Online Profiling Is on the Rise: How Long Until the United States and the European Union Lose Patience with Self-Regulation?

Scott Foster

Follow this and additional works at: http://digitalcommons.law.scu.edu/lawreview

Part of the Law Commons

Recommended Citation
Available at: http://digitalcommons.law.scu.edu/lawreview/vol41/iss1/7

This Comment is brought to you for free and open access by the Journals at Santa Clara Law Digital Commons. It has been accepted for inclusion in Santa Clara Law Review by an authorized administrator of Santa Clara Law Digital Commons. For more information, please contact sculawlibrarian@gmail.com.
ONLINE PROFILING IS ON THE RISE: HOW LONG UNTIL THE UNITED STATES AND THE EUROPEAN UNION LOSE PATIENCE WITH SELF-REGULATION?

Scott Foster*

I. INTRODUCTION

Imagine yourself surfing through Amazon.com, looking for a particular book about traveling through Tuscany that you have not been able to find on the shelves of your local bookstore. You might type "Traveling Tuscany" in the Amazon.com search engine, glance at a few relevant titles, and upon finding the book you want, decide to purchase it online. Giving them your name, address, email, phone number, and credit card number, you click "buy" and the book is promised to arrive on your doorstep in a couple of days.

This is a typical online transaction. The ease with which it is done is helping drive e-commerce to a projected market size of $6.8 trillion by the year 2004. What the customer may not realize is that the above scenario has the U.S. government, the European Union, privacy advocates, and consumers greatly concerned with the protection of personal information. As e-commerce grows and more people connect to the Internet, concerns about online privacy escalate. What you did not see while buying the book is at the center of those

* Comments Editor, Santa Clara Law Review, Volume 41. J.D. candidate, Santa Clara University School of Law; B.A., Stanford University.
2. E-commerce, or electronic commerce, is the use of computers and electronic communications in business transactions, i.e., business-to-consumer or business-to-business transactions. See High-Tech Dictionary (visited May 12, 2000) <http://www.currents.net/resources/dictionary/index.html>.
concerns.

The moment you arrived, Amazon.com or a third party placed a "cookie" in your computer which allowed them to "see" every click you made. In addition, the required information you gave Amazon.com to purchase the book is stored in a database of profiles, and is matched with your clickstream. If it was your first time visiting the site, the site created a personal online profile about you; if you were a return visitor, the site updated your profile, and a banner ad might have attempted to use that profile to offer you a book corresponding to one of your past inquiries. In addition, Amazon.com added your name and address to mailing lists, and this created online profile may even be sold to third parties for undisclosed purposes.

Online profiling is increasing and emerging as its own separate industry. Independent companies who serve targeted Internet ads to web sites drive the online profiling industry. Imagine how much personal information

4. A cookie is a set of data that a web site server gives to a browser the first time the user visits the site that is updated with each return visit. See, e.g., High-Tech Dictionary (visited July 15, 2000) <http://www.currents.net/resources/dictionary/index.htm>.

5. The remote server saves the cookie's information about the user, and the user's browser does the same, as a text file stored in the Netscape or Explorer system. See id.

6. Clickstream refers to the trail one makes as one clicks from web page to web page.

7. In 1998 the Federal Trade Commission announced its first Internet privacy case, in which GeoCities, operator of one of the most popular sites on the World Wide Web, agreed to settle Commission charges that it had misrepresented the purposes for which it was collecting personal identifying information from children and adults through its online membership application form and registration forms for children's activities on the GeoCities site. See FEDERAL TRADE COMMISSION (FTC), SELF-REGULATION AND PRIVACY ONLINE: A REPORT TO CONGRESS, July 1999 at 16 n.16 [hereinafter REPORT]. See also Deborah Kong, Online Privacy a Hot Issue for the FTC, S.J. MERCURY NEWS, Dec. 27, 1999, at 1E [hereinafter Kong, Online Privacy] (In an interview with the FTC Commissioner, the Commissioner stated that one of the biggest privacy breaches the FTC had investigated involved GeoCities.).

8. See Deborah Kong, Online Profiling is on the Increase, S.J. MERCURY NEWS, Jan. 3, 2000, at 1C [hereinafter Kong, Online Profiling]. See also REPORT, supra note 7, at 2 (explaining how an entire industry has emerged to market a variety of software products designed to assist web sites in collecting and analyzing visitor data and in serving targeted advertising).

9. See Kong, Online Profiling, supra note 8, at 1C ("[O]nline advertising companies [are] scrambling to build profiles of computer users. They plan to sift through the details and deliver targeted ads to consumers who are most likely to respond.").
Amazon.com collected as you bought the book in the above scenario — quite a bit. Now, after having bought your book on traveling through Tuscany, imagine yourself visiting Webvan to buy groceries online.

