LET THE MARKET DO ITS JOB: ADVOCATING AN INTEGRATED LAISSEZ-FAIRE APPROACH TO ONLINE PROFILING REGULATION*

INTRODUCTION

Imagine that you are a consumer who not only watches Warner Brothers movies through the Time Warner cable box, but also surfs the Internet on America Online ("AOL") and subscribes to magazines published by Time Inc. While you enjoy receiving offers about new products and services tailored to your particular interests through your AOL email account, you do not know much about the information collection practices of the newly created media giant AOL-Time Warner, Inc. More importantly, you are "afraid of the unknown" and, more precisely, of the company pooling the information collected about you into a very detailed profile that includes your home address, credit card number, personal tastes in books and movies, shopping habits and more.[1]

Advances in computer technology and increased consolidation in the media and Internet industries make it possible for such detailed personal information to be collected and shared more easily than ever before.[2] This provides many benefits to society and individual consumers alike. For example, it is easier for both law enforcement to track down criminals and banks to prevent fraud. For individuals, it is easier to learn about new products and services, allowing better-informed consumer purchasing decisions.[3] Further, these technological advances are beneficial to the economy in general because they allow companies to increase earnings and facilitate efficient distribution of goods by targeting advertisements to a specific consumer market that has expressed a desire for the advertised product (as shown by their informational

* An earlier version of this note was awarded First Place in the 2002 Computer Law Association Information Technology Law Writing Competition.

1 *See generally* Marilyn Geewax, *Public Anger Growing Over Net Privacy Issues*, ATLANTA J. & CONST., Mar. 4, 2001, at G1.

2 *See* Stephanie Geraci, *Privacy in 2000: The Year in Review*, E-COM., Jan. 2001 (discussing DoubleClick's now defunct plan to merge with Abacus Direct Corp. and use cookies to link data collected online with consumer names and addresses collected off-line); *see also* Julie Tuan, *Annual Review of Law and Technology III*, 15 BERKELEY TECH. L.J. 353 (2000) (explaining that advances in technology combined with "convergence and mega mergers" make it possible that "information generated from seemingly different sources may end up in the hands of a single corporate giant.").

3 *See Federal Trade Commission: Privacy Initiatives, at* http://www.ftc.gov/privacy/index.html (last visited Mar. 8, 2002).

profile).[4]

The greatest developments in data collection occur on the Internet, where newly developed technology tools allow online companies to pool vast amounts of consumer data and track consumer movement online.[5] As these developments progress, the lack of knowledge about information collection practices combined with incomprehensible privacy policies of many online companies, cause consumers to be concerned about the privacy of their personal information.[6] This is particularly true in the arena of online profiling, where Web site operators and other data compilers are able to create extremely detailed profiles regarding Web users, cross-match the data with consumer information collected from off-line sources such as catalogs and registration forms, and sell the profiles to a third party.[7] In response to these consumer concerns, the Federal Trade Commission ("FTC") issued a report to Congress in May 2000, recommending that broad federal legislation be enacted to implement fair information collection principles across the entire online industry.[8]

This note will argue that rather than adopting this legislation that sweeps so broadly, a more flexible market-based approach should be taken that better protects consumers while retaining the economic benefits of online profiling. This will be argued by analyzing the economic benefits of online profiling, the exact nature of consumer concerns, and the potential costs of the proposed legislation.

In Part 1, this note analyzes the benefits and concerns associated with online profiling. Part 2 explains the current regulatory framework. Part 3 discusses the legislative recommendation made by the FTC and shows that such a broad act of legislation is not a workable solution. Part 4 proposes a flexible integrated approach for regulating online profiling that combines market forces and industry efforts with law enforcement resources. This approach consists of four interrelated elements: 1) encouraging the progress of industry self-regulation; 2) utilizing emerging technologies; 3)

---

[4] *See infra* text accompanying notes 22-24.

[5] *See generally* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193 (1998) (analyzing various exploitative uses of data in online transactions).

[6] *See infra* notes 33-47 and accompanying text.

[7] *See* Courtnay Youngblood, *A New Millennium Dilemma: Cookie Technology, Consumers and the Future of the Internet*, 11 J. ART & ENT. LAW 45 (2001).

[8] *See generally* FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE (May 2000), *available at* http://www.ftc.gov/os/2000/05/index.htm [hereinafter PRIVACY ONLINE REPORT].

expanding consumer education; and 4) enhancing governmental enforcement of existing privacy laws.

BACKGROUND: ONLINE PROFILING DEFINED

Technology has enhanced the ability of online companies to collect, store, transfer, and analyze large amounts of data generated by consumers.[9] Consumer data are often collected directly by Web site operators using marketing and registration surveys, and various other forms.[10] Alternatively, data are collected by third parties, such as advertising networks, which display "banner ads," or small graphic advertisements, on individual Web sites.[11] In addition to supplying banner ads, network-advertising companies also gather consumer data about those who view their advertisements using "cookies"[12] and "Web bugs"[13] to track an individual's Web activities.[14] These devices provide information regarding a consumer's online purchases and online travels, as well as the types of

---

[9] *See* Kang, *supra* note 5, at 1224-34; Federal Trade Commission, Online Profiling: Benefits and Concerns, Statement Before the United States Senate Committee on Commerce, Science, and Transportation, (June 13, 2000), *available at* http://www.ftc.gov/os/2000/06/onlineprofile.htm [hereinafter Online Profiling Statement]; *see also* Quincy Maquet, *A Company's Guide to an Effective Web Site Privacy Policy*, 2 J. INTELL. PROP. 1 (2000).

[10] *See generally* Debra A. Valentine, *Privacy on the Internet: The Evolving Legal Landscape*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 401 (2001); Jonathan Cody, *Protecting Privacy Over the Internet-Has the Time Come to Abandon Self-Regulation*, 48 CATH. U. L. REV. 1183, 1186 (1999) (explaining that Web sites collect personal information from a consumer directly by using online contests, surveys, purchase orders for goods and services, and site registration materials).

[11] *See* FED. TRADE COMM'N, ONLINE PROFILING, 3-4 (June 2000), *available at* http://www.ftc.gov/os/2000/06/onlineprofilingreportjune2000.pdf [hereinafter ONLINE PROFILING REPORT] (explaining that these third party network advertising companies manage and provide advertising for many unrelated Web sites). "DoubleClick, Engage and 24/7 Media, three of the largest Internet advertising networks, all estimate that over half of all online customers have seen an ad that they delivered." *Id.* at 3.

[12] A cookie is "a small piece of code," which is deposited into users' computers by a Web site server. It transmits back to the Web site information about that user's activity on that particular site, as well as about the other sites the user has visited since the cookie was deposited. *See* Youngblood, *supra note 7, at* 48-49; *DoubleClick Probed for Privacy Breaches*, E-COM. No. 11, at 4 (March 2000) (noting that "the cookie allows [W]eb sites to recognize particular users on future visits, enabling [W]eb sites to provide personalized information or to automate the log-in process"); *see also* http//www.cookiecentral.com.

[13] "'Web bugs' are tiny graphic image files embedded in a Web page, . . . invisible to the naked eye. The Web bug sends back to its home server . . . the address of the computer that downloaded the page on which the bug appears"; the URL of that page, the time of downloading, and the type of browser, as well as "the identification number of any cookie on the . . . [user's] computer previously placed by that server"). ONLINE PROFILING REPORT, *supra* note 11, at 3 n.12.

[14] See Joshua Sessler, *Computer Cookie Control: Transaction Generated Information and Privacy Regulation on the Internet*, 5 J.L. & POL'Y 627, 634 (1997) (discussing related types of user data compilers, such as the "Oil Change program, which produces a tailor-made list of items found on various hard drives"; Click Stream Data, which lists the items on a Web site that the users have clicked on; and DoubleClick, which receives information transmitted from cookie files thereby enabling the transmission of tailored advertisements each time a Web site is visited by the same user).

advertisements and information a consumer seeks.[15]

It is important to distinguish between two separate types of information collected online: personally identifiable information and non-personally identifiable information. Personally identifiable information refers to data that is used to locate a person, including his or her name, address, telephone number, or email address.[16] Non-personally identifiable information is not linked to any particular person and is typically collected from "click stream information compiled as a browser moves among different Web sites, serviced by a particular network advertiser."[17]

Consumer information collected directly by Web site operators is often personally identifiable because a user is usually required to submit personal information such as his or her name and email address in order to register at a particular Web site.[18] By contrast, the profile information collected by network advertisers is usually non-personally identifiable because a profile only corresponds to the identification number of the cookie on a user's computer, rather than to that particular user's name or email address.[19] Once collected, this information is combined with demographic and psychographic[20] data collected offline, resulting in a profile that attempts to predict the consumer's tastes, needs, and purchasing habits, and thereby enable online companies to develop targeted marketing programs to satisfy the consumer's desires.[21]

---

15 *See* Heather Green, *Privacy Online: The FTC Must Act Now,* BUS. WK., Nov. 29, 1999.

16 *See* NETWORK ADVERTISING INITIATIVE, SELF REGULATORY PRINCIPLES FOR ONLINE PREFERENCE MARKETING BY NETWORK ADVERTISERS, *at* http://www.ftc.gov/os/2000/07/NAI%207-10%20Final.pdf (last visited Mar. 7, 2002) [hereinafter NAI PRINCIPLES].

