Washington University Law Review

Volume 79 | Issue 3

January 2001

Surfing the Net Safely and Smoothly: A New Standard for Protecting Personal Information from Harmful and Discriminatory Waves

Tammy Renée Daub

SURFING THE NET SAFELY AND SMOOTHLY: A NEW STANDARD FOR PROTECTING PERSONAL INFORMATION FROM HARMFUL AND DISCRIMINATORY WAVES

INTRODUCTION

Imagine yourself having been in the following situations: in high school, you surfed the Web to gather research for a psychology class on depression and suicide; last year, you looked into Web sites that provide information about a genetic disease that runs in your family; six months ago, you bought inflammatory CDs on Amazon.com for a friend or listened to this music on RealNetworks; a week ago, you looked at law firm Web sites to research attorneys who can help clean up the traffic violations on your driving record; yesterday, you researched student loan information online.

In each of these scenarios, you took the chance that the personal information you disclosed online (including your surfing habits and any information you provided while visiting the Web site) might be used in a harmful or discriminatory way.[1] For example, an advertising agency, health care provider, future employer, credit agency, or insurance company might be interested in obtaining this information.[2] Given the lack of protection of privacy rights in the online environment, these parties could obtain this information themselves or a Web site operator could sell it to them.

Although the United States Constitution does not expressly mention privacy, Justice Douglas recognized a right to privacy under the "penumbra theory" articulated in the famous Supreme Court case *Griswold v. Connecticut*.[3] Under this theory, the Supreme Court has recognized rights that can be found in the shadows or emanations of the Bill of Rights.[4]

---

1. *See* Kalinda Basho, *The Licensing of Our Personal Information: Is It a Solution to Internet Privacy?*, 88 CAL. L. REV. 1507, 1517 (2000) (describing privacy expert Jeffrey Reiman's recognition that threats to our privacy pose a danger to our ability to engage freely in activities on the Internet).

2. *See id*. at 1516.

3. 381 U.S. 479, 484 (1965) ("[S]pecific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance. Various guarantees create zones of privacy.") (citation omitted). *See also* Roe v. Wade, 410 U.S. 113, 152 (1973).

4. *Griswold*, 381 U.S. at 484. In addition, the Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." U.S. CONST. amend. IV. In order to raise a Fourth Amendment challenge to a government search or seizure, a defendant must establish a legitimate expectation of privacy upon which the government infringed. *See* Katz v. United States, 389 U.S. 347, 353 (1967). The legitimate expectation of privacy test entails a two-prong inquiry: (1) whether the defendant had an actual (subjective) expectation of privacy; and (2) whether society is prepared to recognize that

Despite the legal recognition that an individual's interest in maintaining privacy deserves constitutional protection, consumer concerns about a lack of privacy in the online environment were evident in a 1998 Harris poll on consumer privacy. The poll found the following: "Nearly nine in ten Americans (88%) say they are 'concerned about general threats to their privacy.' Eight in ten (82%) feel they have 'lost all control over how companies collect and use their personal information." Three-fourths (78%) say they have not given information to a company online because of their concern with a lack of privacy compared with 42% in 1990; and two in five (43%) said they had 'exercised an opportunity to opt-out.'[5]

This Note evaluates the problem underlying these scenarios and statistics. Part I first examines the history of the collection and use of personal information in the traditional sense, and second in the transactional sense. Part II considers how the online industry, Congress, the Federal Trade Commission (FTC), and other academics and theorists are approaching the problem of online privacy of personal data. Part III develops background on the discriminatory and harmful effects of online profiling of personal information and analyzes the various approaches attempting to address the problem of online privacy. In Part IV, I conclude that although the regulatory approach is currently the best way to address the abuse of personal

---

expectation as reasonable. Smith v. Maryland, 442 U.S. 735, 740 (1979). The Supreme Court has also held that a person does not have a legitimate expectation of privacy in information that he or she voluntarily provides to a third party. *See, e.g., Smith*, 442 U.S. 735 (1979) (holding that defendant lacked a legitimate expectation of privacy in phone numbers dialed from his phone because he voluntarily provided the numbers to the telephone company); United States v. Miller, 425 U.S. 435, 445 (1976) (holding that the defendant did not have a legitimate expectation of privacy in bank records since he exposed information in records to bank employees).

Courts have applied this assumption of risk rationale to deny an expectation of privacy in electronic information voluntarily given online. *See* United States v. Charbonneau, 979 F. Supp. 1177, 1184 (S.D. Ohio 1997) (holding that a user did not have a legitimate expectation of privacy in an e-mail transmission).

However, "traditional Fourth Amendment jurisprudence is ill-suited to answer" whether or not a user retains a legitimate expectation of privacy in his or her clickstream data. Gavin Skok, *Establishing a Legitimate Expectation of Privacy in Clickstream Data*, 6 MICH. TELECOMM. & TECH. L. REV. 61, 62 (2000) (arguing that the assumption of risk principles to online expectation of privacy is flawed because it does not take into account the extent of intrusion that occurs when clickstream data is collected and because users are unaware of the type or extent of data that Web site operators collect). *See also* United States v. Hambrick, 55 F. Supp. 2d 504, 508 (W.D. Va. 1999) ("Cyberspace is a nonphysical 'place' and its very structure, a computer and telephone network that connects millions of users, defies traditional Fourth Amendment analysis."). Although the cases discussed in this footnote involve governmental as opposed to private intrusion into online privacy, they demonstrate that a public policy interest exists in protecting online privacy in general. In addition, user ignorance about the type or extent of personal information collected online calls for protection against intrusions of online privacy, whether by the government or a private entity.

5. Beth Givens, *Symposium on Internet Privacy: Privacy Expectation in a High Tech World*, 16 SANTA CLARA COMPUTER & HIGH TECH L.J. 347, 350 (2000).

information, it is not an adequate solution. I propose a new standard for privacy policies, which should be incorporated into legislation, in order to prevent the discriminatory and harmful effects of online profiling.

I. HISTORY OF THE COLLECTION AND USE OF PERSONAL INFORMATION

A. "Traditional" Collection and Use

The "traditional" collection of information refers to when consumers voluntarily and knowingly provide personal information to others.[6] For example, the government gathers information from citizens when they fill out tax forms and applications for various social programs, including Social Security, food stamps, Medicare, and Medicaid.[7] In addition, private industry collects information in this traditional way when consumers apply for credit cards or membership to programs, register for access to Web sites, or enter contests.[8] Employers also collect personal information from employees when they gather data for various documents, including applications and timesheets.[9]

Legislative protection of the privacy of personal data in the United States collected in this traditional way applies to particular industries or particular kinds of information.[10] Several federal statutes regulate the privacy of personal data.[11] These statutes protect personal information given to

---

6. Seth Safier, *Between Big Brother and the Bottom Line: Privacy in Cyberspace*, 5 VA. J.L. & TECH. 6, ¶29 (2000), *at* http://www.vjolt.net/vol5/issue2/vti2a6-safier.html (noting that a "consumer . . . provides personal information when she registers, applies, enrolls or requests information, products, services or jobs"). The traditional method of collection occurs in both the offline, brick and mortar world, as well as in the online world of cyberspace. Thus, the defining characteristic of traditional collection of personal information is not where it occurs but rather that it involves voluntarily and knowingly giving your information out.

7. *See id.* ¶33 (pointing out that "products and services are increasingly becoming contingent" so that an individual needs access to one product or service, such as a credit card, in order to gain access to another product or service, such as video rental store membership).

8. *See id.* ¶32.

9. *Id.* ¶34. *See also* Oscar H. Gandy, Jr., *Legitimate Business Interest: No End in Sight? An Inquiry into the Status of Privacy in Cyberspace*, 1996 U. CHI. LEGAL F. 77, 86 (1996) (emphasizing that "[i]nformation provided directly on the application represents only a fraction of the information that employers believe they need" as employers often require other information, such as the results of physical and psychological examinations).

10. Existing privacy legislation has been described as "sectoral," meaning that the laws are narrow and apply only to particular sectors of industry or information. *See* Karl D. Belgum, *Who Leads at Half-time?: Three Conflicting Visions of Internet Privacy Policy*, 6 RICH. J.L. & TECH. 1, ¶24 (1999), *available at* http://www.richmond.edu/jolt/v6i1/belgum.html; Scott Killingsworth, *Minding Your Own Business: Privacy Policies in Principle and in Practice*, 7 J. INTELL. PROP. L. 57, 79 (1999).

11. For an excellent compilation of e-commerce legislation, see generally *Baker & Mckenzie, Congress: E-Commerce Legislation and Regulation*, *at* http://www.bmck.com/ecommerce/congress.

traditional collectors such as the Department of Motor Vehicles,[12] video rental stores,[13] cable operators,[14] and educational institutions.[15]

B. "Non-traditional" Collection and Use or "Transaction Generated Information":[16] the Process of Online Profiling

"Transaction generated information" involves consumers interacting directly with cyberspace through networked technology, such as a computer, a telephone, an ATM machine, or a credit or debit card, in such a way that they are not aware of exactly how or what kind of personal information is being collected.[17] Usually, when Web sites collect transaction generated information, the consumer has already had personal information collected via the traditional method, which produced "identifiers" such as identification numbers, including credit card numbers or a Social Security number, or passwords.[18] In complex networks, identifiers can link to previous identifiers, creating a detailed informational profile of an individual.[19]

After this transaction generated information is collected, it is processed in such a way that information is classified, categorized, sorted, and then stored.[20] The most widespread use of this compiled personal information is direct marketing, which involves tailoring marketing and advertising to

---

htm (last visited Mar. 23, 2001) (providing a list of enacted and pending legislation relating to e-commerce).

12. Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2721 (2000) (safeguarding the personal information of licensed drivers from improper use or disclosure of information contained in their drivers' records).

13. Video Privacy Protection Act, 18 U.S.C. § 2710 (1988) (preventing a video rental store from revealing the titles of movies a customer has rented).

14. Cable Communications Policy Act, 47 U.S.C. §551 (2000) (requiring cable operators to obtain written or electronic consent before disclosing personal information).

15. Family Education Rights & Privacy Act, 20 U.S.C. § 1232(g) (1974) (limiting the improper disclosure of children's personal information and giving parents the right to inspect their children's information).

16. Safier, *supra* note 6, ¶ 36.

17. *See id.*

18. *Id.* Information collected using the traditional method is more valuable after it has been processed or entered cyberspace through a computer, for example, because it is inexpensive and efficient to transfer and can be combined with other information previously collected. *Id*.

19. *Id.* The following hypothetical scenario illustrates how a profile might be compiled:

> [I]magine that Bob purchases a new maroon blazer from the Gap with his recently acquired Gap charge card. Perhaps Bob's first identifier (the Gap identifier or charge account number) links to his bank account number, which then links to his credit card number, and all the corresponding information. The credit card identifier might, in turn be linked to a Social Security number, and thereby, Bob's census, IRS, health, insurance, spring break arrest and employer information.

Id. ¶ 37.

20. *Id*. ¶ 53.

specific audiences or groups of consumers.[21] The cyberspace version of real space direct marketing also occurs through the use of intelligent agents[22] and push technologies,[23] which one commentator has deemed "direct marketing on steroids."[24] These technologies memorize and process a consumer's clickstream,[25] purchases, and amount of money and time spent shopping online and deliver ads targeted to meet the consumer's interests and preferences apparent in his or her profile.[26]

For example, Web sites identify repeat users through the use of "cookies," small files inserted into a user's hard drive, which the Web site accesses

---

21. *Id.* ¶ 60. *See also* Gandy, *supra* note 9, at 89 (noting that "profiles are used by direct marketers to estimate the probability of an affirmative response by consumers they have assigned to different categories or groups").

22. The definition of an "agent" is as follows:

> A program that searches through archives or other repositories of information on a topic specified by the user. Agents of this sort are used most often on the Internet and are generally dedicated to searching a single type of information repository, such as posting on Usenet groups . . . . *Also called* intelligent agent.

COMPUTER DICTIONARY 19 (Microsoft Press 3d ed. 1997).

23. The definition of "push technology" is as follows:

> A data distribution technology in which selected data is automatically delivered into the user's computer at prescribed intervals or based on some event that occurs. Contrast with *pull technology*, in which the user specifically asks for something by performing a search or requesting an existing report, video or other data type.