Typing in “webvan.com,” the first banner ad you may see is an intriguing one for some restaurant-quality pasta sauce. The banner may tempt you to click on its ad because you enjoy high-quality food, and cost is a secondary concern. The fact that such an ad appeared on your screen was no accident. In fact, an independent company working with Amazon.com collected your request for traveling through the beautiful countryside of Italy and used that information to predict that you would be interested in high-quality, high-cost food at Webvan. Since the independent company had a partnership with each web site, it had the ability to add to your profile and target you from either site.11

Your personal profile gets bigger with every click as you surf the Web. Online advertising companies already practice this “surveillance” and compile extensive databases full of such personal information gathered from the hundreds of web sites with whom they do business.12

The U.S. is not alone in its concern over online privacy. In fact, the European Union (E.U.) has already adopted legislation toward this aim requiring the U.S. to take certain “adequate” steps to ensure privacy for the Europeans who do business with U.S. companies.13 Because of the global nature of e-commerce and the potential revenue that might be realized by a global market, the U.S. cannot afford to ignore the E.U. Directive.14 The U.S. response has been to approach online privacy through a self-regulatory framework, believing that market forces will make web sites comply with consumers’ demands for protection of their personal information.15 However, for the most part, web sites have

11. See Kong, Online Profiling, supra note 8, at C1.
12. See id.
15. See Kong, supra note 7, at 1E (interviewing Orson Swindles,
been unwilling to give consumers the protection of personal information that the E.U., privacy advocates, and consumers demand.\textsuperscript{16}

This comment examines the online profiling industry and its privacy concerns,\textsuperscript{17} and asserts that the self-regulation approach to protecting personal information online is failing.\textsuperscript{18} This comment argues the need for legislation since self-regulation has been unable to satisfy both consumer and E.U. criteria for online privacy protection.\textsuperscript{19} More specifically, enacting Senator Edward Markey's Electronic Privacy Bill of Rights Act of 1999\textsuperscript{20} would attain "adequacy" in the eyes of the E.U. and renew consumer confidence in the online marketplace.\textsuperscript{21}

II. BACKGROUND

A. Online Profiling

Online profiling is the practice of collecting information about consumers' interests, gathered primarily by tracking their movements online, and using the resulting consumer profiles to create targeted advertising on web sites.\textsuperscript{22} Through a user's browser,\textsuperscript{23} a web site might know the location of the computer he utilizes, what software and hardware he is using, details of the link he clicked on to reach the web site, and possibly even his email address.\textsuperscript{24} Collection of such personal information is done both explicitly and in more subtle ways.\textsuperscript{25}

Explicit methods include personal data collection through
registration pages, survey forms, order forms, and online contracts.26 Recently, General Motors Corporation began offering consumers free Internet service in exchange for the ability to monitor and track them.27 The service requires users to give their names and addresses as well as answer questions ranging from what kind of car they own, to whether they purchased or leased the car, and if they would consider buying online.28 To avail oneself of the service, subscribers must agree to allow the company to use software to track the sites they visit and to keep a small window that flashes ads every thirty seconds on their screen.29 Signing up with General Motors’s free service, users know what they are getting themselves into. However, this is not always the case.

1. The Use of Cookies to “Watch” Surfers

“Cookies” constitute a more subtle way to collect personal data.30 Profile-based advertising relies heavily on these unique strings of computer code placed in one’s computer.31 Cookies allow the web site or independent company to monitor every web page a user visits, every online advertisement he views, and every mouse click he makes.32 Often placed unknowingly in the user’s computer, cookies allow a company such as eToys.com to say, “Welcome back, Dana.”33

In the past, only one web site could understand a particular cookie.34 However, advertising services, such as

26. See REPORT, supra note 7, at 2.
27. See Deborah Kong, GM offers a ‘honey’ of a deal on Net service, S.J. MERCURY NEWS, Jan. 14, 2000, at 1C. ("We're using the free access, the free e-mail, as the honey to attract the bees,' said Mark Goldston, NetZero's chairman and chief executive. The technology is 'like a GPS tracking system. The minute you come on, it knows who you are, it knows where you go.").
28. See id.
29. See id.
30. See supra note 4.
33. See Electronic Privacy Information Center, Surfer Beware III: Privacy Policies without Privacy Protection (Dec. 1999) (visited Jan. 20, 2000) <http://www.epic.org> (stating that cookies can be generated the instant one arrives at a web site and also when one clicks on a banner ad).
34. See Robert O'Harrow, Jr., Honing in on privacy; As databases collect personal details well beyond credit-card numbers, it's time to guard yourself,
DoubleClick Inc., now use cookies to track and profile the behavior of people at related sites across the Web without the knowledge of the computer user.\textsuperscript{35}

