2007

E-Commerce and Information Privacy: Privacy Policies as Personal Information Protectors

Corey A Ciocchetti, *University of Denver*

American Business Law Journal
Volume 44, Issue 1, 55–126, Spring 2007

E-Commerce and Information Privacy: Privacy Policies as Personal Information Protectors

*Corey A. Ciocchetti**

I. INTRODUCTION

Armed with $29.95, a computer, and my name and address, I recently purchased my identity. Determined to discover the extent of my personal information readily available in cyberspace, I undertook this assignment by opening my browser and ordering a comprehensive background check on myself.[1] Fifteen minutes later, via e-mail, I received the results and discovered a neatly organized vita including an extensive address history (stemming back to my days as a second-grader), my past and present property ownership records, political party affiliation, various information concerning my current neighbors and past relatives (including my father-in-law's ex-wife), and much more.[2] Adding in a free Google search utilizing only my first and last name, I instantaneously obtained detailed employment information, a chronology of my educational history, a list of my community service activities, and a recent picture.[3]

---

*Assistant Professor, Business Ethics and Legal Studies, Daniels College of Business, University of Denver; J.D., 2002, Duke University School of Law; MA (Religious Studies), 1999, University of Denver; BA (Economics) and BSBA (Finance), 1998, University of Denver; Member, Colorado Bar. Thanks to Jillian Ciocchetti and John Holcomb for their thoughtful advice and constant support!

[1]The background check was provided by Intelligent Investigations, http://www.intelligentinvestigations.com (last visited Sept. 14, 2006) and is on file with the author.

[2]Additionally, this background check is designed to produce the following pieces of information, if applicable: known aliases; results of a nationwide criminal search; sexual offense conviction records; bankruptcies; tax liens and judgments; UCC filings; airplane and boat registrations; and hunting, fishing, and concealed weapons permits. *Id.*

[3]Google, Search for "Corey Ciocchetti," http://www.google.com/search?hl=en&q=corey+ciocchetti (last visited Oct. 5, 2006).

Individually, each of these pieces of personal information represents a mere pixel of my life, but when pieced together, they present a rather detailed picture of my identity. This type of data is commonly referred to as personally identifying information (PII)[4] and the concept of piecing together personal data to form an individual profile, or "digital dossier,"[5] is known as data aggregation.[6] The more comprehensive the data aggregation, the more attention such aggregation merits because of the potential problems created when this cache of personal information is accessed inappropriately.[7] Such unauthorized access may result in cases of identity theft, stalking, harassment, and other invasions of privacy.[8] Problematically, the U.S. legal system attempts to prevent such abuses primarily through a sector-based regulatory regime whereby some transmissions of PII are strictly regulated while others remain completely unregulated.[9] Web site visitors—who are confronted with these differing information privacy statutes in fine print but desire to quickly purchase a particular good or service online—have become accustomed to ignoring the implications of submitting their PII

---

[4]*See, e.g.*, Grayson Barber, *Personal Information in Government Records: Protecting the Public Interest In Privacy*, 25 ST. LOUIS U. PUB. L. REV. 63, 118 & n.332 (2006) (defining personally identifying information with reference to the Privacy Act of 1974, 5 U.S.C. § 552a(a)(4) (2000)); TRUSTe, *Guidance on Model Web Site Disclosures*, http://www.truste.org/docs/Model_Privacy_Policy_Disclosures.doc (last visited Sept. 29, 2006) ("personally identifiable information" is used throughout the TRUSTe literature—including in its *Model Web Site Disclosures*—to refer to any information submitted via a Web site that can identify the person submitting such data).

[5]*See* DANIEL SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 1–10 (2004).

[6]Daniel Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 506–11 (2006) (describing data aggregation as an important part of a larger, defined group of activities that affect privacy).

[7]*See, e.g.*, David Lazarus, *Cool iPods also Play Stolen Data*, S.F. CHRON., Apr. 7, 2006, at D1 (discussing a case where a suspect allegedly stored stolen PII in the form of tax returns, credit files, and loan applications on an iPod); Tom Zeller, Jr., *U.S. Arrests 7 on Charges of Credit Data Trading*, N.Y. TIMES, Mar. 29, 2006, at C4 (discussing a U.S. Secret Service investigation into various online forums where stolen PII was traded).

[8]*See, e.g.*, Dave Wedge, *Authorities Allege BC Student Hacker Stole $$ and Info*, BOSTON HERALD, Feb. 7, 2003, at 10 (demonstrating various invasions of privacy caused when a Boston College computer science student installed key-logging software on various campus computers to monitor the online activities of fellow classmates).

[9]*See* discussion *infra* Part III.

online.[10] This neglect leads to vast amounts of PII being distributed into cyberspace where such information is virtually irretrievable and may be intercepted or purchased by commercial entities, governments, or individuals for marketing or other more sinister purposes.[11] In some cases, this information may only surface in a legitimate comprehensive background check, but in a more menacing scenario, it may wind up in the hands of a remotely located identity thief without the consent or control of the person the information identifies.

This article offers a solution to this problem by proposing a new federal law designed to make electronic privacy polices more effective. It argues that a well-written, conspicuously posted, standardized electronic privacy policy will help maintain the delicate balance between protecting PII and preserving transactional efficiency in a world filled with powerful data processing systems. Part II begins this analysis by detailing the historical background of privacy policies in the United States, presenting a synopsis of the PII debate in America, introducing the concept of an electronic privacy policy, and identifying the major problems plaguing contemporary policies. Part III analyzes U.S. law as it relates to electronic privacy policies, identifies particular strengths and weaknesses, and concludes with an analysis of various federal and state privacy policy enforcement actions as well as industry self-regulation techniques. Part IV suggests a systematic reform designed to strengthen the protection of PII without excessively burdening e-commerce efficiency by calling for the enactment of a new federal law—referred to in this article as the E-Commerce Privacy Policy Awareness Act (EPPAA)—that would require all commercial Web sites collecting PII in interstate commerce to post a compliant electronic privacy policy. This legislation would preempt conflicting state laws, supplement existing sector-specific federal legislation, and require privacy policies to analyze seven key areas of information privacy without requiring any specific content. This section

---

[10]*See, e.g.*, B.J. Fogg et al., Consumer Reports WebWatch, *How Do People Evaluate a Web Site's Credibility: Results from a Large Study* 86 (Oct. 29, 2002), http://www.consumerwebwatch.org/pdfs/stanfordPTL.pdf (in a survey asking 2,600 Web site visitors which aspects they use to determine a Web site's credibility, fewer than one percent of respondents claimed that a posted privacy policy influenced this decision).

[11]*See, e.g.*, Jay MacDonald, *How Much are Your Personal Details Worth*, BANKRATE.COM, http://www.bankrate.com/brm/news/pf/20060221b1.asp (last visited Sept. 29, 2006) (the article catalogs the "going price" on 46 separate items of PII stemming from a military record worth $35 to a phone number worth $0.25).

includes a model privacy policy template designed to aid companies in complying with the new law. Part V concludes by recapping the argument and calling for Congress to consider a bill along the lines of the proposed EPPAA.

II. A Privacy Policy Primer

It is exceedingly difficult to pinpoint a precise moment in time when companies, en masse, began implementing electronic privacy policies. In actuality, the concept evolved slowly over time from a set of carefully crafted fair information practices dealing with automated data-collection systems into the rather standardized, legalese-filled documents that exist today. This section walks through this evolution, beginning in the 1960s with a discussion of first principles and ending in the twenty-first century with an analysis of the effectiveness of contemporary policies from the perspective of typical e-commerce consumers.

A. From Fair Information Practices to Electronic Privacy Policies: A Brief Background

The concept of a stand-alone company privacy policy document evolved from a related concern with how the federal government was utilizing the PII of American citizens.[12] Beginning in the 1960s computerized collection and use of personal information began to draw critical national attention.[13] Continuing technological advancement allowed larger and larger amounts of PII to be aggregated and distributed more quickly and efficiently than most people thought possible prior to this period. At the same time, this increase in efficiency triggered a realization that such technology

---

[12] *See, e.g.*, Solove, *supra* note 5, at 13–26.

[13] "From the mid-1960s to the mid-1970s, privacy emerged as central political and social concern. In tune with the heightened attention to privacy, philosophers, legal scholars, and others turned their focus on privacy, raising public awareness about the growing threats to privacy from technology." Daniel J. Solove & Marc Rotenberg, Information Privacy Law 22 (2003). For a more thorough analysis concerning the privacy debates occurring during this period see, for example , Vance Packard, The Naked Society 229–51 (1965); Alan F. Westin & Michael A. Baker, Databanks in a Free Society: Computers, Record-Keeping and Privacy 3–5, 220–23 (1972).

generated serious privacy implications.[14] From this point forward, governmental and private groups began searching for a list of values critical to the protection of an individual's information privacy.[15] The ensuing debates led to various policy statements—commonly referred to as statements of fair information practices—created to memorialize the values each group found most important.[16] In 1973 the federal Department of Health Education and Welfare (HEW) created the first set of fair information practices issued by the U.S. government.[17] During this undertaking a HEW committee analyzed existing automated data-collection practices and related privacy protections.[18] They issued a report recommending the adoption of a Code of Fair Information Practices (the HEW Code) to be applied to the management of computerized data-collection systems.[19] The HEW Code attempted to establish fairness in the automated collection and handling of PII through adherence to the following five fair information principles: (1) openness, (2) disclosure, (3) secondary use, (4) correction,

---

[14]"In 1965, a new problem was placed on the congressional agenda by subcommittee chairs in both the House and the Senate. The problem was defined as the invasion of privacy by computers and evoked images of *1984*, the 'Computerized Man,' and a dossier society. Press interest was high, public concern was generated and resulted in numerous letters being sent to members of Congress . . ." Priscilla M. Regan, Legislating Privacy: Technology, Social Values, and Public Policy 82 (1995), *reprinted in* Solove & Rotenberg, *supra* note 13, at 22.

[15]*See, e.g.*, Robert Ellis Smith, Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet 327–32 (2004).

[16]*Id.*

[17]U.S. Dep't of Health, Education, and Welfare, Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Comm. On Automated Personal Data Systems (MIT Press 1973), http://www.epic.org/privacy/hew1973report/ [hereinafter HEW Report]. The then HEW Secretary, Elliott L. Richardson, formed an HEW committee—the Secretary's Advisory Committee on Automated Personal Data Systems—in 1972 in response to concern that the computerization of data collected on individual citizens may produce harmful consequences. *Id*. at Preface. This committee, through the HEW Report (a 346-page document), "produced the first portrait of information gathering and its impact on personal privacy ever provided by the U.S. government." Smith, *supra* note 15, at 327.

[18]Smith, *supra* note 15, at 327–28 (this committee comprised 25 members whose "lasting contribution was development of a Code of Fair Information Practice, five principles for managing automated data systems.").

[19]A member of the HEW committee later stated that the actual name "Code of Fair Information Practice" was derived from the title of the Code of Fair Labor Practice. Smith, *supra* note 15, at 329.

and (5) security.[20] Upon its release, the principles of the HEW Code became fairly well accepted in the business and international communities.[21] In fact, the federal Privacy Act of 1974[22]—enacted to protect PII maintained in government agency record systems—required all federal agencies to comply with the new HEW Code.[23] At the same time, the

---

[20]HEW REPORT, *supra* note 17, at 41–42. These categories may be elaborated on as follows:

(1) Openness: no entity shall create and utilize secret personal data record-keeping systems;

(2) Disclosure: individuals must be granted a right to find out what PII is recorded and how it is used;

(3) Secondary Use: individuals must consent to any use of PII different from the purpose for which the information was first collected;

(4) Correction: individuals must be allowed to correct collected PII; and

(5) Security: organizations creating, using, maintaining, or disseminating records of PII must take reasonable precautions to prevent data misuse.

Id. The HEW REPORT urged that the federal government apply this Code of Fair Information Practices "to all of its data gathering on individuals." SMITH, *supra* note 15, at 328. Since the publication of the HEW REPORT in 1973,

> a canon of fair information practice principles has been developed by a variety of governmental and inter-governmental agencies. In addition to the HEW Report, the major reports setting forth the core fair information practice principles are: The Privacy Protection Study Commission, *Personal Privacy in an Information Society* (1977); Organization for Economic Cooperation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980); Information Infrastructure Task Force, Information Policy Committee, Privacy Working Group, *Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information* (1995); U.S. Dept. of Commerce, *Privacy and the NII: Safeguarding Telecommunications-Related Personal Information* (1995); *The European Union Directive on the Protection of Personal Data* (1995); and the Canadian Standards Association, *Model Code for the Protection of Personal Information: A National Standard of Canada* (1996).

FTC, PRIVACY ONLINE: A REPORT TO CONGRESS 48 n.28 (June 1998) [hereinafter FTC PRIVACY ONLINE], *available at* http://www.ftc.gov/reports/privacy3/priv-23a.pdf (internal citations omitted and emphasis in original).

[21]Robert Ellis Smith states that "[t]here was general acceptance of the HEW Code from the start—from IBM Corp. after it conducted its own study, from the Business Roundtable of major corporate executives, within Congressional committees, among the emerging cadre of privacy advocates, and from academics [within the United States] and Europe. Many tried to improve on it, but no one did." SMITH, *supra* note 15, at 330.

[22]5 U.S.C. § 552(a) (2000).

[23]While the federal government has applied the HEW fair information practices to federal agencies, it is interesting to note that "most states do not have a statute comparable to the federal Privacy Act; only about a third of states have adopted such a statute." SOLOVE & ROTENBERG, *supra* note 13, at 474.

international community also became interested in fair information practices and issued separate statements unrelated to the HEW Code but containing similar fair information practices principles.[24] Seven years later the second major code developing the concept of fair information practices was issued by the Organisation for Economic Cooperation and Development (OECD).[25] The *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OECD Guidelines), were designed to harmonize national data-protection laws and reiterate to the world the importance of PII protection.[26] The OECD Guidelines are much more

---

[24]*See, e.g.*, The Swedish Data Act of 1973, *Datalagen*, SFS 1973:289 (this was one of the first national laws dealing with privacy and personal information); *see also* DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES 94 (1989) (Flaherty claims that "the Swedish model of data protection had enormous and direct influence on the development of data protection in Western European countries.").

[25]OECD, OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (2001), *available at* http://www1.oecd.org/publications/e-book/9302011E.PDF [hereinafter OECD GUIDELINES].

[26]The OECD fair information practices can be summarized as follows:

(1) Collection Limitation: 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, complete and kept up-to-date.

(3) Purpose specification: the purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment [sic] 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 Paragraph 9 except:
   a. with the consent of the data subject; or
   b. by the authority of law.

(5) Security safeguards principle: personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized 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 about usual residence of the data controller.

(7) Individual participation principle: an individual should have the right:
   a. To obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
   b. To have communicated to him, data relating to him

detailed than those in the HEW Code and set a higher standard for collectors of PII.[27]

Although the HEW Code, the OECD Guidelines, and other similar codes of fair information practices developed since the 1970s have been influential, the U.S. Congress has not passed comprehensive federal legislation requiring consistent application of fair information practices to the collection, use, storage, or dissemination of PII by private entities. Instead, the federal government has incorporated certain fair information practices into various sectoral regulations and left others to be enforced by governmental agencies or incorporated into industry self-regulation efforts.[28]

---

1. Within a reasonable time;
2. At a charge, if any, that is not excessive;
3. In a reasonable manner; and
4. In a form that is readily intelligible to him.

c. To be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and

d. To challenge data relating to him and, if the challenge is successful, to have the data erased; rectified, completed or amended.

(8) Accountability principle: a data controller should be accountable for complying with measures which give effect to the principles stated above.

See OECD GUIDELINES, *supra* note 25, at 14–16.

[27]"The OECD Guidelines set out eight principles for data protection that are still the benchmark for assessing privacy policy and legislation . . . The principles articulate in only a couple of pages a set of rules that have guided the development of national law and increasingly the design of information systems." Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1 (2001).

[28]*See, e.g.*, Fair Credit Reporting Act of 1970, Pub. L. No. 91-508, 84 Stat. 1114 (Oct. 26, 1970) [hereinafter FCRA] (codified as amended at 15 USC §§ 1681–1681t (2000)) (§ 1681(a)(4) of the FCRA was enacted in part to "respect a consumer's right to privacy"); Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, 92 Stat. 3641 (Nov. 10, 1978) [hereinafter REPA] (codified at 12 U.S.C. § 35 (2000)) (§ 3403 of the RFPA deals with the confidentiality of financial records); Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified at scattered sections of 18 U.S.C.) [hereinafter ECPA] (§ 2702 of the ECPA makes it a violation to disclose certain customer records or certain communications in electronic storage); Cable Communications Policy Act of 1984, Pub. L. No. 98-549, 98 Stat. 2794 (June 19, 1984) [hereinafter CCPA] (codified at scattered sections of 15, 18, 46, 47, and 50 U.S.C.) (§ 551(a) of the CCPA requires that covered entities provide their customers with hard copy privacy notices discussing the collection and use of customer PII). In fact, the United States has left a great deal of the regulation in this area to industry groups such as the Direct Marketing Association and to independent third-party verification programs such as TRUSTe and BBOOnline. *See* discussion *infra* Part IV. Marc Rotenberg, a much-cited privacy scholar, discusses the ineffectiveness of this sectoral regulatory approach that occurred through the 1990s and is still in effect today by stating that "[t]he coverage of U.S. law was

This regulatory void helped bring about many of the problems currently encountered in privacy policies because unregulated companies are not required to comply or even think about fair information practices or internal information privacy practices. In 1998 the U.S. Federal Trade Commission (FTC or the Commission) attempted to bridge this gap between regulated and unregulated industries by proposing its own set of four fair information practices designed to incorporate select fair information practices into the landscape of industry self-regulation occurring within the United States.[29] These principles were significantly less rigorous than the HEW Code and the OECD Guidelines but represented a more realistic option for businesses to accept, given the lack of any standardized information privacy regulation within the country at the time of their introduction. Although they have changed slightly over time, the four current FTC fair information practices are: (1) notice, (2) choice, (3) access, and (4) security.[30]

In a report to Congress, the FTC designated notice as the most fundamental of its chosen fair information practices.[31] Elaborating on this point, the Commission urged Congress to require commercial Web sites to

---

uneven: Fair Information Practices were in force in some sectors and not in others. There was inadequate enforcement and oversight. Technology continued to outpace the law." Rotenberg, *supra* note 27, ¶ 48.

[29]FTC Privacy Online, *supra* note 20, at 7.

[30]In 1998 the FTC actually promulgated five fair information practices: notice, consent, access, security, and *enforcement*. FTC Privacy Online, *supra* note 20, at 7 (emphasis added). The Commission added that the "absence of enforcement mechanisms significantly weakens the effectiveness of industry-promulgated guidelines as a self-regulatory tool." *Id*. at 17. "This is especially true if member companies fail to voluntarily adhere to suggested policies." *Id*. Recently, however, enforcement was dropped as a fair information practice and the other four —notice, choice, access, and security—were retained. *See, e.g*., FTC, Statement of Chairman Pitofsky, Privacy Online: Fair Information Practices in the Electronic Marketplace 1 (May 22, 2000) [hereinafter FTC Pitofsky Statement], http://www.ftc.gov/reports/privacy2000/pitofskystmtonlineprivacy.htm#N_1_ (Chairman Pitofsky only labeled notice, choice, access, and security as "Fair Information Practice Principles" and did not mention enforcement).

[31]FTC, Prepared Statement of the Federal Trade Commission on "Privacy Online: Fair Information Practices In the Electronic Marketplace, Before the Senate Comm. on Commerce, Science, and Transportation 7 (May 25, 2000) [hereinafter 2000 FTC Statement], http://www.ftc.gov/os/2000/05/testimonyprivacy.htm. In this statement, the FTC called for congressional legislation setting a basic level of protection to be implemented by commercial Web sites. *Id*. § III. Under this new legislation all e-commerce Web sites collecting PII would be required to abide by the *four* FTC fair information practices. *Id*. (emphasis added).

> provide consumers clear and conspicuous notice of their information practices, including what information they collect, how they collect it (e.g., directly or through nonobvious means such as cookies), how they use it, how they provide Choice, Access, and Security to consumers, whether they disclose the information collected to other entities, and whether other entities are collecting information through the site.[32]

The concept of notice, contained in most codes of fair information practices, can be considered directly responsible for the eventual creation of both offline and online privacy policies. Such policies were developed to provide notice to customers of a company's privacy practices before any commercial transaction occurred. Unfortunately, little attention was paid to the fact that this notice can only function as an effective privacy tool when it is both readable and discoverable.[33]

The second FTC fair information practice, individual choice, stems from the idea that granting Web site visitors a choice about how companies handle their PII should provide greater information privacy protection. The Commission continues to urge e-commerce Web sites to

> offer consumers choices as to how their personal identifying information is used beyond the use for which the information was provided (e.g., to consummate a transaction). Such choice [encompasses] both internal secondary uses (such as marketing back to consumers) and external secondary uses (such as disclosing data to other entities).[34]

For example, if a company adopts choice as a privacy principle, visitors submitting PII to consummate a transaction should not find their information disseminated in any way unrelated to that transaction without their explicit permission or without having an opportunity to opt out of such disclosure.