ALLEN FREEDMAN, THE COMPUTER GLOSSARY: THE COMPLETE ILLUSTRATED DICTIONARY 335 (8th ed. 1998). The definition of "push" is as follows:

> [T]he process whereby the network delivers information to a client machine without waiting for the user to request it. Push technology makes the World Wide Web work rather like TV; the user selects a "channel" and views whatever is being sent out at the moment. This contrasts with the way web browsers traditionally work, where the user manually selects information to retrieve from the Web. . . . Push technology is useful for delivering information that has to be updated minute by minute, such as stock market quotes or new bulletins.

DOUGLAS A. DOWNING ET AL., DICTIONARY OF COMPUTER AND INTERNET TERMS 378-79 (6th ed. 1998).

24. Safier, *supra* note 6, ¶ 65.

25. The definition of "clickstream" is as follows: "[t]he trail of mouse clicks made by a user performing a particular operation on the computer. It often refers to linking from one page to another on the World Wide Web." FREEDMAN, *supra* note 23, at 63. Clickstream is also defined as follows:

> The path a user takes while browsing a Web site. Each distinct selection made on a Web page adds one click to the stream. The further down the clickstream the user goes without finding the sought item, the more likely he or she is to depart to another Web site. Analysis of usage pattern helps Web site designers create user-friendly site structures, links, and search facilities.

COMPUTER DICTIONARY, *supra* note 22, at 92.

26. *See* FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE, Part II (2000) [hereinafter PRIVACY ONLINE] (describing how network advertising companies supply banner ads and gather data about consumers who view their ads through profiles linked to the identification number of the advertising network's cookie on the consumer's computer). Often, these "anonymous" profiles are merged with personally identifiable information collected through the traditional method of collecting personal data. *Id.* For a definition of "cookie," see *infra* note 27.

when the user visits the site again in the future.[27] In addition to collecting information that users do not voluntarily provide, such as the user's e-mail address, the type of browser,[28] the type of computer being used, and the Internet address (URL),[29] Web sites use cookies to track clickstream data,[30] including surfing patterns, shopping habits and preferences, and purchasing power.[31]

---

27. The definition of "cookie" is as follows:

> On the World Wide Web, a block of data that a Web server stores on a client system. When a user returns to the same Web site, the browser sends a copy of the cookie back to the server. Cookies are used to identify users, to instruct the server to send a customized version of the requested Web page, to submit account information for the user, and for other administrative purposes.

COMPUTER DICTIONARY, *supra* note 22, at 119. *See also* FREEDMAN, *supra* note 23, at 335 (defining "cookie file" as "[a] file that contains information (cookies) created by Web sites that is stored on the user's hard disk. It provides a way for the Web site to keep track of a user's patterns and preferences and, with the cooperation of the Web browser, to store them on the user's own hard disk in the COOKIES.TXT file"). A third definition of cookie is as follows:

> [I]formation stored on a user's computer by a WEB BROWSER at the request of software at a Web site. Web sites use cookies to recognize users who have previously visited them. The next time the user accesses that site, the information in the cookie is sent back to the site so the information displayed can vary depending on the user's preferences. The term *cookie* comes from a 1980s prank computer program called Cookie Monster that would interrupt users and demand that they type the word "cookie" before continuing.

DOWNING ET AL., *supra* note 23, at 106.

28. A "Web browser" is defined as follows:

> A client application that enables a user to view HTML documents on the World Wide Web, another network, or the user's computer; follow the hyperlinks among them; and transfer files. Text-based Web browsers, such as Lynx, can serve users with shell accounts but show only the text elements of an HTML document; most Web browsers, however, require a connection that can handle IP packets but will also display graphics that are in the document, play audio and video files, and execute small programs . . . . In addition, most current Web browsers permit users to send and receive e-mail and to read and respond to newsgroups.

COMPUTER DICTIONARY, *supra* note 22, at 505.

29. A "URL" (Uniform Resource Locator) is defined as follows:

> The address that defines the route to a file on the Web or any other Internet facility. URLs are typed into the browser to access Web pages, and URLs are embedded within the pages themselves to provide the hypertext links to other pages. The URL contains the protocol prefix, port address, domain name, subdirectory names and file name. Port addresses are generally default and are rarely specified. To access a home page on a Web site, only the protocol and domain name are required. For example, http://www.computerlanguage.com retrieves the home page at The Computer Language Company's Web site. The http:// is the Web protocol, and www.computerlanguage.com is the domain name.

FREEDMAN, *supra* note 23, at 443.

30. For a definition of clickstream, see *supra* note 25.

31. *See* Michael Gartner, *Report from the Ombudsman*, BRILL'S CONTENT, Oct. 2000, at 26 (describing a Web site that denied access if a user's browser had been set to turn off cookies, thereby limiting a user's choices to either no access to the Web site in order to prevent their online behavior from being tracked or access to the Web site in exchange for accepting cookies); Tim McDonald, *Is Gen X Hooked on Cookies?*, E-COMMERCE TIMES (Aug. 22, 2000), *at* http://www.ecommercetimes.com/news/viewpoing2000/view-000822-1.shtml (equating cookies with labels

C. The Discriminatory and Harmful Effects of the Online Collection and Use of Personal Information: Internal Secondary Uses and External Secondary Uses[32]

1. Amazon.com: A Case of Price Discrimination?

In September 2000, online shoppers in the DVD section of Amazon.com noticed that they were getting charged different prices for the same DVD item.[33] Amazon claimed that its price variations were part of a random price test to examine the effects of price variations on buying habits.[34] Consumers, journalists, and privacy advocates expressed skepticism that this price variation was random and alleged that Amazon was testing prices based on demographics,[35] especially in light of Amazon's announcement two weeks

---

because Web sites can sell personal information acquired through the use of cookies to companies such as credit and insurance companies).

32. *See* PRIVACY ONLINE, *supra* note 26 (describing internal secondary uses as those in which the Web site engages and external secondary uses as those in which third parties engage). In the year 2000, consumers sued various Web sites for allegedly collecting and using personal information of users without notifying them or obtaining their consent or doing so in violation of the Web site operator's privacy policy. Matthew P. Graven, *Leave Me Alone*, PC MAGAZINE, Jan. 16, 2001, at 158. Among these Web sites were: Amazon and Alexa Internet, a Web-navigation service provider owned by Amazon, sued in early 2000 for allegedly collecting personal information and sending it to Amazon without notifying consumers or obtaining their consent; e-tailer Buy.com, sued in March and April of 2000 for allegedly sharing personal information with third party advertising services without notifying users or obtaining their consent; Quicken.com, a personal-finance site sued for collecting confidential personal data and sharing it with third parties in violation of its privacy policy; and RealNetworks, an online audio and video company, sued between late 1999 and early 2000 for allegedly tracking users' online recording and listening habits in violation of its privacy policy. *Id.*

In addition, eGames, Inc., a developer and distributor of computer games, recently settled a suit that the Michigan Attorney General brought against the company. *See* Steven Bonisteel, *Michigan Reaches Privacy Pact with eGames over 'Spyware,'* NEWSBYTES (Jan. 12, 2001), *at* http://www.newsbytes.com/news/01/160454.html. EGames sells inexpensive games online and on CDs through retailers including Wal-Mart, Kmart, Target, and CompUSA. *Id.* Some of the company's games install third-party software, called "spyware," on consumers' computers. *Id.* This spyware enabled an advertising company, Conducent, Inc., to interact with eGames's users' computers. *Id.* However, the Attorney General alleged that eGames had not adequately informed consumers of this spyware. *Id.* Moreover, the Attorney General alleged that eGames allowed third parties to track consumers' browsing behavior at eGames's Web site without notifying users. *Id.* In the settlement, eGames will remove the spyware from future games and online "demo" versions of its games, and it will post a privacy policy disclosing its information practices. *Id. See also* Press Release, Chris De Witt, Attorney General: Jennifer M. Granholm (Jan. 10, 2001) (on file with author).

33. Keith Regan, *Amazon's Friendly Deception*, E-COMMERCE TIMES (Sept. 18, 2000), *at* http://www.ecommercetimes.com/news/viewpoint2000/view-000918-2.shtml.

34. *Id.*

35. Keith Dawson, *Amazon Says 'Oops' to Keep the Press at Bay*, THE INDUSTRY STANDARD (Sept. 28, 2000), *available at* http://www.thestandard.com/article/0,1902,18973,00.html (discussing another reporter's theory that Internet retailers have the power to make dynamic pricing the norm in the future); Lori Enos, *Amazon Apologizes for Pricing Blunder*, E-COMMERCE TIMES (Sept. 28, 2000), *at* http://www.ecommercetimes.com/perl/story/?id=4411 (describing consumer outrage at the

prior to the price variation discovery that customers' personal information (including past buying patterns and shopping preferences) was a business asset that could be shared with third parties.[36]

Price discrimination occurs when a seller charges different prices to consumers for the same "commodity."[37] Examples of lawful price discrimination include charging children, adult, and senior citizens different prices for the same movie ticket or for admission to an amusement park; charging those who purchase a one-way versus a round-trip airline ticket different prices for the same ticket; and charging customers who have discount coupons less than those who do not.[38]

However, price discrimination is not always lawful, particularly if it does not reflect the different costs of dealing with different buyers or if it does not result from a seller's efforts to match a competitor's prices.[39] In the case of Amazon, loyal customers were charged higher prices than others, which does not reflect the lower cost of dealing with those who buy regularly from the online company.[40] Moreover, the highest price a consumer is willing to pay for a particular commodity is easily revealed in cyberspace, because of the rampant use of technologies such as cookies.[41] Therefore, the Internet readily facilitates forms of price discrimination.[42] The *Amazon* case illustrates the

---

difference in pricing); David Streitfield, *On the Web, Price Tags Blur*, WASH. POST, Sept. 27, 2000, at A1 (noting that the effects of dynamic testing in cyberspace are more detrimental to consumers than in real space).

36. Regan, *supra* note 33. *See also* Keith Regan, *Amazon Announces Controversial Privacy Policy*, E-COMMERCE TIMES (Sept. 1, 2000), *at* http://www.ecommercetimes.com/perl/story/4180.html ("Despite growing consumer fears about online privacy, Amazon.com . . . will notify its 23 million customers that it has revised its policy to reflect the fact that customer information may be sold as an asset.").

37. *See* http://www.ftc.gov/bc/compguide/discrim.htm. Price discrimination is also defined as "[t]he practice of charging different prices to different customers despite the cost of production being the same." DONALD RUTHERFORD, DICTIONARY OF ECONOMICS 361 (1992).

38. *Id. See also* THE NEW PALGRAVE: A DICTIONARY OF ECONOMICS 952-54 (1987) (describing price discrimination more thoroughly).

39. *See* http://www.ftc.gov/bc/compguide/discrim.htm.

40. *See* Regan, *supra* note 33 (speculating that Amazon reasoned that "since customer X has made 10 purchases from Amazon in recent months—all single-item, apparent impulse buys—why not tack an extra dollar or two onto the prices that pop up on his Web page?"); Streitfield, *supra* note 35 (quoting customers who noted that Amazon's alleged variable pricing was not going to earn customer loyalty).

41. Streitfield, *supra* note 35. Although store prices might vary from neighborhood to neighborhood, depending on the socioeconomic status of residents, price discrimination methods in real space "are sledgehammers compared with the Internet's scalpel. The Web provides a continuous feedback loop . . . . It's as if the corner drugstore could see you coming down the sidewalk, clutching your fevered brow, and then doubles the price of aspirin." *Id.*

42. Interview with Lawrence Lessig, Professor of Cyberlaw, Stanford Law School, in St. Louis, Mo. (Nov. 1, 2000). *See also* Streitfield, *supra* note 35 (noting that the software company, BroadVision Inc., offers a Retail Commerce Suite, which it claims will allow any e-commerce retailer

discriminatory effects of one possible internal secondary use of personal information collected online.