17 *Id.* (listing examples of non-personally identifiable data as information on the Web sites visited by surfers; the timing and duration of such visits, search terms entered into search engines, "click through" responses to online advertisements, and the prior Web page a user visited before visiting the site monitored by the particular ad network).

18 *See id.* at 3; *see also* Maquet, *supra* note 9, at 8 (noting that online companies gather information, such as name, gender, address, age, income level, lifestyle, personal hobbies and interests, directly from consumers by using registration and similar forms featured on its Web site).

19 *See* Ethan Hayward, *Legislative Updates: The Federal Government as Cookie Inspector: The Consumer Privacy Protection Act of 2000.* 11 J. ART & ENT. LAW 227, 227 (2001) ("Web advertisers often use a cookie's transmission pattern to build a user profile based on the type of Web sites the user visits most frequently, and will use that profile to target banner ads and email to that user every time she logs on.").

20 *See* ONLINE PROFILING REPORT, *supra* note 11, at 5 n.18. "Psychographic data links objective demographic characteristics like age and gender with more abstract characteristics, such as ideas, opinions and interests." *Id.* Data mining specialists later use this data to identify a target market for specific products and services. *Id.*

21 *See* PRIVACY ONLINE REPORT, *supra* note 8, at 44 n.34 (defining online profiling as "aggregating information about consumers' interests, gathered primarily by tracking their movements online and using the resulting consumer profiles to deliver targeted advertisements on Web sites"). *But see* Online Profiling Statement, *supra* note 9, at 7 n.28 (noting

I. Online Profiling: Benefits and Concerns

A. *Benefits*

Collecting profile information online provides tremendous benefits to businesses, consumers, and the overall economy. For businesses, the increased flow of information offers the unprecedented ability to examine consumer behavior in order to minimize marketing and distribution costs—a powerful competitive advantage in the price aggressive marketplace.[22] The information flow allows businesses to track consumer purchases, recommend new products or services, and provide sales, marketing, and customer services more efficiently and more effectively.[23] It also allows companies to create the right product and deliver it at the right time to meet customer demands.[24] Moreover, profiling increases the ability of online companies to measure consumer reaction to new ideas, and to promote the creation of new products and services, because it reduces the risks and expenses of introducing new products into the market.[25]

By profiling consumers online, the Internet marketer can increase its profit margins while passing valuable savings along to consumers.[26] Targeted advertising provides consumers with offers and information about goods and services in which they are per-

---

that non-personally identifiable profiles that are derived from tracking consumer's activities on the Web can be merged with personally identifiable information only if consumers reveal their identity to the Web site on which the network advertisers display banner ads).

22 *See* Shaun A. Sparks, *The Direct Marketing Model and Virtual Identity: Why the United States Should Not Create Legislative Controls on the Use of Online Consumer Personal Data*, 18 Dick. J. Int'l L. 517 (2000) (analyzing the direct marketing model and advocating a free market approach to online information collection).

23 *See* Online Profiling Report, *supra* note 11, at 9 (stating that businesses benefit from the practice of target advertising because they avoid wasting marketing dollars on consumers who clearly have no interest in their products).

24 The Information Marketplace: Merging and Exchanging Consumer Data, Public Workshop of the Federal Trade Commission (Mar. 13, 2001), http://stlr.stanford.edu/stlr/articles/00_stlr_2 [hereinafter FTC Public Workshop]; *see also* Kent Walker, *Where Everybody Knows Your Name. . .A Pragmatic Look at the Costs of Privacy and the Benefits of Information Exchange*, 2000 Stan. Tech. L. Rev. 2, *available at* http://stlr.stanford. edu/STLR/Articles/00_STLR_2/index.htm (last visited Mar. 20, 2002) (explaining that the Internet permits brand identification and actual purchasing in a single transaction; that technology permits precisely focused demographics, which increases the odds that a consumer will be interested in a particular product or service).

25 *See* Online Profiling Report, *supra* note 11, at 10 (noting that entrepreneurs could use consumer profiles to assess demand for prototypical products and services); Valentine, *supra* note 10, at 402 (stressing that "an entire industry has emerged to market a variety of software products designed to assist Internet sites in collecting and analyzing visitor data and in serving targeting advertising."); Jeff Sovern, *Opting In, Opting Out, or No Options at All-The Fight for Control of Personal Information*, 74 Wash. L. Rev. 1033, 1050 (1999) (stating that absent marketing research offered by informational databases, some sellers may find it too risky and costly to introduce new products).

26 *See* Sparks, *supra* note 22, at 530.

sonally interested, such as free videos for proclaimed movie buffs, good deals on a house for a newly married couple, or low cost airfare for college students planning to fly home for a holiday.[27] These kinds of tailored discounts reduce the cost of living for millions of Americans.[28] Moreover, the resulting increase in advertising dollars spent on the Internet creates free and subsidized Internet services for consumers.[29]

In addition, information-gathering tools such as cookies provide many convenience-oriented benefits for Internet surfers, by storing names and passwords so that consumers do not need to sign in each time that they visit a Web site.[30] Other benefits include the availability of personalized home pages and other customized content, such as local news and weather, or favorite stock quotes.[31]

Finally, targeted advertising created by online profiling offers larger macro-economic benefits. It significantly diminishes entry-level barriers encountered by small start-up companies by allowing them to advertise exclusively to consumers who have demonstrated an interest in their particular product or service. In fact, a number of new businesses that recently entered the market provide goods and services to consumers relying solely on the information collected from these consumers online.[32] Thus, the combined benefits of online profiling are advantageous to individual consumers, businesses, and the entire economy because they facilitate the efficient distribution of goods, reduce overall transaction costs, and produce greater availability of goods and services.

---

27 *See* Walker, *supra* note 24, at 7; *see also* Sovern, *supra* note 25, at 1048 (noting that, in 1995, consumers bought close to $600 billion worth of goods and services through direct marketing channels).

28 *See id.* at 1048-49; Walker, *supra* note 24, at 7-8. ("The virtually costless communications of the Internet let consumers and businesses buy and sell less expensively by cutting out the middle-man and overhead {costs}. And they facilitate advertising the availability of perishable goods that were never before considered perishable things like airline tickets, and long distance time.").

29 *See* Online Profiling, Public Workshop of the United States Department of Commerce and Federal Trade Commission, http://www.ftc.gov/bcp/profiling/index.htm (Nov. 8, 1999).

30 ONLINE PROFILING REPORT, *supra* note 11, at 8-9; *see also* John MacDonnell, *Exporting Trust: Does E-Commerce Need a Canadian Privacy Seal of Approval?*, 39 ALBERTA L. REV. 346, 354 (Sept. 2001).

31 *Id.*

32 *See* Walker, *supra* note 24, at 9 (describing a new online company called Free-PC Inc., based upon "the premise that people would part with certain information and put up with a constant barrage of ads in exchange for a $500 computer."). Privacy advocates predicted this idea to bea loser, but within days of the announcement, the company received more than 1.2 million applications. *Id.*

B. *Privacy Concerns*

The most consistent and significant concern expressed by consumers in regards to online profiling is that it is conducted without their knowledge.[33] The presence of a network advertising company on a particular site, the placement of cookies, and the tracking of a consumers online behavior are usually invisible to the targeted individual.[34] Generally, there are only two ways for consumers to discover that a particular site is engaging in online profiling. The Web site can disclose this information in its privacy policy or consumers can configure their browsers to notify them before accepting cookies.[35] This "lack of notice" is problematic for the collection of personally identifiable information as well as non-personally identifiable data.

In a recent report addressing consumer attitudes toward online profiling, AT&T found that 52% of the respondents were concerned about Web cookies, while another 12% said they were uncertain as to what a cookie was.[36] Of those who were aware of cookies, 56% said they had changed their cookie settings to allow them to receive a notification before accepting a cookie.[37] Thus, the survey demonstrates that a significant number of informed consumers do exercise some measure of control over the collection of their data online, but relatively few of them are aware that the tools exist. Moreover, in the 1994 Harris Survey, 51% percent of respondents indicated that they would be concerned if the online services to which they subscribed engaged in "subscriber profiling" for advertising purposes.[38] The same respondents, however, were less concerned about subscriber profiling if they received notice

---

[33] *See* Online Profiling Statement, *supra* note 9, at n.38; *see also* ONLINE PROFILING REPORT, *supra* note 11, at 10-11.

[34] Hayward, *supra* note 17, at 230 ("Web marketers often engage . . . . . in 'data mining', employing software to search firm's databases for information . . . useful to their own store of knowledge. Most of this activity occurs undetected by the average surfer."); *see also* ONLINE PROFILING REPORT, *supra* note 11, at 11 (proposing that most Internet surfers only see the Web sites they visit; banner ads appear as invisible part of the site; and cookies are placed without notice to the surfers); *see also* Online Profiling Statement, *supra* note 9, at 8.

[35] *See* ONLINE PROFILING REPORT, *supra* note 11, at 11.

