may have been stolen, 10 times more than it originally reported ." *Id.* "The company said there were 59 separate instances in which unauthorized users 'may have fraudulently acquired personal identifying information' . . . Unauthorized . . . users often used log-in names and passwords that were assigned to legitimate customers." *Id.*

92. *See, e.g.,* Paula L. Green, *The Network Is the Risk*, RISK & INSURANCE Sept. 5, 2005, *available at* http://www.accessmylibrary.com/coms2/summary_0286-9651716_ITM. The author discusses data theft and states that in August 2005:

> The Zotob virus disabled CNN and ABC News, showing how vulnerable computer networks really are. In the financial services world, e-thieves can make off with financial data without leaving a trace. . . As computer criminals become as sophisticated and swift as the technology they use to commit their crimes, corporate executives are taking a closer look at whether they should invest in network-risk insurance.

Id.

93. *See, e.g.,* Don Canning, *Emerging Technology: Staying Ahead of Hackers*, May 1, 2007, http://windowsfs.com/enews/staying-ahead-of-hackers-web-application-security-for-the-insurance-industry. "Computer Crime and Security Survey, conducted by 'Over 90 percent of companies surveyed detected security breaches with over 80 percent incurring financial loss as a result.'" *Id*. "These types of figures show that it's time for companies to take action." *Id*.

94. Ben Malisow, *Valuing Secure Access to Personal Information*, SECURITY FOCUS, Aug. 19, 2004, http://www.securityfocus.com/infocus/1797.

data stored in its databases, as well as stay on top of current security technology.[95]

E. *Enforcement* of Penalties for Broken Privacy Commitments

Enforcement involves two interrelated concepts: (1) a legal regime containing penalties for violations of privacy promises; and (2) the enforcement of the regime. It is a bit awkward to categorize enforcement as a fair information practice because governments provide enforcement while companies are responsible for providing notice, choice, access, and integrity. Regardless, it is "generally agreed that the core principles of privacy protection can only be effective if there is a mechanism in place to enforce them."[96] Therefore, enforcement merits a place as a Key FIP.

Under a self-regulatory regime, businesses have little incentive to protect privacy at the expense of profits, and victims of misleading privacy policies have a slim chance of obtaining redress.[97] While aggrieved parties can report violations to the FTC, they must then wait, cross their fingers and hope for a large-scale enforcement action.[98] A massive legal response in the form of an enforcement action is unlikely, however, as

---

95. *See, e.g.,* Fed. Trade Comm'n, Protecting Personal Information: A Guide for Business, http://www.ftc.gov/infosecurity/ (last visited Feb. 9, 2008).

96. *See* Fed. Trade Comm'n, Fair Information Practice Principles, http://www.ftc.gov/reports/privacy3/fairinfo.shtm. The report states that:

> [a]bsent an enforcement and redress mechanism, a fair information practice code is merely suggestive rather than prescriptive, and does not ensure compliance with core fair information practice principles. Among the alternative enforcement approaches are industry self-regulation; legislation that would create private remedies for consumers; and/or regulatory schemes enforceable through civil and criminal sanctions.

Id.

97. *See, e.g*., *Privacy Online 2000*, *supra* note 39. "Only 20% of the busiest sites on the World Wide Web implement to some extent all four fair information practices in their privacy disclosures. Even when only Notice and Choice are considered, fewer than half of the sites surveyed (41%) meet the relevant standards." *Id*.; Paul Venezia, *IBM Enhances the Honor System*, InfoWorld, June 23, 2003, *available at* http://www.infoworld.com/infoworld/article/03/06/20/25FEprivacyibm_1.html ("Most privacy policies look great on paper, but enforcing them is based almost exclusively on the honor system.").

98. The FTC currently accepts complaints online. *See* Fed. Trade Comm'n, Before You Submit a Complaint, https://www.ftccomplaintassistant.gov/ [hereinafter *FTC Complaints*] (last visited July 26, 2008). The long wait occurs because the FTC does not resolve individual consumer complaints:

> [y]our complaints can help [the FTC] detect patterns of wrong-doing, and lead to investigations and prosecutions. The FTC enters all complaints it receives into Consumer Sentinel, a secure online database that is used by thousands of civil and criminal law enforcement authorities worldwide. *The FTC does not resolve individual consumer complaints*.

Id. (emphasis added). Part IV discusses ways a privacy nutrition label can improve this complaint process. *Id.*

the FTC has brought fewer than thirty actions over the past ten years.[99] This self-regulatory regime came to be after much lobbying from the businesses community.[100] Prior to 1998, the FTC supported self-regulation; however, as of July 1998, the Commission recognized the problems mentioned throughout this article and began to argue for federal regulation requiring companies to adhere to FIPs.[101] Best practices require that a company disclose exactly how a visitor can report a violation of a privacy policy promise. This article argues that a legally required privacy nutrition label, strengthened by an enforcement agenda by the FTC, can properly embody this FIP.

IV. THE FUTURE OF PRIVACY POLICIES: THE CONCEPT OF A PRIVACY LABEL

The previous sections describe the serious problems inherent in contemporary privacy policies and analyze five Key FIPs that can increase

---

99. *See* Fed. Trade Comm'n, Enforcement: Cases, http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html (last visited July 27, 2008) (showing that the FTC has brought 24 enforcement actions since February 1999).

100. *See, e.g., Guarantee Safety*, *supra* note 59, stating that:

> Many Web businesses have hoped that privacy policies, voluntary statements listing how their sites intend to use the information they collect about visitors, would prove that self-regulation, rather than government intervention, can ensure the safety of personal data online. "If government does it, it's going to get screwed up, and it's going to get screwed up badly," said Harris N. Miller, president of the Information Technology Association of America, a trade group representing 11,000 software, Internet, telecommunications and e-commerce companies.

Id.