2. Online Targeted Advertising and Direct Marketing: Discrimination of a Different Sort

a. The Case of DoubleClick, Inc.[43]

In January 2000, a California woman filed suit against DoubleClick, a major Web advertising firm that manages advertising for approximately 1,500 Web sites,[44] alleging that the company used cookies to identify Internet users and gather their personal information without their consent and in violation of its privacy policy.[45] This suit arose one month after DoubleClick had acquired Abacus Direct, a direct marketing company that maintains a database on the purchasing power and consumer spending habits of Americans.[46]

The plaintiff further alleged that DoubleClick combined its use of cookie technology with the information it acquired from Abacus Direct to build a more detailed profile of consumers, including their names; addresses; retail, catalog, and online purchase histories; and demographic data.[47] With the acquisition of Abacus Direct, DoubleClick allegedly integrated its "anonymous" records of its consumers' surfing habits using cookies with the Abacus database, creating the ability to identify its consumers.[48] In addition to the California suit, the FTC launched an investigation into DoubleClick's method of collecting and using the personal data of online consumers in mid-February 2000.[49]

---

to engage in price discrimination); LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 155 (1999) ("Economists will argue that in many contexts this ability to discriminate—in effect, to offer goods at different prices to different people—is overall a benefit . . . but these values are just one side of the equation. Weighed against them are the values of equality.").

43. *See* Web site at www.doubleclick.com.

44. Paul A. Greenberg, *FTC Launches Investigation into DoubleClick*, E-COMMERCE TIMES (Feb. 17, 2000), *at* http://www.ecommercetimes.com/perl/story/2529.html.

45. Sandeep Junnarkar, *DoubleClick Accused of Unlawful Consumer Data Use*, CNET NEWS.COM (Jan. 28, 2000), *at* http://news.cnet.com/news/0-1005-200-1534533.html.

46. *Id.*

47. *Id.*

48. Will Rodger, *Activists Charge DoubleClick Double Cross*, USATODAY.COM, *at* http://www.usatoday.com/life/cyber/tech/cth211.htm (last modified June 7, 2000).

49. Chet Dembeck & Robert Conlin, *Beleaguered DoubleClick Appoints Privacy Board*, E-COMMERCE TIMES (May 17, 2000), *at* http://www.ecommercetimes.com/perl/story/3348.html. In January 2001, the FTC closed its investigation upon finding the following:

> Based on this investigation, it appears to staff that DoubleClick never used or disclosed consumers' [personally identifiable information] for purposes other than those disclosed in its

b. FTC v. Toysmart.com[50]

In July 2000, the FTC filed a lawsuit in federal court alleging that Toysmart sold or shared personal information of its customers in breach of its privacy policy.[51] The company's privacy policy stated that personal customer information would never be shared with a third party.[52] Nevertheless, the company placed information, including names, addresses, and credit card numbers, up for sale as part of its bankruptcy proceedings in order to settle its debts to creditors.[53] Moreover, the company had a privacy seal of approval

---

> privacy policy. Specifically, it appears that DoubleClick did not combine [personally identifiable information] from Abacus Direct with clickstream collected on client Web sites. In addition, it appears that DoubleClick has not used sensitive data for any online preference marketing product, in contravention of its stated privacy policy.

Letter from Joel Winston, Acting Associate Director, Division of Financial Practices, Federal Trade Commission (Jan. 22, 2001) (on file with author).

50. *FTC v. Toysmart.com, LLC,* No. 00-11341-RGS (D. Mass. filed July 10, 2000). *See also In re Toysmart.com LLC,* No. 00-1395-CJK (Bankr. E.D. Mass. filed June 9, 2000).

51. Paul A. Greenberg, *Toysmart Flap Triggers Privacy Bill,* E-COMMERCE TIMES (July 13, 2000), *at* http://www.ecommercetimes.com/perl/story/3766.html.

52. Michelle Singletary, *A Web of Broken Promises,* WASH. POST, July 16, 2000, at H1. The privacy policy stated: "Personal information voluntarily submitted by visitors to our site, such as name, address, billing information and shopping preferences, is never shared with a third party." *Id.* at H14.

53. *Id*. Another failed dot-com company, Living.com, was sued to prevent it from selling customer information in September 2000. Greg Sandoval, *Texas Officials, Living.com Reach Settlement on Privacy,* CNET NEWS.COM (Sept. 25, 2000), *at* http://news.cnet.com/news/0-1007-200-2864965.html?tag=st.ne.ni.rnbot.rn.ni. The online furniture company reached an agreement with the Texas Attorney General to destroy customer financial information, including credit card, bank account, and social security information. *Id.* However, the agreement also gave Living.com permission to sell names and e-mail addresses, but only after notifying customers and giving them the choice to opt out. *Id.*

As more and more dot-coms go bankrupt, the issue posed in the Toysmart.com and Living.com cases—whether personal information linked to a privacy policy should be considered a company asset of the bankruptcy estate that may be sold without limitations—will arise more often. *See generally* Andrew B. Buxbaum & Louis A. Curcio, *When You Can't Sell to Your Customers, Try Selling Your Customers (But Not Under the Bankruptcy Code),* 8 AM. BANKR. INST. L. REV. 395 (2000) (arguing that bankruptcy law recognizes the enforceability of privacy policies in determining whether customer lists can be sold during bankruptcy proceedings); Marjorie Chertok & Warren E. Agin, *Restart.com: Identifying, Securing and Maximizing the Liquidation Value of Cyber-Assets in Bankruptcy Proceedings*, 8 AM. BANKR. INST. L. REV. 255, 300 (2000) (discussing how federal agencies and/or certifying agencies may ban the sale of customer lists during bankruptcy proceedings); Hal F. Morris & Flora A. Fearon, *Texas Attorney General: Privacy Is Not for Sale,* 2000 AM. BANKR. INST. J. 1 (Oct. 2000) (describing the conflict between the privacy rights of consumers and the business interests of creditors in determining whether the personal information of consumers constitutes a property interest of the debtor when it goes bankrupt).

Although §541(c)(1) of the Bankruptcy Code defines the property included in an estate, it does not define the scope of a debtor's interest in property. 11 U.S.C.A. §541 (2001). However, the Supreme Court's decision in *Butner v. United States* suggests that if a dot-com did not have a property interest in a customer list containing personal information before bankruptcy, then it does not have one after filing. Bunter v. United States, 440 U.S. 48 (1979). In this case, the Supreme Court held that:

from TRUSTe.[54] Toysmart agreed to a settlement, which forbids the sale of its customer information except under very limited circumstances.[55]

c. FTC v. Geocities[56]

In 1998, the FTC filed suit against GeoCities, which promised members that personal information would be shared with others to provide members

---

> Property interests are created and defined by state law. Unless some federal interest requires a different result, there is no reason why such interests should be analyzed differently simply because an interested party is involved in a bankruptcy proceeding. Uniform treatment of property interests by both state and federal courts within a State serves to reduce uncertainty, to discourage forum shopping, and to prevent a party from receiving "a windfall merely by reason of the happenstance of bankruptcy."

Id. at 55.

In addition, House Bill 833, the Bankruptcy Reform Act of 1999, requires that bankruptcy clerks release all public data held in electronic form to the public. Public L. No. 95-598, 92 Stat. 2549, Title IV §401(a) (1999). The benefits of such disclosure therefore conflict with individual privacy concerns. *See* Richard Lauter, *Privacy Concerns and Safeguards in the Governmental Dissemination of Bankruptcy Data on the Internet,* 2000 AMER. BANKR. INST. J. 1 (May 2000).

The Department of Justice, the Department of Treasury, and the Office of Management and Budget recently requested public comment regarding their study of how a consumer's filing for bankruptcy relief affects the privacy of personal information. The FTC responded with a comment that addressed the privacy and identity theft concerns that the collection and use of personal information in personal bankruptcy cases. The comment suggested that agencies engage in the following: (a) "consider the extent to which highly sensitive information must be included in public record data; (b) prohibit the commercial use by trustees of debtors' nonpublic data for purposes other than those for which the information was collected; and (c) evaluate the interplay between consumer's privacy interests and the Bankruptcy Code." *The Federal Trade Commission on "Recent Developments in Privacy Protections for Consumers" Before the Subcomm. on Telecomms., Trade and Consumer Protection of the Comm. on Commerce,* 106th Cong. (2000) (statement of Robert Pitofsky, Chairman, Federal Trade Commission). *See also* Public Comment on Financial Privacy and Bankruptcy, 65 Fed. Reg. 46,735 (July 31, 2000) (requesting public comment on financial privacy and bankruptcy). For the FTC staff comment, see http://www.ftc.gov/be/v000013.htm.

54. *Id.*

55. Press Release, FTC, FTC Announces Settlement with Bankrupt Web Site, Toysmart.com, Regarding Alleged Privacy Policy Violations (July 21, 2000), *available at* http://www.ftc.gov/opa/2000/07/toysmart2.htm (on file with author). Under the settlement agreement, Toysmart agreed to file an order in Bankruptcy Court, stating that it could sell the customer list only if it would be part of a package deal including the sale of the entire Web site to a "Qualified Buyer," a company in a related market. *Id.* The Qualified Buyer must adhere to Toysmart's privacy policy, and if it decides to change it, it must provide notice to consumers and obtain their affirmative consent. *Id.* The FTC has brought other law enforcement actions to protect privacy online. *See also* FTC v. Liberty Fin. Cos., Inc., FTC Dkt. No. C-3891 (filed Aug. 12, 1999) (challenging a Web site operator's false representations that information collected from children in an online survey would be maintained anonymously); FTC v. Sandra Rennert et al., No. CV-S-00-0861-JBR (D. Nev. filed July 6, 2000) (involving an FTC settlement with an online pharmacies that allegedly collected consumers' personal medical information without notifying consumers of their information practices settled with the FTC; *FTC v. ReverseAuction.com, Inc.* No. 00-0032 (D.D.C. filed Jan. 6, 2000) (in which online auction site that allegedly collected consumers' personal information from a competitive site and sent deceptive, unsolicited e-mail spam to those consumers seeking their business).

56. FTC v. Geocities, FTC Dkt. No. C-3849 (filed Feb. 12, 1999).

with advertising they requested, but in reality the company was selling members' information to third parties that used it for other purposes, including targeting members for advertising and solicitations beyond those that the member requested.[57] The parties reached a settlement in which GeoCities agreed to post a clear and conspicuous privacy policy, informing users about what information is collected and for what purpose, to whom it will be disclosed, and how users can access their information and delete it.[58]

II. DIFFERENT APPROACHES TO THE PROTECTION OF ONLINE PERSONAL INFORMATION

A. The Industry: Self-Regulation

Despite the pending legislation in Congress that would regulate online privacy and the resistance of consumer and privacy advocates to new laws protecting the personal information of online shoppers, the current approach to solving the potential abuses of the collection and use of personal information on the Internet is self-regulation.[59] In 1997, the Clinton Administration issued a report detailing a framework for global electronic commerce, known as the Magaziner Report, which stated that it supported self-regulation for the time being, but if consumer privacy was not sufficiently protected through self-policing, it would reconsider this approach.[60]

As part of its endorsement of industry self-regulation, the FTC articulated "fair information practices" for Web sites to follow in its 1998 report entitled *Privacy Online: Fair Information Practices in the Electronic Marketplace*.[61] First, consumers are entitled to clear *notice* of a Web site's practice of collection and use of personal information.[62] Second, consumers should be given *choices* as to how their information is used.[63] For example, Web sites

57. Press Release, FTC, *Internet Site Agrees to Settle FTC Charges of Deceptively Collecting Personal Information in Agency's First Internet Privacy Case* (Aug. 13, 1998), *available at* http://www.ftc.gov/opa/1998/9808/geocitie.htm (on file with author).

58. *Id*.

59. Joel R. Reidenberg, *Restoring Americans' Privacy in Electronic Commerce*, 14 BERKELEY TECH. L.J. 771, 775 (1999).

60. *Id*.

61. PRIVACY ONLINE, *supra* note 26; Killingsworth, *supra* note 10, at 69-72 (describing the FTC's fair information practices principles).

62. PRIVACY ONLINE, *supra* note 26, at 4. To give notice, "data collectors must disclose their information practices before collecting personal information from consumers." *Id.* at 4.