[36] LORRIE FAITH CRANOR, ET AL., AT&T LABS, BEYOND CONCERN: UNDERSTANDING NET USERS' ATTITUDES ABOUT ONLINE PRIVACY (1999), http://www.research.att.com/library/trs/TRs/99/99.4 [hereinafter AT&T REPORT]. AT&T analyzed 381 questionnaires compiled by American Internet users in November 1998, based on a sample drawn from the Family PC Magazine/Digital Research, Inc. Family Panel. AT&T acknowledged that the sample was not statistically representative of American Internet users. Nevertheless, it is indicative of the attitudes of the future Internet user population.

[37] *See id.* at 3.

[38] *See* FED. TRADE COMM'N, PUBLIC WORKSHOP ON CONSUMER PRIVACY ON THE GLOBAL INFORMATION INFRASTRUCTURE (Dec. 1996) (discussing legal challenges and consumer privacy concerns in the booming Internet marketplace), *available at* http://www.ftc.gov/bcp/privacy/wkshp96/privacy.htm.

that a profile would be created and were informed as to how it would be used. Consumers given some level of control over the use of their profile information were also less likely to be concerned about subscriber profiling.[39] Thus, it appears that many Internet users are not opposed to the use of persistent identifiers that compile profile information, such as cookies, as long as the there is an adequate level of transparency regarding the Web site's information collection practices.[40]

The second major concern of privacy advocates is the extensive scope and continuous nature of online monitoring.[41] As previously mentioned, advertising networks monitor the behavior of Internet users as they travel across thousands of seemingly unrelated Web sites over an infinite period of time, creating profiles far more detailed than that of any individual online company.[42] Although the profiles are generally non-personally identifiable, Internet users worry that online companies could develop the potential to match these non-personally identifiable online profiles with personally identifiable information, such as names and addresses, and sell this information to third parties.[43] Some privacy groups go even further and suggest that if consumers fear online monitoring, it will "discourage valuable uses of the Internet."[44]

While there is no evidence of diminished Internet use among American consumers, many surfers do consider what type of information is collected, the purpose for which information is collected, whether information is personally identifiable, and whether information is shared with other parties.[45] Where only non-personally identifiable information is concerned, most Internet users are quite willing to provide data related to their interests, purchases,

---

39 *See id.* at 7.

40 *See* AT&T REPORT, *supra* note 36, at 2 ("78% of respondents said they would definitely or probably agree to Web sites using persistent identifiers (possibly implemented using cookies) to provide a customized service . . . [60% of respondents said they] would agree to the use of such an identifier to provide customized advertizing.").

41 See Online Profiling Statement, *supra* note 9, at 4.

42 *See id.*

43 *See* Sparks, *supra* note 22, at 535 (explaining that privacy advocates are worried about online companies merging profiles with personally identifiable data through such methods as "cookie synchronization [where] once a site owner discovers the user's identity, the Web site owner may then share that knowledge with other Web site owners"; and "data triangulation," which is the practice of "obtaining several small items of data on an individual user . . . and then attempting to match that data against a larger more complete identity file"). *But see* Malla Pollack, *Opt-In Government: Using the Internet to Empower Choice-Privacy Application*, 50 CATH. U. L. REV. 653, n.85 (2001) (stating that experts strongly disagree as to the likelihood that non-personally identifiable information will be linked with personally identifiable information).

44 *See* ONLINE PROFILING REPORT, *supra* note 11, at 13.

45 *See* AT&T REPORT, *supra* note 36, at 2.

and online travel destinations.[46]

When faced with disclosing their personal information, however, consumer fears predictably escalate. At the same time, many indicated that their concerns about the collection of personally identifiable information for the purpose of online profiling would diminish if they received clear notice regarding the kind of data that would be collected and the purpose for which it would be used. Consumer concerns also diminish depending on whether an opportunity to restrict certain uses of personal data was provided.[47]

Several conclusions emerge from these surveys. First, consumers view the collection of non-personally identifiable information as less threatening to their privacy than the collection of personally identifiable data. Second, many consumers misunderstand the nature and purpose of profiling technology, as well as its limitations, and are largely unaware of available control measures. Leading to a "fear of the unknown," this information gap is exacerbated by three factors: (1) a lack of comprehensible privacy policies; (2) minimal explanation of a Web site's information collection practices; and (3) general distrust of online companies.[48]

II. Current Regulatory Framework

A. *Government Authority*

Congress has addressed the private sector's collection, use, and disclosure of personally identifiable information through limited legislation targeting specific industries.[49] In addition, the FTC has been actively involved in addressing the issue of online privacy over the past several years.[50] The FTC has authority over the collection and dissemination of personal data collected online pursuant to Section 5 of the Federal Trade Commission Act,[51] and the Children's Online Privacy Protection Act,[52] which governs the collection of personal information from children under the age of

---

46 *See* Online Profiling, *supra* note 29, at 107-10.

47 *See* Online Profiling Report, *supra* note 11, at 15.

48 *See* FTC Public Workshop, *supra* note 24, at 3. When discussing consumer concerns about matching profiles with personally identifiable information, Commissioner Swindle noted that there is a "huge misunderstanding deficit that parallels and matches the trust deficit."

49 *See* Cody, *supra* note 8, at 1199 (indicating that Congress enacted the Electronic Communication Privacy Act of 1986, 18 U.S.C. § 2510-2522 (1986), to protect some forms of electronic privacy, and the Fair Credit Reporting Act, 15 U.S.C. § 1681 (1994), to govern the collection and disclosure of personal information in the credit reporting industry).

50 *See* Privacy Online Report, *supra* note 8.

51 15 U.S.C. § 41 (2002).

52 15 U.S.C. § 6501 (2002). *See also* 15 U.S.C. § 6801-6809 (2002) (governing the protection of individual financial information).

13.[53] However, the FTC has limited ability to require companies to adopt specific information practice policies, or abide by the fair information practice principles on their Web sites, especially on portions of those sites not directed at children.[54]

B. *Industry Self-Regulation*

The FTC has long encouraged the Internet industry to address consumer concerns regarding online information collection practices through self-regulation.[55] In response to the FTC and market support for self-regulation,[56] many private industry groups have issued guidelines addressing the implementation of privacy protection measures in relation to the information collection practices of industry members.[57] For example, the Bankers Roundtable has established guidelines for members of the banking industry concerning the institution of privacy protection principles.[58] The Direct Marketing Association also provides its members with privacy principles, recommending that marketers who operate Web sites post a conspicuous notice to consumers regarding information collection practices and provide consumers with an opportunity to prohibit the disclosure of personal information.[59] Moreover, the Individual Reference Services Group and the Interactive Services Association provide principled guidelines to Web site operators and Internet service providers regarding online information collection practices.[60]

Another industry-wide initiative that seeks to have companies implement fair principles for the practice of collecting information over the Internet is online privacy seal programs. These programs require companies to implement and use fair information collection practices, and have their compliance monitored.[61] One such program is TRUSTe. TRUSTe affords monitoring functions to ensure that its members adhere to their posted privacy policies. Companies from any industry wishing to become a TRUSTe participant

---

53 *See id.* at 34.

54 *See id.*

55 *See id.*

56 *See* Cody, *supra* note 10, n.207 (describing the industry and marketing groups lobbying for self-regulation).

57 *See id.* at 1217-20.

58 *See id.*

59 *See id.*

60 *See id.* Individual Reference Services are computerized database services that sell personal identifiable information collected from public records and publicly available sources, as well as non-public sources. The leading industry members formed a group to develop self-regulatory principles regarding their information collection practices.

61 *See* PRIVACY ONLINE REPORT, *supra* note 8, at 35; *see also* Cody, *supra* note 10, at 1218.

and obtain a "privacy seal" to be displayed on their site, must post an online privacy policy, which is easy to locate and easy to comprehend, giving visitors notice that a company is a licensee of the TRUSTe program.[62] TRUSTe participants must provide certain opt-out opportunities as well.[63] There are many similar programs, which award seals to online companies that practice specified information collection principles.[64]

With respect to self-regulatory efforts at the corporate level, leaders such as IBM, Microsoft, Disney, Intel, Procter and Gamble, Novell, and Compaq have voluntarily committed their companies to require that their advertising partners post comprehensible privacy policies in order receive advertising revenue.[65] There is also an expansion of associations working to encourage other Web site operators to take initiative and ensure that their companies not only establish but promote the adoption and implementation of voluntary privacy policies.[66] One such association is www.NetCoalition.com, whose membership consists of chief executives officers from leading commercial Web sites. Moreover, in 1999, following a public workshop on online profiling, industry members formed the Network Advertising Initiative ("NAI"), an organization comprised of leading Internet network advertisers, to develop a self-regulatory framework for the online profiling industry.[67]

III. FTC's Proposed Regulatory Framework: Broad Legislation

A. *Description of the Legislative Proposal*

Over the past five years, the FTC issued a number of reports to Congress analyzing the development of the online industry.[68] In a

---

62 *See* Cody, *supra* note 8, nn. 239-45.

63 *See id.*

64 *See, e.g.*, the Better Business Bureau ("BBB"), *at* http://www.bbbonline.org/privacy/ (last visited Mar. 14, 2002) (establishing the BBB Online Privacy Program, which awards seals to online businesses that verifiably follow reasonable information collection practices); SecureAssure, *at* http://www.secureassure.org/ (last visited Mar. 14, 2002) (allowing Web sites to display their seal if certain security, privacy and reliability standards are met); Privacy Bot.com, *at* http://www.privacybot.com (last visited Mar. 14, 2002) (stating that Privacy Bot is a privacy seal program that requires compliance with certain privacy standards and an annual fee before an online business can display the "trust mark" on its Web site).