101. *Compare Privacy Online 1999*, *supra* note 31, stating that:

> [S]elf-regulatory initiatives . . . reflect industry leaders' substantial effort and commitment to fair information practices. They should be commended for these efforts. . . . Only a small minority of commercial Web sites, however, have joined these programs to date. Similarly, although the results of the GIPPS and OPA studies show that many online companies now understand the business case for protecting consumer privacy, they also show that the implementation of fair information practices is not widespread among commercial Web sites. Based on these facts, the Commission believes that legislation to address online privacy is not appropriate at this time. We also believe that industry faces some substantial challenges. Specifically, the present challenge is to educate those companies which still do not understand the importance of consumer privacy and to create incentives for further progress toward effective, widespread implementation.

Id.; *Privacy Online 2000*, *supra* note 39, which states that the FTC now:

> believes that industry's limited success in implementing fair information practices online, as well as ongoing consumer concerns about Internet privacy, make this the appropriate time for legislative action. The Commission's proposed legislation would require all consumer-oriented commercial Web sites, to the extent not already covered by the COPPA, to implement the four widely-accepted fair information practice principles [notice / choice / access / security or integrity], in accordance with more specific regulations to follow. Such legislation, in conjunction with self-regulation, would ensure important protections for consumer privacy at a critical time in the development of the online marketplace.

Id.

policy effectiveness. Problematically, the current self-regulatory environment has proven that companies are not prone to adhere to these FIPs on their own.[102] Congress can help remedy the situation by requiring companies to discuss how their privacy practices relate to the Key FIPs. Federal legislation can improve privacy without requiring specific policy language and without taking the form of a comprehensive information privacy regime that will hamper the efficiency that drives e-commerce.[103] This final substantive part discusses the concept of a privacy nutrition label ("Label") as part of this middle ground solution. Labels provide a conspicuous and clear explanation of how a company incorporates FIPs and serve as standardized diagrams designed to become regular viewing among Web surfers.

Before beginning this discussion, it is interesting to note that the information privacy arena is loaded with individuals and organizations continually proposing ideas aimed at fixing privacy-invasive

---

102. *See, e.g.,* Privacy Rights Clearinghouse, A Review of the Fair Information Principles (Feb. 2004), http://www.privacyrights.org/ar/fairinfo.htm (last visited Aug. 1, 2008). The article states that:

> [S]everal industry groups in the U.S. have formulated their own sets of Fair Information Principles, for example the Direct Marketing Association, the Information Industry Association, and the individual reference services industry . . . These groups have developed such policies primarily in response to the Clinton Administration's self-regulatory approach. . . . It is the opinion of the Privacy Rights Clearinghouse that the strongest of the privacy principles. . . have not been incorporated into the daily practices of industry members.

Id. This problem likely explains the willingness of the FTC to change positions from advocating for self-regulation to advocating for Congressional action as explained in footnote 101.

103. The European Union created a comprehensive information privacy regime that is much more restrictive than the privacy nutrition label regime proposed in this article. *See generally EU Directive, supra* note 36. The *EU Directive* states that:

> 1. Member States shall provide that personal data must be:
> a. processed fairly and lawfully;
> b. collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. . . .
> c. adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
> d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
> e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.
> 2. It shall be for the controller to ensure that paragraph 1 is complied with. *Id.* at Ch. 2, Art. 6.

Id.

problems.[104] Therefore, it is surprising that the idea of a privacy nutrition label has not merited much academic attention to date.[105] Although the concepts of privacy policy reform and standardization have many proponents – including the FTC[106] – relevant literature rarely mentions privacy nutrition labels.[107] A few companies have proposed mechanisms similar to a label on their own initiative; however, these policies generally take the form of condensed privacy notices or summary privacy policies and do not represent a true privacy nutrition label.[108] This final

104. *See*, *e.g.,* Center for Democracy and Technology, http://cdt.org/; The Privacy Rights Clearinghouse, http://privacyrights.org/; and the Electronic Privacy Information Center, http://epic.org/.

105. *See, e.g.*, Patrick Gage Kelley, Sungjoon Steve Won & Lorrie Faith Cranor, POSTER SESSION: *Design of a Privacy Label for P3P Policies* (2008), *available at* http://cups.cs.cmu.edu/soups/2008/posters/kelley.pdf (advocating in a poster session for a privacy nutrition label but focusing more on the design attributes than on the content). KLEIMANN COMMC'N GROUP, INC., EVOLUTION OF A FINANCIAL PRIVACY NOTICE: A REPORT ON THE FORM DEVELOPMENT PROJECT (2006), *available at* http://www.ftc.gov/privacy/privacyinitiatives/ftcfinalreport060228.pdf (analyzing the best practices of designs for standardized privacy notice – not a privacy label – for policies required under the Gramm-Leach-Bliley Act).

106. *See, e.g., Privacy: A Nutrition Label for Your Privacy Policy*, NAT'L JOURNAL'S TECHNOLOGY DAILY, Mar. 18, 2002. "Dozens of leading Web sites are adopting the Internet's version of nutrition labels, giving visitors a quick overview of how well they honor surfers' personal privacy, reports . . . The labels offer consumers a simpler alternative to the lengthy, legalese-filled privacy policies." *Id*. *See also* Fed. Trade Comm'n, *The Case for Standardization of Privacy Policy Formats: Statement by Commissioner Sheila F. Anthony*, *available at* http://www.ftc.gov/speeches/anthony/standardppf.shtm (last visited July 27, 2008) [hereinafter *Standardization*]. She argued for standardization in e-commerce privacy policies utilizing a nutrition label format:

> The NLEA food labels . . . provide excellent examples of standardized formats that convey complex but important information for consumers. A number of benefits that would flow from standardizing the formats including creating a level playing field for industry and providing consumers with easy to understand information about the information sharing practices of the companies with which they do business. A standardized privacy format could provide consumers more confidence in the online marketplace that will only be good for business in the long run.