63. *Id*. To qualify as offering choices, "consumers must be given options with respect to whether and how personal information collected from them may be used for purposes beyond those for which the information was provided." *Id.*

should allow consumers to "opt-in" to allow use of information beyond the purpose for which it was first provided or "opt-out" to not allow such use.[64] Third, consumers should have reasonable *access* to their personal information.[65] Fourth, Web sites should protect the *security* of consumers' personal information.[66] The FTC also identified *enforcement* as an important element of a self-regulation program.[67]

In an effort to seek compliance with these principles, two self-regulatory initiatives, TRUSTe and BBBOnLine, were launched. TRUSTe grants licenses to Web sites to use a special logo indicating the Web site has a privacy policy and that it follows certain fair information practices.[68] TRUSTe may conduct audits to evaluate compliance with the companies' privacy policies.[69] BBBOnLine is a project of the Better Business Bureau.[70] Its goal is to provide an enforcement mechanism for privacy disputes that occur online.[71]

Moreover, various coalitions of electronic retailers and advertisers have recently developed self-regulation plans, which have included efforts to enforce standards for consumer privacy.[72] For example, the FTC and the Department of Commerce endorsed an industry self-regulation plan that the Network Advertising Initiative (NAI) developed in July 2000.[73] The NAI

---

64. *Id.*

65. *Id*. To qualify as offering access, "consumer should be able to view and contest the accuracy and completeness of data collected about them." *Id.*

66. *Id*. To give security, "data collectors must take reasonable steps to assure that information collected from consumers is accurate and secure from unauthorized use." *Id.*

67. *Id.* The FTC defines enforcement as "the use of a reliable mechanism to impose sanctions for noncompliance with these fair information practices." *Id.*

68. *See* Reidenberg, *supra* note 59, at 777.

69. *Id*.

70. *Id*. at 778.

71. *Id*.

72. *See* Rob Garretson, *Electronic Retailers Plan Self-Regulation*, WASH. POST, July 19, 2000, at E3 ("[T]he Electronic Retailing Association outlined a series of steps it plans to take to combat online fraud and violations of its privacy guidelines, which will include expelling offenders from the association . . . publicizing the offenses." The Electronic Retailing Association (ERA) is a trade group representing 479 retailers that sell their products on television, radio, and the Internet. *Id. See also* John Schwartz, *Online Firm Plan Retail Guidelines*, WASH. POST, June 6, 2000, at E1 (describing the proposal adopted by the seven-company coalition, including America Online, AT&T, Dell, IBM, and Microsoft, calling for consumer protection guidelines).

73. Chet Dembeck & Jennifer Hampton, *FTC Backs Away from Net Privacy Regulation*, E-COMMERCE TIMES (July 28, 2000), *at* http://www.ecommercetimes.com/news/articles2000/000728-5.shtml. In November 1999, the FTC and the Department of Commerce held a public workshop on the practice of online profiling, in which third-party network advertisers engage, in order to educate the public about the practice and to evaluate the industry's efforts to implement the FTC's fair information practice principles. *The Federal Trade Commission on "Recent Developments in Privacy Protections for Consumers" Before the Subcomm. on Telecomms., Trade and Consumer Protection of the Committee on Commerce*, 106th Cong. (2000) (statement of Robert Pitofsky, Chairman, Federal Trade

constitutes about ninety percent of the network advertising market.[74]

Finally, the NAI developed the *Self-Regulatory Principles for Online Preference Marketing* (OPM).[75] Under this agreement, advertisers will display notices on Web sites about when and how they are collecting personal information from users, and users will have the right to opt out.[76] Consumers will also be given access to their own personal information.[77] In addition, NAI companies agreed not to use consumers' medical or financial information for marketing purposes and not to use Social Security numbers or gender for profiling.[78]

B. Congress: Pending Legislation

Although the current trend is self-regulation, several pending bills in Congress reflect many legislators' support for federal regulation to protect the online consumer privacy of personal information.[79] The Senate Committee on Commerce, Science, and Transportation concluded hearings in early October 2000 on two bills: the *Consumer Internet Privacy Enhancement Act*[80] and the *Consumer Privacy Protection Act*.[81]

Commission). After the workshop, the NAI companies submitted drafts of self-regulatory principles to the FTC and the Department of Commerce. *Id*. In July 2000, the two agencies endorsed the NAI's plan. *Id.*

74. Dembeck & Hampton, *supra* note 73.

75. *Id*.

76. *Id*.

77. *Id*.

78. *Id*. In addition to self-regulatory initiatives such as TRUSTe, BBBOnline, and the self-regulatory plans of various coalitions, Internet, software, and computer companies increasingly engage in the practice of hiring privacy officers. Erich Luening, *EarthLink Boosts Privacy Efforts with New Exec*, CNET NEWS.COM (Dec. 13, 2000), *at* http://news.cnet.com/news/0-1005-200-4132109.html. For example, Earthlink, an Internet service provider for approximately 4.6 million subscribers named Les Seagraves as its chief privacy officer in December 2000 in order to protect customers' personal information. *Id.* Among his tasks will be to revise the company's privacy policy and lead a privacy council composed of EarthLink employees. *Id.*

In November 2000, IBM chose Harriet P. Pearson to be its chief privacy officer to "articulate and develop its privacy policy for employees and customers" and "to work with software and technology groups to ensure that all parties adhere to IBM's privacy standards." *Id*. *See also* Erich Luening, *Privacy Officers Get a Seat in Executive Boardrooms*, CNET NEWS.COM (Dec. 11, 2000), *at* http://news.cnet.com/news/0-1007-200-4065560.html?tag=st.ne.ni.rnbot.rn.ni.

Legislative proposals have also been introduced to establish a government-wide chief information officer (CIO) to manage information and technology policies. Erich Luening, *Washington Debates Need for Technology Policy Chief*, CNET NEWS.COM (Sept. 12, 2000), *at* http://news.cnet.com/news/0-1007-200-2762382.html?tag=st.ne.ni.rnbot.rn.ni.

79. For an excellent compilation of e-commerce legislation, see http://www.bmck.com/ecommerce/congress.htm.

80. S. 2928, 106th Cong. (2000).

81. S. 2606, 106th Cong. (2000). In addition to these two bills, Congressman Frelinghuysen, a Republican from New Jersey, recently introduced House Bill 89 on January 3, 2001, the first online

1. The Consumer Internet Privacy Enhancement Act[82]

The Consumer Internet Privacy Enhancement Act[83] has a Republican sponsor, two Democratic co-sponsors, and one Republican co-sponsor.[84] The Act essentially codifies the FTC's fair information practice principles of

---

privacy bill introduced in 107th Congress. H.R. 89, 107th Cong. (2001). The bill would require the FTC to draft regulations to protect the online privacy of personal information collected from users whom the Children's Online Privacy Protection Act of 1998 (COPPA) does not cover. H.R. 89, § 502. COPPA protects children under 12 and makes it "unlawful for an operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed." 15 U.S.C. § 6502(a)(1) (2000). House Bill 89 has been referred to the House Committee on Commerce. *See also* Robert MacMillan, *ISP Shield Bill, House Tech Measures Debut*, NEWSBYTES (Jan. 4, 2001), *at* http://www.newsbytes.com/news/01/160051.html.

In a speech, the Chairman of the Senate Democratic Privacy Task Force, Senator Leahy, summarized the "failure" of the 106th Congress to address the privacy rights of Americans. 146 CONG. REC. S11,777 (daily ed. Dec. 14, 2000). He cited the Democratic Senators who have sponsored privacy legislation in Congress: Senators Boxer, Breaux, Bryan, Byrd, Cleland, Daschle, Dorgan, Dodd, Durbin, Edwards, Feinstein, Feingold, Harkin, Hollings, Inouye, Johnson, Kennedy, Kohl, Lautenberg, Mikulski, Murray, Robb, Rockefeller, Sarbanes, Schumer, Torricelli, and Wellstone. *Id.*

However, he named the Republican majority responsible for the failure to get any privacy legislation enacted, particularly in the areas of online medical and financial information. *Id.* More specifically, Leahy described his proposed bill, the Electronic Rights for the 21st Century Act, Senate Bill 854, as an example of legislation that went "nowhere." *Id*. at S11,778. This bill would have prevented disclosure of internet service providers' subscriber information without their permission. *Id.*

In his speech, Leahy also described the failed effort of various bills that aimed to protect financial and medical information. *Id.* For example, the Financial Information Privacy and Security Act of 1999, Senate Bill 1924, would have provided privacy protection for personal financial information by codifying the principles of notice, accuracy, and consent. *Id.* The Financial Information Privacy Protection Act of 2000, Senate Bill 2513, which the Clinton Administration proposed, would have given consumer[s] more control over the collection and use of their financial and health-related information by financial institutions. *Id*. at S11,779.

In addition to financial privacy bills, he described how various bills that aimed to protect the privacy of medical records also failed. *Id.* Among these proposals were, first, Senate Bill 573, the Medical Information Privacy and Security Act, which would ensure the protection of personally identifiable health information and, second, an amendment to the FY 2001 Labor HHS Appropriations bill to prevent insurance companies and employers from using personal genetic information to discriminate against individuals or raise their insurance rates. *Id.*

Leahy concluded with his ambitions for the 107th Congress:

> It is my hope that we put partisan politics aside in the 107th Congress and take a hard look at how we can and should protect the fundamental right of privacy in the 21st Century. As each day passes, new financial services, new online services, and new medical data bases are taking shape and institutional practices employing these new technologies are taking root. Unless we decide that privacy is worth protecting—and soon—the erosion of our privacy rights will become irreversible.

Id.

82. S. 2928, 106th Cong. (2000).

83. *Id*.

84. *Id.* The Republican sponsor is Senator McCain; the Democratic co-sponsors are Senator Boxer from California and Senator Kerry from Massachusetts. The Republican co-sponsor is Senator Abraham from Michigan. *Id.*

notice, consent, security, and enforcement, although it does not specifically enumerate them as such.[85]

The bill devotes an entire subsection to describing the requirements for a Web site's statement on notice.[86] This subsection requires that Web sites notify consumers of the ways users may choose not to have their personal information used, thereby adopting an opt-out standard.[87] The FTC would be responsible for enforcement of the Act, and violations would be treated as violations of a rule defining an unfair or deceptive trade practice.[88] The relevant sentence of Section 5 of the FTC Act reads as follows: "Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are declared unlawful."[89] Guided by case law, the FTC has identified the following three factors that it considers when applying the prohibition against consumer unfairness: (1) whether the practice injures consumers; (2) whether it violates established public policy; (3) whether it is unethical or unscrupulous.[90] The Supreme Court quoted these factors with approval in the 1972 case of *Sperry v. Hutchinson*.[91] Since then, the Commission has continued to refine the standard of unfairness in its cases and rules.[92]

---

85. *See id.* (a bill "to protect the privacy of consumers who use the Internet").

86. Senate Bill 2928 section 2(b)(1) states the following:

> In general . . . notice consists of a statement that informs a user of a website of the following:
>
> (A) The identity of the operator of the website and of any third party the operator knowingly permits to collect personally identifiable information from users through the website . . . .
>
> (B) A list of the types of personally identifiable information that may be collected online . . . .
>
> (C) A description of how the operator uses such information, including a statement as to whether the information may be sold, distributed, disclosed, or otherwise made available to third parties for marketing purposes.
>
> (D) A description of the categories of potential recipients of any such personally identifiable information.
>
> (E) Whether the user is required to provide personally identifiable information in order to use the website . . . .
>
> (F) A general description of what steps the operator takes to protect the security of personally identifiable information collected online . . . .
>
> (G) A description of the means by which a user may elect not to have the user's personally identifiable information used by the operator for marketing purposes or sold, distributed, disclosed, or otherwise made available to a third party . . . .

Id.

87. *Id.* § 2(b)(1)(G).

88. *Id*. § 3.

89. 15 U.S.C. 45(1)(1) (1994).

90. *FTC Policy Statement on Unfairness* (Dec. 17, 1980), *available at* http://www.ftc.gov/bcp/policystmt/ad-unfair.htm.

91. *Id*.

92. *Id*.