The third FTC fair information practice, access, encompassed the idea that visitors submitting PII should be entitled to access such information while it is stored within company databases.[35] The FTC understood that access is important to ensure accuracy, amend collected PII, and/or

---

[32]2000 FTC Statement, *supra* note 31, § III(1).

[33]*See* discussion *infra* Part IV.A (Part IV of this article offers potential solutions designed to make privacy notices more readable, discoverable, and effective).

[34]*Id*. § III(2).

[35]FTC Privacy Online, *supra* note 20, at 9.

delete personal information.[36] There are certain instances, such as within an individual credit report, where people should not be entitled to alter the PII collected by a company and, for example, erase a bankruptcy filing. In other instances, however, it is important to allow such access in order for the PII to paint as accurate a picture as possible about the person to whom it pertains. In 2000 the FTC urged Congress to pass legislation requiring companies to, among other privacy-protective measures, "offer consumers reasonable access to the information a Web site has collected about them, including a reasonable opportunity to review information and to correct inaccuracies or delete information."[37]

Security, the fourth and final FTC fair information practice, is rapidly becoming the most important one in the twenty-first-century e-commerce environment as company Web sites and other electronic operations are under continued threat of security breaches. In a world of nearly infinite database capacity, security breaches have the potential to release millions of PII records into the hands of malintentioned parties such as hackers or rogue employees. In implementing security as a fair information practice, the Commission encouraged Web sites to "take reasonable steps to protect the security of the information they collect from consumers."[38]

Although Congress failed to enact legislation requiring e-commerce operations to adopt the FTC fair information practices, the executive branch began to urge the private sector to develop privacy solutions in lieu of legislation.[39] Within these initiatives, companies were encouraged by the government to incorporate some or all of the FTC fair information practices.[40] Though it is difficult to determine which company created the first electronic privacy policy, as e-commerce blossomed in the late 1990s and early 2000s, the concept adapted to the new Internet medium and the electronic privacy policy began to emerge on many company home

---

[36] *Id.*

[37] *Id.* § III(3).

[38] *Id.* § III(4).

[39] *See, e.g.,* William J. Clinton & Albert Gore, Jr., A Framework for Global Electronic Commerce 13 (1997), *available at* http://www.technology.gov/digeconomy/framewrk.htm.

[40] *Id.* (This report notes that the "Administration supports private sector efforts now underway to implement meaningful, consumer-friendly, self-regulatory privacy regimes. These include mechanisms for facilitating awareness and the exercise of choice online, evaluating private sector adoption of and adherence to fair information practices . . .").

pages.[41] Today many companies now distribute their policies on their Web sites in lieu of promising to send the visitor a hard copy version.[42]

This attention to fair information practices and privacy policies, combined with ever-advancing technology, helped fuel an intense debate between advocates of two approaches dealing with PII protection: (1) a dignity approach and (2) a market approach.[43] The dignity approach piggybacks on the theory that individuals possess a fundamental right to maintain a sphere of privacy that should be protected from major invasions.[44] Proponents of the dignity approach claim that PII should be part of this protected sphere and should not be freely alienable in a marketplace with information asymmetries and differing power relationships stacked against the individual.[45] This approach is found prominently in the data-protection regime in the European Union through its controversial Privacy Directive,[46] whose Tenth Recital states:

> Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law; whereas, for that reason, the approximation of those laws

---

[41]James Neff, *Shopping for Privacy Online: Consumer Decision-Making Strategies and the Emerging Market for Information Privacy*, 2005 U. ILL. J. L. TECH. & POL'Y 1, 2–3 (2005) (stating that "by the end of 2001, nearly all of the most frequently visited Web sites had implemented detailed information practices accompanied by published privacy policies.").

[42]*See, e.g.*, IBM, *Privacy*, http://www.ibm.com/privacy/us/ (last visited Apr. 28, 2006) (IBM has posted its entire privacy policy online and does not indicate that any Web site visitor is entitled to receive a hard copy).

[43]For a balanced analysis of this debate, see, for example, Jerry Kang & Benedikt Buchner, *Privacy in Atlantis*, 18 HARV. J.L. & TECH 229, 230–57 (2004) (presenting an analysis of the two most prominent sides in this debate—the dignity approach and the market approach). My article advocates that Congress consider a new federal law encompassing attributes propounded by both sides of this debate. *See* discussion *infra* Part IV.A.

[44]*See, e.g.*, Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 973–74 (1964) (arguing that protecting an individual's right to privacy enhances "individuality and human dignity" and that invasions of privacy lead to a diminishment of human dignity).

[45]Kang & Buchner, *supra* note 43, at 234–54.

[46]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) [hereinafter EU Privacy Directive].

> must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community.[47]

On the other hand, proponents of the market approach argue that individuals should hold an alienable property interest in their PII free from major governmental regulation.[48] This approach would allow the market—made up of buyers, sellers, and competition—to determine the most efficient allocation of this valuable property interest.[49] For example, an individual surfing the World Wide Web would be allowed to determine whether to submit requested pieces of PII in return for free access to Web site content or pay to access a Web site containing similar information without having to submit any PII. If the PII requests are too intrusive, individuals may always withhold their valuable PII and move to a competitor's product that is less privacy intrusive. Beyond these two major positions in the debate, a few alternative theories have been proposed to address the tension between protecting PII and enhancing e-commerce efficiency.[50] At the end of the day this debate will continue to rage as technology advancements create even more efficient data aggregation opportunities.

---

[47] *Id.*

[48] To view a few examples arguing for PII as a property interest, see, for example, RICHARD A. POSNER, ECONOMIC ANALYSIS OF THE LAW 46 (6th ed. 1998) (arguing that data privacy law as functionally "a branch of property law"); *Developments in the Law—The Law of Cyberspace*, 112 HARV. L. REV. 1574, 1634–49 (1999) (arguing that a "property regime is preferable in cyberspace because transaction costs are extremely low, enabling individuals to reach bargains that reflect their actual preference levels"); Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381, 2383 (1996) (arguing that "personal information, like all other forms of information, is property.").

[49] *See* Kang & Buchner, *supra* note 43, at 230–33 (presenting the argument that the market approach would allow individuals to determine their unique "optimal mix" of privacy).

[50] A third popular theory, albeit somewhat related to the PII-as-property view, prefers a contractual approach to the meting out of PII. This contractual approach "allows parties to make promises regarding personal data and the processing of data" within default limits set by relevant regulations. Kang & Buchner, *supra* note 43, at 232. For an analysis of this theory, see, for example, Pamela Samuelson, *Privacy As Intellectual Property?*, 52 STAN. L. REV. 1125, 1151–59 (2000) (arguing for the adoption of "modified trade secrecy default rules for protecting personal data" instead of solely grounding an interest in property law). For other alternative theories in the debate, see, for example, ROLF H. WEBER, REGULATION MODELS FOR THE ONLINE WORLD 160–70 (2003) (presenting a survey of different approaches to data privacy regulation) and Robert Gellman, *Enforcing Privacy Rights: Remedying Privacy Wrongs—New Models: A Better Way to Approach Privacy Policy in the United States*, 54 HASTINGS L.J. 1183, 1211 (2003) (arguing that the states have historically been more effective in protecting PII than the FTC).

B. The Evolution of Privacy Policies—Theory Versus Reality

An electronic privacy policy is a written description posted on a company's Web site explaining how the company applies specific fair information practices to the collection, use, storage, and dissemination of personal information provided by visitors.[51] In theory, the privacy policy concept relies on the idea that a company will adhere to certain fair information practices and that Web site visitors will thoroughly read the policy, understand its terms and implications, and then choose whether to continue to use the Web site and/or submit personal information. At the end of this theoretical process, the policy has served its purpose because the visitor will either leave or continue clicking through the Web site, cognizant of the privacy implications. Unfortunately theory does not always mesh with reality. Currently privacy policies are not meeting such aspirations as studies show that Web site visitors are not clicking, reading, or understanding privacy terms and implications or basing any decision as to whether to continue on the Web site based on the privacy policy.[52] There are two major reasons behind this failure: (1) electronic privacy polices are rarely legally mandated and, therefore, companies have little incentive to raise awareness of their importance and (2) the typical language and placement of these polices limits their effectiveness.[53]

---

[51]In most instances, the text of an electronic privacy policy is located on a separate page of the Web site rather than on the home page itself. This page is generally reached via a hyperlink located at the bottom of a company's home page. *See, e.g.,* Microsoft Corp, http://www.microsoft.com/ (last visited Oct. 1, 2006); National Basketball Association, http://nba.com (last visited Oct. 1, 2006).

[52]*See, e.g.,* Joseph Turrow, Americans and Online Privacy: The System is Broken: A Report from the Annenberg Public Policy Center of the University of Pennsylvania 3 (June 2003), http://www.annenbergpublicpolicycenter.org/04_info_society/2003_online_privacy_version_09.pdf (utilizing a nationwide survey to argue that American adults using the Internet misunderstand privacy policies and are ignorant of the potential data flows including their PII); Harris Interactive and the Privacy Leadership Institute, Privacy Notices Research: Final Results 2 (Dec. 2001), *available at* http://www.ftc.gov/bcp/workshops/glb/supporting/harris%20results.pdf (utilizing a nationwide survey to show that 40% of respondents do not spend more time reading electronic privacy policies because of a lack of time and interest while 29% of respondents do not spend more time reading electronic privacy policies because they feel that such policies are difficult to understand and read).

[53]Interestingly, some companies may fail to even create a privacy policy because the creation of a policy may subject the company to legal ramifications if any privacy promise made is later broken. Such misrepresentations may be enforced by the FTC as being unfair or deceptive acts/practices. *See* discussion *infra* Part III.

As of 2006 only companies operating within the financial and health care industry sectors that collect information from California residents or targeting children under the age of thirteen are required to compose or post an electronic privacy policy.[54] Ironically, posting a privacy policy may be more troublesome than failing to create one in the first place because any breach of a privacy policy commitment opens the company up to public scrutiny and potential enforcement action by the FTC as an unfair or deceptive act or practice.[55] Therefore, companies offering no promises of privacy protection on their Web sites have no legally binding obligations to break and allow themselves the opportunity to handle PII as they see appropriate and without consequences. Under these circumstances it would seem legally advantageous for companies that create privacy policies to disclaim as many potential liabilities as possible in order to avoid legal liability.[56] Unfortunately the current situation offers little incentive for companies to raise awareness of the importance of privacy policies.

Web site visitors are not appropriately reading or understanding these policies because many Web sites inconspicuously post their electronic privacy policies and make them difficult for the average Internet user to understand.[57] In today's hustle-bustle world, visitors to Web sites rush to

---

[54]There are instances, however, where companies in unregulated sectors create and post effective privacy policies without any legal requirement to do so. *See, e.g.*, TheTennisLadder.com, *Privacy Policy*, http://www.thetennisladder.com (last visited Apr. 26, 2006) (this Web site facilitates tennis matches and is not situated within any economic sector regulated by the information privacy legislation covered in Part III). Other federal laws require the creation of a hard-copy privacy policy but do not mention any sort of electronic posting requirement. *See, e.g.*, Cable Communications Policy Act of 1984, 47 U.S.C. § 551(a)(1)–(2) (2000) (requiring cable operators to provide a hard-copy privacy policy to subscribers at the time of entering into an agreement to provide services, and at least annually thereafter, and that such policy cover the collection of certain PII).

[55]*See* discussion *infra* Part III.

[56]*See* discussion *infra* Part V for an example of a prominent American company that collects PII online but that does not have a privacy policy posted. This company is operating well within its legal rights by taking this course of action.

[57]A recent study released in the first quarter of 2006 and conducted by the Customer Respect Group (CRG) studied how companies treat their online customers and found that during the period studied all companies surveyed posted a privacy policy but that only "48 percent of those policies have a friendly tone" while the other 52 percent contained a neutral tone. Customer Respect Group, First Quarter 2006 Report on the High Technology and Computing Industries, (Jan. 9, 2006), *available at* http://www.customerrespect.com/default.asp [hereinafter 2006 CRG Survey]. This is compared to a similar study, released by the CRG in the second quarter of 2005, showing that 82 percent of companies operating in the

locate the home page and then the information they desire.[58] With the average Web surfer spending "one minute or less on a linked web document," it would make sense that very few take the time to scroll to the bottom of the home page where privacy policy links reside and click on the small-print links displayed.[59] Even if they do think about clicking further, these links generally deal with Web site terms of use and company contact information in addition to privacy policy information, appealing to only a few intellectually curious visitors.[60] Once inside the actual privacy policy a visitor quickly encounters a vast array of legalese (e.g., "heretofore," "personally identifiable information," and "nonaffiliated third parties") and tech-speak (e.g., "cookie technology," "Web beacons," and "spyware/adware").[61] A major study found that the language of contemporary privacy polices is best suited for someone who has completed at least three years of college, whereas the consensus among language

---

high-technology and computing industry provided a privacy policy with a friendly tone with the other 18 percent portraying a neutral tone. CUSTOMER RESPECT GROUP, SECOND QUARTER 2005 REPORT ON THE HIGH TECHNOLOGY AND COMPUTING INDUSTRIES (2005), http://www.customerrespect.com/default.asp?hdnFilename=research_ind_hightech.htm [hereinafter 2005 CRG STUDY]. This previous study also showed that, while 92 percent of these companies provided a link to their privacy policy on the bottom of all Web site pages, only three percent provided a prominent link on all pages of the company Web site. *Id.*

[58]*Surfers Impatient with Search Engines*, BBC NEWS, June 27, 2003, http://news.bbc.co.uk/1/hi/technology/3023514.stm (discussing a study by the Penn State School of Information Sciences and Technology which "found that people are getting frustrated with search engines and making snap judgements [sic] about websites").

[59]*Id.*

[60]*See, e.g.*, Monster.com, http://www.monster.com (last visited Oct. 1, 2006) (the bottom of the Monster.com home page contains the following hyperlinks in small font: (1) Find Jobs; (2) Post Resume; (3) Network Now; (4) Career Advice; (5) Research Companies; (6) Scholarship Search; (7) Online Degrees; (8) Español; (9) My Monster Login; (10) Buy Employer Products; (11) Post a Job; (12) Partner with us; (13) Employer Login; (14) Help; (15) Contact Us; (16) About Monster; (17) Monster Store; (18) Site Map; (19) Privacy Statement; (20) Be Safe; (21) Terms of Use; (22) Work At Monster; (23) Investor Relations; and (24) Monster Employment Index). The "Privacy Statement" link is the eighteenth link in a list of twenty-four links located in small print and at the bottom of the Monster.com home page. *Id.* This example makes it easy to see how a person spending only a few minutes on a Web site may neglect to read the privacy policy and understand the implications of submitting their PII.

[61]*See, e.g.*, MARK HOCHHAUSER, LOST IN THE FINE PRINT, READABILITY OF FINANCIAL PRIVACY NOTICES (July 2001), http://www.privacyrights.org/ar/GLB-Reading.htm (reviewing sixty privacy policies of financial institutions for ease of readability, grade level and writing style and finding that twelve were written a at the graduate school level with the rest written between a thirteenth- and a sixteenth-grade level).

scholars is that documents distributed to the general public should be written at an eighth-grade reading level.[62]

Effective privacy policies are crucial in an environment where digital accumulation of vast amounts of information can lead to digital dossiers on so many people.[63] Web site visitors should have a certain understanding as to how their personal information will be used by its collectors. This understanding must include how this information will be used for internal purposes, how it will be shared among affiliated and nonaffiliated third parties, and how it will be stored and protected. The goal is for Web site visitors who feel that their personal information may be misused or disseminated in an undesirable manner to be more likely to refuse to conduct e-commerce transactions with such Web sites. However, because the average Web site visitor does not understand the implications of submitting information electronically, he or she is less likely to sense a potential misuse and withhold PII.[64] Changing visitor expectations to anticipate potential information privacy weaknesses can, at least partially, be accomplished by restructuring the current legal regime to improve the effectiveness of electronic privacy policies. Fixing these problems will allow such policies to serve an important purpose in the world of electronic privacy and reframe notice as one of the most important fair information practices.

---

[62]*See, e.g.*, Carlos Jensen & Colin Potts, *Privacy Policies as Decision-Making Tools: An Evaluation of Online Privacy Notices*, Proceedings of ACM Conference on Human Factors in Computing Systems: Vienna, Austria, CHI 471–78 (2004), *available at* http://www-static.cc.gatech.edu/grads/j/Carlos.Jensen/Publications/p471-jensen.pdf. They found, after studying 64 high-traffic and health-care-related Web sites, that "only 6% of policies are readable by the most vulnerable 28.3% of the population [with less than or equal to a high school education], and that 13% of policies were only readable by people with a post-graduate education." *Id*. at 477. *See also* George R. Milne & Mary J. Culnan, *Using the Content of Online Privacy Notices to Inform Public Policy: A Longitudinal Analysis of the 1998–2001 U.S. Web Surveys*, 18 The Information Society 345, 345–59 (2002) (studying popular Web sites and finding that the average privacy policy was written at an eleventh through fourteenth [second-year college] grade reading level).

[63]Solove, *supra* note 5, at 16–26.

[64]This trend is evident in the ChoicePoint data breach scandal where customers apparently felt comfortable submitting their PII to ChoicePoint prior to various incidents where 160,000 consumer records were compromised due primarily to the company's inadequate data security practices. *See ChoicePoint Complaint*, *infra* note 175, at 3–7.

III. The Law Governing Electronic Privacy Policies

In the United States today, a handful of federal and state laws combine with private-sector self-regulation to govern the content and use of electronic privacy policies.[65] Within this environment, the relevant regulations are targeted toward a few specific economic sectors, leaving the majority of e-commerce operations outside of their reach. The only recompense available to Web site visitors suffering injuries stemming from information

---

[65]It is important to keep in mind that other countries have enacted information privacy protections that are far more comprehensive than U.S. protections. *See, e.g.*, EU Privacy Directive, *supra* note 46. The Directive

> establishes common rules for data protection among the Member States of the European Union . . . The directive imposes obligations on the processors of personal data. It requires technical security and the notification of individuals whose data are being collected, and outlines circumstances under which data transfer may occur. The Directive also gives individuals substantial rights to control the use of data about themselves. These rights include the right to be informed that their personal data are being transferred, the need to obtain "unambiguous" consent from the individual for the transfer of certain data, the opportunity to make corrections in the data, and the right to object to the transfer. Data regulatory authority, enforcement provisions, and sanctions are also key elements of the directive.

Solove & Rotenberg, *supra* note 13, at 714–15. Because the EU Privacy Directive is far more protective of PII than the sectoral laws in the United States, questions continually arise as to whether data protection standards in the United States comply with the requirements of the Directive. The Directive states that data transfers containing PII of European Union residents can be blocked if third-party countries involved in the processing do not provide an "adequate level of [data] protection." EU Privacy Directive, *supra* note 46, at Art. 25. Because of the fear that U.S. laws might not offer such an "adequate level of protection," both European Commission regulators and the U.S. Department of Commerce (DOC) negotiated a "safe harbor" agreement in 1998 to ensure that certain U.S. data protection standards would be considered "adequate" under the Directive. *See* Solove & Rotenberg, *supra* note 13, at 742–43. *See also* U.S. Dep't of Commerce, Safe Harbor Privacy Principles, July 21, 2000, *available at* http://www.export.gov/safeharbor/SHPRINCIPLESFINAL.htm; U.S. Dep't of Commerce, *Safe Harbor*, http://www.export.gov/safeharbor/ (last visited Oct. 1, 2006) (this section of the DOC Web site provides detailed information on the safe harbor agreement). Adherence to the safe harbor agreement requires companies to implement specific information privacy standards and have their names posted on a list maintained by the DOC; breaches of the safe harbor standards will be enforced by the FTC. *See* U.S. Dep't of Commerce, Safe Harbor List, http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list (last visited Oct. 1, 2006). Although a detailed analysis of international privacy regulations is outside of the scope of this discussion, an analysis of the conclusions of this article in an international context may prove important as e-commerce continues to expand globally.

privacy violations rests on the small chance of an enforcement action brought by the FTC or by a state attorney general. Although each of the laws discussed below contains important privacy-enhancing attributes, their sectoral nature leaves loopholes, which unscrupulous, unregulated companies may exploit. These gaping holes in U.S. law demonstrate the importance of enacting a new, more comprehensive, federal law covering e-commerce businesses not regulated by these laws. As a prelude, it is important to consider key sectoral-based laws,[66] FTC and state unfair or deceptive practices enforcement actions, and industry self-regulation efforts. It is clear existing regulations are very narrowly tailored, but each can contribute to a more effective regulatory regime.