65 *See* Privacy Online Report, *supra* note 6, at 17-19.

66 *See id.*

67 *See* Will Rodger, *Online Profiling Firms To Police Themselves*, USA Today, Nov. 8, 1999, *http://usatoday.com/life/cyber/tech/review/crg571.htm* (stating that some of the largest online profiling companies established a self-regulatory organization in an attempt to delay potential new privacy rules from Congress and the FTC); *see also supra* note 14.

68 *See generally* Fed. Trade Comm'n, The FTC's First Five Years, Protecting Consumers Online (Dec. 1999), *available at* http://www.ftc.gov.

May 2000 report, the majority recommended that broad federal legislation be enacted to further implement fair principles of online information collection practices in the Internet industry, despite acknowledging the continued progress in self-regulation.[69]

The legislation recommended by the FTC would require all consumer-oriented commercial Web sites that collect personally identifiable information generated by consumers online, directly or indirectly, to comply with four information collection principles:[70] (1) notice, requiring Web sites to provide consumers with conspicuous notice of their information practices, including the type of information collected, the methods by which information is collected, whether information is disclosed to third parties, and whether third parties are permitted to collect information through using the site; (2) choice, requiring Web sites to offer consumers choices as to how their personal information is used beyond the use for which it is provided; (3) access, requiring Web sites to offer consumers reasonable access to personal information actually collected, which includes a reasonable opportunity to review and correct inaccuracies within such information; and (4) security, requiring Web sites to take reasonable steps in order to protect and secure consumer information actually collected. The FTC also identified enforcement as a "critical ingredient in any governmental or self-regulatory program to ensure privacy online."[71]

In a July 2000 report, the FTC expanded upon its recommendation for legislation to address online profiling.[72] The previously proposed legislation would have applied to all network-advertising companies, as well as to all consumer-oriented commercial Web sites that permit network-advertising companies to collect consumer information.[73] The FTC also extended the "notice" requirement by requiring host Web sites to provide clear notice about cookies or similar technology used by network advertising companies to collect non-personally identifiable information.[74]

Shortly after the FTC issued the July 2000 report, several privacy bills were proposed in Congress. The Consumer Privacy Protection Act of 2000, for example, incorporated the principles of

---

69 *See* PRIVACY ONLINE REPORT, *supra* note 8, at 38.

70 *See id.* at 36-37 (describing the four fair information collection principles: notice, choice, access, and security).

71 *See* ONLINE PROFILING REPORT, *supra* note 11, at 20.

72 *See* FED. TRADE COMM'N, ONLINE PROFILING PART 2, RECOMMENDATIONS (July 2000), *available at* http://www.ftc.gov/os/2000/06/onlineprofilingreportjuly2000.pdf [hereinafter ONLINE PROFILING REPORT-PART 2].

73 *See id.* at 5.

74 *See id.* at 10 n.33.

fair information practices, advocated an opt-in approach to the practice of data collection, and established the Office of Online Privacy to monitor e-commerce privacy issues.[75] Other bills included the Consumer Internet Privacy Enhancement Act,[76] which required strict opt-out procedures, and the Secure Online Communication Enforcement Act, which proposed to extend restrictions to Web site operators regarding the disclosure of personal information.[77] Despite the efforts of many privacy advocates, however, the 106th Congress did not pass any of these proposed privacy bills.

B. *Analysis of the Legislative Proposal: Not an Optimal Solution*

While these legislative proposals offer a seemingly workable solution, such broad government regulation of the entire online industry is unwarranted, will produce more costs than benefits for all e-commerce participants, and will be difficult to implement.

First, governmental intervention is not warranted because there is no evidence that the market failed to respond to consumer concerns. While the May 2000 FTC report concluded that self-regulatory efforts are inadequate to address consumer privacy concerns, the FTC recommendation in favor of legislation was not based on substantive analysis and, therefore, is not justifiable.[78]

The FTC recommendation was based on a privacy survey that reviewed privacy disclosures among commercial Web sites in the United States. The privacy survey assessed the effectiveness of self-regulation by examining a sample of random Web sites ("the random sample") and a sample of the most popular Web sites ("the most popular sample").[79] The survey showed that 20% of the random sample sites and 42% of the most popular sample sites had disclosures satisfying all four principles.[80] The FTC found that when compared to "similar figures" from a 1999 survey, the survey

---

75 *See* Hayward, *supra* note 19, at 255-56, 258 (explaining S. 2606, 106th Cong. (2000)).

76 *See id.* at 258 (describing S. 2928, 106th Cong. (2000)).

77 *See id.* at 258-59 (referring to S. 2063, 106th Cong. (2000)).

78 *See* Commissioner Thomas B. Leary, Fair Information Practices in the Electronic Marketplace, Statement Before the United States Senate Committee on Commerce, Science, and Transportation (May 25, 2000), *at* http://www.ftc.gov/os/2000/05/privacyleary.htm [hereinafter Leary, Dissent in Part] (noting in partial dissent that the 2000 Privacy Survey fails to demonstrate that the market has not responded adequately to consumer demand because the survey only measures "inputs," or the prevalence of privacy policies; it doesn't measure "outputs," or the impact of these policies on consumer attitude and behavior); *see also* Orson Swindle, Fair Information Practices in the Electronic Marketplace, Statement Before the United States Senate Committee on Commerce, Science, and Transportation (May 25, 2000), *at* http://www.ftc.gov/os/2000/05/privacyswindle.htm [hereinafter Swindle Dissent] (dissenting).

79 *See* PRIVACY ONLINE REPORT, *supra* note 8, at app.A.

80 *See id.* at app.C tbl.4.

results indicate that self-regulatory efforts alone are insufficient to address information privacy concerns, and broad legislation applicable to all commercial Web sites and third party advertising networks was necessary.[81] Thus, this privacy survey, showing a mere snapshot of privacy disclosures online, formed the basis of the FTC recommendation in favor of sweepingly broad legislation contained in the May 2000 report to Congress.[82]

A close analysis of the 2000 privacy survey, however, reveals that significant progress was being made in regards to both self-regulation, specifically where posting privacy policies and privacy disclosures were concerned, and the effect of market forces. Neither of these areas was adequately evaluated by the FTC.[83] The privacy survey established that 88% of Web sites in the random sample and 100% of the most popular sample Web sites posted at least one privacy disclosure.[84] Furthermore, the survey indicates that 62% of the random sample sites and 97% of the most popular sample sites posted a privacy policy, which was an impressive increase from the 1998 figures of 44% and 81%, respectively.[85]

In addition, the survey showed vast improvement in regards to industry efforts to implement fair information collection practices. Figures indicate that 55% of sites in the random sample and 89% of sites in the most popular sample met all four requirements when measured individually.[86] The fact that 89% of the most popularly visited sites implemented the information collection principles indicates that the market forces work well by rewarding those sites displaying the most comprehensive and transparent privacy disclosures.

When the privacy report combined all four measurements, however, the results were much lower: 20% of the random sample sites and 42% of the most popular sample sites implemented all four fair information collection principles. Yet, Congress did not insist that all four of the principles be met in the Gramm Leach Bliley Act, even though that legislation addressed the protection of personal financial information.[87] If implementation of all four

---

81 *See* PRIVACY ONLINE REPORT, *supra* note 8, at 36-38.

82 The FTC's 2000 report to Congress also relied on the results of several consumer confidence studies in support of its legislative recommendation. *See id.* at 2-3.

83 *See* Swindle Dissent, *supra* note 78, at 2.

84 *See* PRIVACY ONLINE REPORT, *supra* note 8, at app.C tbl.2a. These figures rose from 14% and 71% in 1998, to 66% and 93%, respectively, last year.

85 *See* PRIVACY ONLINE REPORT, supra note 8, at 10. *See id.* at 11.

86 *See id.* at app.C tbl.4.

87 See Swindle Dissent, *supra* note 78, at 8 (referring to the Gramm Leach Bliley Act, 15 U.S.C. § 6801-6810, which provides *inter alia* that financial institutions must disclose their privacy policies to affiliates and third parties).

principles was not required for protecting highly sensitive personal information,[88] then there is even less need for such strict requirements in the area of online profiling due to the non-personally identifiable nature of profile information.

As Commissioner Swindle noted in his dissenting statement, the report's comparison of the May 2000 survey figures—20% in the random sample and 42% in the most popular sample—to the 1999 surveys is unhelpful because the 1999 surveys did not define notice, choice, access and security to include the more demanding elements required by the 2000 privacy survey.[89] The results of the 2000 survey, when measured against a more reliable framework, demonstrate that industry efforts to address privacy issues continue to develop and improve.[90] This progress is further enhanced by market forces that reward those Web sites with the most comprehensive privacy disclosures.[91] As Commissioner Swindle cautioned, "legislation should be reserved for problems that the market cannot fix on its own and should not be adopted without consideration of the problem legislation may create."[92]

Moreover, the FTC's reliance on consumer opinion surveys is an unreliable and insufficient reason to recommend legislation that sweeps so broadly. While consumer surveys may be useful in analyzing general attitudes among Internet surfers regarding information disclosure online and the nature of consumer concerns, these surveys do not clearly indicate the need for a legislative policy approach. For example, a recent study conducted by the Information Technology Association of America found that many people believe that businesses are better at protecting sensitive information than the government.[93]

In general, the surveys indicate that consumer reactions to scenarios involving online data collection are extremely diverse. The varied types of information collected and different tastes for privacy suggest that a one-size-fits-all approach to online privacy is un-

---

88 *See id.* ("Once beyond sensitive financial and medical information, the importance of Access . . . diminishes.").