2. The Consumer Privacy Protection Act[93]

The Consumer Privacy Protection Act[94] has a Democratic sponsor, ten Democratic co-sponsors, and no Republican co-sponsors.[95] The bill lists various congressional findings including the following: industry self-regulation schemes, which are not enforceable, do not provide sufficient consumer protection; establishing personal privacy rights and industry obligations is important in order to boost consumer confidence in the Internet; and the ease of collecting and using personal information on the Internet is becoming increasingly efficient and easy.[96] The bill attempts to regulate online consumer privacy of personal information,[97] as well as individual privacy in the offline marketplace for consumers of books and recorded music[98] and for subscribers of satellite television services.[99]

The online privacy section of the bill (Title I) more or less codifies the notice, consent, access, and security requirements of the FTC's fair information practice principles.[100] It requires that Web sites obtain a user's

93. S. 2606, 106th Cong. (2000).

94. *Id.*

95. *Id.* The Democratic sponsor is Senator Hollings from South Carolina. The ten Democratic co-sponsors are: Senator Breaux from Louisiana, Senator Cleland from Georgia, Senator Feingold from Wisconsin, Senator Rockefeller from West Virginia, Senator Bryan from Nevada, Senator Durbin from Illinois, Senator Inouye from Hawaii, Senator Byrd from West Virginia, Senator Edwards from North Carolina, and Senator Kerrey from Nebraska.

96. *Id.* § 2.

97. *Id.* at tit. I.

98. *Id.* at tit. II.

99. *Id.* at tit. IV.

100. S. 2606 tit. I, § 102 (2000), states the following:

> (a) Notice.—An Internet service provider, online service provider, or operator of a commercial website may not collect personally identifiable information from a user of that service or website unless that provider or operator gives clear and conspicuous notice in a manner reasonably calculated to provide actual notice to any user . . . that personally identifiable information may be collected from that user. The notice shall disclose—
>
> (1) the specific information that will be collected;
>
> (2) the methods of collecting and using the information collected; and
>
> (3) all disclosure practices of that provider or operator for personally identifiable information so collected, including whether it will be disclosed to third parties.
>
> (b) Consent.—An Internet service provider, online service provider, or operator of a commercial website may not—
>
> (1) collect personally identifiable information from a user of that service or website, or
>
> (2) . . . disclose or otherwise use such information about a user of that service or website, unless the provider or operator obtains that user's affirmative consent, in advance, to the collection and disclosure or use of that information.
>
> (c) Access.—An Internet service provider, online service provider, or operator of a commercial website shall—
>
> (1) upon request provide reasonable access to a user to personally identifiable information

"affirmative consent" prior to collecting or using personal information, which is the equivalent of adopting an opt-in standard.[101] The FTC would enforce the Act, treating violations as unfair or deceptive trade practices.[102]

C. The FTC: Self-Regulation and Federal Regulation

Since 1995, the FTC has been investigating online privacy issues, in part through the use of privacy surveys.[103] In its 1998 and 1999 reports to Congress, the Commission described the fair information practice principles and called for industry efforts to implement them.[104]

However, based on the results of its 2000 Survey, which examined the information practices of a large number of U.S. commercial sites on the World Wide Web, the FTC decided to expand its recommendation to include the enactment of legislation to ensure the protection of online consumer privacy.[105] While praising industry self-regulatory initiatives and encouraging the industry to continue them in its May 2000 report to Congress, the Commission concluded that self-regulation was insufficient.[106]

---

that the provider or operator has collected . . .

(2) provide a reasonable opportunity for a user to correct, delete, or supplement any such information . . . and

(3) make the correction or supplementary information a part of that user's personally identifiable information for all future disclosure . . .

(d) Security.—An Internet service provider, online

service provider, or operator of a commercial website shall establish and maintain reasonable procedures necessary to protect the security, confidentiality, and integrity of personally identifiable information maintained by that provider or operator . . . .

Id. at tit. I, § 102.

101. *Id.* § 102(b)(2).

102. *Id.* at tit. III, § 302(a).

103. PRIVACY ONLINE, *supra* note 26. *See generally* Roscoe B. Starek, III & Lynda M. Rozell, *A Cyberspace Perspective: The Federal Trade Commission's Commitment to On-line Consumer Protection*, 15 J. MARSHALL J. COMPUTER & INFO. L. 679 (1997) (describing the FTC's commitment to enforcement of its consumer protection statutes online).

104. PRIVACY ONLINE, *supra* note 26.

105. *Id*. at 36.

106. *Id*. at ii. The FTC's 2000 Survey examined two groups of Web sites: (1) a random sample of 335 Web sites and (2) 91 of the 100 business sites. *Id.* The results show that 97% of the random sites and 99% of the busiest sites collect an e-mail address or some other piece of personal identifying information. *Id.* In addition, the survey found that only 20% of the random sites and 42% of the busiest sites implement, at least in part, all four fair information practice principles. *Id*. Moreover, while most sites allow the placement of cookies by third parties, the majority of sites do not disclose this fact to consumers. *Id.* at 7.

The FTC's proposed legislation would codify the fair information practice principles and give an implementing agency the authority to promulgate more detailed rules and enforce them.[107]

D. Other Approaches

1. The European Rights-Based Approach

Many advocates of online consumer privacy regulation recommend that the United States follow the lead of European Union (EU) countries, many of which have adopted comprehensive privacy and data protection laws.[108] The EU enacted two directives providing citizens with protections from abuses of personal information and required each EU state to enact analogous legislation.[109]

The European Telecommunications Directive and the European Data Protection Directive, enacted in 1998, set forth the privacy rights of consumers.[110] These rights include: the right to know where the data originated, the right to have inaccurate data changed, the right to recourse if unlawful data processing occurs, and the right to opt-out of allowing the use of the data.[111] Under these directives, every EU country will have a Privacy Commissioner or agency that enforces these rights.[112] Furthermore, the directives prohibit the collection and use of personal information about EU citizens outside of the EU to countries that are not in compliance with EU privacy protection laws.[113]

2. Market-Based Approaches

On the other side of the spectrum are those who oppose any regulation of cyberspace.[114] The proponents of a market-based approach believe that regulation leads to inefficiency and prevents the growth of online commerce,

---

107. *Id*. at 36.

108. *See* David Banisar & Simon Davies, *Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments*, 18 J. MARSHALL J. COMPUTER & INFO. L. 1, 10-13 (1999).

109. *Id*.

110. *Id*.

111. *Id*. at 12.

112. *Id*.

113. David Bender & Danice M. Kowalczyk, *Avoiding Intellectual Trespass in the Global Marketplace: Encryption & Privacy in E-Commerce*, 5 VA. J.L. & TECH. 2 (2000), *available at* http://www.vjolt.net/vol5/symp2000/v5i1a2-Bender_kowalczyk.html.

114. *See generally* Safier, *supra* note 6, ¶ 124.

the growth of the direct marketing industry, and the development of cyberspace.[115]

The "privacy market opportunists" support the development of markets in personal data through the transfer of ownership or property rights in personal data from those who collect data off a Web site to the data subjects themselves.[116] For example, consumers conducting transactions online with Web sites would exchange their information for money or credit for other online goods and services.[117]

The World Wide Web Consortium (W3C) has also developed a market-based approach called the Platform for Privacy Preferences (P3P), a project that enables the marketplace to give users more control over their personal information.[118] P3P involves the development and delivery of software tools and services that give users knowledge of Web sites' information practices.[119] After users have selected their privacy preferences in their browser, it will only enter Web sites that have privacy policies that meet these preferences.[120]

A third market-based approach is simply to use specific software programs to prevent Web sites from collecting and using personal data.[121] For example, software programs such as anonymous browsing services keep your identity concealed,[122] while cookie managers identify and block specific

---

115. *Id*. ¶¶ 124-26.

116. Belgum, *supra* note 10, ¶¶ 39-54.

117. *Id*. ¶ 43. *See also* Pamela Samuelson, *Book Review: A New Kind of Privacy? Regulating Uses of Personal Data in the Global Information Economy*, 87 CAL. L. REV. 751 (1999) (discussing how economists recommend granting property right to individuals in their personal information to solve the data privacy problem).

118. *Online Privacy: Hearing Before the US Senate Commerce Comm.*, 106th Cong. (2000) (statement of Daniel J. Weitzner, Technology and Society Domain Leader, World Wide Web Consortium), *available at* http://www.w3.org/2000/05/25-Senate-Privacy-Testimony.html. *See also* Safier, *supra* note 6, at 28-30.

119. *Id. See also* Neil Weinstock Netanel, *Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory*, 88 CAL. L. REV. 395, 478-80 (2000).

120. *Id*. The author describes this result of P3P as "machine-to machine communication and possibly, negotiation, without a person getting involved at either end." *Id.* at 479.

121. For a comprehensive review of software products that thwart the online collection of personal information, see Graven, *supra* note 32, at 153.

122. Anonymous browsing services offer a wide variety of levels of security, convenience, and cost. *Id.* at 152-55. For example, some retrieve pages from remote sites and send them to your browser without revealing your identity. However, they do not conceal the page itself or your URL from your network administrator (see *infra* note 29 for a definition of URL). *Id.* at 152-55. Other anonymous browsing services conceal URLs from your Internet Service Provider (ISP) or network administrator, but don't protect the content of the pages you viewed. *Id.* Services that provide the tightest security actually encrypt the URL and page data. *Id.* Some encrypt only HTTP data, while others encrypt data transferred through FTP, like a software download. *Id.*

The following are anonymous browsing services: SafeWeb (www.safeweb.com) encrypts all HTTP data and is free; IDzap (www.idzap.com) conceals your identity from remote sites through

types of cookies.[123]

3. An Approach Combining Law and Technology

Another proposed solution to the problem of online profiling of personal information combines support for the development of technology such as P3P with government backing of this technology.[124] This solution entails the government supporting a property regime in which individuals' personal information is viewed as property over which they have control, and before it can be transferred or taken, negotiation must take place.[125]

4. Common Law Tort Protection

Another approach to protecting online personal information is to sue transgressors for violating the common law tort doctrine of invasion of privacy.[126] In a famous law review article, Samuel D. Warren and Louis Brandeis define the right to a zone of privacy, including "the right to be let alone," that would protect against private party intrusion.[127] Professor

---

IDzap's servers, which act as a proxy between a user's PC and the remote site; IDsecure, which costs $15 every three months or $50 a year, encrypts all traffic to and from a user's PC and supports all browsers but only HTTP protocol; Anonymizer.com offers various packages, including a basic free proxy-style service and a more secure service for $14.99 every three months, which can encrypt cookies and URLs but not the content of data; Subdimension (www.subdimension.com), a free service that conceals URLs, but not page titles; Zero-Knowledge System's Freedom (www.zeroknowledge.com) is $49.95 per year for five anonymous identities, provides an encrypted connection, and allows a user to browse using an anonymous identity; and Privada-Control (www.privada.com) is $5 a month and installs an application on a user's PC that directs Web traffic to and from a user's browser through Privada's servers, thereby concealing a user's identity. *Id.* at 152-55.

123. Cookies either engage in user profiling, "monitor a Web site's usability," or track a user's surfing habits. *Id.* at 157. Some cookie management programs can target specific kinds of cookies and block them. *Id.* at 158.

The following are cookie managers: McAfee Internet Privacy Service (www.mcafee-at-home.com) and Symantec's Norton Internet Security 2001 block all advertiser cookies and create lists of sites from which a user can decide to accept or reject cookies for $69.95 a year and $71.35 a year respectively; IDcide's Privacy Companions (www.idcide.com), which can be downloaded for free, blocks cookies that track users' surfing habits and notifies users when sites attempt to gather such information; Limit Software's Cookie Crusher 2.6 (www.thelimitsoft.com) and Kookaburra Software's Cookie Pal (www.kburra.com), which cost $15 each, let a user view the Web site issuing the cookie and allow a user to set preferences for accepting or rejecting cookies from sites. *Id.* at 157-58.

124. Lessig, *supra* note 42, at 159-62.

125. *Id. Cf.* Mark Rotenberg, *What Larry Doesn't Get: Fair Information Practices and the Architecture of Privacy*, 2001 STAN. TECH. L. REV. 1 (forthcoming), *available at http://stlr.stanford.edu/stlr/articles/o1_stlr_1/index.htm.*

126. Safier, *supra* note 6, ¶ 101.

127. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890).