Id.

107. Articles advocate for privacy policy standardization but without using a privacy nutrition label as the vehicle. *See, e.g.,* Karim Z. Oussayef, Note, *Selective Privacy: Facilitating Market-Based Solutions to Data Breaches by Standardizing Internet Privacy Policies*, 14 B.U. J. SCI. & TECH. L. 104, 128-30 (Winter 2008) [hereinafter *Selective Privacy*] (advocating for standardization of privacy policies using privacy seals as the vehicle and having the FTC award seals to companies with complaint privacy policies). *See also* William S. Challis & Ann Cavoukian, *The Case for a U.S. Privacy Commissioner: A Canadian Commissioner's Perspective*, 19 J. MARSHALL J. COMPUTER & INFO. L. 1, 36 (2000) (stating that the standardization of P3P technology – discussed below and not quite the same thing as a standardized privacy policy – makes such technology "a potentially useful tool for implementation of either voluntary codes or legislated public policy initiatives.").

108. Robert Lemos, *MSN Sites Get Easy-To-Read Privacy Label*, CNET, Mar. 11, 2005, *available at* http://news.cnet.com/2100-1038_3-5611894.html. Lemos states that MSN:

> [h]as adopted a standard format for displaying information on its practices on MSN portals in the United States, Canada, Australia and Hong Kong. The

section attempts to make an early contribution to the discussion regarding the logistics and content of a true privacy nutrition label.

A. Privacy Nutrition Labels: The Basics

The Nutrition Labeling and Education Act ("NLEA") of 1990 required food labeling for the purpose of informing consumers of nutritional content and to entice them to make healthier food choices.[109] More specifically, Congress mandated:

> [T]hat every covered food would have a uniform nutrition label disclosing the amount of calories, fat, salt and other nutrients. The legislative history notes that to make this information meaningful, FDA would be required to issue standards providing that uniform serving size information and information concerning the number of servings be furnished on the food label. . .
>
> The NLEA requires that a health claim on conventional foods be stated in a manner that enables consumers to understand the relationship of the substance to the disease and its relative significance in the context of a total daily diet. The format is universal and consumers can easily determine the amount of calories, fat, salt, and other nutrients foods contain. The format is easy to read and understand.[110]

NELA labels have successfully raised consumer awareness regarding the nutritional value of different foods.[111] The privacy nutrition label would be a direct descendant of these NELA labels and would target consumer awareness of privacy practices. It is helpful to consider Labels

---

> changed format . . . summarizes the data the company collects, how it intends to use the data and what choices a consumer has regarding their information. 'We want someone to read this like a nutritional label and quickly compare and see what data we collect and what you can opt out of,' said Diane McDade, director of policy and privacy for the Technology Care and Safety group at MSN.

Id. These new statements are really privacy policy summaries and not a standardized privacy nutrition label placed on company homepages. The practice of creating a different version of the same policy (i.e., summary version and full-text version) is referred to as multi-layering. *See, e.g.,* The Center for Information Privacy Leadership, Ten Steps To Develop a Multilayered Privacy Notice, http://www.hunton.com/files/tbl_s47details%5Cfileupload265%5C1405%5Cten_steps_whitepaper.pdf (last visited Aug. 1, 2008) (describing the best practices regarding the creation of multi-layered privacy policies).

109. *See* 21 U.S.C. § 343, § 343(q)(1)-(5) (2000) (stating that foods created for human consumption and offered for sale must contain standardized labels with specific nutritional information such as the serving size, number of servings and number of calories).

110. *Standardization*, *supra* note 106 (internal citations omitted).

111. *See id.* (stating that the "NLEA's nutrition labeling regulations have been extremely successful. . .There is high consumer awareness of the labels and some evidence that many consumers are making healthier choices about the food they eat.") (internal citations omitted). *See generally* Bruce Silverglade, *The Nutrition Labeling and Education Act - Progress to Date and Challenges for the Future*, 15(1) Journal of Public Policy & Marketing 148, 148-56 (1996) (discussing the NELA nutrition labeling requirement and its successes).

as a type of stoplight for Web surfers. Each Label will indicate, in a standardized manner, whether a company's privacy practices are privacy-protective (indicating it is safe to go forward) or privacy-invasive (stop!).[112] Because Labels will require a clear discussion of policy terms it is unlikely that visitors will encounter a yellow light in the form of a confusing policy label.

The goal of a Label regime is for visitors to open a specific Web page, encounter the Label, read and understand its meaning and, hopefully, find guidance on whether to submit PII. Because each Label will describe a company's privacy practices as they relate to each component of notice, choice, access, integrity, and enforcement visitors will be able to submit PII only to websites that fit their privacy requirements.[113] Labels will also standardize the look and feel of privacy policies and be located on a company's homepage.

The enactment of a nutrition label law would be a unique accomplishment in the world of information privacy. Today, the most used privacy notification instruments to a Label are: (1) the *Privacy Bird;*[114] and (2) the Platform for Privacy Preferences Project ("P3P").[115] Problematically, companies are not legally required to utilize either option in their privacy policies making these solutions voluntary. Additionally, both the *Privacy Bird* and P3P face major obstacles such as required download onto a user computer or complicated technical interfaces that depend upon honest and clear company disclosure.

For example, the *Privacy Bird* is a downloadable software program that monitors company privacy practices.[116] The *Privacy Bird* program:

---

112. *See Standardization*, *supra* note 106.

> Online privacy policies . . . appear to have been written by lawyers for lawyers. As a general rule, privacy policies are confusing, perhaps deliberately so, and industry has no incentive to make information sharing practices transparent. If privacy polices [sic] were presented in a standard format, a consumer could more readily ascertain whether an entity's information sharing practices sufficiently safeguard private information and consequently whether the consumer wishes to do business with the company.

Id.