A. Federal Regulation Targeting Electronic Privacy Policies

On a national level, Congress has chosen to regulate electronic privacy policies through sectoral legislation. Any unregulated sectors are left under the watch of the FTC, which has the authority, but not necessarily the manpower, to enforce privacy policy promises under its general unfair and deceptive practice powers.[67] The four major sectors where federal law

---

[66]This article does not touch on every regulation governing invasions of privacy and, therefore, pieces of legislation only tangentially relating to data collection as well as common law invasion of privacy torts are left out. *See, e.g.*, Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801–11, 1821–29, 1841–46, 1861–62 (2000) (dealing with electronic surveillance and physical search procedures involving persons involved in terrorist activities against the United States on behalf of a foreign power); Financial Recordkeeping and Reporting of Currency and Foreign Transactions Act (the Bank Secrecy Act) of 1970, 31 U.S.C. § 1051–1709 (2000) (requiring certain financial institutions to maintain records and file reports to be used in certain criminal, regulatory, and tax investigations); Computer Matching and Privacy Protection Act of 1988, 5 U.S.C. § 552a(o) (2000) (amending the Privacy Act of 1974 by requiring computer matching undertaken by certain federal agencies to follow certain procedures designed to protect individuals applying for and receiving federal benefits); Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227 (2000) (governing the conduct of telephone solicitation restricting the methods marketers may use to conduct telemarketing); Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (Oct. 26, 2001) (codified in scattered sections of 8, 12, 18, 22, 31, 42, and 50 U.S.C.) (designed to deter and punish terrorist acts both within the United States and abroad by expanding the power of U.S. governmental agencies). See also SOLOVE, *supra* note 5, at 56–75, for a comprehensive analysis of information privacy law in the United States. I am not aware of any other article discussing these regulations in the context of privacy policies and, therefore, this analysis should prove helpful.

[67]The FTC had seven regional offices and only around 1,000 full-time employees in 2005. *See* FTC, *Regional Offices*, http://www.ftc.gov/ro/romap2.htm (last visited Oct. 1, 2006) (presenting

regulates privacy policies are: (1) children under the age of thirteen—covered by the Children's Online Privacy Protection Act of 1998 (COPPA),[68] (2) financial institutions—covered by the Gramm-Leach-Bliley Act of 1999 (GLBA),[69] (3) health care providers/institutions—covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA),[70] and (4) federal government agencies—covered by the E-Government Act of 2002 (EGA).[71] Of these four major federal laws, only COPPA and EGA directly target electronic privacy policies while GLBA and HIPAA indirectly touch upon such policies in ancillary provisions.

1. Federal Regulation Directly Targeting Electronic Privacy Policies

The federal government is slowly attempting to protect individuals against misuses of their PII. Congressional efforts generally occur via ex post facto regulations drafted in response to major security snafus or other bad acts committed by e-commerce companies.[72] Two of the primary federal statutes promulgated in this area, COPPA and EGA, apply directly to electronic privacy policies while others, such as GLBA and HIPAA, only indirectly touch upon their use. Problematically, all of these regulations

---

a map of the seven regions containing FTC offices); FTC, BUDGET SUMMARY: FISCAL YEAR 2007 24 (2006), *available at* http://www.ftc.gov/ftc/oed/fmo/budgetsummary07.pdf (laying out the actual number of full-time employees in 2005). The press laments the fact that the FTC does not have the resources it needs to undertake its consumer protection missions. *See, e.g.*, Elizabeth Millard, *FTC Targets X-Rated Spam*, EWEEK.COM, July 21, 2005, http://www.eweek.com/article2/0,1759,1839536,00.asp?kc=EWRSS03119TX1K0000594 (discussing the idea that the FTC does not have the "manpower to go after spammers to the degree that everyone would like them to.").

[68]Pub. L. No. 105–277, 112 Stat. 2681 (Oct. 21, 1998) (codified as amended at 15 U.S.C. §§ 6501–06 (2000)).

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

[70]Pub. L. No. 104–191, 110 Stat. 1936 (Aug. 21, 1996) (codified as amended in scattered sections of 26 and 42 U.S.C.).

[71]Pub. L. No. 107–347, 116 Stat. 2899 (Dec. 17, 2002) (codified as amended in scattered sections of 5, 10, 13, 15, 18, 28, 31, 40, 41, and 44 U.S.C.).

[72]*See, e.g.*, Complaint, In the Matter of Geocities, FTC Docket No. C-3859 (Feb. 5, 1999), *available at* http://www.ftc.gov/os/1999/02/9823015cmp.htm (in this case Geocities collected PII from young children and then sold such information after promising in its privacy policy that such information would not be sold).

govern only narrow industry sectors or select consumer groups as opposed to the e-commerce economy in general.

a. COPPA. Congress designed COPPA to protect young children by requiring Web sites collecting PII from children under the age of thirteen to electronically disclose company privacy practices and obtain parental consent prior to using, collecting, or disclosing this information.[73] This statute is very narrow in scope and only applies to companies operating Web sites directed to children under age thirteen or to companies operating general-audience Web sites but who are under the "actual knowledge" that they are collecting PII from children under age thirteen.[74] As with the other federal statutes striving to protect PII, many consumer groups are left unprotected.[75]

On the other hand, COPPA offers strong PII protection for the consumers it actually covers. The statute requires Web sites falling under its jurisdiction to post an electronic privacy policy[76] containing explanations of, among other things: (1) the types of PII collected from children,[77] (2) whether such information is obtained actively or passively,[78] (3) how

---

[73]15 U.S.C. § 6502(b)(1)(a)(i)–(ii) (2000). *See also* Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888 (Nov. 3, 1999) (to be codified at C.F.R. pt. 312) (presenting a statement of basis and purpose for the COPPA).

[74]*Id.* at §6502(a)(1). Along with companies operating Web sites, operators of online services directed at children, or with actual knowledge that such service is collecting PII from children, are also covered by the COPPA. *Id.*

[75]These groups must rely on the EGA, GLBA, HIPAA, or a miscellaneous state statute to force companies to post, and then abide by, their privacy policies. The new EPPAA proposed in this article would eliminate this gap by covering all e-commerce sites in interstate commerce. *See* discussion *infra* Part IV.

[76]15 U.S.C. § 6502(b)(1)(A)(i) and 16 C.F.R. § 312.3(a) and § 312.4 (2006).

[77]15 U.S.C. § 6502(b)(1)(A)(i) and 16 C.F.R. § 312.4(b)(2)(ii) (2006). COPPA discusses PII but uses the term "personal information." 15 U.S.C. § 6501(8) and 16 C.F.R. § 312.2 (2006). Personal information covered by COPPA includes: (1) first and last name, (2) home or other physical address including a street name and name of a city or town, (3) e-mail address, (4) telephone number, (5) Social Security Number, (6) any other identifier that the FTC determines permits the physical or online contacting of a specific individual, and (7) information concerning the child or the parents of that child that the Web site collects online from the child and combines with an identifier listed above. *Id.*

[78]16 C.F.R. § 312.4(b)(2)(ii). Active information gathering occurs through Web site areas where children are asked to submit PII while passive collection occurs thorough means—such as cookies—where a child may be unaware that PII is being obtained. *See Blistex Privacy Policy,*

this information will be used,[79] (4) whether the information will be disseminated to third parties,[80] and (5) that a parent may review and delete a child's PII and refuse to consent to additional collection.[81] The policy must also contain contact information pertaining to the operators of the Web site so that parents have the opportunity to contact these administrators with questions or comments.[82] These specific requirements are privacy enhancing and are designed to create a situation where children's PII will not be collected without the informed consent of a parent.

Logistically, COPPA requires that the Web site contain at least a hyperlink to the electronic privacy policy and that this hyperlink be placed in a clear and prominent place on the Web site home page and at all places where children may be required to submit PII.[83] COPPA defines a clear and prominent hyperlink as one where the text of the link is in a different color, type size, or font from the text located on the rest of the Web page

---

http://www.blistex.com/Privacy_Policy.htm (last visited Oct. 1, 2006) (provides a nice example of active and passive PII collection definitions within an electronic privacy policy); *see also* Children's Online Privacy Protection Rule, 64 Fed. Reg. 22,754 (Apr. 27, 1999) (to be codified at C.F.R. pt. 312) (introducing the active/passive PII collection distinction).

[79]15 U.S.C. § 6502(b)(1)(A)(i) and 16 C.F.R. § 312.4(b)(iii) (2006).

[80]15 U.S.C. § 6502(b)(1)(A)(i) and 16 C.F.R. § 312.4(b)(2)(iv) (2006). If the information will be disseminated to third parties the privacy policy must identify the third parties, describe the type of business such third parties are in, explain how such parties will use the PII obtained, and state whether or not the third parties have agreed to maintain the confidentiality, security, and integrity of the PII obtained. *See* 16 C.F.R. § 312.4(b)(2)(iv) (2006).

[81]16 C.F.R. § 312.4(b)(2)(vi) (2006).

[82]16 C.F.R. § 312.4(b)(2)(i) (2006). This contact information must include the: (1) name, (2) mailing address, (3) telephone number, and (4) e-mail address of all operators maintaining PII from children obtained through the Web site. *Id*.

[83]16 C.F.R. § 312.4(b) (2006). Web sites are not required to cut and paste the entire privacy policy on the home page but merely to provide a hyperlink to the policy itself; this hyperlink must be located close to the area where children may enter PII. *See* FTC, Bureau of Consumer Protection, You, Your Privacy Policy and COPPA, How to Comply with the Children's Online Privacy Protection Act 2 [hereinafter COPPA Compliance Brochure], http://www.ftc.gov/bcp/conline/pubs/buspubs/coppakit.pdf (last visited Oct. 1, 2006). General audience Web sites with a specific children's area need not post the COPPA privacy policy on their main home page but only on the secondary home page containing the children's area and then on whichever pages collect PII from children. *See* 16 C.F.R. § 312.4(b) (2006).

where such hyperlink resides.[84] COPPA also requires that privacy policies be written in language that is clear and understandable.[85] Concerning enforcement, violations of COPPA may be treated as unfair or deceptive acts and/or practices prohibited under the Federal Trade Commission Act (FTC Act)[86] and enforced by the FTC.[87] COPPA preempts any state or local law that would conflict with its provisions,[88] but allows state attorneys general to initiate civil actions based on COPPA violations and serve in the place of parents over the course of such lawsuits.[89]

COPPA has many privacy-enhancing attributes that can be carried over into the proposed EPPAA. Especially important are the requirements that policies disclose how the PII will be used and whether it will be disseminated to third parties. These disclosures allow parents the opportunity to comprehend the privacy obligations surrounding the submission of their children's PII. A prominently placed privacy policy hyperlink and a clearly written policy are also attributes that will be present in the EPPAA and will add to the discovery, readability, and renewed effectiveness of electronic privacy policies. The strong preemption clauses are also useful because they disallow conflicting laws allowing businesses to comply with only one federal law concerning children's online privacy rather than a multitude of potentially conflicting state laws. Finally, allowing both the FTC and state attorneys general to enforce COPPA provisions is positive as it allows for more resources aimed at protecting children's PII.

---

[84]*See* Section 312.4 Notice, 64 Fed. Reg. 59894 (Nov. 3, 1999) (to be codified at 16 C.F.R. pt. 312). Web sites may also utilize a contrasting background in order to set off the privacy policy hyperlink from the other text and information located on the Web site home page. *See* COPPA Compliance Brochure, *supra* note 80, at 2. These links must also be titled in such a manner as to let the visitor know that the link will take them to the company's privacy policy and cannot contain vague labels such as "Legal Notice" or "Important Information." *Id*. at 3.

[85]16 C.F.R. § 312.4(a) (2006).

[86]15 U.S.C. § 57a(a)(1)(B) (2000).

[87]15 U.S.C. § 6502(c) and § 6505(a).

[88]15 U.S.C. § 6502(d).

[89]15 U.S.C § 6504(a)(1).

b. EGA. EGA[90] requires that all federal government agencies and agency contractors conduct and publish a privacy impact assessment.[91] EGA also requires that all agencies and contractors operating Web sites intended to interact with the public post a machine-readable electronic privacy policy.[92] These policies must be clear and be posted on the main home page and any other known main entry points and on pages where substantial personal information from the public is collected. These policies must state, among other things: (1) what information is being collected, (2) why it is being collected, (3) the intended use, (4) with whom the information will be shared, (5) notice and opportunities for consent to information sharing, and (6) how the information will be secured.[93]

Although EGA is important because it directly requires the creation and posting of electronic privacy policies, it only applies to government

---

[90]Pub. L. No. 107-347, 116 Stat. 2899, 2932-39 (codified as amended in scattered sections of 5, 10, 13, 31, 40, 41, and 44 U.S.C.).

[91]*See* 44 U.S.C. § 3501. Such assessments must analyze, among other things: (1) what information is collected, (2) why it is being collected, (3) its intended uses, (4) with whom it will be shared, (5) what notice will be provided to Web site visitors, and (6) how such information will be secured. *Id*.

[92]*See* 44 U.S.C § 3501(c)(2). For more information on machine-readable privacy policies and the P3P technological standard, see the discussion *supra* Part III.D. The Office of Management and Budget (OMB) was charged with developing regulations implementing the privacy provisions of the EGA. *See* 44 U.S.C. § 3501(c)(1)(a). The OMB issued its regulations on June 2, 1999 directing agencies to post clear privacy policies on the World Wide Web. MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES: PRIVACY POLICIES ON FEDERAL WEBSITES, M-99-18 (June 2, 1999), *available at* http://www.whitehouse.gov/omb/memoranda/m99-18.html. This guidance stated:

> As a first priority, [agencies] must post privacy policies to [the agency's] principal web site by September 1, 1999. By December 1, 1999, add privacy policies to any other known, major entry points to [agency] sites as well as at any web page where [the agency collects] substantial personal information from the public. Each policy must clearly and concisely inform visitors to the site what information the agency collects about individuals, why the agency collects it, and how the agency will use it. Privacy policies must be clearly labeled and easily accessed when someone visits a web site.

Id.

[93]44 U.S.C. § 3501(c)(1)(B)(i)–(vii). The Privacy Act of 1974 "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." U.S. DEP'T OF JUSTICE, OVERVIEW OF THE PRIVACY ACT OF 1974 1 (May 2004), http://www.usdoj.gov/04foia/1974intro.htm. *See also supra* note 22.

agencies and agency contractors (another example of sectoral regulation leaving a gap in the U.S. legal regime). Like COPPA, EGA contains certain privacy-enhancing attributes that can be carried over into the proposed EPPAA. For instance, the EGA requirement that all covered privacy policies state the intended use of any PII collected is important to give consumers a true picture of the relevant information-privacy implications. Additionally, the requirement to disclose how PII will be secured is crucial in today's world of identity fraud.

2. Federal Regulation Indirectly Targeting Electronic Privacy Policies

While COPPA and EGA directly target electronic privacy polices, GLBA and HIPAA indirectly touch upon such polices. For example, GLBA was passed primarily to deregulate the financial services sector by allowing certain financial institutions to combine and offer a wide variety of services to the public under one umbrella. Although GLBA contains privacy provisions, such provisions are ancillary. This is not to suggest that these GLBA privacy provisions do not have teeth. In fact, the privacy protections of GLBA as well as HIPAA forced companies to reconsider their privacy practices in attempts to comply and also required a great outlay of resources for compliance purposes. Both of these statutes have something to offer to the proposed EPPAA.

a. GLBA. E-commerce Web sites offering financial products and services to individuals are covered by the Financial Services Modernization Act of 1999 (better known as GLBA).[94] GLBA covers only financial institutions but defines this term in a broad manner to include, among other institutions, commercial banks, investment banks, mortgage companies, and check-cashing businesses.[95] Even though the term "financial

---

[94]Pub. L. No. 106-102, 113 Stat. 1338 (Nov. 12, 1999) (codified as amended in scattered sections of 12 and 15 U.S.C.). Although e-commerce is the focus of this article, the GLBA also applies to brick-and-mortar establishments. *See* 16 C.F.R. § 313.3(k) (2006) (explaining the definition of a financial institution by giving examples).

[95]The GLBA uses the definition of a financial institution found in the Bank Holding Act of 1956 (BHA) to construe the definition of a financial institution under the GLBA; the BHA considers any institution that is "significantly engaged in financial activities" to be a financial institution and, therefore, covered under the reach of the GLBA as well. *See* 12 U.S.C. § 1843(k) (2000). This article will refer to these entities, when discussing the GLBA, as "covered financial institutions."

institution" has broad implications within this particular industry sector, GLBA does not apply to businesses outside of this sphere, limiting its overall impact on e-commerce privacy policy reform. Additionally, under its mandate, GLBA only protects the nonpublic personal information concerning an individual's finances that is collected by covered financial institutions—a category of PII referred to as personally identifiable financial information (PIFI).[96] Nevertheless, GLBA does offer some privacy-enhancing attributes that should be factored into any broader, national legislation proposal. For instance, GLBA contains ancillary information privacy components promulgated by the FTC—better known as the "Financial Privacy Rule" and the "Safeguards Rule."[97]

The Financial Privacy Rule requires covered financial institutions to keep consumers apprised of the institution's privacy policies and procedures and limits the uses of PIFI collected from consumers.[98] This rule requires that covered financial institutions provide accurate, clear and conspicuous,[99] and reasonably understandable[100] privacy policy notices, both when a customer relationship is formed and then

---

[96]The GLBA defines "personally identifiable financial information" as information that: (1) is provided by a consumer to a financial institution, (2) results from any transaction with the consumer or any service performed for the consumer, or (3) is otherwise obtained by the financial institution. 15 U.S.C. § 6809(4)(A)(i)–(iii) and 16 C.F.R. § 313.3(0)(1)(i)–(iii) (2006).

[97]See 16 C.F.R. pt. 313 (2006) for the FTC Privacy of Consumer Information Final Rule (the Financial Privacy Rule) and 16 C.F.R. pt. 314 (2006) for the FTC Standards for Safeguarding Customer Information Final Rule (the GLBA Safeguards Rule). The GLBA Safeguards Rule "requires financial institutions to have a security plan to protect the confidentiality and integrity of personal consumer information." FTC, The Gramm-Leach-Bliley Act, The Safeguards Rule, http://www.ftc.gov/privacy/privacyinitiatives/safeguards.html (last visited Oct. 1, 2006).

[98]*See* 16 C.F.R. pt. 313 (2006).

[99]15 U.S.C. § 6803(a). The definition of "clear and conspicuous" was defined by the FTC in the Financial Privacy Rule. 16 C.F.R. § 313.3(b)(1) (2006). The FTC defined the phrase as a notice that is "reasonably understandable and designed to call attention to the nature and significance of the information in the notice." *Id*. The annual notice requirement can be found in 16 C.F.R. § 313.5(a)(1) (2006).

[100]The FTC stated that a company makes its privacy policy language "reasonably understandable" as long as it is able to: (1) present the information in the notice in clear, concise sentences, paragraphs, and sections; (2) use short explanatory sentences or bullet lists whenever possible; (3) use definite, concrete, everyday words and active voice whenever possible; (4) avoid multiple negatives; (5) avoid legal and highly technical business terminology whenever possible; and (6) avoid explanations that are imprecise and readily subject to different interpretations. 16 C.F.R. § 313.3(b)(2)(i)(A)–(F) (2006).

annually for the duration of such customer relationship.[101] If the covered financial institution's privacy policy is posted on the institution's Web site, the hyperlink to a company policy must be clearly and conspicuously posted.[102] The FTC has interpreted this requirement to mean that the policy may be posted on the home page in its entirety[103] or via a hyperlink as long as such link is of a size, font, and/or color designed to call attention to itself.[104] As mentioned briefly above, under the Financial Privacy Rule, all people dealing with the financial institution are split up into three groups: customers,[105]

---

[101]*See* 16 C.F.R. § 313.4 (2006). It is important to note that these privacy policies must accurately reflect the covered financial institution's actual privacy policies and practices. *Id*. In fact, the FTC brought an enforcement action against Sunbelt Lending Services Inc. alleging, inter alia, that the company failed to provide adequate privacy policy notices as required by the Privacy Rule of the GLBA. *See* Decision and Order, In the Matter of Sunbelt Lending Services, Inc., FTC Docket No. C-4129 (Jan. 3, 2005), http://www.ftc.gov/os/caselist/0423153/050107do0423153.pdf.

[102]*See* Privacy of Consumer Financial Information, 65 Fed. Reg. 33,649-33,650 (May 24, 2000) (to be codified in 16 C.F.R. pt. 313) (providing an explanation of "clear and conspicuous" postings).

[103]If a covered financial institution provides the actual text of the notice on a Web page (particularly the institution's home page), it must design the notice to call attention to the nature and significance of the information within it by utilizing text or visual cues to encourage scrolling down the page if necessary to view the entire notice and ensure that other elements on the Web site (such as text, graphics, hyperlinks, or sound) do not distract attention from the notice by either: (1) placing the notice on a screen that consumers frequently access, such as a page on which transactions are conducted, or (2) placing a hyperlink on a screen that consumers frequently access, such as a page on which transactions are conducted, that connects directly to the notice and is labeled appropriately to convey the importance, nature, and relevance of the notice. 16 C.F.R. § 313.3(b)(2)(iii)(A)–(B) (2006).

[104]The FTC states that a link is designed to call attention to itself if it calls attention to the nature and the significance of the information by: (1) using a plain-language heading to call attention to the notice; (2) using a typeface and type size that are easy to read; (3) providing wide margins and ample line spacing; (4) using boldface or italics for key words; (5) using a form that combines the notice with other information; and (6) using distinctive type size, style, and graphic devices, such as shading or sidebars, when combining this notice with other information. 16 C.F.R. § 313.3(b)(2)(ii)(A)-(E) (2006).