89 *See id.* (finding that the majority report acknowledged that the scoring models were not identical because the surveys asked different questions).

90 *See id.* at 8 (stressing that when using the most comparable approach, the survey's estimate as to Web sites implementing all four principles rises to 25% for the random sample and 57% for the most popular sample, showing a remarkable one year improvement in self-regulatory efforts).

91 *See id.*

92 *Id.* at 4.

93 *See Surveys Point to More Security and Privacy Woes*, INFO. SECURITY, Dec. 2000, *available at* http://www.infosecuritymag.com/articles/december00/departments_news.shtml.

likely to succeed.[94] In fact, even members of the FTC have not reached a consensus as to whether legislation is the best solution, illustrated by their sharply divided vote on the proposal with which Commissioner Swindle strongly dissented.[95] Commissioner Leary commented that he considers the recommendation for legislation too broad because it "suggests the need for across-the-board substantive standards when, in most cases, clear and conspicuous notice would be sufficient."[96] A final note bears mentioning: Online commerce continues to grow despite growing concern about privacy. This suggests perhaps that many consumers do not act upon their fears or, alternatively, that such generalized fears may be adequately addressed by the provision of additional information by individual Web sites.[97]

Second, implementing the proposed legislation will impose significant costs on the online industry, which may cripple its development and hurt consumers in the long run. Because the online industry thrives on technological innovation, the worst thing a company might hear a person say is, "We are from the government. We are here to help."[98] The Advisory Committee Report, which helped form the basis of the FTC's proposal for legislation, recommended that each commercial Web site implement a security program to protect personal data that it collects.[99] Such security programs may assess risks, implement a security system, manage policies and procedures, or audit and conduct internal assessment.[100]

The labor and technology costs of complying with the proposed legislative standards will likely reduce the sales of online companies as well as the economic and convenience-oriented benefits provided to consumers. Some evidence suggests that the costs

---

94 *See* AT&T REPORT, *supra* note 36, at 4.

> To meet the needs of the varied clusters of people, public policy should support flexibility. Both the technical and self-regulatory approaches promote privacy . . . disclosure upon which users can make their own decisions . . . We acknowledge that an eventual solution might rely upon . . . legal, self-regulatory and technical approaches to the problem.

Id. at 18; *see also* Valentine, *supra* note 10, at 411 (suggesting that one reason for the lack of federal legislation to protect Internet privacy is because there is no consensus that one general approach solves all privacy problems).

95 The FTC's vote on this issue was 3-2, with Commissioner Swindle dissenting and Commissioner Leary concurring in part and dissenting in part. *See* PRIVACY ONLINE REPORT, *supra* note 8.

96 Leary Dissent in Part, *supra* note 78, at 1.

97 *See* Swindle Dissent, *supra* note 78, at 15-16.

98 Fernando Piera, *International Electronic Commerce: Legal Framework at the Beginning of the XXI Century*, 10 CURRENTS: INT'L TRADE L.J. 8 (2001).

99 *See* PRIVACY ONLINE REPORT, *supra* note 8, at 32.

100 *See id.*

of complying with such privacy regulations may be too high for online companies. A May 2001 study conducted by the American Enterprise Institute and the Brookings Joint Center for Regulatory Studies analyzed the potential costs to seventeen companies in ten states.[101] The study concluded that the companies would need to spend an average of $100,000 to make necessary infrastructure changes in order to comply with the proposed legislative standards.[102] This figure climbs to $9 billion if *only* five to ten percent of the current 3.6 million Web sites implemented the proposed legislative standards.[103] Thus, if every commercial Web site implemented these principles, as the proposed legislation requires, the cost will be substantially higher than $9 billion. These costs, while undoubtedly burdensome to most online companies, may prove to be ruinous to smaller companies.[104] If it becomes too burdensome for companies to engage in online profiling, many would be forced to use more expensive methods of reaching consumers, which would inevitably translate into higher prices for products and services and, in some cases, even eliminate some products from the market altogether.[105]

This effect will significantly reduce the benefits derived from targeted advertising and online profiling that consumers currently enjoy.[106] It is not at all clear that even the most "privacy concerned" consumers, who make up only one quarter of the Ameri-

---

101 *See* Anne Saita, *Privacy's Pretty Penny*, INFO. SECURITY, July 2001, *available at* http://www.infosecuritymag.com/articles/july01/departments_news.shtml. This study was based on several privacy bills, including the Consumer Internet Privacy Enhancement Act, which requires all commercial websites to define the type and methods of information collection, as well as its intended usage and to provide an opt-out opportunity.

102 *See id.* Moreover, a partner in a Chicago-based law firm, who specializes in privacy issues, stated that these "estimates may actually be conservative, compared to actual costs, given that . . . not all respondents included the cost of consulting and legal services, software modification, additional hardware and privacy policy changes." *Id.*

103 *See id.*

104 *See, e.g.*, Walker, *supra* note 24, at 10 (stating that "government-created standards for all consumer–oriented commercial Web sites may cause some online companies, particularly smaller ones," not wealthy enough to pay for lobbyists or lawyers, "to limit their online services or exit the marketplace altogether"); Lynn Burke, *Kids' Sites Cite COPPA Woes*, WIRED NEWS, Sept. 2000, *at* http://www.wired.com/news/politics/0,1283,38666,00.html (observing that the Children's Online Privacy Protection Act (COPPA) has forced many Web sites to eliminate children's programming); Stefanie Olsen, *DoubleClick Turns Away From Ad Profiles*, CNET NEWS, Jan. 8, 2002, *at* http://news.com/2100-1023-803593.html (stating that DoubleClick decided not to continue its "intelligent" targeting service in 2002 due to continuing attacks from federal regulators and privacy advocates concerning its practice of compiling consumer profiles).

105 *See* Sovern, *supra* note 25, at 1051.

106 *See* William McGeveran, *Programmed Privacy Promises: P3P and Web Privacy Law*, 76 N.Y.U. L. REV. 1812, 1825 (2001) (noting that if overreaching privacy protection rules make personalization too costly for online companies, they will almost certainly impose fees or service charges on surfers, thus "externalizing the cost of some surfers' desire for privacy on all who use the Web").

can public, would support broad federal regulation if it meant foregoing or limiting the enjoyment of the benefits that flow under the current scheme of collection practices which rely primarily on self-regulation.[107]

In addition, the legislation may inadvertently create greater consumer costs. Technological innovation and continuous evolvement of industry standards are the hallmarks of the online environment.[108] Since formal government legislation, by its nature, cannot adjust quickly to this rapidly changing medium, it may very well curb technological innovation and the development of efficient commercial practices.[109] As a result, the technological and industrial development of better privacy protection will be inhibited, or in some cases extinguished altogether, leaving the online consumer worse off than he or she is now.

Third, the proposed legislation is difficult to implement across the entire online industry. In its May 2000 report, the FTC acknowledged that the principles of access and security present unique implementation issues and require further consideration before their parameters can be defined.[110] For instance, considerable disagreement exists among FTC members as to how "reasonable access" should be defined for the purpose of implementing the access principle.[111] In addition, implementing fair information principles in the context of online profiling conducted by network advertisers presents additional implementation issues due to the invisible third party relationship between network advertisers and consumers, and the presence of multiple network advertisers on a particular Web site.[112] For example, it is unclear how a "host" Web site can provide notice about the information collection activities of each third party network advertiser who sends a "banner ad" to its site.

Finally, no consensus has been reached as to the bounds of a proper legislative framework, which is evident in light of the FTC's

---

107 *See* Walker, *supra* note 24, at 24-25 (asserting that the regulators' "assumptions of universal interest in privacy suggest a universal willingness to sacrifice benefits of information exchange for greater privacy."). Yet a recent survey noted that although people are concerned in regards to the privacy of personal information collected online, they realize that personalized Web service is convenient and efficient, and many are willing to have their information gathered if they see a real benefit and there are appropriate safeguards in place.

108 *See* Bradford L. Smith, *The Third Industrial Revolution: Policymaking for the Internet*, 3 COLUM. SCI. & TECH. L. REV. 1, 3 (2001) (endorsing the use of self-regulatory and other "extra-legal solutions to address the challenges posed by online information collection").

109 *See id.* at 18.

110 *See* PRIVACY ONLINE REPORT, *supra* note 8, at 17-29.

111 *See id.*

112 *See* ONLINE PROFILING REPORT-PART 2, *supra* note 72, at 1.

present turnabout in position concerning the issue of regulating the online industry.[113] In a recent speech, the Chairman of the FTC announced that the FTC would not seek new privacy laws any time soon, but would instead focus on the enforcement of existing laws because "it is too soon to conclude that we can fashion workable legislation" to achieve the goals in mind.[114]

Meanwhile, it would be premature for the online industry to breathe a sigh of relief, because many privacy advocates expect the 107th Congress to pass some legislation addressing online profiling.[115] To avoid strict government regulation, the online industry should demonstrate its commitment to self-regulation, as well as its ability to adequately protect consumers while preserving the advantages of online profiling.