113. *See id.* (describing the benefits of a standardized privacy policy format and stating that "consumers could easily determine what an entity's information sharing practices are and then determine whether it meets their privacy objectives.").

114. *See* Privacy Bird, http://www.privacybird.org/ (last visited Aug. 1, 2008) [hereinafter *Privacy Bird*].

115. *See* Platform for Privacy Preferences Project, http://www.w3.org/P3P/ (last visited Aug. 1, 2008) [hereinafter *P3P*].

116. *See Privacy Bird*, *supra* note 114. Stating that:

> Privacy Bird is a tool that can be added to your Internet Explorer Web browser. It allows you to enjoy all the benefits of the Internet, while helping you to remain aware of Web site privacy policies. The software will search automatically for privacy policies at every web site you visit. You can tell the software about your pri-

> [s]earches automatically for privacy policies at every web site you visit. You can tell Privacy Bird about your personal privacy preferences, and it will notify you as to whether each site's policies match your privacy preferences by displaying a bird icon in the top right of your browser's title bar. You can click on the bird at any time to open the Privacy Bird menu.[117]

This program uses an icon of a bird that turns different colors depending upon whether a firm's privacy policy meets the user's privacy specifications.[118] The major problem associated with the *Privacy Bird* program is that a specific website "must be encoded according to the Platform for Privacy Preferences (P3P) standard in order for the Privacy Tool to fetch it. If the policy contains an error or if it has expired or is not valid, the yellow bird will appear."[119] Users encountering a yellow bird will be stuck between leaving a website because their software program cannot determine its privacy practices or proceed forward in the midst of unclear privacy practices. A privacy nutrition label eliminates these problems because visitors will be able to determine a website's privacy practices upon each visit – they will never encounter a "yellow bird."

P3P operates similarly to the *Privacy Bird* as a user enters privacy preferences into a program that checks compatibility with specific websites upon entrance. P3P is privacy-protective because:

> The Platform for Privacy Preferences Project (P3P) enables Websites to express their privacy practices in a standard format that can be retrieved automatically and interpreted easily by user agents. P3P user agents will allow users to be informed of site practices (in both machine- and human-readable formats) and to automate decision-making based

---

vacy concerns . . . and it will tell you whether each site's policies match your privacy preferences.

Id.

117. *See* Privacy Bird Tour, http://www.privacybird.org/tour/1_3_beta/tour.html (last visited Aug. 1, 2008) [hereinafter *Privacy Bird Tour*].

118. *See id.* The site discusses this color change and states that:

> The singing GREEN BIRD appears when Privacy Bird determines that a web site's privacy policy matches your preferences. If the site contains images or other embedded content that do not have privacy policies associated with them, or that have privacy policies that do not match your preferences, a red exclamation point will appear next to the notes in the bird's song bubble. . . . The angry RED BIRD appears when Privacy Bird determines that a web site's privacy policy conflicts with your preferences. . . . The uncertain YELLOW BIRD appears when Privacy Bird is unable to fetch or read a privacy policy from the web site you are visiting. The Privacy Tool will only fetch a policy encoded according to the Platform for Privacy Preferences (P3P) standard. If the policy contains an error or if it has expired or is not valid, the yellow bird will appear. While a web page is loading and Privacy Bird is in the process of looking for the accompanying privacy policy, the yellow bird will appear to be turning its head from side to side. . . . The sleeping GRAY BIRD appears when Privacy Bird is disabled.

Id. (emphasis in original).

119. *See id.*

> on these practices when appropriate. Thus users need not read the privacy policies at every site they visit.[120]

One of the biggest problems with P3P is that website visitors need not read privacy policies to receive protection and will never become familiar with their terms.[121] This is acceptable unless and until the P3P software: (1) fails to read a company's policy correctly; or (2) becomes corrupted on a user's computer. These accidents will leave a visitor unprotected and unable to determine specific privacy practices. A privacy label, on the other hand, will require visitors to read it in order to gain an accurate understanding of privacy practices. Because Labels must be clear, consistent reading by visitors should lead to improved understanding of privacy policies over time.

The Label proposed in this article differs from the current options because it will be mandatory. In fact, unlike the *Privacy Bird* and P3P, website visitors will not have to take any action to obtain its benefits. A privacy Label cannot malfunction and companies face enforcement actions if their Labels are non-compliant. Additionally, each Label will discuss a company's practices regarding the Key FIPs – something not required by either the *Privacy Bird* or P3P. The next section discusses how a privacy nutrition label requires companies to discuss the Key FIPs through standardized statements.

B. Privacy Nutrition Labels: Incorporating Key FIPs

An effective privacy label law requires companies to discuss, in a standardized manner, their policies regarding the Key fair information practices. This article advocates that companies discuss each FIP by choosing from a variety of pre-written statements to include in their La-

120. P3P, *supra* note 115.

121. Other problems with P3P have been proposed. *See, e.g.,* Electronic Privacy Information Center, *Pretty Poor Privacy: An Assessment of P3P and Internet Privacy*, (2000), *available at* http://epic.org/reports/prettypoorprivacy.html. This article discusses the demerits of P3P, stating that:

> P3P fails to comply with baseline standards for privacy protection. It is a complex and confusing protocol that will make it more difficult for Internet users to protect their privacy. P3P also fails to address many of the privacy problems specifically associated with the Internet. Earlier versions of P3P were withdrawn because the developers recognized that the proposed negotiation process was too burdensome for users and that the automatic transfer of personal information would be widely opposed. It is anticipated that this version of P3P will also be significantly overhauled once it is reviewed. Companies that seek to promote online privacy will not burden web visitors with P3P. Good privacy standards will be built on Fair Information Practices and genuine Privacy Enhancing Techniques that minimize or eliminate the collection of personally identifiable information. Simple, predictable rules for the collection and use of personal information will also support consumer trust and confidence. P3P, on the other hand, is likely to undermine public confidence in Internet privacy.