[105]*See* 16 C.F.R. § 313(h) (2006). Under the GLBA, a customer is merely a "consumer who has a customer relationship" with the particular financial institution. *Id*. A customer relationship is defined as a continuing relationship between the financial institution and the customer whereby the financial institution provides one or more financial products or services to the customer to be used primarily for personal, family, or household purposes. 15 U.S.C. § 6809(11) and 16 C.F.R. § 313.3(h)(i)(1) (2006).

consumers,[106] and nonconsumers.[107] Privacy policies must be distributed to consumers before disclosing any PIFI to nonaffiliated third parties,[108] upon the formation of the customer relationship and then not less than annually after the formation of such relationship.[109] The language of any privacy policy must describe, among other things: (1) categories of the PIFI collected,[110] (2) categories of the PIFI disclosed to affiliated entities and nonaffiliated third parties,[111] (3) categories of affiliates and nonaffiliated third parties to whom PIFI is disclosed,[112] (4) categories of PIFI of persons who have ceased to be customers of the financial institution as well as categories of affiliated and nonaffiliated third parties to whom the PIFI will continue to be disclosed,[113] (5) notice of the customer's option to opt out of disclosure to nonaffiliated third parties including the methods they may use to exercise this opt-out,[114] and (6) polices and practices related to the protection of the confidentiality and security of consumers' PIFI.[115] Additionally, under GLBA and its implementing regulations, covered financial institutions may share PIFI with affiliated entities without offering any form of consent but they must create the ability to opt out before sharing PIFI with unaffiliated parties.[116]

---

[106]*See* 16 C.F.R. § 313.3(e) (2006). Under the GLBA a consumer is defined as "an individual who obtains, from a financial institution, financial products or services which are to be used primarily for personal, family, or household purposes, and also means the legal representative of such individual." 15 U.S.C. § 6809(9).

[107]The term "nonconsumers" is a catchall title used in this article for any person not categorized as a customer or a consumer—although the GLBA or the Financial Privacy Rule do not define this concept in this way. The GLBA does not require that covered financial institutions offer many privacy protections to nonconsumers as the Financial Privacy Rule is targeted toward consumers and customers. 16 C.F.R. § 313.3(e) (2006).

[108]16 C.F.R. § 313.3(4)(a)(2) (2006).

[109]16 C.F.R. §§ 313.4–313.5 (2006).

[110]16 C.F.R. § 313.6(a)(1) (2006).

[111]15 U.S.C. § 6803(a)(1); 16 C.F.R. § 313.6(a)(2) (2006).

[112]16 C.F.R. § 313(6)(a)(3) (2006).

[113]15 U.S.C. § 6803(a)(2); 16 C.F.R. § 313.6(a)(4).

[114]16 C.F.R. § 313.6(a)(6) (2006).

[115]15 U.S.C § 6803(a)(3); 16 C.F.R. § 313.6(a)(8) (2006). 16 C.F.R. § 313.6(c)(6)(i)-(ii) (2006).

[116]15 U.S.C. § 6802(b); 16 C.F.R. § 313.10 (2006).

The Safeguards Rule, on the other hand, requires covered financial institutions to take appropriate measures to safeguard the security, confidentiality, and integrity of consumers' PIFI described in the privacy policy by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards.[117] For the purposes of the proposed EPPAA, the Financial Privacy Rule is more relevant due to its focus on creating more effective privacy policies.

Unlike COPPA, GLBA does not preempt state laws that provide greater protection.[118] Therefore, under GLBA, a state may pass legislation requiring a more comprehensive privacy policy structure or more inclusive privacy policy content for financial services institutions. Neither GLBA nor its implementing regulations directly allow any private right of action to sue a covered financial institution for a privacy violation. Rather, in situations where such enforcement power is not delegated to any other federal regulatory institution, the FTC has begun to enforce the privacy protections of GLBA.[119]

The most privacy-enhancing aspects of GLBA are: (1) its "reasonably understandable" language requirement and (2) its procedures for updating customers on privacy policy modifications. GLBA joins COPPA, EGA, and HIPAA in requiring that the average customer be able to understand

---

[117]*See* 16 C.F.R. pt. 316 (2006). In connection with the written information security program, covered financial institutions must: (1) employ at least one person to oversee the program; (2) assess the security risks to personal information and the plan's ability to control such risks; (3) design and implement safeguards to help control these risks; (4) require, via written contracts, that services providers to also protect this information; and (5) implement testing and monitoring of the program and then modify the program based on the results. *Id*.

[118]15 U.S.C. § 6807(a) and (b) and 16 C.F.R. § 313.17 (2006). The GLBA also holds that its privacy protections "shall not be construed as superseding, altering or affecting any statute, regulation, order, or interpretation in effect in any State, except to the extent that such statute, regulation, order, or interpretation is inconsistent with the provisions of [the privacy protections subchapter of the GLBA], and then only to the extent of the inconsistency." *Id*. § 6807(a).

[119]15 U.S.C. § 6805(a)(1)-(7). Congress also allowed the insurance authorities in each state to enforce the privacy provisions of the GLBA. *Id*. § 6805(a)(6). For a taste of the type of case enforced by the FTC, see, for example, Decision and Order, In the Matter of Nationwide Mortgage Group, Inc., FTC Docket No. 9319 (Apr. 12, 2005), *available at* http://www.ftc.gov/os/adjpro/d9319/050415dod9319.pdf (the complaint filed by the FTC alleged that Nationwide Mortgage Group, Inc. failed to implement appropriate safeguards for collected PIFI and failed to distribute the privacy policies required under the Financial Privacy Rule). *See also* discussion *infra* Part III.C.

the implications of submitting PII to a financial institution. This helps eliminate one of the biggest problems facing contemporary privacy policies —the lack of understandable policy terms. Additionally, requiring covered financial institutions to update their customers concerning privacy policies helps keep companies accountable for informing people about policy modifications. On the other hand, GLBA's distinction between consumers, customers, and nonconsumers is not helpful in the larger e-commerce context because all people entering PII should be informed of and protected by a privacy policy, regardless of their status at the time of data entry. Another aspect of GLBA that will not be carried over to the proposed EPPAA is the mandatory opt-out provision for secondary use of PII. Companies should be allowed to set their own standards for secondary use and require only that these standards be properly disclosed, in plain language, in the privacy policy. This way, Web site visitors will have a choice as to whether they want to disclose their PII and businesses will have the flexibility to determine their own privacy policy terms.

b. HIPAA. HIPAA[120] was passed primarily to "improve portability and continuity of health insurance coverage."[121] This sectoral-based legislation applies to most health plans[122] (including employer-sponsored health plans),[123] health care clearinghouses,[124] and health care

---

[120]Pub. L. No. 104-191, 110 Stat. 1936 (Aug. 21, 1996) (codified as amended in scattered sections of 26 and 42 U.S.C.).

[121]Pub. L. No. 104-191, Preamble.

[122]Health plans include "individual and group plans that provide or pay the cost of medical care. . . . [including] health, dental, vision, and prescription drug insurers, health maintenance organizations ('HMOs'), Medicare, Medicaid, Medicare+Choice, and Medicare supplement insurers, and long-term care insurers." U.S. Dep't of Health and Human Services, OCR Privacy Brief: Summary of the HIPAA Privacy Rule 2 (May 2003) [hereinafter OCR HIPAA Summary]. Health care plans also include most "employer-sponsored group health plans, government and church-sponsored health plans, and multi-employer health plans." *Id.*

[123]*See* OCR HIPAA Summary, *supra* note 122, at 2–4. But HIPAA does not cover decisions employers make in an employment context. *Id.*

[124]Health care clearinghouses are "entities that process nonstandard information they receive from another entity into a standard (i.e., standard format or data content), or vice versa." OCR HIPAA Summary, *supra* note 122, at 3. Health care clearinghouses that merely receive personally identifying health information (PIHI) to process transactions for health plans or health care providers are not covered by 15 C.F.R. pt. 164 (2005) [hereinafter HIPAA Privacy Rule]. *Id.*

providers[125] that transmit PIHI[126] in certain electronic transactions.[127] Although the primary purpose of HIPAA is to protect insurance coverage, ancillary provisions were added by the Department of Health and Human Services (DHHS) through administrative rule making that were intended to provide privacy protection for some forms of sensitive health information.[128] Like the other sectoral-based laws discussed above, HIPAA offers a few unique attributes that are useful in the proposed EPPAA.

To comply with the HIPAA Privacy Rule, entities must create compliance procedures as well as distribute privacy policies that state how a patient's PIHI will be protected by such privacy procedures.[129] These notices must be written in "plain language" and be distributed at the first point of service delivery between an individual and a health care provider as well as to any person requesting a copy.[130] Additionally, such

---

[125]Health care providers include all providers of services (such as hospitals) and all providers of medical or health services (such as physicians, dentists, and other practitioners) and "any other person or organization that furnishes, bills, or is paid for health care." OCR HIPAA SUMMARY, *supra* note 122, at 2.

[126]The acronym PIHI is utilized in this article while HIPAA and its implementing regulations refer to this information as "individually identifiable health information" or "protected health information." 45 C.F.R. § 164.501 (2005). PIHI covered by the HIPAA is information, including demographic data, that relates to: the individual's past, present, or future physical or mental health or condition or the provision of health care to the individual, or the past, present, or future payment for the provision of health care to the individual and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual. OCR HIPAA SUMMARY, *supra* note 122, at 4. PIHI includes "many common identifiers (e.g., name, address, birth date, Social Security Number)." *Id*. The HIPAA Privacy Rule, however, excludes PIHI that any covered entity maintains in its capacity as an employer. *Id*.

[127]*See* OCR HIPAA SUMMARY, *supra* note 122, at 2–4.

[128]45 C.F.R. pt. 164 (2005).

[129]While privacy policies under the HIPAA are referred to as "notices of privacy practices," this article will refer to them as privacy policies for consistency. *See* 45 C.F.R. §164.520 (2005) (referring to privacy policies as notices of privacy practices).

[130]HIPAA-compliant privacy policies were required to be posted on April 14, 2003 (except that small health plans were required to comply by April 14, 2004) and, for new enrollees, at the time of their enrollment. HIPAA-covered entities must also make a good faith effort to obtain a written acknowledgment of receipt of the notice in nonemergency situations. If the acknowledgment cannot be obtained the entity must document the efforts made to obtain the acknowledgment and the reasons for the inability to obtain it. The requirement that the privacy policy be distributed on the first visit to a direct health care provider is found at 45 C.F.R. § 164.520(c)(ii)(1)(A) and (B) (2005).

privacy policies must contain a clear explanation of certain issues such as: (1) a header including language stating "This notice describes how medical information about you may be used and disclosed and how you can get access to this information. Please review it carefully,"[131] (2) how the covered health entity may use and disclose an individual's PIHI,[132] (3) an individual's rights with respect to PIHI and how the individual may exercise such rights,[133] (4) the institution's legal duties to protect the privacy of PIHI,[134] and (5) the point of contact for further information or to file a complaint regarding the entity's privacy practices.[135] Covered health institutions must abide by the terms of their posted privacy policies and such policies must contain an effective date.[136] Providers with a direct treatment relationship with a patient must make a good faith effort to obtain an individual's acknowledgement of policy receipt upon the initial

---

[131]45 C.F.R. § 164.520(b)(1)(i) (2005).

[132]The policy must disclose the types of uses and disclosures that the HIPAA-covered entity is permitted to make for the following three uses: (1) treatment, (2) payment, and (3) health care operations as well as the other purposes for which the entity is permitted or required to use or disclosure PIHI without consent. 45 C.F.R. § 164.520(b)(1)(ii)(A) and (B) (2005). This section must also contain a statement that any other uses will not be made without the individual's prior written authorization and that the individual may revoke this authorization. *Id*. § 164.520(b)(1)(ii)(E). This section must contain at least one example *Id*. § 164.520(b)(1)(ii)(A).

[133]45 C.F.R. § 164.520(b)(1)(iv)(A)–(F) (2005). This includes the right to request restrictions on certain uses and disclosures of PIHI including a statement that the HIPAA-covered entity is not required to honor such request, *id*. § 164.520(b)(1)(iv)(A); the right to receive confidential communications of PIHI and to inspect, copy, and amend PIHI, *id*. § 164.520(b)(1)((iv)(B)-(D); the right to an accounting of PIHI disclosures; and the right to obtain a paper copy upon request, *id*. §164.520(b)(1)(iv)(E) and (F).

[134]45 C.F.R. § 164.520(b)(1)(v) (2005). HIPAA-covered entities have a duty to: (1) maintain the privacy of PIHI and to notify individuals of privacy practices related to PIHI, (2) abide by the privacy policy currently in effect, and (3) state that they reserve the right to modify the privacy policy and to make the revised terms applicable to all covered individuals (this statement must also discuss how notice of this revision will be made). *Id*. at § 164.520(b)(1)(v)(A)–(C).

[135]45 C.F.R. § 164.520(b)(1)(vi) and (vii) (2005). This section must contain a statement that an individual will not be retaliated against on the basis of filing a complaint. *Id*. § 164.520(b)(1)(vi). As for the contact information, this section must also contain the name, or title, and a telephone number an individual may use for further information requiring the HIPAA-covered entity's privacy practices. *Id*. §164.520(b)(1)(vii).

[136]45 C.F.R. § 164.520(b)(1)(viii) (2005). This effective date cannot be earlier than the first date upon which the privacy policy was first published. *Id*.

service delivery.[137] Finally, a HIPAA-covered entity must promptly revise and redistribute its privacy policy whenever a material policy change occurs and also inform people about how to obtain the notice once every three years.[138] The HIPAA Privacy Rule also tangentially discusses electronic privacy policies; for example, if any HIPAA-covered entity utilizes a Web site in its business, it must prominently post its privacy policy on any Web page that provides information about its customer service and benefits.[139]

Contrary state laws are preempted by HIPAA,[140] but more restrictive state laws that are not contrary to the federal protections are not preempted.[141] A law is contrary to HIPAA if: (1) it is impossible for a HIPAA-covered entity to comply with both HIPAA and the state law and/or (2) the state law stands as an obstacle for the execution of HIPAA.[142] As for

---

[137]45 C.F.R. § 164.520(c)(2)(ii) (2005). The HIPAA Privacy Rule only requires that this acknowledgment be in writing but does not require any particular content or process of obtaining it. The rule does not require that an individual even sign the acknowledgment—as long as the signature is obtained in various other locations such as a log book. Oral acknowledgments are not acceptable. *See* 67 Fed. Reg. 53240. Other HIPAA-covered entities are not required to obtain such acknowledgment but may choose to if they so desire. *Id*. at 53239.

[138]45 C.F.R. § 164.520(b)(3) (2005) (discussing material revisions) and 45 C.F.R. § 164.520(c)(1)(ii) (2005) (imposing the three-year requirement whereby a HIPAA-covered entity must disclose that the privacy policy is available and how to obtain it).

[139]45 C.F.R. § 164.520(c)(3)(i) (2005). This notice must be placed on, and made electronically available through, the Web site. *Id*.

[140]Social Security Act of 1935, 42 U.S.C. § 1320d-7(a)(1) (2000). This section of the Social Security Act, as amended by HIPAA, states in part that "a provision or requirement under this part . . . shall supersede any contrary provision of State law, including a provision of State law that requires medical or health plan records (including billing information) to be maintained or transmitted in written rather than electronic form." *Id*. On a similar note, a new movement is gaining strength; designed to simplify the conflicts between the differing state laws and HIPAA regarding the exchange of health information, the Health Information Security and Privacy Collaboration is beginning the process of coordination buoyed by an $11.5 million grant from the Department of Health and Human Services. Nancy Ferris, *RFP Seeks State Input About Health Records Exchange*, GOVERNMENT HEALTH IT, Jan. 14, 2006, http://www.govhealthit.com/article91964-01-13-06-Web.

[141]42 U.S.C. § 1320d-7(a)(2)(B).

[142]*Id*. There are exceptions to this test such as when the Secretary of DHHS determines that the contrary state law is necessary to prevent fraud and abuse related to the provision or payment for health care or to ensure the appropriate state regulation of insurance or health plans. *Id*.

enforcement, under the HIPAA Privacy Rule, the Office for Civil Rights of the DHHS (OCR) is charged as the primary enforcement body and individuals are allowed no private right of action.[143]

As demonstrated above, HIPAA has many privacy-enhancing attributes. For example, the requirement that entities evaluate their privacy practices and turn such evaluations into readable privacy policies is a procedure that can be carried over into the proposed EPPAA. This readability standard is key to an effective privacy policy regulatory regime as it allows consumers to become more comfortable with understanding information privacy implications. Also helpful is the fact that patients must be informed of their privacy rights under HIPAA. One of the greatest weaknesses in HIPAA, from a business compliance perspective, lies in its failure to preempt more restrictive state laws. Under this type of preemption provision, businesses may be forced to comply with fifty different state laws, along with HIPAA, leading to the same uncertainly that plagues current privacy policy.

B. State Regulation Targeting Electronic Privacy Policies

Although every state in the nation has some legislation governing a particular aspect of information privacy,[144] California is the most important player when it comes to the regulation of electronic privacy policies.[145]

---

[143]In the past the OCR has "investigated discrimination complaints against health care and social service providers receiving federal assistance." McGuire Woods, Press Room: HIPAA Privacy: What Enforcement Action is Coming (Mar. 10, 2004), *available at* http://www.mcguirewoods.com/news-resources/item.asp?item=905.

[144]Robert Ellis Smith, Compilation of State and Federal Privacy Laws 2 (Privacy Journal 2002).

[145]In fact, California is the most progressive state in the nation when it comes to protecting its residents' information privacy. An example is a new California law creating a security requirement for PII of California residents that is collected and stored by California companies regardless of industry sector. *See* Cal. Civ. Code § 1798.81.5 (2004). The law requires that companies holding such PII "implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." *Id*. Third parties obtaining the PII from the company to which it was initially given must also agree to abide by the security procedures. Therefore, if it withstands challenge, this California statute "will be the first federal or state law to impose such a general requirement." Holly K. Towle, *Information Security Statements can Become Legal Obligations*, Washington Legal Foundation, Legal Opinion Letter, Apr. 22, 2005. Across the country, twenty-one other states have

In fact, the California Online Privacy Protection Act of 2003 (California OPPA) is a groundbreaking statute requiring commercial Web sites and online service operators who collect PII about California residents to provide such residents with a conspicuous electronic notice of posted privacy policies and then to comply with such privacy promises.[146] This law is important because it is the first state legislation to require the posting of an electronic privacy policy as well as compliance with the policy terms regardless of the industry sector within which a company operates.[147] Under California OPPA, privacy polices must contain specific information —such as the PII collected, the categories of parties with whom this PII may be shared, and the process for notification of material changes to such policy—and must be posted in a conspicuous manner on the company's Web site.[148] The PII covered by this law includes a California consumer's[149] name, physical address, e-mail address, telephone number, Social Security Number, and any other identifier "that permits the physical or online contacting of a specific individual."[150] The law preempts all local

---

legislation requiring that customers must be notified of information security breaches. Tony Knotzer & Larry Greenemeier, *Wall Street and Technology, Sad State of Data Security*, CMP Media, Jan. 5, 2006, *available at* http://www.wstonline.com/showArticle.jhtml?articleID=175801687. Another seventeen states are considering similar legislation. *Id*.

[146]*See* Cal. Bus & Prof. Code §§ 22575-22579. The California OPPA went into effect on July 1, 2004 and preempts all local laws that require and regulate the posting of a privacy policy. *Id*. §§ 22578-22579. The entities covered by this law are operators of any commercial Web site and online services that collect PII about California residents who visit or use the Web site. *Id*. § 22575(a). The law does not apply to Internet Service Providers who transmit or store PII about California residents. *Id*. § 22577(c).

[147]Cooley Godward, Cooley Alerts, California Online Privacy Protection Act of 2003 (June 29, 2004), http://www.cooley.com/news/alerts.aspx?ID=38606820.

[148]*Id*. §22575(b)(1) and (3). The law also requires a covered entity, if such entity "maintains a process for an individual consumer who uses or visits its commercial Web site on online service to review and request changes to any of his or her personally identifiable information that is collected through the Web site or online service," to provide a description of that process. *Id*. §225765(b)(2).

[149]A consumer is defined under the law is "an individual who seeks or acquires goods, services, money, or credit for personal, family, or household purposes." *Id*. § 22577(d). Therefore, PII collected from nonconsumers residing in California would fall outside of the scope of this law. This also implies that information collected from businesses or other organizations also falls outside of the scope of the California OPPA.