William Prosser has divided the common law tort doctrine of invasion of privacy into four categories: (1) intrusion upon the plaintiff's seclusion or solitude, or into his private affairs; (2) the public disclosure of private facts; (3) false light privacy; and (4) the misappropriation of one's name and likeness for commercial purposes.[128]

III. ANALYSIS OF THE PROPOSED SOLUTIONS

The purpose of many of the FTC lawsuits discussed in Part I was to address the unfairness of misrepresenting the degree to which these online companies were protecting the privacy of their customers' personal information.[129] A major consequence of such misrepresentation is that consumers are not only unaware that they are being profiled, they are unaware of the purposes and effects of being profiled.[130] For example, DoubleClick's profiling activities would have boosted its "targeted" online advertisements (and those of the third party to which they were sold in the case of Geocities).[131] Additionally, DoubleClick (and Toysmart) could have sold the information to direct marketers, health organizations, insurance companies, credit agencies, or other third parties desiring the information.[132]

Targeted advertising and direct marketing based on the profiling of online personal information can lead to discrimination.[133] While targeted advertising may be viewed as positive discrimination by feeding a consumer his or her own preferences,[134] it also has adverse discriminatory and harmful effects.[135]

---

128. William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960).

129. Killingsworth, *supra* note 10, at 60-61; Greenberg, *supra* note 44; Singletary, *supra* note 52.

130. *See generally* OSCAR H. GANDY, JR., THE PANOPTIC SORT: A POLITICAL ECONOMY OF PERSONAL INFORMATION 207-08 (1993).

131. Greenberg, *supra* note 44.

132. *Id*.

133. *See* GANDY, *supra* note 130, at 80-81 ("The panoptic sort, which depends on ready access to personal information ... is ... a discriminatory technology"); Gandy, *supra* note 9, at 78-79 ("[I]nformation about our status, choices, and communication behavior often forms the basis for differentiation, and such difference forms the basis for discrimination .... my concern about ... privacy in cyberspace is fundamentally a concern with discrimination."). *See also* Belgum, *supra* note 10, ¶ 31 ("Statistically-generated profiles may mask old-fashioned race prejudice or other illicit biases which are explicitly ruled out of order on grounds of public policy").

134. *See* LESSIG, *supra* note 42, at 153 ("[P]roducts are matched to people, and interests to people .... This is discrimination, no doubt, but not the discrimination of Jim Crow. It is the wonderful sort of discrimination that spares me Nike ads."). Despite the convenience and appeal of such personalization, any Web user with a basic amount of technical skill can seek his or her own interests resources on his or her own, without having any personal data collected.

135. *Id.* at 154-56.

> [P]rofiling raises a more sustained collective concern about how it might affect a community. That concern is about manipulation .... The system watches what you ... it fits you into a pattern .... A second concern is about equality .... An efficient and effective system for monitoring makes it

For example, poorer sectors of the population can be excluded and underrepresented in such advertising campaigns because they are based on past purchasing patterns.[136] In addition, companies may decide not to solicit or offer promotions to particular individuals because their profiles categorize them with others who might be credit risks or have lower estimated customer potential, effectively denying them access to particular products or services.[137]

---

possible . . . to make these subtle distinctions of rank.

Id.

136. *See* Gandy, *supra* note 9, at 89-91.

137. *See* GANDY, *supra* note 130, at 130. In *Lake v. Kozmo.com Inc.*, No. 00-00815, plaintiffs alleged that a dot-com was engaging in "online redlining" by not delivering to predominantly African-American neighborhoods (based on zip code) in Washington, D.C. *Id.* This case deals with the issue of substantive discrimination, rather than the discriminatory effects of online profiling (the plaintiffs knew why Kozmo.com first asked users for their zip code on its Web site—to determine whether it delivers there) and is therefore distinguishable. *Id.* Nevertheless, the case provides an idea of the kind of discrimination that could potentially result from the online collection and use of personal information. *See* Kate Marquess, *Redline May Be Going Online*, A.B.A. J., Aug. 2000, at 80; Kenneth Li & Bernhard Warner, *Bad Timing for Kozmo.com's Bad Press*, THE INDUSTRY STANDARD (Apr. 14, 2000), *available at* http://www.thestandard.com/article/display/0,1151,14163,00.html; Michelle Goldberg, *Racial Redlining at Kozmo.com?*, THE INDUSTRY STANDARD (Apr. 14, 2000), *available at* http://www.thestandard.com/article/display/0,1151,14120,00.html. On December 5, 2000, Kozmo settled with the Equal Rights Center for $125,000, which will go toward "bridging the digital divide." In addition, Kozmo recently began service in several new D.C. zip codes. *Kozmo Settles*, THE LEGAL TIMES, Dec. 11, 2000, at 3.

Businesses can use zip codes to determine where consumers live in order to engage in targeted marketing. For example, an online business selling airline tickets might target the users on surf.com who live in Hawaii in order to offer them special flight deals to surf competitions on the islands. Online marketing and targeted advertising, however, can be difficult to distinguish from redlining.

In addition to redlining based on zip codes, businesses engage in this practice when they choose not to sell or market their products to consumers, or hire individuals, based on other demographic information such as race or income, genetic information, and other financial or medical information. This information can be collected traditionally in real space or online in cyberspace.

> For example, businesses could recognize zip codes from low-income areas and choose not to advertise to these groups or could make decisions about an individual's insurance policy based on information they collect about them on the Internet. These types of discriminatory uses of individuals' personal information would limit autonomy.

See Basho, *supra* note 1, at 1544.

A hypothetical situation of redlining by an auto insurance company would be if it rated customers by the zip code in which they reside. MICHAEL ASIMOW ET AL., STATE AND FEDERAL ADMINISTRATIVE LAW 223 (2d ed. 1998). This redlining may be evident in the fact that insurance in some neighborhoods is more expensive or less available than in other neighborhoods. *Id.*

Another example of the kind of discrimination that may result from a lack of online privacy is that which is based on sensitive health information about an individual that may be directly collected on the Internet, or inferred from a user's online surfing habits or clickstream data. For example, the human genome project has facilitated genetic discrimination since the knowledge gained from the project will allow physicians to detect more diseases and predispositions for diseases through a range of genetic tests. As a result, more information about an individual's medical background will be available and the demand for such information will extend to employers, health and life insurers, and law enforcement agencies. COUNCIL ON ETHICAL AND JUDICIAL AFFAIRS, AMERICAN MEDICAL

A. Self-Regulation

The e-commerce industry's efforts to govern the online collection and use of personal information among its own ranks are evident in improved statistics regarding privacy initiatives.[138] In its 1998 Report, the FTC reported that although 92% of the Web sites surveyed in a random sample were collecting "great amounts" of personal information from consumers, only 14% of them disclosed anything at all about their information practices.[139] In contrast, its 2000 Survey results showed that 88% of the Web sites surveyed in a random sample posted at least one privacy disclosure.[140] Moreover, the industry has developed online seal programs to enforce certain fair information practice principles.[141] Notwithstanding these improvements, industry self-regulation remains insufficient to protect online consumer privacy for several reasons.

First, the self-regulatory programs are not broad-based or widespread enough.[142] In the FTC's 2000 Survey, only 20% of the Web sites in a random sample implement to some extent all four fair information practices in their privacy policy disclosures.[143] In addition, only 41% meet the standards for notice and choice.[144] Finally, the entire industry does not comply with self-regulation initiatives.[145] For example, only 90% of the network advertising

---

ASSOCIATION, *Use of Genetic Testing by Employers*, JAMA, Oct. 2, 1991, at 1827.

In a study that was part of the Human Genome Education Model (HuGEM) Project of the Georgetown University Child Development Center and the Alliance of Genetic Support Groups conducted in 1996, the following findings were made: in a survey of 332 members of genetic support groups with one or more of 101 different genetic disorders in the family, 25% of the respondents or affected family members believed they were denied life insurance; 22% believed they were denied health insurance; and 13% believed they were terminated from employment. E. Virginia Lapham et al., *Genetic Discrimination: Perspectives of Consumers*, SCIENCE, Oct. 25, 1996, at 621. In addition, fear of discrimination based on genetic information resulted in 18% not revealing such information to insurers and 17% not informing their employers of such information. *Id.*

For general background on genetic discrimination, see Karen Rothenberg et al., *Genetic Information and the Workplace: Legislative Approaches and Policy Challenges*, SCIENCE, Mar. 21, 1997, at 1755; Marvin R. Natowicz, *Genetic Discrimination and the Law*, 50 AM. J. HUM. GENET. 465 (1992); Lisa N. Geller et al., *Individual, Family, and Societal Dimensions of Genetic Discrimination: Case Study Analysis*, 2 SCI. & ENGINEERING ETHICS 71 (1996). I would like to express my gratitude to Professor Pauline Kim, Professor of Law at Washington University School of Law, who provided me with these articles on genetic discrimination.

138. PRIVACY ONLINE, *supra* note 26.
139. *Id.* at i.
140. *Id.* at ii.
141. *See* Reidenberg, *supra* note 59, at 778.
142. *See* PRIVACY ONLINE, *supra* note 26.
143. *Id.* at 13.
144. *Id.*
145. *Id. See also* Dembeck & Hampton, *supra* note 73.

industry is a member of the Network Advertising Initiative.[146] Thus, the remaining 10% can only be compelled to adhere to the fair information practice principles through legislation.[147]

Secondly, self-regulation has not resulted in large-scale enforcement of the implementation of fair information principles.[148] While the online privacy seal programs have been adopted, and the number of sites enrolled in these programs has increased over the last year, they still have not established a widespread presence.[149] The FTC's 2000 Survey showed that only 8% of Web sites in a random sample display a privacy seal.[150] Moreover, as discussed in Part II many companies that have privacy policies or seals, including Amazon, Doubleclick, Toysmart, and Geocities, have changed or breached their policies. Furthermore, TRUSTe, one of the major online privacy seal programs discussed in Part II.A, was recently caught violating its own privacy policy in August 2000 through the use of a third-party software program.[151]

Third, self-imposed limits by the industry on online collection of certain kinds of "sensitive" personal information, such as their financial background or medical history, is an ineffective method of protecting online consumer privacy.[152] Web site operators and third parties, such as network advertisers, can gather similar information, such as online shopping habits, through tracking a user's clickstream, from which they can infer sensitive personal information.[153]

---

146. Dembeck & Hampton, *supra* note 73.

147. *Id*.

148. PRIVACY ONLINE, *supra* note 26, at ii.

149. *Id*.

150. *Id*.

151. Keith Regan, *TRUSTe Stung by Own Privacy Gaffe*, E-COMMERCE TIMES (Aug. 25, 2000), *at* http://www.ecommercetimes.com/news/articles2000/000825-3.shtml.

152. *See* Dembeck & Hampton, *supra* note 73 (noting that NAI companies agreed not to use consumers' medical or financial information for marketing purposes and not to use Social Security numbers or gender for profiling).

153. *See* GANDY, *supra* note 130, at 200. The author discusses Richard Posner's analysis of privacy rights:

> Posner concludes, with some insight, that the ban on discrimination by race or gender will have little effect so long as those who wish to discriminate can identify correlates of race and gender that predict mean performance just as well. It is this insight, that the panoptic sort is capable of finding analogues or indexes that serve the same funct ion as more politically or socially sensitive indicators, that weakens the long-term utility of any definition of classes of information as being more or less sensitive.

Id.

B. Pending Legislation

Pending legislation would at least ensure a baseline of online consumer privacy protection, which self-regulation is currently failing to do. Among the concerns with online profiles that the Consumer Internet Privacy Enhancement Act and the Consumer Privacy Protection Act do address, through essentially a codification of some of the fair information practice principles, are the following: the general invasion of privacy or loss of control over personal information; receiving undesirable solicitations or junk mail; and the existence of false or inaccurate information in profiles.[154]

However, a major negative consequence of online profiling that pending legislation does not address is the potential for adverse discrimination.[155] Because pending legislation does not consider the fair information practice principles that actually limit the collection, storage, and use of personal information (such as the principles of necessity, minimization, and finality), it does not adequately target the issue of discrimination.[156]

The Consumer Internet Privacy Enhancement Act provides a requirement that a Web site's privacy policy describe the means by which a user may prevent his or her personally identifiable information from being used in certain ways or transferred to a third party.[157] Therefore, it seems to adopt an opt-out standard, putting the burden on the consumer to affirmatively notify the Web site operator that the consumer wishes to limit the uses of the consumer's personal information.[158]

Under this proposed legislation, if an operator requires a user to opt-out, it benefits from the fact that a user's information can be used or collected automatically until or unless the user affirmatively elects not to have it

154. *See* GANDY, *supra* note 130, at 129-30 (discussing some of the results of five group interviews conducted in summer 1998 to assess individuals' thoughts on privacy, particularly their view of legitimate uses of profiles as well as the problems they associate with them).