Id.

bel. Each statement describes a specific policy preference (i.e., opt-in, opt-out or no choice) and the statements as a whole cover the universe of privacy options for each FIP component. Companies must choose the statement that best describes their practice and copy it directly into their Label. Companies will appreciate the fact that, although they cannot draft unique statements for their Label, they are not required to adopt any specific privacy terms. The goal of this standardization is for consumers to see the same types of statements made on different websites over time and become accustomed to the privacy protection offered by the websites they frequent. The following five sections discuss the pre-drafted statements for each Key FIP.

(1) *Notice*

A privacy nutrition label is itself a form of notice. Federal law will mandate standardization for every Label in terms of conspicuous posting and plain English content – subjects of Part III.[122] Labels will still have a notice section, however, and statements here must cover two areas: (1) the location of a company's summary privacy policy and full-text privacy policy; and (2) privacy policy amendments. Companies meet the first requirement by providing a link to their summary and full-text privacy policies, if they exist.[123] There are three options to choose from and each is located below in Figure One. Companies seriously interested in protecting PII will create both a summary privacy policy and a full-text policy and, therefore, choose statements one and two.

Figure One – Privacy Label Template (Notice: Privacy Policy Versions)

Our Privacy Policy	• Read a summary of our policy here [underlined text indicates a hyperlink to the relevant privacy policy section] • Read our full privacy policy here • We do not have a privacy policy

A company choosing the third statement is within its legal rights to do so as most e-commerce firms are not required to post a privacy policy. It is also important to remember that a Label regime does not require companies to create a privacy policy – merely that they honestly and clearly disclose their lack of a policy. With a privacy Label law in effect, however, it is hopeful that website visitors will comprehend the privacy problems surrounding a company operating without a policy and refuse

122. This federal law should cover all companies operating in interstate commerce that have a website that collects PII either actively or passively.

123. Because the design of the Label itself as small and unobtrusive as possible on a homepage, visitors must be directed to the more detailed policies via a clear hyperlink.

to submit PII. This situation will bring about the additional benefit of the market encouraging companies to create privacy policies in order to obtain this valuable PII.

Finally, companies must mention how they amend their privacy policy. This discussion must include a description of how, if at all: (1) any changes will be communicated to visitors; and (2) whether any changes are binding upon visitors who submitted PII under a previous version of the policy. Policy amendment procedures are important because a privacy-invasive policy creates serious threats. Take, for example, a company that promises not to sell PII in its 2007 policy and collects thousands of e-mail addresses. Assume further that this company has a policy allowing privacy policy amendments at any time without obtaining visitor consent or providing visitors with notice. If this same company amends its policy in 2008 to allow selling of collected PII externally, visitors might never know of the change – remember, people do not read privacy policies to begin with and rarely return to check in for updates. Because they receive no notification of the change, they also stand a small chance of realizing that their PII is for sale on the open market. Many of these same visitors would never have submitted information under the 2008 amendment policy but find themselves bound by its terms. Figure Two shows the four options companies have for the policy amendment Label section.

(2) *Choice*

The choice FIP box is the place where the rubber begins to meet the road. Because contemporary e-commerce companies are likely to have a privacy policy, the choice disclosure is the place where privacy-invasive PII practices will stand out. Companies are required to choose statements from three different categories covering the main components of choice. First, a company must describe its PII collection methods by choosing one statement from each of the following categories: (1) passive PII collection; and (2) active PII collection as listed in Figures Three and Four.[124] Second, a company must discuss the ways it utilizes and disseminates PII as listed in Figure Five. Finally, companies must include visitor choice options. This is the point where companies that sell PII on the open market must disclose such sales and whether visitors must opt-in, opt-out, or have no choice in the matter. Because external sharing constitutes one of the greatest threats to an individual's privacy and because individuals do not appreciate external sharing, this requirement should make companies reconsider their PII sharing policies. A company

124. Although this section splits these three categories into three separate charts, they will each be included in a single privacy label under the "Your Choices" section.

Figure Two – Privacy Label Template (Notice: Privacy Policy Amendments)

Our Privacy Policy	• Our policy may change without your consent and without telling you – any information you submitted previously is covered by our new policy • Our policy may change without your consent and without telling you – any information you submitted previously is covered by the previous policy • Our policy may change without your consent but we will e-mail / mail you the key changes – any information you submitted previously is covered by our new policy • Our policy may change without your consent but we will e-mail/mail you the key changes – any information you submitted previously is covered by the previous policy • Our policy may change but we will get your consent before making changes – any information you submitted previously is covered by our new policy • Our policy may change but we will get your consent before making changes – any information you submitted previously is covered by the previous policy • Our policy will not change

must cover the various types of choice visitors are provided by choosing one of the statements listed in Figure Six.

Figure Three – Privacy Label Template (Choice: Passive PII Collection)

Your Choices	• We automatically collect *non-identifiable information* about you via _____ [companies must insert all passive PII collection devices – such as *cookies* and *Web beacons* – and create a hyperlink to definitions in the full-text policy] • We do not collect *non-identifiable information* about you

Figure Four – Privacy Label Template (Choice: Active PII Collection)

Your Choices	• We may ask you to submit *personal information* via a *Web form* or *e-mail query* [companies must enter all applicable collection methods] • We will not ask you to submit *personal information*

Figure Five – Privacy Label Template (Choice: PII Uses)

Your Choices	• Your personal information is used to: [include all applicable PII uses below this statement and these disclosures can be on one line to conserve space] a. Complete *transactions* you initiate b. Contact you will *other offers* for our products / services c. Analyze the *preferences* / *demographics* of our customers d. Share with [or sell to] *companies that help us* conduct business [include a link here to the affiliate definition in the full-text policy] e. Sell to *unrelated parties* [companies can also make a statement here that they never sell personal information]