[150]*Id*. § 22577(a). As defined in the statute, "Personally identifiable information also includes information concerning a consumer that is collected online (such as birthday, weight, hair

regulations requiring the "conspicuous" posting of an Internet privacy policy.[151] Violations of California OPPA occur only after a company is notified that its Web site does not contain a compliant privacy policy and then subsequently fails to comply within thirty days from such notification.[152] Violations must be knowing and willful or negligent and material.[153] Enforcement of this law resides under the protections of the California Unfair Competition Law.[154]

As will be further discussed and analyzed in Part IV, this California law effectively acts as a national regulation in the sense that its reach

> extends beyond California's borders to require any person or company in the United States (and conceivably the world) that operates a Web site that collects personally identifiable information from California consumers to post a conspicuous privacy policy on its Web site stating what information is collected and with whom it is shared, and to comply with such policy. Those who do not comply with [the California OPPA] risk civil suits for unfair business practices.[155]

---

color, etc.) and is maintained by an operator in personally identifiable form in combination with one of the above identifiers." *Id*.

[151]*Id*. §22575(a). A privacy policy will be considered conspicuously posted if:

1. The privacy policy appears on the website homepage;
2. The privacy policy is directly linked to the homepage by an icon that contains the word "privacy," as long as this icon appears in a color different from the background of the homepage; or
3. The privacy policy is linked to the homepage via a hypertext link that contains the word "privacy," is written in capital letters equal to or greater in size than the surrounding text, is written in a type, font, or color that contrasts with the surrounding text of the same size, or is otherwise distinguishable from surrounding text on the homepage.

Id.

[152]*Id*. § 22575(a).

[153]*Id*. § 22576(a) and (b). This interpretation means that a nonmaterial violation may be actionable as long as it is willful and knowing. A nonmaterial violation of the law that is merely negligent is not actionable.

[154]The California Unfair Competition Law can be found in the California Business and Professions Code. CAL. BUS. & PROF. CODE §§ 17200-17209. Possible remedies under the California Unfair Competition Law range from civil penalties to equitable relief. Private rights of action are also allowable. "Operators who violate OPPA may also be susceptible to actions by the Federal Trade Commission, which may bring enforcement action against businesses whose posted privacy policy is deceptive." COOLEY GODWARD ALERT, *supra* note 147.

[155]*Id*.

Other states are considering, but have not yet passed, similar mandatory electronic privacy policy regulations covering commercial Web sites targeting state residents.[156] On a similar note, the Nebraska legislature recently passed a law prohibiting knowingly making a false or misleading statement in a privacy policy published on the Internet or in paper form regarding the use of PII submitted by members of the public.[157] Pennsylvania's deceptive or fraudulent business practices act includes false or misleading statements in commercial privacy policies published on Web sites.[158] The false or misleading statement must be knowingly made in a privacy policy and must concern the use of PII submitted by the public.[159] Violations of this Pennsylvania statute justify a fine between $50 and $500 per offense.[160] By the turn of the century six states passed legislation requiring state agency Web sites to post specific privacy policies stating how PII will be collected and used[161] and as of July 2005 ten additional states have enacted similar statutes.[162] Of all of the state laws regarding information privacy, the proposed EPPAA will draw

---

[156]*Id*. at n.8.

[157]Neb. Rev. Stat. § 87-302(14) (2005) (this section is part of the Nebraska Deceptive Trade Practices statute).

[158]18 Pa. Cons. Stat. § 4107 (2006) (this section covers deceptive or fraudulent business practices in Pennsylvania).

[159]18 Pa. Cons. Stat. Ann. § 4107(A)(10) (West 2005). As with the Nebraska privacy policy statute, this section in the Pennsylvania statute also applies to privacy policies posted on the Internet or otherwise published. *Id*.

[160]*Id*. § 4107(A.1)(4).

[161]Nat'l Conference of State Legislatures, News from the States, State Website Privacy Policies (fall 2001), http://www.ncsl.org/programs/lis/CIP/CIPCOMM/news1101.htm#privacy policies.

[162]*Id*. The sixteen states are: Arizona (Ariz. Rev. Stat. Ann. §§ 41-4151 to -5152 (2004)); Arkansas (Ark. Code Ann. § 25-1-114 (Supp. 2005)); California (Cal. Gov't Code § 11019.9 (West 2005)); Colorado (Colo. Rev. Stat. Ann. §§ 24-72-501 to -502 (2005)); Delaware (Del. Code Ann. tit. 29, §§ 9017C-9022C (2003)); Illinois (5 Ill. Comp. Stat. Ann. 177/1-177/15 (West 2006)); Iowa (Iowa Code § 22.11 (2001)); Maine (Me. Rev. Stat. Ann. tit. 1, §§ 541-542 (Supp. 2005)); Maryland (Md. Code Ann., State Gov't § 10-624(4) (LexisNexis 2004)); Michigan (2003 Mich. Pub. Acts, Act 161 (§ 572(6))); Minnesota (Minn. Stat. Ann. § 13.15 (West 2005)); Montana (Mont. Code Ann. §§ 2-17-550 to -553 (2005)); New York (N.Y.S. Tech. Law §§ 201-207 (McKinney 2003)); South Carolina (S.C. Code Ann. §§ 30-2-10 to -50 (Supp. 2004)); Texas (Tex. Gov't Code Ann. § 2054.126 (Vernon Supp. 2005)); and Virginia (Va. Code Ann. §§ 2.2-3800 to -3803 (2005)).

most extensively from California OPPA and its requirements that a company post a compliant policy without requiring any specific privacy policy terms. This is an important distinction that will force companies to evaluate their privacy practices while also granting them the flexibility to tailor appropriate privacy policies.

In addition to both state and federal statutory compliance, e-commerce businesses must also be cognizant of federal and state administrative agency enforcement actions. Such actions normally target issues falling outside of the scope of the information-privacy regulations.

C. Enforcement of Electronic Privacy Policy Promises

Recognizing that neither federal nor state legislation presents a particularly effective remedy for broken privacy promises outside of regulated sectors, the FTC along with many state attorneys general began keeping an eye on privacy policy promises. These governmental entities most often use their unfair and deceptive practices enforcement authority —primarily enacted for consumer protection purposes—to deal with situations falling outside of the scope of federal and state laws. Recently, the FTC has led the pack in bringing enforcement actions leading to consent orders or negotiated settlements. On the state level, the New York Attorney General is continuing to aggressively pursue broken privacy policy promises through New York state consumer protection statutes.[163]

1. Federal Government Enforcement

The FTC states that privacy is a "central element" of the agency's consumer protection mission.[164] Today the FTC recognizes that rapidly evolving computing technology can exacerbate privacy violations as data collection, storage, aggregation, and dissemination become more inexpensive and efficient.[165] As detailed above, the FTC enforces specific federal statutes—particularly COPPA and GLBA—governing privacy policies but also spends time enforcing broken privacy promises through its authority

---

[163]*See* discussion *infra* Part III.C.2.

[164]FTC, Privacy Initiatives: An Introduction [hereinafter FTC Privacy Initiatives], http://www.ftc.gov/privacy/ (last visited Oct. 1, 2006).

[165]*See id.*

granted by the FTC Act.[166] The FTC Act established the FTC[167] and granted it the power to protect consumers.[168] Section 45(a)(1) of the FTC Act prohibits unfair and deceptive acts or practices in interstate commerce.[169] The FTC is allowed to exercise its general enforcement authority if: (1) it has reason to believe that an unfair or deceptive act or practice is occurring and (2) if it appears to the Commission that bringing an action is in the public interest.[170] The FTC takes this mandate seriously and believes that it has broad authority to protect consumers and that this authority includes enforcing privacy promises Web sites make to visitors.[171] Recently the FTC has used this enforcement power by filing several high-profile complaints against companies that breach promises

---

[166]*See* 15 U.S.C. §§ 41-58 (2000).

[167]*See id*. § 48.

Under the FTC Act,

> the Commission is empowered, among other things, to (a) prevent unfair methods of competition, and unfair or deceptive acts or practices in or affecting commerce; (b) seek monetary redress and other relief for conduct injurious to consumers; (c) prescribe trade regulation rules defining with specificity acts or practices that are unfair or deceptive, and establishing requirements designed to prevent such acts or practices; (d) conduct investigations relating to the organization, business, practices, and management of entities engaged in commerce; and (e) make reports and legislative recommendations to Congress.

FTC, *Legal Resources*, http://www.ftc.gov/ogc/stat1.htm (last visited Oct. 1, 2006). The FTC Act grants the FTC wide jurisdiction to enforce its provisions but a few industry segments—such as financial institutions, airlines, and telecommunications carriers—fall outside of its scope. *Id*. § 45(a)(2).

[169]Commerce is defined in the FTC Act as "commerce among the several States or with foreign nations, or in any Territory of the United States or in the District of Columbia, or between any such Territory and another, or between any such Territory and any State or foreign nation, or between the District of Columbia and any State or Territory or foreign nation." *Id*. § 44. The FTC does not have jurisdiction over purely intrastate commerce.

[170]*See* 15 U.S.C § 45(b). When the FTC chooses to take an enforcement action, it must serve a complaint stating the charges and notice of a hearing date. The person charged in the complaint then has the right to appear and give reasons why it need not cease and desist from the unfair or deceptive practice alleged by the FTC. *Id*. § 45(b). If the FTC renders a cease and desist order, the defendant may contest the order in the U.S. Court of Appeals. *Id*. § 45(c).

[171]*See* FTC, Prepared Statement before the Commerce, Trade and Consumer Protection Subcomm. of the H.R. Comm. of Energy and Commerce, Cybersecurity and Customer Data: What's at Risk for the Consumer? (Nov. 19, 2003), *available at* http://www.ftc.gov/os/2003/11/031119swindletest.htm.

made in electronic privacy policies.[172] The Commission has even brought cases where third parties collecting PII on a Web site operated by another company breach the privacy promises of the operator's Web site.[173] Although the FTC does not require companies to post privacy policies, it has the authority to bring an enforcement action as either an unfair or a deceptive practice, or both, if promises are made and subsequently broken.[174]

Under its unfair practices authority, the FTC has brought several cases since 1999 involving the breach of a promise made in an electronic privacy policy.[175] The typical situation in which the FTC has brought

---

[172]The FTC has the authority to bring enforcement actions in cases other than privacy policy violations. Recently, the FTC brought an action against a company for failing to adequately protect personal data. The FTC categorized this failure as an unfair practice. *See* Agreement Containing Consent Order, In the Matter of BJ's Wholesale Club, Inc., FTC File No. 0423160 (May 17, 2005) [hereinafter *BJ's Consent Order*], *available at* http://www.ftc.gov/os/caselist/0423160/050616agree0423160.pdf.

[173]*See, e.g.*, Agreement Containing Consent Order, In the Matter of Vision I Properties, LLC FTC File No. 0423160 (Mar. 10, 2005), *available at* http://www.ftc.gov/os/caselist/0423068/050310agree0423068.pdf. In the Vision I case, Vision operated e-commerce shopping carts whereby visitors enter PII into the cart to complete a particular transaction for a third-party merchant. The merchants made privacy policy promises that they would not sell or rent this PII. Vision, however, did not make such privacy policy promises. The FTC argued that Vision's renting of this PII violated the merchant's privacy policies and was not adequately disclosed to visitors and, therefore, was an unfair trade practice. The consent order requires that Vision's collection practices be consistent with the particular merchant's privacy promises or that Vision create a clear and conspicuous disclaimer as to the inconsistent uses. *Id*.

[174]The FTC has also brought enforcement actions where no privacy promises were breached, in situations where companies fail to adequately protect PII. For example, the FTC recently brought an unfair practices action against BJ's Wholesale Club, Inc. for failure to employ reasonable and appropriate security measures to protect PII by not encrypting such information in transit, storing it in places where it could be accessed anonymously, failing to limit network access through wireless access points, failing to employ sufficient measures to detect unauthorized access, and storing information for longer periods than necessary. *See* Complaint, In the Matter of BJ's Wholesale Club, Inc., FTC Docket No. C-4148 [hereinafter *BJ's Complaint*], *available at* http://www.ftc.gov/os/caselist/0423160/092305comp0423160.pdf. The case eventually settled, resulting in the issuance of a consent order. *See BJ's Consent Order*, *supra* note 172.

[175]*See*, *e.g.*, Complaint, United States v. ChoicePoint Inc., Civ. No. 1-06-CV-0198 9 (Jan. 30, 2006) [hereinafter *ChoicePoint Complaint*], *available at* http://www.ftc.gov/os/caselist/choicepoint/0523069complaint.pdf (after 163,000 consumer PII records were stolen from ChoicePoint, the FTC charged that the company's failure to implement reasonable security practices covering this PII constituted an unfair practice); In the Matter of Vision I Properties, LLC, Complaint, FTC Docket No. 0423068 1-3 (the FTC charged a company with committing an

deceptive practice actions involves a data security breach incident where a company's promise of data security was not implemented or improperly monitored.[176] The FTC has also brought deceptive practices actions against companies for unauthorized distribution of children's PII,[177] the sale of customer PII during a bankruptcy,[178] the misuse of educational surveys,[179] and the retroactive application of a privacy policy modification.[180]

2. State Government Enforcement

Aside from FTC enforcement actions, a few state attorneys general have brought enforcement actions against companies for violating their electronic privacy promises. These cases are generally brought under state unfair and deceptive practice statutes sometimes referred to as "Little FTC Acts."

For instance, the New York Attorney General, through its innovative Internet Bureau, has brought major enforcement actions under the New York Consumer Protection statutes.[181] Major actions have been brought against large corporations such as DoubleClick, Ziff Davis, Eli Lilly, Juno

---

unfair practice when the company's privacy policy claimed that PII would not be shared with third parties but such information ended up being disseminated through shopping cart software provided by a third party).

[176]*See, e.g.*, Agreement Containing Consent Order, In the Matter of Petco Animal Supplies, Inc, FTC File No. 032-3221 (Nov. 17, 2004), *available at* http://www.ftc.gov/os/caselist/0323221/041108agree0323221.pdf; Guess?.com, Inc., Agreement Containing Consent Order, File No. 022-3260 (June 18, 2003), *available at* http://www.ftc.gov/os/2003/06/guessagree.pdf.

[177]*See, e.g.*, In the Matter of Liberty Financial Companies, Inc., FTC File No. 982-3522 (May 6, 1999), *available at* http://www.ftc.gov/os/1999/05/lbtyord.htm; In the Matter of GeoCities, FTC File No. 9823015 (Aug. 13, 1998), *available at* http://www.ftc.gov/os/1998/08/geo-ord.htm.

[178]Complaint, In the Matter of Toysmart.com, LLC and Toysmart.com, Inc., Civ. No. 00-11341-RGS (July 21, 2000), *available at* http://www.ftc.gov/os/2000/07/toysmartcomplaint.htm. In this highly publicized case, the FTC charged that Toysmart attempted to sell its customers' PII as a stand-alone asset in bankruptcy in violation of a direct privacy policy promise that such PII would not be sold to third parties without customer consent. *Id*. at Count I.

[179]*See, e.g.*, In the Matter of Educational Research Center of America, Inc., FTC File No. 022-3249 (Jan. 29, 2003), *available at* http://www.ftc.gov/os/2003/01/ercaconsent.htm.

[180]*See* Stipulated Consent Agreement and Final Order, In the Matter of Reverseauction, (Jan. 6, 2000) (the FTC brought charges of unfair acts/practices as alternative charges).

[181]Office of the New York Attorney General, *Internet Concerns*, http://www.oag.state.ny.us/internet/internet.html (last visited Feb. 25, 2006). On this Web site a consumer has the ability to file a complaint electronically through the *Internet Concerns* Web page. *Id*.

Online Services, Victoria's Secret, and organizations such as the American Civil Liberties Union.[182] More recently, in 2003 New York Attorney General Elliot Spitzer brought an action against Netscape Communications alleging that the company collected certain PII through its "Smart Download" feature in violation of its electronic privacy policy promises.[183] In another prominent case from a different state, the New Jersey Attorney General settled with Toys 'R' Us concerning charges that the company violated its privacy policy.[184]

These state enforcement actions, combined with federal FTC actions, represent the bulk of electronic privacy policy enforcement, and all of these agencies will have a continuing role to play in protecting consumers from broken privacy policy promises even if Congress chooses to regulate privacy more thoroughly. Outside of the statutory and regulatory enforcement options, the remainder of privacy policy enforcement is made voluntarily through various industry self-regulation efforts.

D. Industry Self-Regulation

In the United States today much of the burden of protecting online PII falls to the e-commerce companies themselves. Such companies may voluntarily engage in some form of self-regulation, such as subscribing to certain privacy technology or agreeing to comply with a third-party self-regulation system such as obtaining a third-party Trustmark.

---

[182]Press Release, Office of the New York Attorney General, Settlement with Netscape Reached in "Spyware" Case (June 13, 2003) [hereinafter *N.Y. Netscape Case*], http://www.oag.state.ny.us/press/2003/jun/jun13b_03.html. *See also* New York Department of Law, 2002 Annual Report, http://www.oag.state.ny.us/annual_report02.pdf.

[183]*N.Y. Netscape Case*, *supra* note 182. New York Attorney General Spitzer alleged that the Smart Download function collected and saved user Uniform Resource Locator (URL) information with each download in violation of Netscape's promise not to save this type of information. *Id*. Upon settlement, Spitzer declared, "I am proud that this office has won yet another victory for consumer privacy . . . When companies misrepresent how data is collected or saved, we will hold these companies accountable." *Id*. Netscape was required to pay $100,000 to the state of New York, consent to periodic privacy audits, and delete all of the URL information it had collected and stored. *Id*.

[184]Nat'l Ass'n of Att'ys Gen., Consumer Protection Report (Jan. 2002). The New Jersey Attorney General claimed that Toys 'R' Us violated its privacy policy promise to protect customer PII by selling it to Coremetrics, an outside data collector. *Id*. As part of the settlement, Toys 'R' Us was required to post a clear and conspicuous link to its privacy policy as well as accept and destroy all of the information returned by Coremetrics. *Id*. at 23.

The Platform for Privacy Preferences (P3P) is a software technology created to monitor Web site privacy policies. The technology was developed in order to allow users of the Web to communicate their privacy preferences more effectively before the Web sites they visit can collect their PII. Using P3P, a user enters specific privacy preferences into a browser by answering several multiple-choice questions created by the P3P program. Upon requesting a particular Web site, the user's browser electronically translates these preferences into a machine-readable format and communicates such preferences to the Web site. When the browser encounters a Web site with privacy policies that do not meet the visitor's privacy standards, the browser notifies the visitor who may then chose whether to proceed and begin to surf the Web site.[185] Although it is yet to be determined how P3P will affect the future privacy environment, as of 2006 the technology appears to be underutilized due to a lack of significant customer and industry buy-in.[186]

---

[185]The P3P home page describes the technology in the following manner:

> The Platform for Privacy Preferences Project (P3P), developed by the World Wide Web Consortium, is emerging as an industry standard providing a simple, automated way for users to gain more control over the use of personal information on Web sites they visit. At its most basic level, P3P is a standardized set of multiple-choice questions, covering all the major aspects of a Web site's privacy policies. Taken together, they present a clear snapshot of how a site handles personal information about its users. P3P-enabled Web sites make this information available in a standard, machine-readable format. P3P enabled browsers can "read" this snapshot automatically and compare it to the consumer's own set of privacy preferences. P3P enhances user control by putting privacy policies where users can find them, in a form users can understand, and, most importantly, enables users to act on what they see.

Platform for Privacy Preferences Project, What is P3P, http://www.w3.org/P3P/ (last visited May 15, 2006). A major problem with the P3P technology from a privacy standpoint is that a user's clickstream history (i.e., Web sites and Web pages previously visited) may still be displayed to the Web site requested even before the P3P alert pops up. Therefore, if the visitor does not agree with the privacy policies of the particular Web site, he has still left his IP address, operating system, and browser model information for the Web site to collect.

[186]James A. Harvey & Karen M. Sanzaro, *P3P and IE6: Good Privacy Medicine or Mere Placebo*, 19 Comp. & Internet L. 4 (Apr. 2002) ("Despite the support P3P has received from Microsoft and other influential members of the W3C, it does not appear that companies are rushing to adopt P3P policies"). For now, at least, companies and practitioners in the area are taking a wait-and-see attitude and further analyzing the many issues raised by P3P prior to adopting P3P policies. *Id*. In fact, "there are many criticisms of P3P and its implementation in [Internet Explorer version 6] that are relevant to consider as part of the overall dialogue." *Id*.

A third-party enforcement program, on the other hand, consists of an independent entity structured to validate the privacy practices of individual companies. The key is that the monitoring institution be respected within both the business and consumer communities. The most recognized third-party enforcement programs today are the third-party seal—or Trustmark—companies.[187] These companies certify that company privacy policies meet certain minimum information-privacy standards like the FTC fair information practices of notice, choice, access, and security.[188] Trustmarks add a layer of trustworthiness to privacy policies because of this independent monitoring and serve the purpose of making the Web site visitor feel more comfortable providing PII.

IV. Privacy Policy Reform Propositions

A. Enacting a Federal Law Targeting Electronic Privacy Policies

This article demonstrates the discrepancy between the information privacy best practices of theory and the electronic privacy policies of today. This dysfunctional situation calls for national legislation directly targeted at developing more efficient, privacy-enhancing, privacy policies. To this end, Congress should enact a new information privacy law. This article proposes such a law, styled as the EPPAA, which is specifically directed at the standardization of fair information practice disclosures within electronic privacy policies.[189] Similar legislation in the form of the Consumer Privacy

---

[187]The two most prominent Trustmark companies are BBBOnline, Inc. and TRUSTe.