IV. Optimal Approach to Online Profiling Regulation: Where Do We Go From Here?

Before advocating any particular solution, policymakers should recognize the need for a flexible approach to regulate online profiling.[116] The need for flexibility stems from several factors. In the first instance, living in a modern informational age, where tremendous amounts of online as well as offline data are disclosed on a daily basis, changes the concept of privacy from notions of complete secrecy to expectations of information accessibility.[117] Consequently, an Internet surfer's individual decision to exchange his or her information for benefits varies considerably, reflecting different privacy expectations[118] and, thus, making it difficult to establish a uniform privacy standard.

In addition, it is evident that non-personally identifiable (profile) information calls for a lower level of protection than personally identifiable information. One can hardly argue that it is

---

113 *See, e.g.*, Daniel Sieberg, *FTC Sidelines the Call for New Privacy Laws*, CNN, Oct. 4, 2001, *available at* http://www.cnn.com/2001/US/10/04/inv.online.privacy/index.html; Mary Mosquera, *FTC to Beef up Privacy Enforcement, Drop New Laws*, Internet week, Oct. 4, 2001, *available at* http://www.internetw/c.com/story/INW20012004S0008.

114 *See* Sieberg, *supra* note 113.

115 *See* Piera, *supra* note 98, at 12; *see also* John Kamp, *Forecasting Privacy in 2002*, TRUSTe Advoc. Newsl., Jan. 2002, *available at* http://www.etrust.com/partners/newsletter/winter2002.htm.

116 *See* FTC Public Workshop, *supra* note 24, at 3 (noting that the policy approach should balance consumer interest with the benefits of tailored advertising, and business interest in serving all markets in the most efficient and effective way); *see also* McGeveran, *supra* note 106, at 10.

117 *See* Daniel J. Solove, *Conceptualizing Privacy*, 90 Cal. L. Rev. 1087 (2002) (arguing that defining privacy as an "expectation in a certain degree of accessibility of information" is more appropriate in today's society, which is driven by constant information exchange).

118 *See supra* text accompanying note 45.

necessary for information regarding a consumer's hobbies and vacation preferences to have the same level of privacy protection as a consumer's name and phone number. More importantly, however, rapid technological innovation is inherent in the online industry and demands flexible regulatory standards that are easy to revise.[119]

In light of the technological complexity, overwhelming scope, and constantly evolving nature of the online industry, one recognizes a need for flexibility, at which point it also becomes apparent that a choice between either pure self-regulation or broad federal legislation is a false one.[120] Therefore, an effective way to approach regulating the online profiling industry should incorporate a role for the government to supplement, but not overwhelm, the market-based self-regulatory framework. Consequently, the essential elements of an efficient and flexible approach to online profiling regulation are as follows.

A. *Industry Self-Regulation: Continual Development*

Self–regulation has been repeatedly recognized as the most efficient and cost-effective method to address consumer concerns about the privacy of personal information collected online because it relies on market forces, rather than government intervention.[121] In areas such as the Internet, the private sector has played a principal role in the development of self-regulations by not only creating but continuously updating technological standards and industry practices. Therefore, a strong case exists for relying on private sector industries to regulate the very phenomenon they created and nurtured.[122]

Market-based solutions, such as self-regulation and emerging technology (privacy protection tools), should be the cornerstone of the modern regulatory approach. Market-based solutions are able to respond to multiple consumer privacy preferences and various online business models more quickly and often with greater

---

119 *See* Smith, *supra* note 108, at 18 (discussing the need for flexible regulations to match the dynamic international character of e-commerce).

120 *See* Valentine, *supra* note 10, at 412 (noting that essentially there is both self-regulation and legislation); *see also* Smith, *supra* note 108, at 2 (suggesting that a modern approach to solving legal problems rooted in technology needs a regulatory framework that incorporates "extra-legal solutions" and a government role in addressing the issues in ways that are more flexible, responsive, and market-oriented).

121 *See, e.g.*, Sparks, *supra* note 22, at 550-551; Valentine, *supra* note 10, at 412 (noting that "self-regulation is the least intrusive and may be the most efficient means to ensure fair information practices").

122 *But see* Smith, *supra* note 108, at 18-19.

flexibility than traditional government regulation.[123] Moreover, the self-regulatory codes are usually developed by industry members, who possess the greatest expertise in industry practices and conditions. When necessary, these codes can be modified and updated more swiftly than legislation.[124] This allows online companies to keep in step with the rapid evolution of online and computer technology, in order to utilize emerging technologies to protect consumer privacy.[125]

As current industry efforts demonstrate, the fair information collection principles recommended by the FTC proposal for legislation can be implemented to a reasonable degree without resorting to across the board legislation. As previously noted, NAI, an organization comprised of leading Internet network advertisers, such as 24/7 Media, AdForce, AdKnowledge, AvenueA, Burst! Media, DoubleClick, Engage, and MatchLogic, was formed in 1999 to develop a self-regulatory framework for the online profiling industry.[126]

One of the distinctive features of the self-regulatory scheme developed by NAI is that, while it shows a commitment to fair information collection principles, it offers a higher level of protection for personally identifiable data as opposed to non-personally identifiable (profile) data, thus providing the flexibility needed to regulate online profilers.[127] In addition, the NAI principles require network advertisers to provide notice and an opportunity to "opt-in" before non-personally identifiable information can be merged with personally identifiable information, thus addressing a major consumer concern about online profiling.[128] The FTC acknowledged that the NAI self-regulatory framework reasonably implements the fair information practice principles.[129]

---

123 *See id.* (discussing key attributes of self-regulation, such as responsiveness to consumer demand, plurality of choices, and structural incentives towards efficiency).

124 *See* Valentine, *supra* note 10, at 412.

125 *See id.*

126 *See* Rodger, *supra* note 67, at 02A; *see also* ONLINE PROFILING REPORT-PART 2, *supra* note 72, app. (describing the principles of NAI, which include not using certain types of sensitive personally identifiable data for online marketing; not merging, without prior affirmative consent (opt-in), personally identifiable information with information previously collected as non-personally identifiable; providing consumers with notice and choice regarding the merger of personally identifiable information and non-personally identifiable information on a going forward basis; and contractually requiring Web publishers to provide notice and choice regarding the collection of non-personally identifiable information for online profiling).

127 *See* ONLINE PROFILING REPORT-PART 2, *supra* note 72, at 3 (noting that the NAI principles require a heightened level of notice, described as "robust notice," before any personally identifiable data can be collected).

128 *See* NAI PRINCIPLES, *supra* note 16, at 7.

129 *See* ONLINE PROFILING REPORT-PART 2, *supra* note 72, at 2.

Currently, over 90% of the network advertising industry participates in the NAI program.[130] This shows that fair information practice principles can be realistically implemented by the private sector without resorting to government regulation. It also demonstrates that the FTC was incorrect when it concluded that "self-regulatory programs . . . cannot ensure that the online market place as a whole will follow the standards adopted by the industry leaders."[131]

B. *Utilizing Emerging Technologies*

If the industry is allowed to develop a self-regulatory framework unburdened by the intrusion of government regulation, it can utilize emerging technology to create greater privacy protection than any potential legislation. The market for privacy protection is growing and companies are increasingly producing various technological privacy tools.[132] For example, the Platform for Privacy Preferences ("P3P") is a new computer protocol that permits consumers to communicate their preferences for sharing personally identifiable information with a Web site.[133] This technology allows the Web site's privacy policy to be automatically translated into an easy to understand format.[134] More importantly, Web users can save their privacy preferences on P3P compatible software. Then, when visiting a P3P compliant Web site, the user's computer compares the preferences with the site's policy, and notifies the user, in simple terms, if there is a discrepancy.[135] Many P3P supporters view this technology as *the* primary component of any regulation regime, "requiring little or no intervention by the law."[136]

Of course, the effectiveness of this privacy program depends

---

130 *See id.* at 10.

131 PRIVACY ONLINE REPORT, *supra* note 8, at 35.

132 *See* Swindle Dissent, *supra* note 78, at 4.

133 *See generally* McGeveran, *supra* note 106 (describing the new technology and advocating the creation of a "P3P privacy market" as a part of the Internet regulation approach); *see also* http://www.w3.org/P3P/.

134 *See* MacDonnell, *supra* note 30, n. 18. ("P3P is an emerging standard that would allow Web sites to translate their privacy policies into a machine-readable format to be automatically read by the browser of a visitor to the site. The browser informs the visitor about whether the policies meet their pre-set privacy expectations.").

135 *See* McGeveran, *supra* note 106, at 1813 (explaining that some privacy-conscious surfers may disclose their mailing address only for the purpose of shipping an order, while others who may disclose their address in order to allow a Web site to add them to a catalog mailing list).