Figure Six – Privacy Label Template (Choice: Visitor Options)

Your Choices	**[OPT-IN:]** We won't share your personal information externally unless you *opt-in* and tell us it's okay **[OPT-OUT:]** We may share your personal information externally unless you *opt-out* and tell us not to **[NO CHOICE:]** You cannot choose how we handle your personal information

(3) *Access*

Halfway through the Label, companies must describe the four components of access – more specifically, a visitor's ability to: (1) view collected PII; (2) change collected PII; (3) remove collected PII; and (4) dispute the accuracy of collected PII.[125] Companies must also provide a hyperlink to the location at which visitors can conduct these activities or an e-mail address to make access requests.[126] As always, executives remain free to create privacy policies that do not allow any PII viewing, changing or deletion and are merely required to disclose this fact. The

125. Some companies already discuss these issues but will need to change the language they use in their Label to comply with these specific access-disclosure requirements. *See, e.g.,* Nielsen.com, Our Commitment to Privacy, http://www.nielson.com (last visited Aug. 2, 2008). Visitors "can access the personally identifiable information that we collect . . . through this website and maintain by contacting our webmaster at Contact@nielsen.com. . . . [and] can request that we correct factual errors in personally identifiable information . . . by sending us a request that credibly shows error." *Id.* Companies should remain free to choose the language they use to describe access in their full-text policy as long as it is consistent with the information in their Label.

126. Some companies currently only provide an e-mail address through which individuals may request to view, change or delete PII and do not have a specific Web page to make such requests. *See, e.g.,* Beagleboard.com, Privacy Policy, http://www.beagleboard.org/privacy (last visited Aug. 1, 2008). This should remain an acceptable practice under a Label regime because smaller companies might not have the resources to create a specific access page.

final statement in the access section involves how visitors may dispute, if at all, the accuracy of PII stored by a company. If companies choose to create their own dispute resolution process, they are required to create a hyperlink to a Web page or document describing the policy or provide an e-mail address to make such a request.[127]

As described above, accessing PII is most important in situations where PII forms the basis of a subsequent decision, such as a request for a credit line, than it is for the basic e-commerce retail transaction. The Label allows visitors to recognize a company's policy on access and then determine how important it is for them to possess the ability to change submitted PII. For example, individuals may submit a few pieces of PII to an anti-virus software company that does not provide the ability to change or delete information if this will be the only transaction they make with the company and if their information is not subject to sale – a fact that is quickly discoverable in the company's Label.

Figure Seven – Privacy Label Template (Access)

Your Information (Access)	• You may [may not] *view* any [or certain pieces] of the personal information we collect [by e-mailing us at _____] • You may [may not] *change* any [or certain pieces] of the personal information we collect [by e-mailing us at _____] • You may [may not] *delete* any [or certain pieces] of the personal information we collect [by e-mailing us at _____] • You may [may not] *dispute* any [or certain pieces] of the personal information we collect [by e-mailing us at _____]

(4) *Integrity*

Threats to PII do not stop upon information collection. In fact, the most serious threats loom after collection, both when PII is stored in a company's databases and shared with unrelated entities.[128] These threats continue to cause damage because people submit information online under the assumption that a company's technology, staff and policies strive to protect it. Problematically, this assumption appears misplaced as security breaches likely represent the most common form of data loss, with over 234 million pieces of PII compromised since January 2005.[129]

127. *See, e.g.,* Equifax, Online Dispute, http://www.equifax.com/online-credit-dispute/ (last visited Aug. 1, 2008) (providing a specific Web page dedicated to disputing the accuracy of PII held by the company with instructions on initiating disputes).

128. *See, e.g.,* Privacy Rights Clearinghouse, A Chronology of Data Breaches, http://www.privacyrights.org/ar/ChronDataBreaches.htm (last visited Aug. 1, 2008) [hereinafter *Chronology*] (showing that the vast majority of data breaches occurring since January 2005 have come after PII collection).

129. *See Selective Privacy*, *supra* note 107, at 116. "Security failures may be the most common cause of data breaches, and . . . maintaining proper security practices is difficult because would-be identity thieves constantly develop new tactics for obtaining private

These breaches occur because some companies underestimate the sophistication and motivation of e-thieves, fail to spend resources on information security, and leave themselves vulnerable to data breaches.[130] Other companies fail to properly monitor access to PII and lose information when employees lose laptops, experience theft or unintentionally e-mail and post sensitive data.[131]

With this in mind, it is clear why integrity of PII merits a place as a Key FIP. Therefore, the Label requires companies to disclose separately the technology they use to: (1) collect; and (2) protect PII.[132] Each piece of technology mentioned in the Label should be hyperlinked to a definition and discussion in the full-text privacy policy. It is important to note that merely because a company discloses that it protects PII via an encrypted database, it does not automatically create liability if a data

---

data." *Id.* One privacy advocacy group catalogues major privacy breaches on its website. *See Chronology, supra* note 128 (indicating that over 234 million personal records "containing sensitive information" [PII] have been subject to data breaches since January 2005).

130. *See, e.g.*, Andrea M. Matwyshyn, *Material Vulnerabilities: Data Privacy, Corporate Information Security, and Securities Regulation*, 3 BERKELEY BUS L. J. 129, 150 (2005) [hereinafter *Data Privacy*] (noting that "[i]nformation criminals . . . are frequently of superior technological proficiency and, in some cases, represent the bleeding edge of technology research and development.").

131. *See id.* Consider that:

> [c]urrent state of corporate information security is bleak. A 2004 worldwide information security study of 8,100 information technology professionals . . . revealed that . . . at least 55% of companies surveyed had not measured the effectiveness of their security policies and procedures. Of particular concern is the extent of the secrecy regarding companies' security failures – more than half of the entities included in the survey do not report their security breaches because they believe the information will damage corporate reputation and the share price.