[188]For example, TRUSTe requires that companies utilizing its trustmark create a privacy policy detailing—at a minimum—company policy relating to:

1. What types of PII is collected and how it will be used;
2. The identity of the party collecting PII;
3. Whether PII is shared with third parties;
4. The use of any tracking technology;
5. Whether PII is supplemented with information from other sources;
6. Choice options available to consumers;
7. How consumers can access PII they have provided;
8. That there are security measures in place; and
9. Procedures for filing and addressing consumer complaints.

[189]The FTC could, instead, propose a similar rule mandating such policies and has the authority under § 57(a) of the FTC Act to prescribe interpretative rules and general statements of policy regarding unfair or deceptive acts or practices without congressional action. *See* 15 U.S.C. § 57(a) (2000). The FTC also has the power to "define with specificity"

Protection Act of 2002 (CPPA) worked its way around Congress over the past four years but was never passed.[190] CPPA would have required all commercial entities operating a Web site collecting PII to adhere to three of the FTC's four fair information practices—notice, choice, and security—and also offer consumers a choice to opt out of PII disclosure.[191] Another similar proposal from academia known as the Model Regime for Privacy Protection deals with fair information practices but was not specifically focused on improving the effectiveness of electronic privacy policies per se.[192]

---

acts or practices which are unfair or deceptive. *See id*. § 57(b). When the FTC undertakes to define these terms with specificity it must: (1) publish notice of the proposed rulemaking, (2) allow all interested persons to submit their views for the public record, (3) provide for an informal hearing, and (4) promulgate a final rule along with a statement of the rule's purpose and basis. *Id*. § 57(b)(1)(A)-(D). This article argues that this action is more appropriate for Congress to undertake because of the importance of the issue and the preemption of conflicting and more restrictive state laws required in order for this law to be effective.

[190]H.R. 4678, 107th Cong. (2002) [hereinafter 2002 CPPA].

[191]*Id*. This law is stricter than the EPPAA proposed in this article in that the 2002 CPPA would have required companies to allow visitors to opt out of PII sharing unrelated to the purpose of the transaction where it was collected while the EPPAA does not require any specific choice provisions such as an opt-out or opt-in provision. *Id*. § 103(a)(1) (as will be discussed below, the EPPAA does not require companies to adopt any fair information practices, but only to post a privacy policy discussing such practices). This opt-out choice would remain in effect for five years or until the visitor chooses otherwise but companies may offer benefits in exchange for consent to use PII. *Id*. § 103. The bill would not require companies to provide visitors with access to their PII or even discuss the fair information practice of access. As for security, the bill would require covered entities to create an organizationwide information security policy—including plans to respond to security alerts. *Id*. § 105. This law contained a restrictive preemption clause that stated: "This title preempts any statutory law, common law, rule, or regulation of a State, or a political subdivision of a State, to the extent such law, rule, or regulation relates to or affects the collection, use, sale, disclosure, or dissemination of personally identifiable information in commerce. No State, or political subdivision of a State, may take any action to enforce this title." *Id*. § 109. Even though it was not passed in 2002, the same law, styled the Consumer Privacy Protection Act of 2005, was proposed again in the 109th Congress. H.R. 1263, 109th Cong. (2005). This bill was referred to the House International Relations Committee and the House Energy and Commerce committee on March 10, 2005 and then to the Subcommittee on Commerce, Trade and Consumer Protection of the House Energy and Commerce Committee on March 22, 2005, where it stalled. *See* The Library of Congress, H.R. 1263, All Information (except text) (Thomas), http://thomas.loc.gov (last visited Mar. 4, 2006) (a search of the U.S. Library of Congress Web site for this bill provided a nice summary of information as to the status of this bill and its current position in the legislative process).

[192]*See, e.g.*, Daniel Solove & Chris Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357, 368–72 (2006).

The proposed EPPAA is more specific than either the CPPA and Model Regime for Privacy Protection in its requirements, and it is less constraind in its scope; both are factors that could influence its successful enactment. EPPAA treats PII as both a fundamental right as well as a property interest. It contains provisions requiring companies to examine policies covering PII collection, use, and dissemination; publish such policies; and then abide by them until the policy is abolished or modified. These requirements are designed to encourage companies to respect PII and understand that such information is an important aspect of an individual's sphere of privacy that must be respected once in the hands of a second party, an attribute more closely related to the fundamental right approach. On the other hand, this law allows the individual to make an informed decision as to whether to trade valuable PII online without governmental overreaching into such a decision, an attribute that is more along the lines of the property approach.

In its final form, this law would create a uniform national standard by requiring any e-commerce company utilizing a Web site collecting PII and engaging in interstate commerce to post a standardized, multilayered privacy policy.[193] This section will discuss the three most important aspects of the proposed EPPAA: (1) its standardized, multilayered notice requirement compelling disclosure of seven fair information practices; (2) its ceiling preemption of state laws directly targeting electronic privacy policies and its floor preemption of state laws indirectly implicating such policies; and (3) its workable enforcement provisions. Part B concludes this section with an annotated EPPAA-compliant privacy policy template analyzing the seven fair information practices requiring disclosure.

---

[193]Commentators charge that laws directed only at e-commerce fail to recognize the privacy issues related to offline transactions. While offline privacy issues are indeed important, this law is targeted at online collections of PII as the same privacy policy problems are not necessarily plaguing the offline community in the same way. For instance, cookie and Web beacon technology are crucial parts of online privacy protection and completely inapplicable to an offline transaction. These electronic PII-gathering technologies pose threats far more serious than the physical collection of PII in a brick-and-mortar retailer. This is not to minimize the threats to PII collected offline—only to state that the two areas are best dealt with differently when discussing privacy policies.

1. EPPAA's Standardized and Multilayered Privacy Policy

The future of electronic privacy polices lies in a multilayered notice format rather than one long and complex document.[194] In fact, during March 2004 twenty-three international privacy officials and experts convened a privacy policy seminar and produced a document declarin that contemporary privacy notices "do not serve a useful communications purpose" and called for an international move to a multilayered policy format.[195] This idea was previously endorsed by the 2003 International Data Protection Conference held in Sydney, Australia.[196] This multilayered format requires the creation of three situation-specific privacy policy documents, each written in plain English[197] and each designed specifically to increase the likelihood that visitors will read and understand the policy. In situations where a company collects PII in places where space is extremely limited—such as a mobile phone or an ATM screen—an abbreviated policy (the first layer) must appear and contain only a brief statement disclosing the name of the party collecting PII, the primary purpose of the

---

[194]This concept of a multilayered policy as an international standard is gaining acceptance among privacy experts worldwide. *See, e.g.*, BERLIN PRIVACY NOTICES MEMORANDUM (April 2004), http://www.hunton.com/files/tbl_s47Details/FileUpload265/681/Berlin_Workshop_Memorandum_4.04.pdf (in 2004 twenty-three privacy experts from consumer organizations and industrial sectors, data protection agencies, and government privacy offices met in Berlin for a privacy workshop and created the memorandum stating that "effective privacy notices should be delivered within a framework with the following core concepts: Multi-layered ... Comprehension and Plain Language and Compliance"). *Id*. at 1.

[195]*Id*. In the United States, the Hunton and Williams, LLP Center for Information Policy Leadership has taken a lead role in advocating for a multilayered privacy policy form. *See* CENTER FOR INFORMATION POLICY LEADERSHIP, TEN STEPS TO DEVELOP A MULTILAYERED PRIVACY NOTICE 1–9 (2006), *available at* http://www.hunton.com/files/tbl_s47Details/FileUpload265/1405/Ten_Steps_whitepaper.pdf (providing examples of effective multilayered privacy policies and a ten-step process businesses may use to create a multilayered policy).

[196]*Id*. at 1.

[197]The concept of a "plain English" disclosure took hold when the Securities and Exchange Commission adopted a rule requiring companies filing prospectuses to ensure that the cover page, summary, and risk factors sections were written in a manner that an average reader could understand. *See* Plain English Disclosure, Securities Act Release No. 7497, 63 Fed. Reg. 6370 (1998) (codified in scattered sections of 17 C.F.R. pts. 228, 229, 230, 239, 274 (2006)). A plain English disclosure is one that contains: "active voice; short sentences; definite, concrete, everyday words; tabular presentation or 'bullet' lists for complex material, whenever possible; no legal jargon or highly technical business terms; and no multiple negatives." *Id*. § III.A. The six plain English requirements are carried over into the EPPAA. The FTC is free to promulgate regulations further elaborating on the EPPAA's plain English provisions.

Figure 1: Sample EPPAA-Compliant Multilayered Electronic Privacy Policy: Layer One

collection, any visitor consent provisions, and the location where the individual may seek the more complete policy information.[198] Where more space is available, such as on a company Web site, a more detailed summary of the privacy policy (layer two) must be posted. In the present context, the second layer consists of a standardized template with bulleted information regarding the seven fair information practices required by EPPAA.[199] The complete privacy policy (layer three) must contain the most detailed description of the seven required fair information practices and must be hyperlinked from the company's home page and from any Web page containing the summary policy or second layer.[200] This multilayered privacy policy system can be very effective in meeting the stated goals of privacy policy theory and can be implemented without great cost or effort via electronic posting.

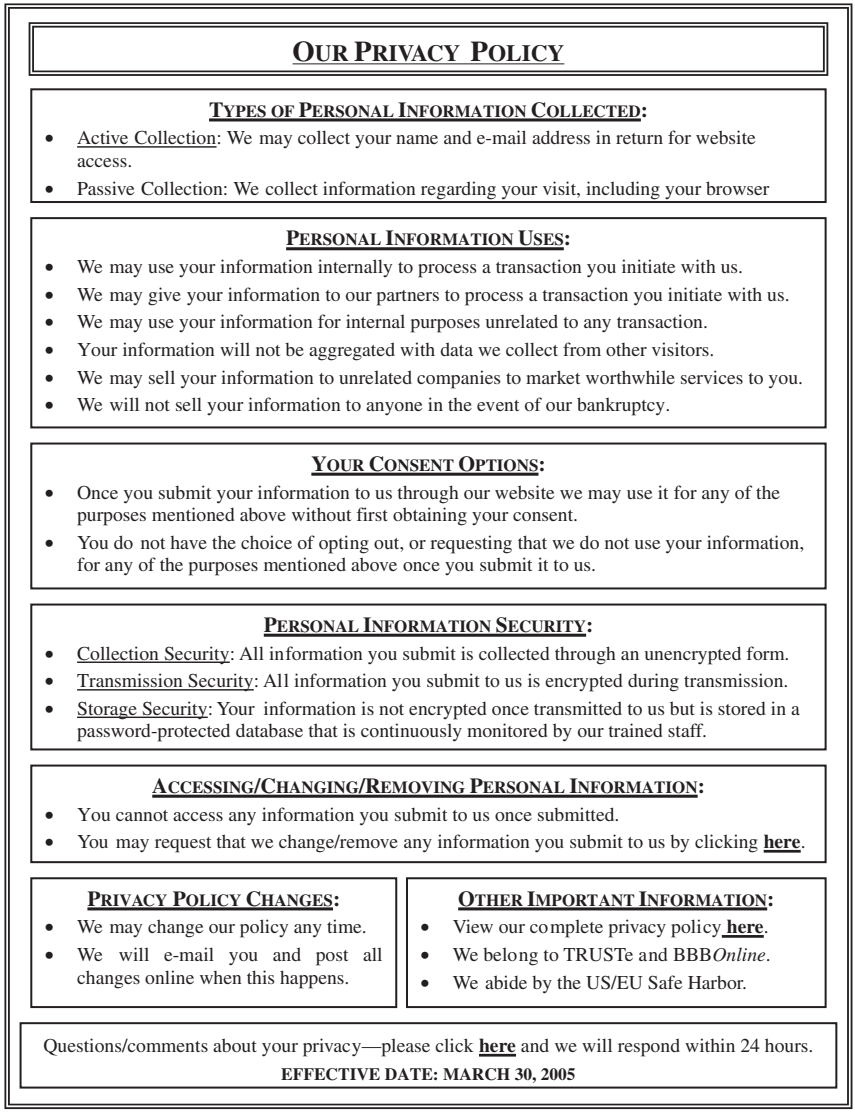
EPPAA would not require any specific content within each layer such as the GLBA requirement of opt-out consent before dissemination to

---

[198]For samples of this first layer of multilayered privacy policies, see, for example, The Ctr. for Info. Pol'y Leadership, White Paper: Multi-layered Notices Explained, *available at* http://www.hunton.com/files/tbl_s47Details/FileUpload265/1303/CIPL-APEC_Notices_White_Paper.pdf (last visited Oct. 1, 2006). This first layer would not be required under the EPPAA for companies not conducting operations utilizing small-screen services. These companies, however, would still be required to post the second and third layers. *See* Figure 1 for an example of an EPPAA-compliant first layer in a multilayered privacy policy.

[199]The seven required headings are detailed below. *See* discussion *infra* Part IV.B. This condensed privacy notice must be hyperlinked from the company's home page and from every place where the company collects PII. It must also contain a clear and conspicuous hyperlink leading to the information contained in Layer Three. *See* Figure 2 *infra* for an example of an EPPAA-complaint second layer in a multilayered privacy policy.

[200]All three layers must be written in plain English.



OUR PRIVACY POLICY

TYPES OF PERSONAL INFORMATION COLLECTED:

- Active Collection: We may collect your name and e-mail address in return for website access.
- Passive Collection: We collect information regarding your visit, including your browser

PERSONAL INFORMATION USES:

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

YOUR CONSENT OPTIONS:

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

PERSONAL INFORMATION SECURITY:

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

ACCESSING/CHANGING/REMOVING PERSONAL INFORMATION:

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

PRIVACY POLICY CHANGES:

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

OTHER IMPORTANT INFORMATION:

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

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

EFFECTIVE DATE: MARCH 30, 2005

Figure 2: Sample EPPAA-Compliant Multilayered Electronic Privacy Policy: Layer Two

nonaffiliated third parties. Instead, the law only requires that the seven fair information practices are discussed and that such disclosure accurately represents actual company policy. For instance, if a company chooses to sell PII to third-party marketers requesting such information without

obtaining any consent, the company complies with EPPAA as long as this practice is accurately disclosed in the policy itself. A company violates an EPPAA provision only if it fails to address each of the seven required fair information practices or fails to list relevant contact information and/or the policy's effective date.[201]

As for standardization, EPPAA would take a similar approach to that taken by the Food and Drug Administration in its standardized food labeling requirements.[202] Every privacy policy complying with EPPAA must appear in a standardized format containing the seven fair information practices from the model template below. The goal of this legislation is for Web site visitors to begin to become accustomed to seeing and understanding these standardized policies and, over time, understanding privacy implications. The true goal, from a privacy perspective, is for Web site visitors to be equipped to make better informed decisions about their information privacy. This federal law would eliminate the biggest problems with the lack of effectiveness in contemporary privacy policies by mandating that compliant policies be written in plain English. Another benefit stems from the idea that companies would not be able to dodge information privacy protection by refusing to post a policy without risking legal actions under the EPPAA enforcement provisions.[203] These requirements are sufficient to force companies to analyze their practices and formulate privacy policies governing their processing of PII without stifling policy direction by requiring specific content.[204]

The end result of this provision should be a standardized, easy to understand, and conspicuously posted multilayered privacy policy crafted to make visitors aware of the company's privacy practices before any PII changes hands. Creating this awareness places the ball in the visitors' court to compare their privacy preferences to the stated privacy practices and

---

[201] *See* discussion *infra* Part IV.B.

[202] *See, e.g.,* The Dietary Supplement Health and Education Act of 1994, Pub. L. No. 103–417, 108 Stat. 4325(1994) (codified in scattered sections of 21 U.S.C.) (requiring, among other things, nutrition and nutrition labeling); Nutrition Labeling and Education Act of 1990, Pub. L. No. 101-535, 104 Stat. 2353 (1990) (codified in part at 21 U.S.C. § 343 (2000)).

[203] Companies in protected industries would not be required to comply with the EPPAA and would operate legally as long as they meet the requirements of all regulations currently governing their operations.

[204] This balance will aid in the passage of the EPPAA because neither side—the privacy advocates and the e-commerce business interests—are pressed to compromise too much.

then take the responsibility to make an informed decision. Under EPPAA, consumers are better able to discover and understand the privacy implications of submitting PII and will begin to train themselves to make better decisions with their information.

2. EPPAA as a Ceiling and a Floor for Preemption Purposes

As for preemption,[205] EPPAA must contain an express preemption clause stating that the legislation is intended to serve as a ceiling as well as a floor.[206] A federal law operating as a ceiling in the context of this article would allow EPPAA to preempt, or invalidate, any existing state law that "directly targets" the posting or content of electronic privacy

---

[205]The idea of preemption in American law originates from the Supremacy Clause of the U.S. Constitution. U.S. CONST. art. VI, § 2, cl. 2. The Supremacy Clause provides that the "Constitution, and the laws of the United States . . . shall be the supreme law of the land." This clause indicates that the federal government, "in exercising any of the powers enumerated in the Constitution, must prevail over any conflicting or inconsistent state exercise of power." *Legal Encyclopedia Information About The Supremacy Clause*, WEST'S ENCYCLOPEDIA OF AMERICAN LAW, *available at* http://www.answers.com/topic/supremacy-clause (last visited Oct. 1, 2006). *See also* McCulloch v. Maryland, 17 U.S. (4 Wheat.) 316, 406 (1819) ("The government of the United States . . . though limited in its powers is supreme; and its laws, when made in pursuance of the Constitution, form the supreme law of the land, 'any thing in the Constitution or laws of any State to the contrary notwithstanding.' "). Preemption of state and local laws in the business arena generally occurs when Congress enacts legislation that directly conflicts with state legislation (express preemption) or when the federal government has chosen to occupy the field forming the basis of the state legislation (implied preemption). At this point the federal law will preempt the state law rendering the state law invalid. Congress has the authority to regulate businesses conducting interstate commerce under the Commerce Clause of the U.S. Constitution. U.S. CONST. art. I, § 8. *See also* ERWIN CHEMERINSKY, CONSTITUTIONAL LAW: PRINCIPLES AND POLICIES § 5.2, 376–401 (Aspen Publishers 2nd ed. 2002) (discussing federal preemption); *Legal Encyclopedia Information About Preemption*, WEST'S ENCYCLOPEDIA OF AMERICAN LAW, http://www.answers.com/topic/preemption (last visited Oct. 1, 2006).

[206]This preemption clause should state something to the effect of "The EPPAA supersedes any statute, regulation, rule or common law that directly targets the posting, standardization and content headings of any electronic privacy policy. This Act does not supersede any statute, regulation, rule or common law that indirectly implicates electronic privacy policies nor does it preempt any conflicting federal law currently in existence." This preemption clause must be clear and specific as to its scope (enacted specifically to regulate the posting, standardization and content headings of electronic privacy policies) and effect (enacted to serve as a ceiling regulation for state/local laws directly targeting electronic privacy policies, as a floor for other state/local laws indirectly implicating such policies and is not effective regarding conflicting federal laws such as the COPPA, GLBA, and HIPAA). *See* discussion *infra* Part IV.A.2.

policies.[207] For instance, EPPAA would not allow any state to enact a more restrictive law such as a state statute allowing a paper policy to suffice, requiring different fair information practices to be covered, or mandating only a single-layered privacy policy format.

This preemption must set the maximum, as opposed to the minimum, standard for laws directly targeting electronic privacy policies because a federal law setting a minimum standard (or a floor) would allow individual states to set a de facto national standard by passing stricter legislation targeted at companies doing business with that state's residents.[208] For example, because e-commerce companies nationwide target California residents, California OPPA, in essence, is able to set a de facto national standard by requiring companies to post electronic privacy policies. If other states were to enact similar legislation with slightly different requirements, businesses across the country would be forced to comply with many differing, potentially conflicting, state laws. This situation tends to: (1) increase the cost of doing business, by raising compliance expenses, a cost generally passed on to consumers in the form of higher prices or (2) allow the state with the strictest regulations to create the national standard if companies choose to comply only with the strictest

---

[207]This is an ideal time to enact this legislation as only California has passed any law directly targeting electronic privacy policies, the California OPPA. *See* discussion *supra* Part III. Although the California OPPA will be preempted by the EPPAA, because both laws are similar and because other state jurisdictions have not legislatively encouraged the use of privacy policies as PII protectors, the EPPAA should prove beneficial.