136 *See id.* at 182. Moreover, recently, the World Wide Web Consortium (WC3) has issued the P3P 1.0 recommendation, which indicates that "it is a stable document, contributes to Web interoperability, and has been reviewed by the W3C Membership, who favor its widespread adoption." *World Wide Web Consortium Recommends P3P*, THE COMPUTER AND INTERNET LAW J., July 2002, at 31.

on the compliance of a Web site. The process of converting an online privacy policy into a P3P compatible policy is extremely easy and takes no more than a few hours.[137] Recently, Microsoft included a modest P3P user agent in the latest version of its browser, Internet Explorer 6.0, which is part of the company's new operating system, Windows XP.[138] Moreover, a significant number of online companies, including many network-advertising giants such as DoubleClick, are currently using various versions of P3P technology.[139]

P3P technology has tremendous potential for further development and improvement. Many companies are working on more ambitious user agents that would operate independently of Internet browsers and allow surfers to ask a series of questions in order to yield a more detailed and sophisticated set of privacy preferences.[140]

If fully implemented, this technology will alleviate many consumer concerns about information collection online. As previously stated, the most consistent and significant concern expressed by consumers regarding online profiling is that it is conducted without their knowledge.[141] Thus, notice remains the most fundamental element of privacy protection. The 2000 privacy survey results show that notice is in fact widely provided, but there appear to be problems with the clarity and comprehensibility of privacy disclosures.[142]

P3P technology provides much needed "clarity and comprehensibility" by allowing consumers to understand how a particular Web site collects and uses personal data. This provides a significant measure of privacy control for concerned consumers. Internet surfers, informed by clear and conspicuous notice, can

---

137 *See* Ari Schwartz, *P3P Basics*, TRUSTE ADVOC. NEWSL., Jan. 2002, *available at* http://www.etrust.com/partners/newsletter/winter2002.htm (presenting a quick summary of how to convert a policy in five steps).

138 *See* McGeveran, *supra* note 106, at 1832. While this user agent's implementation of P3P is limited in several respects, it allows surfers to set certain preferences and use them to automatically evaluate the Web site's privacy policies. Moreover, the current Internet Explorer 6.0 allows surfers to block or delete cookies, and limit its later retrieval.

139 *See World Wide Web Consortium Recommends P3P*, *supra* note 136, at 31 (stating that the "lists of P3P-enabled Web sites and P3P software continue to grow, including both plug-ins and browser based implementations"); *see also P3P Initiatives*, *at* http://www.w3.org/P3P/compliant_sites (last visited Mar. 20, 2002) (listing over 80 Web sites which are using P3P).

140 *See* McGeveran, *supra* note 106, at 1833 ("P3P allows independent persons or organizations to write model sets of preferences for surfers to import into their user agents. Implemented in full, P3P would allow user agents to elicit highly customized sets of preferences.").

141 *See supra* text accompanying notes 32-34.

142 *See* PRIVACY ONLINE REPORT, *supra* note 8, at 24-28 (noting that recent reports have emphasized the confusing nature and contradictory language of the privacy policies).

select the vendors who provide the desired level of privacy protection that they want.[143]

In addition, P3P technology provides necessary flexibility by offering multiple degrees of protection to accommodate varying levels of privacy preferences. Once informed of the site's information collection practices, consumers can avoid sites whose policies they find inadequate without spending a lot of time struggling to understand the extensive legal jargon contained in a typical site's privacy policy. In effect, sites with substandard policies will be provided strong incentives to catch up to consumer demands, thus stimulating the creation of a "privacy market." Such a market retains the benefits of unrestricted information flow and, at the same time, stimulates implementation of increased privacy protection.[144]

P3P technology is but one example of how privacy protection tools that address consumer concerns about online profiling have emerged at an increasing rate. Other technological developments are focused on making the information collected online less personally identifiable. Such developments include anonymizer programs, which allow people to surf the Web without having their actions being linked directly to them.[145] Still other developments have been with filter tools, such as cookie busters, which can be configured to partially or completely block cookies[146] and identity management tools.[147] In addition, there are technology tools that facilitate access, which is one of the fair information collection

---

143 *See* Leary Dissent in Part, *supra* note 78, at 5.

144 *See* McGeveran, *supra* note 106, at 1834-1835 (describing a libertarian approach, where in a P3P privacy market surfers own their personal data and use P3P to negotiate with those who wish to collect it, thereby allowing the privacy market to function efficiently, "reducing the transaction costs of providing extensive details about a site's privacy policy").

145 Lorrie Faith Cranor, Remarks at the United States Department of Commerce Online Privacy Workshop and Technology Fair (Sept. 19, 2000), *available at* http://www.ntia.doc.gov/ntiahome/ptivacy/files/2000transcript.txt (describing one of the most well known anonymizer proxies, Anonymizer.com, which allows a user to configure their Web browser so that all requests they make to the Internet go through this proxy server). "The proxy server takes the request, strips off identifying information, and forwards it to wherever the user wants it to go." *Id.* at 8.

146 *See id.* at 10. Examples of such filtering tools include cookie cutters and child protection software. *See* Scott Sidel, *Cookie Buster*, INFORMATION SECURITY, Nov. 2000. Internet Cleanup software sells for $24.95 and allows the Internet user to remove the traces he leaves behind while surfing. This software also automatically cleans up the browser's cache, cookies and history file. Privacy–conscious surfers can choose not only to delete information about their surfing patterns, but also to "shred" it, making it virtually irrecoverable. *See id.*

147 *See* Cranor, *supra* note 145, at 10 (describing identity management tools, some of which are essentially an "opt-in to targeted advertising, that allow people to create an electronic file with their personal information and have their computer automatically send this information to Web sites only upon user authorization").

principles advocated by the FTC.[148] More and more network advertisers are using these and similar technologies for the exclusive collection of non-personally identifiable information, thus removing the key reason for consumer concern.[149]

Moreover, even without implementing these innovations, current computer technology provided by most Internet browsers allows consumers to partially or completely disable their cookies, as well as opt-out of receiving cookies.[150] Thus, current and emerging technology is one part of the response to consumer concerns about online profiling.[151] Consumers who feel very strongly about protecting privacy can use these tools to control the collection of personal information online, but only if they are aware of its existence. Extensive consumer education, therefore, is the third necessary ingredient of the modern market–based regulatory approach.

C. *Consumer Education: Joint Efforts By Public And Private Sectors*

It has been repeatedly suggested that the real problem driving privacy concerns is a lack of consumer education and information.[152] Presently, consumer awareness is lagging behind the advent of technology, despite FTC efforts to educate the public. As the Secretary of Commerce noted at a recent online technology fair, "[the] industry is doing a good job in developing privacy-enhancing technologies, but the word hasn't gotten out to the consumer."[153] In fact, reports show that less than half of Internet users surveyed knew what a cookie was;[154] only 10% of those surveyed said that they had set their browser to block cookies; and a mere

---

148 *See id.* at 14 (presenting one example of "access" technology produced by Privacy Right, which allows the user to specify what kinds of information uses are acceptable, "basically opting in and out of various things," and then permits the user to view personal data actually collected, as well as companies to which data has been disclosed).

149 *See* Online Profiling, *supra* note 29, at 26-28 (citing examples of such companies that collect only non-personally identifiable information, including Engage and MatchLogic).

150 Interview with Eugene Sapozhnikov, Network Engineer (Jan. 31, 2002) (explaining that users have the option to completely disable cookies on their system or set their Internet browser to prompt if cookies should be accepted). However, since cookies are needed to browse certain Web sites, the best solution is to select an opt-out option. Surfers using Internet explorer or Netscape Navigator can make these changes by simply going to the security options on their Web browser and making the necessary adjustments. *See also* MacDonnell, *supra* note 30, at 354.

151 *See* Lynn Chuang Kramer, *Privacy Eyes Are Watching You: Consumer Online Privacy Protection, Lessons from Home and Abroad*, 37 TEX. INT'L L.J. 387 (2002) (arguing that consumers who really want to protect their privacy can do so by taking matters into their own hands, which involves disabling cookies as well loading privacy protection software into their computers).

152 *See* Swindle Dissent, *supra* note 78, at 3; *see also supra* text accompanying notes 36, 40, 48.

153 Cranor, *supra* note 145, at 4.

154 *See id.*

one in twenty Internet users reported having used software that hides his or her computer identity from Web sites.[155] Thus, many consumers are simply not aware of the tools and options that the market provides, which inevitably leads to a "fear of the unknown."[156]

To bridge the gap between technological advances and public knowledge, extensive consumer education programs, sponsored by both public and private sectors, and directed at Internet surfers and businesses alike, are necessary to empower consumers so that they can make informed choices about online data collection.[157] With respect to the public sector, education programs may include (1) performing informal outreach between seal programs and industry groups; (2) developing guidelines and educational materials for consumers and businesses; and (3) exploring emerging privacy technologies through workshops, reports, and other public meetings.[158]

The private sector, on the other hand, has already stepped up to the plate. The NAI self-regulatory agenda is intended to educate business members and individual consumers about data collection online, profiling, and use issues associated with Internet advertising featured on Web sites and in privacy statements.[159] In addition, NAI has recently launched a special educational Web site to facilitate consumer awareness.[160]

Effective consumer education is necessary to supplement market forces[161] because an efficient market presupposes full and accurate information. In turn, a well-informed body of consumers can discipline the marketplace to provide an appropriate combination of privacy protections. The dynamics of this relationship between consumer education and market forces rewards companies that offer preferred levels of protection, without having to resort to governmental regulation.[162]

---

155 *See id.*

156 *See* FTC Public Workshop, *supra* note 24, at 3 (asserting that most consumers fight to understand technology themselves, which may be the underlying cause of their concerns).