155. *Id*. The author cites the example moderators gave the participants in an interview: a woman whose credit card application was rejected because her profile indicated she was an English major. *Id.* Participants criticized the impersonal nature of profiling. *Id.* For example, insurance companies use information, such as your age and gender, to decide your insurance premiums. Decisions are based on statistics, not on the particular individual. *Id.*

156. *Id*. at 223. The author discusses David Flaherty's twelve principles, which apply to the government's use and collection of personal information. *Id.* He thinks these principles should be applied to the private sector as well. *Id. See also* Reidenberg, *supra* note 59, at 779 (criticizing self-regulatory initiatives and the insufficiency of notice and consent in solving online consumer privacy issues). The author states that the self-regulatory and executive branch approach "seriously misconstrue basic fair information practices principles. These basic principles include key standards, such as purpose limitations, data minimization, and duration of storage that are not satisfied merely through notice and consent; notice and consent are not enough." *Id.*

157. *See supra* note 86 and accompanying text.

158. *See supra* note 86 and accompanying text.

used.[159] Therefore, an opt-out standard requires a user to be aware of a Web site's privacy policy, savvy enough to know of its significance and ramifications, and willing to take the time and effort to opt-out.

Others users, once they become aware that they may opt-out, might immediately take advantage of the opportunity, unless the uses of their personal information are set within clearly defined limits. Perhaps users might be more willing to forgo opting out if, in addition to being given notice of the uses of the information, they are (1) made aware that the purposes of collecting the information are limited and (2) given notice of what the information will *not* be used for.[160]

Under the Consumer Privacy Protection Act, the Web site operator must set an opt-in standard, which puts the burden on the Web site operator to obtain consent before using customer information.[161] Thus, the user benefits from having his personal information not used until or unless he or she affirmatively elects or permits such use.[162]

Under an opt-in standard, users would be given a choice as to whether or not to allow the collection and use of their personal information before it is ever used. Nevertheless, should a user decide to opt-in, the user may not be fully aware or informed of the consequences of a decision to allow such disclosure[163]—particularly if the notice of why and how the information is used and with whom it may be shared is described solely in affirmative terms.[164] Again, perhaps these users would weigh the benefits of opting in more heavily, and to the Web site operator's advantage, if in addition to being notified about what their personally identifiable information might be used for, they were also (1) given assurances that the purposes for collecting their information are limited and (2) given notice as to the purpose for which their information will *not* be used.[165]

---

159. *See supra* note 86 and accompanying text.

160. Such transparency in a privacy policy would also allow consumers to be in a better position to make choices and improve the ability of market forces to promote privacy protection. *See* John D. Feerick, 11 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 6, at 13 (2000) (describing the need to enact statutes that require businesses to articulate with clarity and transparency what their privacy policies are going to be in order to promote consumer choice and prevent market failure).

161. *See supra* note 101 and accompanying text.

162. *See supra* note 101 and accompanying text.

163. *See* GANDY, *supra* note 130, at 207.

164. *See* Feerick, *supra* note 160.

165. *Id.* at 14.

C. The FTC

The FTC approach of combining the continued encouragement of self-regulatory initiatives with its proposed legislation to codify its fair information principles would require a *minimum* threshold of consumer data protection from *all* Web site operators,[166] which would provide greater privacy protection than the status quo. However, like other pending legislation, the FTC approach fails to address the issue of preventing the discriminatory and harmful effects of the use and collection of personal information.

Codifying notice, consent, security, and enforcement does not put enough limits on what a Web site operator may choose to do with your information.[167] A Web site operator's notice and a user's ability to consent to the collection or use of personal data still leaves certain loopholes open. Users may not be aware of the risks to their online privacy, let alone aware of an operator's notice or knowledgeable enough to make an informed decision about whether or not to opt-in or opt-out.[168]

D. Other Approaches

1. The European Rights-Based Approach

At a minimum, the European Data Protection Directive codifies four fair information practice principles, which bear some resemblance to the FTC's principles.[169] Proponents of this European Directive think that the United States should look to it as a model for stronger data protection legislation in the United States.[170] The European approach protects Internet users from certain abuses of personal data and tries to target the potential for the discriminatory or harmful uses of such information. The sensitive data norms contained in the European Data Protection Directive come closest to

166. *See supra* notes 99-100 and accompanying text.

167. *See supra* notes 62-67 and accompanying text.

168. *See infra* notes 225-26 and accompanying text.

169. *See* Samuelson, *supra* note 117. The four elements of the European approach, according to Paul M. Schwartz and Joel R. Reidenberg, authors of *Data Privacy Law: A Study of United States Data Protection*, are: (1) data collection norms; (2) a right for individuals to review information collected about them; (3) sensitive data norms; and (4) enforcement norms. *Id.* at 763.

170. *Id. at* 763-68. According to Samuelson, Schwartz and Reidenberg sympathize with European norms and argue for establishing data privacy rights. *Id.* They explain that the online collection and use of personal data is a privacy issue because people who disclose information to others about themselves for a particular purpose expect their disclosures to have been made under an implied agreement to use that data only for that purpose. *Id.* at 767.

addressing this concern.[171]

In contrast, critics who take a utilitarian approach to data protection criticize the Directive as being too broad.[172] They argue that in the spirit of economic self-interest and free trade, Web site operators should be able to benefit from the use of personal information or the fee they obtain from selling such information.[173] Furthermore, they argue that the European approach inhibits innovation and impedes the flow of routine data within transnational corporations.[174]

Moreover, even if limitations on the collection of sensitive information exist in the Directive, Web site operators and third parties, such as network advertisers, can gather similar information through tracking a user's clickstream, from which sensitive personal information can be inferred.[175]

2. Market-Based Approaches

Several market-based schemes propose to deal with the privacy implications of online collection and use of personal data. Many economists recommend granting individuals property rights in their personal information to solve the data privacy problem.[176] If individuals "owned" their information, as they own real property, they could convey their preferences to the market by charging high prices for their data if they value privacy highly or vice-versa.[177] A licensing scheme would allow an Internet user to retain ownership of his or her information and grant a company permission to use it through a license.[178] Such a scheme would allow consumers to control

171. *Id.* at 763.

172. *See id.* In this book review, the author reviews and compares two books: *Data Privacy Law: A Study of United States Data Protection* by Paul M. Schwartz and Joel R. Reidenberg, and *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive* by Peter P. Swire and Robert E. Litan. According to Samuelson, Swire and Litan "sympathize with both positions." *Id.* at 755. They agree with the Europeans that online personal information should be protected from misuse, and think Europeans having a credible interest in ensuring that other countries are not used to avoid the effect of European laws on European individuals. *Id.*

However, Swire, and Litan also argue that the European Directive is overbroad in that even when the risk of abuse from the flow of European personal data into another country with fewer personal data protections, such as the United States, may be small, the European Directive would restrict such flow. *Id.* In addition, they claim that the Directive may be unenforceable given the global, digital nature of the network. *Id.* at 756.

173. *See id.* at 760.

174. *Id.*

175. *See* GANDY, *supra* note 153 and accompanying text.

176. *See* Samuelson, *supra* note 117, at 770-73. *See* also Basho, *supra* note 1.

177. *See* Samuelson, *supra* note 117, at 770-71.

178. *See* Basho, *supra* note 1, at 1525. The author gives the following example of a license:

> Company *X* is authorized to collect my name, address, income, and online buying habits. It may use this information to determine what products I will be most interested in buying, to make

what information businesses have access to, which businesses have access to it, how businesses use it, and what kind of compensation the consumer should receive.[179]

Although granting consumers property rights would allow them to protect themselves against online profiling, it is not the most desirable, feasible, or effective approach. First, those who view data privacy from a civil rights perspective would argue that granting individuals property rights in personal information is commodifying a civil liberty interest.[180] Second, even proponents concede that many problems could arise under such a licensing scheme.[181] A licensing system would be unmanageable and impractical for consumers and Web site operators alike in that it would involve significant transaction costs.[182] Consumers would have to make an agreement with every Web site they visit, which takes time and effort for both parties.[183] In addition, businesses could decide to deal only with those consumers willing to license their information or make the benefits of sharing personal information so enticing that consumers would decide to share almost anything.[184] Finally, certain Web site operators might not have the resources to contract with users for information.[185]

Another market-based approach to protecting online personal information is the development and use of software technology, such as the P3P software standard, which facilitates the negotiation between a user's preferences and a Web site's privacy policy.[186] Although such technology might give users greater control over their online privacy just like a licensing scheme, it does

---

> decisions about its own product development, and to send me emails about changes to this product. I grant Company *X* the right to distribute my name only to third parties with privacy policies equal to Company *X*'s until 1/1/02 and I will receive $2.00 each time my name is transferred to such a third party. After 1/1/02, Company *X* must cease all use of this information and will no longer have any rights or interest in it.

Id.

179. *Id.* at 1529.

180. *See* Samuelson, *supra* note 117, at 772. The author gathers that "[f]or those who embrace the civil rights concept of data privacy, the notion of protecting personal data by commodifying it would likely be as obnoxious as the notion of protecting the voting franchise by commodifying it." *Id.*

181. *See* Basho, *supra* note 1, at 1527-29.

182. *Id*.

183. *Id*. In order to address this problem, businesses called infomediaries, are beginning to arise. *Id*. Infomediaries, such as Lumeria, negotiate information transactions between users and Web site operators and act as brokers. *Id.* However, these infomediaries are in the development stage, therefore their success is uncertain. *Id.* at 1528.

184. *Id*.

185. *Id*. at 1529. If consumers are not permitted to access Web sites that have not accepted their license agreements because they do not have the resources to enter into these contracts, these Web sites may lose a lot of business. *Id.*

186. *See supra* Part II.D.2.

not sufficiently protect online privacy.[187] First, the W3C has not obtained enough agreement within the industry to conclude the development phase of P3P technology or find enough companies willing to implement the technology.[188] Second, the P3P solution is too complicated for most Internet users—too many "privacy preferences" will only distract consumers away from achieving the simple goal of keeping their personal information private.[189] Third, for Web site operators to encode their Web site's privacy policies in P3P format, a significant mass of Internet users will have to use it.[190] Fourth, even if P3P were universal, it would not be enforceable.[191]

Another market-based solution is to use software programs such as anonymous browsers or cookie managers to protect online privacy.[192] Many of these software packages provide a wide variety of levels of online privacy protection and cost.[193] The major weakness of this solution, however, is that it safeguards the privacy of only those consumers who are educated enough to know about these programs, are technologically savvy enough to understand and know how to use them, and can afford to purchase them.[194] In addition, users that employ these software programs may be refused certain benefits, such as personalization, a free service, or acceptance into a Web site's membership if they do not disclose personal information.[195]

3. An Approach Combining Law and Technology

This approach gives users greater control over their online privacy just like the other market-based approaches with the added advantage of the government backing the scheme.[196] However, government support of this

187. *See* Rotenberg, *supra* note 125.

188. *Id*. at 23.

189. *See* Rotenberg, *supra* note 125, at 13.

190. *See* Netanel, *supra* note 119, at 479 (noting that users who wish to use P3P will face the failure of collective action because Web site operators will prefer to lose these customers than risk the value of obtaining data from the majority of customers who don't use P3P).

191. *Id*. at 480. P3P would not prevent Web site operators from deviating from its information practices. *Id.* Netanel recommends government regulation requiring Web site operators to implement P3P and to enforce it. *Id.*

192. *See generally* Graven, *supra* note 32.