[208]Setting a maximum standard has its detractions. For example, if states are not allowed to enact more restrictive laws, then states are less free to experiment with different solutions attempting to find the most effective/cost-efficient measures to protect PII. This is a valid objection but must be weighted against the costs to businesses and consumers when such experimentation leads to wildly varying standards in an environment where a privacy policy is located in a set medium in all jurisdictions where it is accessed. For instance, if a Colorado law required companies to create detailed policies covering ten fair information practices while Utah required companies to have short and concise policies not exceeding one page, then a company doing business in both jurisdictions would need to create and post a separate privacy policy for each jurisdiction and implement systems to treat PII from residents of each state differently. This might make some sense with only two states involved but becomes messier if twenty or thirty different state laws enter the equation. With a federal law providing a ceiling, however, a company needs to create only one policy to comply. The key is to ensure that the federal law covers all the bases and includes the fair information practices that are important at this point in time. Also important is the fact that states remain free, under the EPPAA, to enact other information privacy legislation that indirectly implicates electronic privacy policies. This will allow enough experimentation to ease concern about the EPPAA's preemption ceiling.

law.[209] The American political system is better served by Congress creating a true national standard.[210]

While EPPAA would serve as a ceiling preempting all state or local laws directly targeting electronic privacy policies, it would serve as a regulatory floor and would not preempt state or local laws "indirectly implicating" such policies. This means that a state could require, without being preempted by EPPAA, e-commerce companies targeting state residents to create and implement data-security programs to protect PII. This state legislation could also require a detailed description of the practice to be disclosed in the privacy policies of companies covered by the state law. This legislation is not preempted by EPPAA because it is not a regulation "directly targeting" electronic privacy policies. Rather, it is a state regulation directly targeting data-security practices and indirectly implicating privacy policies.[211]

Finally, it is important to remember that there are many federal laws in the privacy area that preempt, in some way or another, state laws.[212]

---

[209]For example, if the California OPPA proves to be the strictest of all of the anticipated laws requiring electronic privacy policies, businesses may choose to comply only with the California OPPA because compliance with its terms will mean that the company is complying with the other, less strict, state laws. Again, this allows one state to set a national regulatory standard instead of the national Congress.

[210]To this point California and a select group of other states should be applauded for the excellent job they have done in protecting the information privacy of their residents in lieu of congressional action. As stated above, the EPPAA is virtually the same as the California OPPA and, therefore, there will be little negative effect in California by switching to a uniform national standard.

[211]This partial ceiling/partial floor preemption provision proves to create a somewhat complicated situation because states are free to create a myriad of regulations indirectly targeting privacy policies by requiring privacy-enhancing programs—such as a data security program—to be disclosed in electronic policies. These problems are better than the problems that would be created with a complete ceiling barring any state law indirectly implicating electronic privacy policies. Such a complete ceiling could potentially wipe out data security and opt-out consent laws currently enacted in many states. Because the EPPAA takes the middle ground and acts as a ceiling for any regulation directly targeting privacy policies but acts as a floor in other instances, it should be able to garner the support required for its enactment without creating more problems then it causes.

[212]Examples include the GLBA, which only preempts state laws that are inconsistent with its privacy protections. 15 U.S.C. § 6807(a) (2000) (serving as a floor and allowing more stringent state regulations to be enforced as long as they are consistent with its privacy provisions); HIPAA, 45 C.F.R. § 160.203(b) (2005) (even contrary state laws, if they are more restrictive, are enforceable without violating the HIPAA preemption clause); COPPA 15 U.S.C. § 6502(d) (stating that "[n]o State or local government may impose any liability for commercial activities

Although each specific preemption situation brings with it different outcomes,[213] a uniform standard requiring the companies to think about their privacy policies and then post such policies for all to see is a step forward in a country where self-regulation has not proven to be a completely effective privacy-enhancing system. While EPPAA would not modify, limit, or supersede any other federal information-privacy law currently in existence, it can serve as a privacy-enhancing tool for consumers in all of the industry sectors unregulated by the current sectoral privacy regime.

3. The Enforcement Provisions of EPPAA

Under the proposed statute's enforcement provisions, individuals are allowed to report any company violating the terms of EPPAA but no private right of action is authorized. Complaints can be made in writing or electronically to the FTC or to any state attorney general in jurisdictions within which the company operates.[214] Much like California OPPA, EPPAA would require these enforcement organizations to notify the offender and grant such company thirty days to bring its policy into compliance. If compliance is not obtained after thirty days, then any authorized governmental entity may bring an enforcement action under its unfair and/or

---

or actions by operators in interstate or foreign commerce in connection with an activity or action described in this title that is inconsistent with the treatment of those activities or actions under this section."); and the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub. L. No. 108-107, 117 Stat. 2699 (2003), codified at 15 U.S.C. § 7701 et seq. (Supp. 2004) and 18 U.S.C. § 1037 (Supp. 2004) [hereinafter CAN-SPAM Act] (the CAN-SPAM Act attempts to reduce the amount of spam sent via e-mail by prohibiting forged e-mail headers and deceptive subject lines, requiring sender identification and prohibiting methods whereby large amounts of spam are sent without identifying the sender). *Id*. The CAN-SPAM Act's preemption provisions, which are stronger than those of COPPA, GLBA, and HIPAA, state that the CAN-SPAM Act supersedes any state or local law/regulation/rule that "expressly regulates the use of electronic mail to send commercial messages, except to the extent that any such statute, regulation, or rule prohibits falsity or deception in any portion of a commercial electronic mail message or information attached thereto." *Id*. at § 8(b)(1). This is a partial preemption clause—similar to that in the new EPPAA—as certain state laws directly targeting spam are not invalidated.

[213]*See, e.g*., Roger Allan Ford, Comment, *Preemption of State Spam Laws by the Federal CAN-SPAM Act*, 72 U. Chi. L. Rev. 355, 381 (2005) (arguing that the CAN-SPAM Act's preemption clause has not worked as planned and that it should be interpreted to allow the enforcement of compatible state laws).

[214]As it did with COPPA, GLBA, and HIPAA, the FTC would be authorized to promulgate rules in order to assist with EPPAA compliance. *See* 15 U.S.C. § 57a and discussion *supra* Part III.

deceptive practices statutory authority. It is noteworthy that EPPAA allows for state enforcement in all fifty states but does not allow for a myriad of fifty different state laws directly targeting electronic privacy policies.

The law would classify all nonremedied violations as unfair or deceptive acts or practices prohibited by the FTC Act or by state consumer protection laws.[215] The FTC, or state attorney general, may choose to launch an investigation, stemming from a consumer complaint or on its own volition.[216] For FTC enforcement, as long as the Commission has "reason to believe" that EPPAA was violated, it may begin an administrative adjudication.[217] Upon the filing of the FTC complaint, a company may choose a settlement option and enter into a consent decree; on the other hand, a company may contest the charges and enter into an administrative trial where an administrative law judge will produce an initial decision by issuing a cease-and-desist order or dismissing the complaint.[218] Violations of a final order may result in civil penalties of up to $11,000 per violation as well as additional "consumer redress" penalties for conduct that a reasonable person would have known was "dishonest or fraudulent."[219] States

---

[215]Congress would have the option of increasing the penalties for repeat violators regardless of the number of people injured by the violation and regardless of the length of the violation. These increased penalties are justified because all offending companies have a get-out-of-jail-free card as they are awarded a chance to remedy any EPPAA violation within thirty days of notification of such violation.

[216]*See* FTC, Office of the General Counsel, A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority (2002), http://www.ftc.gov/ogc/brfovrvw.htm#N_1_.

[217]*Id.*

[218]Companies charged in the administrative trial (respondents) may appeal this initial decision to the appropriate federal Court of Appeals. *Id.* If the respondent loses this appeal, the Commission will enter an enforcement order enforcing the initial decision of the Administrative Law Judge but the respondent may still appeal to the U.S. Supreme Court. *Id.* This enforcement order will become binding on the respondent sixty days after it is issued and a respondent is subject to an $11,000 civil penalty for each violation of this order. *Id.* Additionally, the Commission may seek "consumer redress from the respondent in district court for consumer [injury] caused by the conduct that was at issue in the administrative proceeding. In such a suit . . . the Commission must demonstrate that the conduct was such as 'a reasonable man would have known under the circumstances was dishonest or fraudulent.'" *See* 15 U.S.C. § 57b.

[219]*Id.* Recall that, in the ChoicePoint data breach case, the FTC obtained $5,000,000 in consumer redress penalties from the company. *See supra* note 175 (discussing the ChoicePoint case).

would be allowed to follow their specific enforcement practices in actions brought by state governmental entities.

The next section provides a model privacy policy template which would be attached to EPPAA and intended to be used for compliance purposes. The template shows the required fair information practice section for each privacy policy but allows companies to set their own policies internally as long as such policy is disclosed accurately.

B. EPPAA's Model Electronic Privacy Policy Template

There is little doubt that electronic privacy regulation—whether similar to the proposed EPPAA or more comprehensive in nature—will soon require much more of a company's e-commerce operations.[220] This stricter regulatory regime will surely include a privacy policy component that seeks to minimize the problems encountered in contemporary policies. The following template provides a standardized set of fair information practices all companies must utilize when crafting and posting their privacy policies under the proposed EPPAA.

The mechanics of an effective privacy policy are the secret to its success and EPPAA requires two primary mechanical components: (1) all electronic policies must be drafted utilizing plain English and (2) all electronic policies must be posted in a clear and conspicuous manner.

First, and as detailed above, a privacy policy written in plain English is one that avoids the tech-speak and legalese plaguing many Internet-related legal documents.[221] Plain English principles demand, among other things, that sentences be short, deal only with one particular issue, utilize only the active voice and everyday words, and avoid legal jargon.[222] A typical Internet user—that is, someone with a minimal high school education—should be able to understand each section clearly with a one-time thorough reading of the

---

[220] *See, e.g.*, Declan McCullagh, *Congress Edges Toward New Privacy Rules*, CNET NEWS.COM, Mar. 10, 2005, http://news.com.com/Congress+edges+toward+new+privacy+rules/2100-1028_3-5609324.html (discussing the fact that recent information security breaches have created new energy in Congress to craft legislation—potentially applicable to all e-commerce companies—targeted at tightening information security practices).

[221] *See supra* note 197 (analyzing plain English requirements and their derivation from the securities regulation arena).

[222] *Id.*

privacy policy.[223] Second, a privacy policy posted in a clear and conspicuous manner must be indicated by hyperlink entitled "Your Privacy" that is located on the Web site home page and on all other Web pages where the company collects PII. This hyperlink must be in a text style and font size different from other hyperlinks on the same page so that it is set apart in the minds of the Web site visitors. Combined with a plain English requirement, these changes will allow readers to focus on the seven fair information practices detailed below rather than deciphering the complicated language or searching for the appropriate link among other arcane-sounding hyperlink titles.

Once the mechanics described above are appropriately handled, a minimally acceptable privacy policy under EPPAA must contain the following seven fair information practice section headings: (1) Types of Personal Information Collected, (2) Personal Information Uses, (3) Your Consent Options, (4) Personal Information Security, (5) Accessing/Changing/Removing Personal Information, (6) Privacy Policy Changes, and (7) Other Important Information. Every privacy policy must also conclude with a statement detailing the appropriate contact information for the person or department assigned to support information privacy issues, declaring the effective date of the policy and detailing the date and the terms of the most current policy update if applicable. Each of the following sections discusses one of the seven required electronic privacy policy headings, analyzes the categories of information required by EPPAA, and also details why each required disclosure is important.

1. Types of Personal Information Collected[224]

An electronic privacy policy must detail the types of PII the company collects via its Web site and the reasons for such

---

[223]It is important to note that Web site visitors bear some of the burden of reviewing the privacy polices of the places they visit on the Internet and, therefore, the company does not need to create a policy that is oversimplistic. The goal is a policy comprehendible by someone with a ninth- or tenth-grade education.

[224]Although a detailed analysis of a privacy policy complaint with the COPPA is beyond the scope of this section, it is important to realize that, if a company collects personal information from children, the privacy policy should also include a section as to how the company will collect, store, and deal with this information as well. If the Web site is not designed for children under a certain age, this fact should also be disclosed. This article contains a serious discussion of the COPPA privacy policy requirements. *See* discussion *supra* Part III. The Moster.com Privacy Statement disclaims this idea as follows: "The Monster Sites are not intended for children under 13 years of age. We do not knowingly collect personal information from children under 13." Monster.com, *Privacy Statement*, http://about.monster.com/privacy/ (last visited Oct. 1, 2005). Also important is the access and consent provisions allocated to the parents of minors using the Web site.

collection.[225] Information collection may occur actively through visitor submission or passively through cookies, Web beacons, and other types of spyware. The policy should utilize these two categorical descriptions in detailing the types of information collected.[226] If a company elects to collect additional types of information or changes its reasons for collection in the future, it must amend its privacy policy and notify visitors of the update.[227]

Making visitors aware of the types of information collected is important for three key reasons. First, Web site visitors are often unaware that information is being collected from them.[228] Many visitors do not

---

[225]It is important to remember that companies are neither required to collect any certain type of information nor limited in the types of information they may collect. Companies are merely required to describe the types of information collected from visitors. The typical types of information collected may include: name, address, phone number, e-mail address, drivers license number, user ID and password, purchases, financial history, PC configuration, clickstream and navigation data, visitor use of interactive features, demographic information, economic information, postings, political affiliations, and health information. It is important for the privacy policy to spell out every category of PII collected from visitors rather than summarize the collection with a phrase such as "personal information of different types will be collected from you."

[226]Some sites miscategorize these categories into information that is PII and information that is anonymous. *See* Law.com, *Your Privacy,* http://www.law.com/service/privacy_policy.shtml (last visited Oct. 1, 2006). This categorization is misleading, however, because passive information collection occurring through cookies, Web beacons, and spyware potentially identifies a visitor as IP address and domain information can be collected from the visitor. Even a statement that a company does not attempt to link IP addresses to individuals and, therefore, the IP address information is anonymous can be misleading because the information can easily be traced back to a specified computer by a hacker or a rogue employee. Therefore, the best practice is for a company to categorize the collection process as active and identifying rather than passive and anonymous.

[227]A privacy policy stating that a company "may collect" certain types of PII in the future is misleading as visitors will not process the true privacy practices of the company upon reading the policy and any subsequent change in policy would occur without notice. It is also important that the company state how it will handle PII obtained prior to the policy modification. The best practice is to treat this information as described on the policy governing the Web site when the visitor submitted the information. This may be impracticable and cost-prohibitive depending upon the number of policy modifications and companies will have to choose which policy the old information will fall under and disclose this practice in every modification of its policy.

[228]This is primarily done through cookies and Web beacons. A cookie is a file that a Web site sends to a visitor's browser, records information about the visit, and then stores the information on the visitor's computer. The next time the Web site is visited, the cookie will recall certain information so that it does not have to be reentered into the Web site. A temporary cookie will be deleted after a browser is closed and a permanent cookie will remain on the visitor's computer until deleted or disabled. Cookies only contain the information

understand that information they submit via an online form is kept in a database and may be mined for later and potentially unrelated uses. Attempting to inform all visitors of this information collection and storage/retrieval ability constitutes a good faith effort to level the playing field to a point before the information collection occurs.[229] Second, if a Web site chooses to collect a great deal of information, including information unrelated to the transaction at hand, visitors may choose an alternative Web site requiring less-burdensome PII disclosure. Because visitors will note that information unrelated to the transaction is being collected they will be able to ascertain that pieces of information are being used for purposes unrelated to their visit to the Web site. Armed with this knowledge visitors may choose to leave the site and take their business elsewhere. Therefore, a privacy policy section describing all of the information collected will force companies to choose more carefully which types of PII are truly required for each transaction and to think about whether collecting information for unrelated purposes is truly an effective aspect of the business strategy. Third, if visitors are informed of the information collected by the Web site, they are less likely to fall prey to a phishing attack requiring information not listed in the privacy policy.[230]

---

provided by the visitor and cannot locate and pull information off of the user's hard drive and send it back to the Web site. Temporary cookies are sent when a user fills out an online application or when a visitor is directed to a certain site from another site. Permanent cookies are often used when a visitor requests information or documentation from a Web site or when a Web site engages in a visitor-tracking program. Visitors may still use the Web sites without accepting the cookies although this process will make navigating the Web site a bit more tedious. The CRG Study found that the vast majority of companies surveyed used cookies but that only twenty-five percent of such companies fully explained in their privacy policies as to why these cookies were used. 2006 CRG Study, *supra* note 57. Web beacons are small pixels that exist on Web pages and collect certain types of PII.

[229]An interesting dilemma occurs, however, when considering the use of passive information-gathering tools as such tools have the ability to collect information as soon as a browser is directed to a Web site. Companies should strive to place these tools at a Web page subsequent to the home page to allow users a chance to read the privacy policy before being subjected to such passive information gathering.

[230]A phishing attack occurs when a Web site customer is e-mailed and asked to provide PII to update an account or for other purposes. This e-mail is sent from a party unrelated to the company allegedly requesting the information and is intended to steal this PII and use it to commit different forms of identity or other theft. If a Web site customer knows that a Web site does not collect Social Security Number information, then any e-mail purporting to be from such company and requesting a Social Security Number should raise a red flag.

It is also important for a company to detail the reasons for collecting the PII identified by its privacy policy. Traditional reasons for information collection are to: (1) complete a request,[231] (2) administer and improve the Web site,[232] (3) customize content and create a digital identification, (4) conduct telemarketing, (5) create instant offers and conduct target marketing campaigns, (6) create a history of visits and interests, (7) assist in research and development, (8) conduct internal investigations, and (9) assist in law enforcement activities. Visitors should be told whether or not their PII will be aggregated with the PII of other visitors and, if so, how this aggregation of data will be used.

2. Personal Information Uses

As important as the types of personal information collected is the manner in which the company uses such information. There are three business-related uses for PII that, if applicable, should be described in this section of the privacy policy: (1) an interaction use, (2) an internally disconnected use, and (3) an externally disconnected use.

First, a company may use the information for internal purposes related to the reason the visitor interacted with the Web site in the first place (an interaction use). Visitors interact with a company's Web site in order to obtain goods or services and are generally required to submit certain PII to consummate the transaction. Companies must be allowed to use the information voluntarily transmitted by visitors through this interaction in a manner reasonably necessary to facilitate the transaction.[233] Second, a company may use the information for internal purposes disconnected to the reason the visitor interacted with the Web site (an internally disconnected use). As companies are becoming more adept at understanding the benefits of e-commerce and the profit potential inherent in stores of PII, Web sites are beginning to utilize collected PII by

---

[231]This may include the processing of payment information.

[232]This includes account renewal and support services (such as product and service updates).

[233]Information may be shared with nonaffiliated third parties and still fall within this category if the third party's services are utilized to perform a business function related to the transaction at hand. A business function may include the: (1) mailing of statements, (2) updating of subscriber information lists, and/or (3) providing customer support and service. *See* Law.com, P*rivacy Policy: With Whom Does ALM Share the Information it Gathers and/or Tracks*, http://www.law.com/service/privacy_policy.shtml (last visited Oct. 1, 2006).

sending this data to their affiliates for marketing-related purposes. A recent study of the high-technology and computer industries shows that most companies studied share information among affiliates for marketing purposes.[234] There are also a few non-marketing-related disconnected uses of PII collected voluntarily and involuntarily from visitors and utilized to create bulletin boards and chat rooms.[235] Visitors may not be aware of the precise definition of a company affiliate and, therefore, the policy should properly identify the nature of all affiliated parties and define their affiliation in this section. Finally, a company may choose to disseminate the information outside of its affiliate structure and into the hands of third parties operating in cyberspace or offline (an externally disconnected use).

In this section of the privacy policy a company need not define the exact manner in which the PII will be used but should categorize—using plain English terminology—each information use as an (1) interaction use, (2) internally disconnected use, and/or (3) externally disconnected use.[236] After choosing which categories apply, the policy should then provide a comprehensive list as to the types of entities within each category to which the information will be provided and how each party is allowed to use the information.[237]

In this section, a privacy policy should also detail the potential uses of information upon the sale, merger, or bankruptcy of the company. Recall that this became a major issue when Toysmart declared bankruptcy and intended to sell its customer list as a stand-alone asset in violation of its privacy policy promise never to sell customer PII to third parties.[238]

---

[234]*See* 2006 CRG Study, *supra* note 57.

[235]Another interesting phenomenon occurs when visitors choose to post personal information on a public forum, chat room, or bulletin board on a Web site. At this point, other Web site users may view this information. Privacy policies should disclose that posting of this information could lead to improper or unsolicited uses of this information. The policy should also disclaim responsibility for these various uses of personal information and also inform visitors that each visitor is responsible for guarding personal information on public parts of the Web site.

[236]See Figure 2 *infra* to view a plain English use of these categories.

[237]It is not necessary to provide a detailed list of the specific parties to whom PII is being disclosed under each category. For example, under the externally disconnected category, a company would comply by stating that it disseminates information to nonaffiliated third parties such as direct marketing companies and data aggregation companies.

[238]*See* discussion *supra* Part III.

3. Your Consent Options

Once the types of personal information collected are explained, the reasons for such collection are identified, and the visitor is apprised of any uses of PII, the policy should discuss the appropriate visitor consent provisions. The idea of visitor consent deals with the method of gaining approval to use PII for each of the three different information uses described above and forms one of the most contentious areas of debate in the information privacy arena. There are two primary forms of consent companies may choose: (1) opt in and (2) opt out. The staunchest privacy advocates consistently seek an opt-in system whereby companies must contact providers of PII to gain their express consent prior to each internally disconnected and externally disconnected use of their PII. The majority of companies, on the other hand, prefer an opt-out regime whereby the provider of PII must expressly decline the use of personal information. Without a valid opt out, companies may use any PII obtained in compliance with the privacy policy terms and for any of the three core information uses.