Id. (internal citations omitted). *See also Selective Privacy*, *supra* note 107, at 118-19:

> Perhaps the most common type of security breach involves stolen or lost laptops. . . . Even the FTC has fallen victim to computer theft. Privacy breaches often involve laptops because each employee carries a separate copy of private information. It only takes one of them to act carelessly for all the data to become compromised. In addition, computer hardware is an attractive target for thieves. Sometimes the thieves are unaware of the private information, which minimizes the risk of privacy invasions. However, thieves who initially target hardware could also discover and misuse private data.

Id. (internal citations omitted).

132. For example, PII can be securely collected via online forms if encrypted during the transfer. *See, e.g.,* Center for Democracy and Technology, Getting Started: Top Ten Ways to Protect Privacy Online, http://www.cdt.org/privacy/guide/basic/topten.html (last visited Aug. 2, 2008).

> Online forms may be digitally transported in ways that leave them vulnerable to undesired access. Alternatively, online forms may be encrypted so that only the intended recipients can readily translate the information. Ensuring that your information is stored and transferred in secure ways is one of the keys to protecting your privacy. . . . You should not input sensitive personal information about yourself (such as financial or medical data) on Web pages that are not secure.

Id.

breach occurs. The legal system is equipped to determine whether: (1) the breach was intentional or negligent and impose liability; or (2) the company met its duty of care and dismiss a case.[133]

Figure Eight – Privacy Label Template (Security)

Information Security (Security)	**[COLLECTION]:** Your personal information is collected via a *secure sockets layer*,[134] and/or [companies must state the primary ways in which PII is protected and then link to the definition of each term in the full text policy] **[STORAGE]:** Your personal information is stored in our *encrypted databases*, and/or [companies must state the primary ways in which PII is stored and then link to the definition of each term in the full text policy]

(5) *Enforcement*

If Congress passes a privacy nutrition Label requirement, it would be wise to task the FTC with enforcement. The FTC currently deals with large-scale privacy policy violations and commences enforcement actions.[135] The Commission has the knowledge necessary to administer a Label regime and consumers are at least familiar with its consumer protection mission. Upon gaining enforcement capacity, the FTC should

133. However, an analysis of the circumstances listed in the Privacy Rights Clearinghouse's *Chronology of Data Breaches* indicates that the vast majority of instances stem from a company's negligent failure to protect PII adequately. *See Chronology*, *supra* note 128. Some of the most egregious examples occur when institutions expose PII online for months at a time before securing the information. *See id.* (summarizing an instance of exposure at the Iowa College of Engineering where the institution notified some of "its former students that some of their personal information, including Social Security numbers, was inadvertently exposed on the Internet for several months"). *See also* Kathryn E. Picanso, Note, *Protecting Information Security under A Uniform Data Breach Notification Law*, 75 FORDHAM L. REV, 355, 376-82 (2006) (discussing the applicability of tort law to data breaches).

134. Transmission of information online uses a secure sockets layer.

> [The layer] relies on the use of a digital certificate to identify a computer, the e-commerce server. The consumer's browser validates the server's certificate, and then uses the public key in the certificate to share a symmetric key with the server. For the remainder of the session, the shared symmetric key is used to encrypt communications between the browser and the server, preventing credit card or other sensitive information from being sent over the Internet in the clear.

Jane Kaufman Winn, Symposium, *Clash of the Titans: Regulating the Competition between Established and Emerging Electronic Payment Systems,* 14 BERKELEY TECH. L.J., 675, 696 (1999).

135. *See, e.g.,* Elbert Lin, *Prioritizing Privacy: A Constitutional Response to the Internet*, 17 BERKELEY TECH. L.J. 1085, 1118 (2002). "Drawing on the Federal Trade Commission Act ("FTCA"), the FTC has broad investigative authority over unfair business practices." *Id.* Moreover, "[t]he FTC has become the federal government's default Internet regulatory commission, both issuing recommendations for government policy and prosecuting websites for informational privacy violations." *Id.*

create a clear and comprehensible area on its website that deals exclusively with privacy policies. This area must contain an online complaint form exclusively for policy violations. The FTC need not investigate every complaint but should categorize each one by company and industry and contact companies with multiple complaints. The FTC can give companies an opportunity to fix their privacy problems or else face an FTC enforcement action.

The Label will help the FTC in its enforcement abilities because of the requirement that companies explain how a visitor can report a privacy policy violation. This explanation must also include a link to the new FTC complaint page. Companies interested in more clarity are free to explain different types of policy violations (i.e., misleading practices or conflicts between privacy promises and company actions) in the full text version. Additionally, studies show that companies will better protect information if they fear governmental prosecution.[136] Figure Nine below shows exactly how companies must phrase information about the enforcement FIP on their Label.

Figure Nine – Privacy Label Template (Enforcement)

Report Violations (Enforcement)	You may notify the Federal Trade Commission of our policy violations *here*

Figure Ten below encompasses the information in Figures One through Nine and serves as a summary for companies to consult when drafting their privacy nutrition label. The actual privacy Label will be much smaller once companies determine the applicable language and cut out the alternative statements. In fact, the final format located on a company's homepage should fit unobtrusively in the bottom corner. A typical example of a Label from a company with privacy-protective privacy practices is shown in Figure Eleven.

136. *See Data Privacy*, *supra* note 130, at 160 (stating that "the responses of information security professionals in [a recent study] demonstrate that corporate security improves with an increase in the fear of prosecution").