193. *See* Graven, *supra* note 32. Without software programs, such as cookie managers, most browsers accept all cookies by default. *Id.* A user can change his or her browser's security settings to accept all, reject all, or be notified each time a cookie is encountered. *Id.* However, the first option means a user's surfing habits will be monitored and tracked without limits, and this information will be resold to online marketers and advertisers; the second option means never receiving a customized Web site experience; and the third option is tiresome. *Id.*

194. For an idea of how these software programs work and their cost range, see *id.*

195. Basho, *supra* note 1, at 1524.

196. *See supra* Part II.D.3.

technology is dependent upon the other parties involved, including users and the industry.[197] As previously discussed, the W3C has neither obtained enough agreement within the industry to conclude the development phase of P3P technology nor has it found enough companies willing to implement the technology.[198] In addition, the P3P solution is too complicated for most Internet users.[199] As long as these other parties do not support the development and use of this technology, the government will be hard pressed to support it.[200]

4. Common Law Tort Protection

This approach is an insufficient way to protect online personal information because courts generally maintain a deferential negligence standard.[201] They tend to require significant personal injury before requiring transgressors to pay damages to victims.[202] If many individuals suffer harm due to the collection and use of online personal information, but each individual's harm is minimal, the value of judgment for each individual's case often prevents adjudication and settlement.[203] While a class action may be appropriate in this situation, judges will often refuse to certify these kinds of classes because each individual will suffer different injuries and damages.[204]

IV. PROPOSAL FOR A NEW STANDARD

In order to target the discriminatory and harmful effects of the online collection and use of personal information, legislation regulating online consumer privacy should replace the traditional fair information practice principles of *notice* and *consent* with the principle of *purpose* (while maintaining the other FTC principles).[205] Notice informs users how their personal information is collected and used, while consent allows users to give or deny permission of the use of their information.[206] Purpose would not do away with notice and consent; rather, it would incorporate both principles, in

197. *See supra* Part II.D.3.
198. *See* Rotenburg, *supra* note 21, at 23.
199. *Id*. at 13.
200. *See supra* Part II.D.3.
201. Safier, *supra* note 6, ¶ 108.
202. *Id*.
203. *Id*.
204. *Id*.
205. *See supra* notes 62-64 and accompanying text; Part II.A.
206. *See supra* notes 62-64 and accompanying text; Part II.A.

addition to putting minimal limits on how online personal information is collected and used.[207]

In order for a Web site operator to adopt the principle of purpose, it would have to meet the following criteria. First, it would need to limit the use of personal data (collected directly, through tracking clickstreams or through depositing cookies), for the purpose of targeted advertising, to those who opt-in.[208] Second, it would prohibit *any* internal uses of personal information that have discriminatory and harmful effects, such as price discrimination.[209] Third, it would use discretion in sharing or selling personal information with third parties. Lastly, it would expressly inform users as to the purposes for which their information will be used *as well as* the purposes for which their information will *not* be used.[210]

The following is an example of a statement in a privacy policy that would incorporate purpose:

> Personal information will *not* be used to further discriminatory and harmful ends, such as price discrimination, or sold to third parties, such as insurance companies, credit agencies,[211] or health organizations, which would use the information to further such ends. Targeted or personalized advertising *is* one purpose of the collection of personal information, but only if users choose to opt-in to this practice.[212] If personal information is sold to third parties for a fee or shared with them, discretion will be used in contracting with the third parties, and the purpose for which these third parties are using this information will be scrutinized.

Formal regulation is the best approach to targeting the discriminatory and

---

207. In the alternative, purpose could be added as a separate principle. However, since overlap exists among each principle's function it seems more reasonable to consolidate them.

208. *See* Gandy, *supra* note 9, at 128-29 (advocating a statutory requirement of fully informed, affirmative consent that favors the individual over the organization); Reidenberg, *supra* note 59, at 780 (noting how the FCC found opt-out to be an insufficient basis for the protection of personal information under the Telecommunications Act of 1996).

209. *See supra* Part I.C.1.

210. *See Feerick*, *supra* note 160, at 14.

211. Although the Fair Credit Reporting Act (FRCA) regulates "consumer reports" that "consumer reporting agencies" collect and use, it does not apply to any other kind of personal information (such as basic demographics, medical information, or personal habits or preferences) that can be collected online. The FRCA defines a consumer report as involving a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living. Fair Credit Reporting Act, 15 U.S.C. §1681a(d),(f) (2000); Interview with Michael Greenfield, Professor, Washington University School of Law, in St. Louis, Mo. (Feb. 1, 2001).

212. *See supra* note 208.

harmful effects of online profiling.[213] The FTC's 2000 Survey demonstrates that too many loopholes exist in the self-regulatory approach to effectively protect online privacy.[214] Regulation ensures that consumers are guaranteed at least a modicum of protection of their personal information, no matter which Web site they visit.[215]

Although the e-commerce industry should be able to benefit from legitimate uses of personal information, it should not be able to benefit from abuses of such information.[216] A basic level of protection should be in place for harmful or discriminatory uses of personal information collected online.[217]

As many of the proposed bills in Congress make clear, the fair information practice principles of notice and consent are crucial to protecting online privacy.[218] However, these two principles would be more effective if they were incorporated within the principle of purpose. When a Web site operator states the purposes for which it collects and uses personal information, it is putting users on *notice* as well.[219] Purpose limitations also connote that information will not be used in ways that are not *consented* to.[220] Besides being able to incorporate notions of notice and consent, purpose adds narrow limits to what a Web site operator can do with a user's personal information.

Codifying purpose in this way conveys to users that the operator is aware of these limits. Instead of merely informing them and giving them a choice, a Web site operator conveys through purpose that users will be protected from discriminatory and harmful information practices, regardless of whether or not they have notice or have given consent.

Purpose should be included in online privacy legislation in order to target the discriminatory and harmful effects of the online collection and use of personal information for several reasons. First, purpose has traditionally been

213. *See supra* Parts II.B, III.B. A major criticism of regulation comes from those who believe in the free market and believe that if the market acts rationally, it will create privacy protections. However, the market does not act rationally when consumers do not understand their choices or have a lack of information about them, resulting in market failure. One explanation for this market failure is the lack of transparency and clarity in the way that privacy policies are written. *See* Feerick, *supra* note 160.

214. *See supra* note 106 and accompanying text.

215. *See supra* Parts II.B, III.B.

216. For support of this view, see generally Belgum, *supra* note 10; Reidenberg, *supra* note 59; Safier, *supra* note 6; Gandy, *supra* note 9.

217. For support of this view, see generally Belgum, *supra* note 10; Reidenberg, *supra* note 59; Safier, *supra* note 6; Gandy, *supra* note 9.

218. *See supra* Part II.B.

219. *See supra* notes 62-64 and accompanying text.

220. *See supra* notes 62-64 and accompanying text.

articulated as a fair information practice principle. The Organization for Economic Co-operation and Development (OECD) has enumerated eight basic principles, including collection limitation, purpose specification, and use limitation.[221] In addition, scholars have identified principles such as necessity, minimization, and finality, which limit collection "to that which is necessary and relevant" and require purposes to be determined before information is collected.[222]

Second, the principle of purpose should be included in any online privacy legislation in order to circumvent partisan politics in Congress and get Republicans and Democrats to agree on common ground.[223] If the legislation focuses on targeting the harmful or discriminatory risks involved in the lack of online privacy, then it is more likely that Republicans will join forces with the Democrats.[224]

A third reason to include purpose as a principle is in order to shift the burden of protecting an individual's online privacy away from the user and onto the Web site operator.[225] The public is not knowledgeable enough about the risks to their online privacy, let alone how to protect its online privacy.[226]

---

221. Jonathan P. Cody, *Protecting Privacy over the Internet: Has the Time Come to Abandon Self-Regulation?* 48 CATH. U. L. REV. 1183, 1206 (1999). The OECD drafted its own privacy guidelines, which the United States helped negotiate and endorsed, enumerating eight basic principles: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability. *Id.* In 1998, the OECD determined that these privacy guidelines applied to protecting privacy on the Internet. *Id*. at 1207.

222. *See* GANDY, *supra* note 130, at 223 (arguing that David Flaherty's principles should apply to government actors as well as private actors). David Flaherty identifies several principles he thinks should regulate the control of personal information systems under government control including openness, necessity, minimization, finality, informed consent, controlling linkage and exchange, accuracy, access, and anonymity. DAVID FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES 380 (1989).

223. *See* 146 CONG. REC. S11,777 (daily ed. Dec. 14, 2000). In his speech evaluating efforts to enact privacy legislation during the 106th Congress, Senator Leahy criticized partisan politics:

> During this Congress, for example, instead of focusing on ways to enhance privacy safeguards, the largest number of hearings (thirteen) and innumerable briefings held by the Senate Judiciary Committee or its subcommittees were directed at dissecting the manner in which the Department of Justice handled the investigation and prosecution of certain cases involving national security-related information and campaign financing . . . . In our next Congress, it is my hope that we will not be distracted by such partisan pursuits, but that are time will be better spent on crafting privacy legislation that will make a real difference in the lives of every American.

Id.

224. *Id*.

225. *See* Gandy, *supra* note 9, at 77-80 (discussing the "growing disparity between what individuals know about the organizations whose actions influence their lives and what these organizations know about them").

226. *Id*. In a telephone survey conducted in 1994, 26% of the respondents who expressed a concern about an "interactive profiling system" were unable to indicate what bothered them about the system while 61% of those who expressed this concern identified informational privacy as the source of their concern. *Id*. at 122. In addition, 69% of the respondents agreed that it was a "bad thing" that

If users lack such knowledge, then providing them with notice and the ability to opt-in or opt-out will not protect them from harmful collection or use of their personal information.[227]

Fourth, the principle of purpose will boost overall user confidence in surfing the web, registering at Web sites, and in online shopping.[228] If users have a minimum expectation that Web site operators will be held accountable if they collect or use personal information in a way that has adverse discriminatory or harmful effects, they might decide not to opt-out or they might decide to opt-in.[229] Although purpose would be shifting the burden away from user and onto the Web site operator, it would benefit both parties.[230]

Finally, the principle of purpose should be included in online privacy legislation, as a means of preventing harmful or discriminatory effects, in order to preserve a benefit of the Internet that does not exist in real space.[231] One of the benefits of anonymity on the Internet is equality.[232] Depriving users of the right to keep their personal information (including demographics, financial and medical information, and surfing habits) private is depriving society of one of the most basic advantages of the Internet.[233]

CONCLUSION

Enacting legislation is the best approach to protecting online consumer privacy. The other approaches—self-regulation and market-based

---

information such as income level, residential area, and credit card use could be used to "offer goods and services to you." *Id.* at 123.

Moreover, because online behavior is tracked at different times and different locations, each new piece of information that is collected is added to a profile one at a time. Therefore, an online profile describes "knowledge" about behavior in probabilistic terms—making a user unable to protect his or her privacy interests. Jeffrey H. Reiman, *Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future*, 11 SANTA CLARA COMPUTER & HIGH TECH L.J. 27, 37-38 (1995).

227. *See* Reimon, *supra* note 226, at 220.

228. *See* Basho, *supra* note 1, at 1513-14. The author notes that "the market's failure to provide consumers with adequate control over their personal information undermines consumer confidence in e-commerce. Therefore, businesses can increase online commerce by creating and abiding by fair privacy policies. In fact, the Internet marketplace is beginning to realize that 'good privacy practices are good business.'" *Id.* (footnote omitted).

229. *See id.*

230. *See id.* at 1509 (contending that current American privacy laws and self-regulatory regimes do not "succeed in balancing consumers' interests in controlling uses of their information and benefiting from its disclosure with commercial entities' interest in obtaining and using that information").

231. LESSIG, *supra* note 42.

232. *See id.*

233. *Id.*

approaches—are not widespread, effective, or feasible. More specifically, this legislation must target the adverse discrimination and harmful effects that result from the online collection and use of personal information.

Although some current legislative proposals codify notice, consent, access, and security, they do not adequately target this problem. A bill that would accomplish this goal would codify the principle of purpose, incorporating the principles of notice and consent and putting limits on the uses of personal information, in order to prohibit Web site operators from using personal information towards further harmful or discriminatory ends.

Legislation that addresses a real problem that underlies the lack of online privacy will be more likely to pass muster in Congress, balance users' privacy rights against the interests of the e-commerce industry, and safeguard the equality that results from anonymity on the Internet.

Tammy Renée Daub[*]

---

* B.A. (1997), Duke University; J.D. Candidate (2002), Washington University School of Law. I would like to thank Professors Michael Greenfield, Lawrence Lessig, and Pauline Kim for their insight and assistance.