In general, electronic opt-in provisions come in two forms—the check-the-box provision and the e-mail confirmation provision. Under the check-the-box provision a visitor merely clicks on a Web form box authorizing the company to use any PII collected in accordance with the terms of the privacy policy. An e-mail confirmation provision, on the other hand, requires a visitor to affirmatively click on a link in an e-mail sent to them by the Web site to expressly opt in to use of PII. Some Web sites require both provisions as part of their opt-in policy. This option is the least popular of the two because of the idea that people are more likely to stick with the default situation when visiting a Web site requesting their personal information. In fact, the 2006 Customer Respect Survey found that only thirty-seven percent of the companies surveyed utilized an opt-in regime in which visitors were required to consent before being e-mailed marketing materials.[239] The other sixty-three percent of companies surveyed utilized an opt-out regime and e-mailed marketing materials to visitors unless the

---

[239]2006 CRG Study, *supra* note 57. This thirty-seven percent is down from forty-five percent of companies requiring opt-in consent during the second quarter of 2005 as reported by the previous version of the same CRG study. *Id*. at http://www.customerrespect.com/default.asp?hdnFilename=research_ind_hightech.htm (last visited Oct. 1, 2006).

company received an opt-out request or failed to provide any option whatsoever to opt out or opt in.[240]

Companies utilizing the opt-out option should inform visitors through their privacy policies as to how the visitor can opt out of various information uses. The typical form of opt-out alternatives ranges from Web form boxes visitors may check to the mailing of written requests. Under this system, until a visitor affirmatively opts out companies are implicitly authorized by such customer to use PII for any information use specified in the privacy policy.[241]

This model privacy policy advocates for, but does not require, an opt-out regime for all interaction and internally disconnected uses and an opt-in provision for all externally disconnected uses.[242] Requiring companies to gain consent for every informational use would be prohibitively expensive, create unnecessary contact between the company and its customers, and decrease the availability of worthwhile business services.[243] Logistically, EPPAA-compliant privacy polices must contain information regarding visitor consent and this information must be clearly labeled as such and located in a prominent place in the policy itself. Regardless of the option chosen by a company, if it offers any form of visitor choice at all, the actual choice must not be unreasonably burdensome.[244] Once a customer

---

[240]*Id.*

[241]Interestingly, if a company does not have a privacy policy—and is not required to have one—an opt-out regime allows companies to utilize PII in a variety of ways regardless of whether a visitor opts out. Cases like this often end in lawsuits where the company argues that the visitor consented to the use of the PII in question by further using the Web site and the visitor arguing that no consent was granted.

[242]Again, companies are free to disregard the form of consent advocated by this model template as long as the company's consent policy is accurately described. Entities in regulated industries are required to follow certain consent procedures. *See* discussion *supra* Part III.

[243]*See, e.g.*, Robert W. Hahn, *An Assessment of the Costs of Proposed Online Privacy Legislation* 13–14 (May 7, 2001), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=292649 (last visited Oct. 1, 2006) (arguing that a mandatory opt-in regime will harm consumers in general if Web sites currently offering free services and earning revenue by marketing PII are forced to charge for their services because they cannot muster the resources to obtain opt-in consent for continued dissemination).

[244]The best practice for an electronic opt-in or opt-out policy is to allow visitors to click on a link to choose privacy preferences. These links should be contained in the privacy policy itself under a section entitled "Your Consent." A hyperlink option is the least intrusive and will likely be the most effective because it allows visitors to one-stop shop—that is, to read the privacy policy and then exercise their option in the same sitting.

has made a removal request, the company must ensure that steps are taken to promptly honor that request and remove the subscriber's PII from situations where it may be disseminated beyond the scope of the consent. Although no privacy policy should affirmatively state that the opt-out request will be honored one hundred percent of the time, each should lay out the practices implemented by the company to honor the privacy request.

4. Personal Information Security

Before the ubiquitous usage of computers for information storage, personal information was normally stolen through an intrusion at the physical site where the information was kept (generally inside a company building). Today information may be stolen not only through a geographically specific physical act but also from afar through computer hacking and other sinister electronic methods. To compensate for these new threats, contemporary privacy policies often disclose that the company cannot guarantee that personal information will never be used for improper purposes. These types of statements are legalese for "we are disclaiming any responsibility for any possible misuse of your personal information—so tough luck! And, by the way, as long as you continue to use our Web site you are implicitly accepting our disclaimer."[245]

This privacy policy section must describe how personal information is protected from accidental loss, unauthorized access,[246] use alteration, or disclosure at three stages: (1) during the collection process, (2) after the information is collected and while it is being stored within the company, and (3) at the point of dissemination. Companies must consider that both external as well as internal threats are able to compromise PII if inadequate security procedures are implemented. Strong information protection measures will sit well with Web site visitors who are more likely to use a Web site if they feel their PII will be securely maintained.[247] This section of

---

[245]A major problem with the policy is that no party is taking responsibility for the protection of PII in cyberspace and, therefore, no party has an incentive to help protect this information.

[246]Are outsiders granted access to the informational databases instead of obtaining the information via dissemination? This type of access may lead to security breaches.

[247]Visitors are concerned about breaches of their PII because they are beginning to understand that once information is released into the hands of another party, it is basically irretrievable. The only way a person might identify that information has been used inappropriately is by checking bank and credit card statements as well as credit reports.

the policy will increase the goodwill the company builds with its existing customer base as well as with the consumer population in general. This improving consumer sentiment should provide a welcome change as recent security breaches at large public companies and governmental institutions have received negative publicity resulting in calls for increased governmental regulation covering data collection practices and PII protection.[248]

This section should cover the use of encryption technology, if applicable. Encryption is a "fundamental technology used to convert human-readable cleartext into encoded ciphertext."[249] Electronic data can be encrypted via encryption hardware or encryption software. A recent Enterprise Strategy Group research report showed that only seven percent of respondents claimed that they "always" used encryption technology when their data is backed up while sixty percent claimed that they "never"

The delay between the item showing up on the report and the time the fraud occurred makes it much more difficult to combat the fraud.

[248]*See, e.g.*, *ChoicePoint Complaint*, *supra* note 175 (recounting the poor PII-management practices leading to the ChoicePoint security breach). Other examples of private enterprises, universities, and governmental entities experiencing major security breaches in the recent past are: America Online (AOL), CardSystems Solutions, LexisNexis, the University of California–San Diego, Sam's Club, and the U.S. Department of Justice (DOJ). *See, e.g.*, Privacy Rights Clearinghouse, A Chronology of Data Breaches, http://www.privacyrights.org/ar/ChronDataBreaches.htm (last visited Oct. 6, 2006). AOL experienced an internal security breach when the company discovered an employee selling subscriber e-mail addresses. CardSystems Solutions, a credit card payment processor, exposed credit card numbers of more than 40 million cardholders. LexisNexis, an information aggregator, admitted that hackers gained access to the PII of over 300,000 customers. At the University of California–San Diego, over 380,000 individuals had their PII exposed to hackers. Sam's Club, a division of Wal-Mart Stores Inc., experienced an attack where hackers were able to steal the credit card information of at least 600 customers. The DOJ mistakenly exposed Social Security Numbers on its Web site, www.usdoj.gov. These breaches have led to scrutiny by Congress as well as state legislatures. *See, e.g.*, Johnathan Krim, *Consumers Not Told of Security Breaches, Data Brokers Admit*, WASH. POST, Apr. 14, 2005, at E-5 (discussing heated discussions between ChoicePoint and LexisNexis corporate officers and U.S. Senators during a Senate Committee Hearing concerning the recent security breaches); Jon Swartz, *2005 Worst Year for Breaches of Computer Security*, USA Today, Dec. 29, 2005, at B-1 (stating that over 55 million Americans were subjected identity theft due to a security breach compromising their PII during 2005 alone and that these breaches are causing anxiety with the lack of governmental intervention).

[249]Jon Oltsik, *Information Security, Enterprise Data Privacy* 4 (Apr. 2005), http://whitepaper.informationweek.com/shared/write/collateral/WTP/50758_07886_61050_Jon_Oltsik_Whitepaper-_Vormetric.pdf?ksi=1175512&ksc=1236673246.

encrypt this type of data.[250] An important part of encryption occurs through the secure socket layer (SSL). SSLs make it difficult for unauthorized third parties to intercept credit card, as well as other personal, information transmitted from a customer to a company through its Web site. A SSL encrypts information while it is in transmission but not while it is in storage. The policy should also describe how visitors can be sure that they are visiting a secure page by noting the change in the URL text as well as with a small lock appearing in the browser's status bar. This encryption disclosure should be made for all three areas covered in this section: (1) collection, (2) storage, and (3) dissemination.

5. Accessing/Changing/Removing Personal Information

This required privacy policy section should contain information notifying customers as to how they may access, change/update, or remove their PII collected by the company.[251] The most efficient and effective manner to accomplish this is for the electronic policy to contain a hyperlink placed where visitors can access and change their PII, and then modify the company Web site to accommodate this access. A visitor clicking on this link should be required to enter a username and password and then obtain authorization to access the personal information dossier. All changes may be made on this online form and submitted to the company Web site for automatic updating.[252] Companies in unregulated sectors are not required to offer visitors any right to access or change any PII collected electronically. Sticking to the general theme of company choice, this model policy does not require companies to allow visitors rights of access and amendment as long as this decision is clearly declared in the privacy policy language.

---

[250]*Id*. This study surveyed 388 storage professionals and asked, "Does your company encrypt data as it is backed up to tape?" *Id*. Interestingly, twelve percent of storage professionals surveyed claimed that they did not know whether or not data backed up to tape was encrypted by their employer. *Id*.

[251]This section mimics the COPPA, *see supra* Part III, and its requirement that parents be able to update and remove their child's PII.

[252]For some companies an electronic form allowing visitors to access and change their PII is cost prohibitive. In these situations, companies can designate an employee to handle telephone, e-mail, or postal mail requests.

6. Privacy Policy Changes

Companies must be allowed to change the terms of their privacy policies as corporate strategy evolves and business conditions dictate. The primary consequence of this self-determination from the information privacy perspective is that privacy policy modifications are often made without existing customers being notified and without an opportunity to remove their PII. Without an effective modification notice requirement, existing customers will be hard pressed to discover these changes and will believe that they are using the Web site consistently with the privacy terms available during previous visits. A current example of this practice occurs in the Wal-Mart.com privacy policy. Within this policy, Wal-Mart urges Web site visitors to check the company's privacy policy "periodically for changes."[253] Under these circumstances, the party with the best knowledge that the changes have occurred and the extent of such changes (Wal-Mart) requires the less-informed party (the Web site visitor) to take the initiative to discover any modifications.[254] In fact, the Wal-Mart policy also states that visitors who use the company's Web site subsequent to a privacy policy modification imply their consent to all of the terms of the policy as modified.[255]

This is in contrast to EPPAA's model policy, which would require that visitors be notified of all material changes to a company's electronic privacy policy. Therefore, if a company decides to materially alter its privacy practices, these changes should be available to customers either through a privacy update alert icon or link prominently placed on the company home page and/or via an e-mail sent to all available visitor accounts.[256] A privacy policy should include a statement as to how the company will use one or both of the above avenues to notify all customers providing personal information about the material changes. The updated policy

---

[253]Wal-Mart.com USA, LLC, *Our Privacy Policy* [hereinafter *Wal-Mart Privacy Policy*], http://www.walmart.com/catalog/catalog.gsp?cat=121240&path=0%3A5436%3A120160%3A119833%3A119834%3A121240 (last visited Oct. 1, 2006).

[254]This is especially difficult if the changes are not highlighted prominently in the modified privacy policy. Without any idea of which sections were modified, customers would be forced to compare, line by line, each version of the privacy policy to discover any discrepancies. This is a task where even the most diligent Web site visitor might struggle.

[255]*See Wal-Mart Privacy Policy, supra* note 253.

[256]A brief recap of every material policy change along with the modification's effective date must also be placed at the end of the privacy policy after the policy effective date statement.

should immediately be posted on the Web site and replace the prior privacy policy with all material changes singled out in plain English and in a manner that compares the old and new policy terms. Posting such a link or sending an e-mail to alert visitors of the changes is an inexpensive and relatively effective practice. With these steps taken, customers will then have the option of reading the updated policy and noting the changes. If a visitor chooses to ignore the modification notification, the onus rests with the visitor and not the company.

The final part of this policy section should describe how the company will treat PII collected prior to each subsequent policy modification. Some companies may choose to categorize visitor information chronologically and respect the terms of each policy under which it was submitted. Other companies may choose to place all information, regardless of its collection date, under the terms of the most recent privacy policy. This option is less expensive as it does not force companies to create software and databases to manage the different information cut-off dates and to train representatives on how to deal with each specific time period. This option is also more privacy-intrusive as parties are stuck with policies they never assented to. As with the other sections of this template, however, EPPAA only requires that companies accurately state their policy-modification practices. Visitors must then read such statements and choose whether they will submit their PII.

7. Other Important Information[257]

This final substantive section of the electronic privacy policy is reserved for miscellaneous—but still important—company-specific privacy policy information. For instance, if a company is operating under a Trustmark, this would be the place to discuss the implications. This is also the place to post the hyperlink to the detailed privacy policy—layer three of the multilayered policy. Companies need not place any information under this heading other than the hyperlink just mentioned and may, instead, include a statement that all of the relevant privacy policy information is contained in the previous headings.

---

[257]Some multilayered privacy policies title this section "Important Information," but a more effective title is "Other Important Information" crafted to indicate that all of the material previously displayed in the privacy policy is important as well.

8. Company Contact Information and Effective Dates

Although not necessarily considered to be fair information practices, the final section of the privacy policy must briefly discuss specific contact information and effective/modification dates of the privacy policy. The first bullet in this section should explain precisely how a customer can contact an authorized company representative trained on information privacy issues. This person should be able to handle specific privacy policy questions as well as complaints alleging company noncompliance with its policy. This section should also detail how promptly such customer may expect a response to any inquiry.[258] While customers may prefer a telephone number to be listed as company contact information, listing only an e-mail address is an option as different companies may not have the resources to make a trained privacy policy representative available via telephone. If the policy lists an e-mail address as a primary or secondary contact point, this account should be regularly monitored and responses should occur within the time frame stated in the policy and all responses should come from a trained company representative. Without a company's voluntary acceptance of a Trustmark, customers must funnel all complaints and comments through the contact information listed in the policy itself.[259] However, if a company without a Trustmark does not abide by its commitments, it runs the risk of an enforcement action by the FTC or a state attorney general.[260] The second bullet must list the effective date of the policy along with any dates and other key information related to any material policy change, if

---

[258]Many companies use the term "commercially reasonable" when describing response times. For instance, the Privacy Statement at Monster.com states, "We will use commercially reasonable efforts to promptly answer your question or resolve your problem." Monster.com, *Privacy Statement*, http://about.monster.com/privacy/ (last visited Oct. 1, 2006).

[259]This article argues that acceptance of a Trustmark should be voluntary for a company. This is consistent with the general approach in privacy policy law of allowing the customer, once properly informed, to choose whether the privacy commitments are adequate. Requiring companies to use a Trustmark service would be overly paternalistic and unrealistic as such marks have not gained widespread industry or consumer acceptance. *See* discussion *supra* Part III.

[260]In Part III this article discusses the potential privacy-promise enforcement options. *See* discussion *supra* Parts III & IV.A.

applicable.[261] This section, like all of the other sections, must be written in plain English.

Requiring a privacy policy template similar to the model template provided in this analysis will, over time, allow Web site visitors to efficiently and effectively compare company uses of the PII they may be asked to submit. Each of the seven information headers listed above are crucial for a policy to be effective and the EPPAA would require these headers to be included in the second and third layers of every company policy subject to its jurisdiction. Although there is no guarantee that all Web site visitors will understand, or care to understand, company policies complying with EPPAA, such a law would help to combat the current lack of visitor awareness of privacy implications stemming from submitting PII into cyberspace.

V. CONCLUSION

This article identifies the tension created when unique privacy threats accompany data-processing advancements. This tension is alleviated when companies adopt a set of fair information practices to deal with such data processing. Because fair information practices are not taken seriously, today's policies are generally unreadable and inconspicuously posted. These characteristics combine to make many privacy policies ill-suited to garner appropriate public attention. Moreover, the legal and self-regulatory regimes targeting electronic privacy policies are poorly equipped to

---

[261]As detailed above, the California OPPA requires companies collecting certain types of PII from California residents to state the effective date on all privacy policies; the proposed federal EPPAA would expand this requirement to include the effective date of any material policy changes as well. Therefore, a company adopting a privacy policy on January 1, 2005 and materially amending such policy on January 1, 2006 to allow address information to be sold to affiliated companies—and with the amended policy affecting only PII collected after January 1, 2006—would be required to contain a statement similar to the following:

Effective Date:	January 1, 2005.
Policy Changes:	On January 1, 2006 we changed this policy. We are now allowed to sell your address to other companies we own. Beginning January 1, 2006, every time we collect your address on our website we are authorized to sell this information to these select companies. Please click here to view this policy change in detail.

remedy this problem alone. This inadequacy is caused by federal privacy regulations targeting only a select few economic sectors. Companies operating outside of these regulated areas are free to craft their own data-processing practices completely disregarding fair information practices and privacy policy disclosures. Although some companies ignore this legal void and create effective privacy policies, as a general rule such policies: (1) remain inconspicuously linked near other mundane topics, (2) are too long and abound with legalese allowing companies to disclaim major responsibilities,[262] or (3) are completely ignored by companies

---

[262]The following is a section of Ford Motor Company's privacy policy concerning the company's granting of a limited license to a visitor for use of Ford's Web site:

> This site is provided by Ford Motor Company (Ford) and may be used for informational purposes only. By using this site or downloading materials from this site, you agree to abide by the terms and conditions, set forth in this agreement. If you do not agree to abide by these terms and conditions, do not use this site or download materials from this site.
>
> Subject to your continued compliance with the terms and conditions set forth in this agreement, Ford grants you a non-exclusive, non-transferable, limited right to access, use, display, and listen to this site and the information, images, sounds, and text ("materials") thereon. You agree not to interrupt or attempt to interrupt the operation of the site in any way.
>
> Ford authorizes you to view and download the materials at this site only for your personal, non-commercial use. This authorization is not a transfer of title in the materials and copies of the materials and is subject to the following restrictions:
>
> 1. [Y]ou must retain, on all copies of the materials downloaded, all copyright and other proprietary notices contained in the materials;
> 2. [Y]ou may not modify the materials in any way or reproduce or publicly display, perform, distribute, or otherwise use them for any public or commercial purpose;
> 3. [Y]ou must not transfer the materials to any other person unless you give them notice of, and they agree to accept, the obligations arising under these terms and conditions of use.
>
> This site, including all materials, is protected by worldwide copyright laws and treaty provisions, whether or not a copyright notice is present on the materials. You agree to comply with all copyright laws worldwide in your use of this site and to prevent any unauthorized copying of the materials. Except as expressly provided herein, Ford Motor Company does not grant any express or implied right to you under any patents, trademarks, or copyrights.

Ford.com, *Privacy*, http://www.ford.com/en/support/privacyStatement.htm?referrer=home&source=botnav (last visited Oct. 1, 2006) (emphasis added). Research has shown that privacy policies are most effective when written at a ninth-grade reading level. There are not many ninth-graders who understand the phrase—and certainly not the implication of—"worldwide copyright laws and treaty provisions."

collecting PII.[263] These problems, combined with the fact that California OPPA and similar state laws require additional precautions for companies targeting state residents, make company compliance more difficult and expensive.

The federal EPPAA proposed in this article would help alleviate these problems by requiring all commercial entities operating Web sites that collect PII to conspicuously post an electronic privacy policy written in plain English. Companies remain free to set their own policies internally but such policies must discuss the company practices specifically related to the seven fair information practices required by the Model Privacy Policy Template attached to EPPAA. Compliant policies must also disclose company contact information as well as the effective date of the policy and of any policy modifications. While this law will neither solve the information privacy dilemma nor force visitors to read or understand company privacy policies, at the end of the day legally required compliance with this template will force companies to take a closer look at their PII practices and, eventually, encourage better protection of this information. Additionally, the fact that companies are allowed to craft their own privacy practices and corresponding privacy policies will encourage creativity and new ways to promote economic efficiency while also protecting information privacy.

---

[263]*See, e.g.*, Jewels By Park Lane Inc., http://www.jewelsbyparklane.com/ (last visited Oct. 1, 2006). This Web site collects names, e-mail addresses, and ZIP codes and much more. Under the *Contact* section of the Web site the company states, "Jewels by Park Lane was founded in 1955 . . . in Chicago, Illinois. Today, still family-owned and operated, Park Lane is recognized and respected as the world's leading jewelry direct sales/in-home marketing company. Countless thousands of representatives experience tremendous success and reward through their affiliation with Park Lane." *Id.* at http://www.jewelsbyparklane.com/main.php?view=contact (last visited Oct. 1, 2006). Therefore, the "world's leading jewelry direct sales/in-home marketing" company chooses not to post a privacy policy and is within its legal rights to do so.