Figure Ten – Privacy Label Template (Including all Options)

Category (*Applicable FIP*)	Our Privacy Label (choose all applicable statements)
Our Privacy Policy (*Notice*)	• Read a summary of our policy here[137] • Read our full policy here[138] • We do not have a privacy policy ——— • Our policy may change without your consent and without telling you – any information you submitted previously is covered by our new policy[139] • Our policy may change without your consent and without telling you – any information you submitted previously is covered by the previous policy • Our policy may change without your consent but we will e-mail / mail you the key changes – any information you submitted previously is covered by our new policy • Our policy may change without your consent but we will e-mail / mail you the key changes – any information you submitted previously is covered by the previous policy • Our policy may change but we will get your consent before making changes – any information you submitted previously is covered by our new policy • Our policy may change but we will get your consent before making changes – any information you submitted previously is covered by the previous policy • Our policy will not change
Your Choices (*Choice*)	• We automatically collect non-identifiable information about you via _____ • We do not collect non-identifiable information about you • We may ask you to submit personal information via ____ • We will not ask you to submit personal information ——— • Your personal information is used to: a. Complete transactions you initiate b. Contact you will other offers for our products / services c. Analyze the preferences / demographics of our customers d. Share with [or sell to] companies that help us conduct business e. Sell to unrelated parties ——— • We won't share your personal information externally unless you opt-in and tell us it's okay[140]

137. Insert a link to the company's summary privacy policy at this point.
138. Insert a link to the company's full text privacy policy at this point.
139. Insert a link to the company's PII-change page here – if applicable.
140. Insert a link to the company's opt-in page here – if applicable.

	• We may share your personal information externally unless you opt-out and tell us not to[141] • You cannot choose how we handle your personal information
Your Information (*Access*)	• You may [may not] view any [or certain pieces] of your personal information we collect • You may [may not] change any [or certain pieces] of your personal information we collect[142] • You may [may not] delete any [or certain pieces] of your personal information we collect[143] • You may [may not] dispute any [or certain pieces] of your personal information we collect
Information Security (*Security*)	**[COLLECTION:]** Your personal information is collected _____ **[STORAGE:]** Your personal information is stored _____
Report Violations (*Enforcement*)	You may notify the Federal Trade Commission of our policy violations here[144]

Figure Eleven – Sample Privacy Label (Including Privacy-Protective Terms)

Category	Our Privacy Label
Our Privacy Policy	• Read our summary privacy policy and our full privacy policy • Our policy may change without your consent but we'll email you key changes
Your Choices	• We automatically collect personal information about you via cookies and Web beacons and may ask you to submit personal information via Web forms • Your personal information is used to: (1) complete transactions you initiate, (2) analyze the preferences and/or demographics of our customers, (3) contact you will other offers for our services and (4) share with companies that help us conduct business • We won't share your personal information externally unless you opt-in and tell us it's okay
Your Information	• You may view, update and delete any of your personal information we collect • You may dispute any of the personal information we collect from you here

141. Insert a link to the company's opt-out page here – if applicable.

142. Insert a link to the company's PII-change page here – if applicable.

143. Insert a link to the company's PII-deletion page here – if applicable.

144. Insert a link to the company's full privacy policy section dealing with the FIP of enforcement.

Information Security	• Your personal information is collected via a secure socket layer • Your personal information is stored on our encrypted databases
Report Violations	• You may notify the Federal Trade Commission of our policy violations here

V. CONCLUSION

Web surfers should be wary of the information trail they leave online. In fact, each piece of PII they submit could make its way onto the open market and into a digital dossier. These unofficial, non-sanctioned data files are filled with personally identifying information and potentially become more dangerous as they expand. Dossier creation is simple in an e-commerce environment filled with sophisticated databases and millions of individuals entering vast amounts of PII online without thinking much about the consequences. Companies contribute to this problem by happily collecting information that they mine for marketing purposes, analyze for customer demographics and share with both affiliated and unrelated parties. Each of these events can pose serious threats to the individual whom the information identifies assuming it falls into the hands of bad actors.

These threats represent the primary rationale behind the creation and posting of electronic privacy policies. Theoretically, companies are supposed to consider their privacy practices carefully and create conspicuous and clear privacy policies. Visitors are supposed to locate and comprehend these policy terms and only submit PII to websites meeting their privacy preferences. Problematically, however, contemporary policies are ineffective in the current self-regulatory environment as many companies seemingly lack serious commitment to drafting clear and conspicuous policies and to incorporating fair information practices.[145] Consumers generally ignore these ill-drafted privacy policies, which exacerbates the problem. Congress must act now to shore up privacy protection before consumer confidence decreases to the point where e-commerce loses its momentum.

Any federal legislative solution must not excessively hamper the efficiency that makes the Internet an increasingly popular tool of com-

145. See, e.g., *Selective Privacy*, supra note 107, at 125:

> [S]uccessful market solutions to privacy issues depend on consumers' ability to understand and analyze privacy policies. If consumers cannot compare one privacy policy to another, they will be unable to effectuate their preferences. Unfortunately, privacy policies are usually long, complex, and difficult to understand. They often include undefined terms or legal concepts that are unfamiliar to most consumers. Conspicuously missing from most privacy policies is what the companies can do with consumer information.

Id. (internal citations omitted).

merce. Excessive entanglement of government and industry could occur if Congress reacts to the problems occurring in the self-regulatory regime and enacts a European-style PII regime requiring companies to: (1) adhere to particular PII terms; or (2) clear all data collection practices through a governmental agency. Instead, a less restrictive solution can improve privacy protection as long as companies must discuss their privacy practices in relation to the Key FIPs of notice, choice, access, integrity and enforcement. This article proposes that a privacy nutrition label can incorporate these FIPs in a clear, conspicuous and standardized manner that will help consumers become accustomed to looking for and comprehending privacy information. The FTC should serve as the enforcement entity that holds companies accountable for adhering to the Label law. It is likely that Labels will be controversial at first because they take up precious homepage space and may not lead to increased privacy awareness. However, the current problems with e-commerce privacy policies merit some type of legislative solution and a Label requirement increased awareness of the nutritional value of different foods. In the end, e-commerce companies are likely to support Label legislation in order to avoid the more restrictive PII regime that looms on the horizon unless the protection of personally identifying information receives more attention.