157 *See* Chairman Timothy J. Muris, Remarks at the Privacy 2001 Conference (Oct. 4, 2001), *available at* http://www.ftc.gov/speeches/muris/privisp1002.htm.

158 *See id.*

159 *See* NAI PRINCIPLES, *supra* note 16, at 11-12.

160 *See id.* (describing an educational Web site located at http://www.networkadvertizing.org).

161 *See* Kramer, *supra* note 15, at 416 (arguing that "neither industry self-regulation nor governmental regulation will succeed unless consumers are willing to take charge of protecting their privacy," which involves awareness of profiling and information use issues, and the use of cookie disabling tools and privacy protection software).

162 *See* Swindle Dissent, *supra* note 78, at 16 (noting that if consumer fears about security are exaggerated or there is merely a "fear of the unknown," the solution is to restore con-

D. *Enforcement: The Government's Role*

As promising as market and industry efforts are at protecting consumer profile information, there is still an obvious need for enforcement to ensure that sites deliver what they promise and do not deviate from stated privacy policies. In its 2000 report, the FTC identified enforcement as a key component in protecting consumer privacy online.[163] At the same time, an adequate level of enforcement can be achieved without legislative enactment.

The FTC already has the power to address privacy policy violations by bringing an action against any Web site whose privacy policy violates Section 5 of the FTC Act.[164] Not only can the FTC challenge violations of stated privacy policies, but the FTC also can challenge deceptive practices—policies that promise more protection than they actually provide.[165] Recent cases brought by the FTC against certain online companies illustrate that the FTC has a broad scope of authority. This authority allows the FTC to challenge violations of promises made in online privacy policies and protect consumer privacy online.[166] Thus, privacy advocates are incorrect when they argue that consumers have no real remedy against privacy violations.[167] This is not to say, however, that a better system is not needed to enforce the existing laws, which is directed toward improving Web site compliance with stated privacy policies.[168]

---

sumers' confidence through notice and education rather than enacting rules that may restrict their choices).

163 *See supra* text accompanying note 70.

164 *See* Valentine, *supra* note 10, at 405-07 (explaining that Section 5 of the FTC Act "protects consumers' information privacy whenever a company collects or disseminates personal data in an unfair or deceptive manner").

165 *See* Leary Dissent in Part, *supra* note 78, at 7.

166 *See* Valentine, *supra* note 10, at 405. In 1998, the FTC brought an action against GeoCities for falsely representing that mandatory information their members provided would not be released to third parties without permission. Ultimately Geocities settled the case by agreeing to disclose its information practices accurately. In addition, the FTC brought an action against ReverseAuction.com for allegedly violating its privacy policy. The proposed settlement prohibits Reverse Auction from misrepresenting its privacy policy and the information collection practices of other companies. *See id;* Muris, *supra* note 157, at 10 n.26. (stating that the FTC brought an action against Toysmart.com, alleging that the company misrepresented that personal information collected from users on its Web site would not be released to third parties). Another example of the FTC's authority involves the case against Liberty Financial Companies, Inc., which settled charges alleging that its Web site misrepresented that childrens' personal information collected online would be held anonymously. *See id.*

167 *See* Muris, *supra* note 157, at 7 ("[T]here is a great deal we can do under existing laws to protect consumer privacy."); *see also* FTC Public Workshop, *supra* note 24, at 2 (noting that issues related to the real harm that might be caused by information collection online are well addressed by existing laws).

168 *See* PRIVACY ONLINE REPORT, *supra* note 8, at 24; *see also* Muris, *supra* note 157, at 3-7 (discussing an expanded privacy agenda of the FTC, which includes a 50% increase regard-

The other aspect of the enforcement plan is derived from the industry's "seal programs."[169] Web site enrollment in such programs has grown modestly.[170] For example, TRUSTe, the first online privacy seal program, has grown to more than 1200 licensed Web sites that represent a variety of industries.[171] In addition, over 450 Web sites representing 244 companies have obtained licenses to display the Better Business Bureau OnLine Privacy Seal since the program's inception last year.[172] Notably, the CPA Web Trust Program, which features a privacy component in its program requirements, has licensed its seal to 28 Web sites. Moreover, 6 companies have been licensed to display the PWC Better Web online privacy seal on their web sites.[173] In its 2000 report, the FTC found that nearly one-half of the most frequently visited Web sites use a seal program.[174] While this alone is an impressive number, market forces, supplemented by consumer education, provide the appropriate incentives for the remaining 50% of online companies to enroll in privacy seal programs, at the risk of losing customers to other Web sites that offer better privacy protection.[175]

Furthermore, evidence suggests that many consumers believe that a combination of privacy policies and privacy seals program provide a level of user confidence comparable to privacy laws.[176] Thus, government enforcement of the existing privacy laws, combined with industry "seal" programs, can provide the necessary enforcement element, which, according to the FTC, is "crucial to success and credibility of self-regulation."[177]

One may wonder why concerns about online profiling still circulate among American Web surfers, despite obvious progress in private sector efforts to provide the optimal level of privacy protec-

---

ing resources devoted to protecting privacy, expanding administrative review of privacy policies, and improving the FTC's complaint handling system).

169 *See supra* notes 62-66.

170 *See generally* PRIVACY ONLINE REPORT, *supra* note 8.

171 *See id.* at 6.

172 *See id.*

173 *See id.*

174 *See* PRIVACY ONLINE REPORT, *supra* note 8, at 20.

175 *See* NAI PRINCIPLES, *supra* note 16, at 12 (stating that the NAI self-regulatory scheme requires its members, constituting over 90% of the online profiling industry, to work with a third party enforcement program, such as a "seal program" that certifies third party advertising).

176 *See* AT&T REPORT, *supra* note 36, at 2 (noting that when researchers described the situation wherein a Web site with information related to a favorite hobby asks for a surfer's name and mailing address to provide free coupons and discounts, 48% of the respondents stated they would be more inclined to provide the information if there was a law preventing the site from misusing the information; 28% replied that they would share the information if the site had a privacy policy; and 58% replied that they would provide information if the site had both a privacy policy and a seal of approval from a well known organization).

177 PRIVACY ONLINE REPORT, *supra* note 8, at 34.

tion. If the industry has not yet proven that it is able to fulfill its promises (which may be the reason why privacy concerns still float about), it is because many self-regulatory frameworks and developing technologies are still works in progress and have yet to reach their full potential.[178] As discussed earlier, most consumers are not aware of the less harmful nature of profile information, as compared to the nature of personally identifiable information. Many are also unaware of the vast amount of technological privacy tools currently at their disposal.

Although market processes, complimented by traditional remedies against consumer deception, should ultimately provide the ideal combination of information disclosures and privacy protections, these forces sometimes work slowly.[179] Yet, at the same time, the online industry will continue to make privacy protection a priority because its ability to generate earnings depends on consumer trust and the willingness of consumers to participate in online transactions.[180] In the interest of all e-commerce participants, the government should give these promising developments a chance before resorting to broad legislation, and support industry efforts with consumer education and the enforcement of existing privacy laws.[181]

CONCLUSION

The online profiling industry thrives on the free flow of information. This allows for a highly efficient personalized surfing experience, greater availability of goods and services, and reduced transaction costs for consumers and businesses alike. Imposing artificial legislative limitations on information flow will significantly reduce, and in some cases eliminate, the tremendous economic and efficiency gains that online profiling offers to all who participate in e-commerce.

There is no question that consumer concerns about online profiling must be addressed. However, an optimal solution must accommodate varying degrees of consumer privacy preferences, as well as the rights of online companies to collect and use profile information. Online profiling, after all, provides significant micro- and macro-economic benefits.

The private sector will continue to address this issue through

---

178 For example, NAI was only formed in 1999.

179 See Leary Dissent in Part, *supra* note 78, at 2.

180 *See, e.g.*, ONLINE PROFILING WORKSHOP, *supra* note 29, at 89, 135-38.

181 *See* Swindle Dissent, *supra* note 78, at 3.

self-regulation and technological developments because it is in its best interest to do so. The industry has shown incredible progress toward implementing fair information collection principles and using emerging technologies to provide better privacy protection. However, given the dynamic nature, technological complexity, and novelty of the industry, these efforts need time to gradually come into fruition.

Supplementing market forces with governmental enforcement of existing privacy laws will allow self-regulatory frameworks and technological privacy tools to develop, thus providing greater privacy protection to consumers. Enacting broad legislation, on the other hand, will almost certainly discourage further innovation. Consequently, a flexible approach that combines market forces, industry efforts, and law enforcement is far superior to broad legislation in addressing consumer concerns about online profiling, while simultaneously preserving its unprecedented benefits.

*Svetlana Milina***

** Notes Editor, Cardozo Arts and Entertainment Law Journal; J.D. Candidate, June 2003, Benjamin N. Cardozo School of Law; B.S. in Finance, *magna cum laude*, May 2000, New York University. The Author wishes to thank the staff and board of the *Cardozo Arts and Entertainment Law Journal*. The Author also would like to thank Professor Peter Yu for all his guidance.