2. Widely Used Profiling is Big Business

Most web sites participate in the billion-dollar business of online profiling.\textsuperscript{36} In fact, a 1999 survey of the top one hundred web sites by the Online Privacy Alliance ("OPA"), found that 98% collected personal information.\textsuperscript{37} Three billion dollars was the total amount spent on mailing lists in 1996,\textsuperscript{38} and according to one estimate, direct marketing-generated electronic commerce could rise to thirty billion dollars by 2002.\textsuperscript{39} The direct marketing industry reportedly employs more than eighteen million people,\textsuperscript{40} and the business is growing at a rate estimated at twice that of the United States's gross national product.\textsuperscript{41}

The size of the deals between Internet marketing companies further demonstrates the enormity of the online profiling industry. The largest merger to date was the DoubleClick, Inc.\textsuperscript{42} merger with Abacus Direct Corporation.\textsuperscript{43} The merger was a $1.7 billion stock transaction,\textsuperscript{44} bringing together clickstream data "from the five billion ads DoubleClick serves per week and the two billion personally identifiable consumer catalog transactions recorded by DoubleClick Inc., now use cookies to track and profile the behavior of people at related sites across the Web without the knowledge of the computer user.\textsuperscript{35}

2. Widely Used Profiling is Big Business

Most web sites participate in the billion-dollar business of online profiling.\textsuperscript{36} In fact, a 1999 survey of the top one hundred web sites by the Online Privacy Alliance ("OPA"), found that 98% collected personal information.\textsuperscript{37} Three billion dollars was the total amount spent on mailing lists in 1996,\textsuperscript{38} and according to one estimate, direct marketing-generated electronic commerce could rise to thirty billion dollars by 2002.\textsuperscript{39} The direct marketing industry reportedly employs more than eighteen million people,\textsuperscript{40} and the business is growing at a rate estimated at twice that of the United States's gross national product.\textsuperscript{41}

The size of the deals between Internet marketing companies further demonstrates the enormity of the online profiling industry. The largest merger to date was the DoubleClick, Inc.\textsuperscript{42} merger with Abacus Direct Corporation.\textsuperscript{43} The merger was a $1.7 billion stock transaction,\textsuperscript{44} bringing together clickstream data "from the five billion ads

WASHINGTON POST, Jan. 2, 2000, at H1.

35. See id.


37. See Culnan, supra note 16.


40. See Fenrich, supra note 38, at 956.

41. See ARTHUR M. HUGHES, THE COMPLETE DATABASE MARKETER 5 (rev. ed. 1996) ("It is and will continue to be the hottest growth area in advertising for the foreseeable future.").

42. DoubleClick, Inc. is a leader in global Internet advertising solutions. See DoubleClick Homepage (visited Jan. 20, 2000) <http://www.doubleclick.com>.

43. See Lohr, supra note 32, at C1 ("Abacus... is an information company whose database contains the catalog-buying habits of 88 million households.").

44. See Macavinta, supra note 36.
Another notable transaction concerned Engage Technologies and AdKnowledge. In September of 1999, Engage agreed to buy AdKnowledge for $193 million in stock in order to add to its customer base and expand its Web advertising services.

B. Privacy Concerns

1. How Do People Feel About Profiling?

Notwithstanding the substantial benefits that consumers may receive through e-commerce and the Internet in general, consumers still care deeply about the privacy of their personal information in the online marketplace. According to Forrester Research, privacy is the number one concern of Internet users. In fact, privacy is such a substantial factor influencing how consumers spend their money that in 1999, privacy concerns cost e-commerce companies $2.8 billion in lost sales.

Since 1998, the Federal Trade Commission (FTC) has raised concerns about protecting the privacy of children's personal information online. The Commission testified...
before Congress to this end, and on October 21, 1998, President Clinton signed into law the Children's Online Privacy Protection Act of 1998 ("COPPA"). The Act went into effect April 21, 2000 and applies to the online collection of personal information from children under thirteen. The Act governs what web site operators must include in their privacy policy, when and how to seek verifiable consent from a parent, and what responsibilities an operator has to protect children's privacy and safety online.

2. The Pros and Cons of Profiling

"Thousands of web sites currently use cookies which allow sites and advertisers to 'remember' users across pages of a site, across multiple visits to a site, and across multiple sites." The concern about profiling centers around people wanting to know what is happening at the back-end when they are looking at targeted ads. The practice of online profiling has an unsettling effect on consumers when they think about someone following their every click and sharing this information with others without prior consent. People have this gut reaction about profiling because they do not know what information is being collected about them and they do not have choices about the collection or use of that personal information. The combined effect causes consumer confidence to decline.

On the other hand, when used properly, cookies may serve to enhance a user's Web viewing experience. Online retailers argue that collection of data enables them to give a more personalized shopping experience. They assert that

---

54. See id.
55. See id.
57. The back-end refers to hardware, software, and processes which reside or take place on the company side, i.e., not on the user's computer. The front-end, accordingly, refers to that which resides or takes place on the user's computer.
58. See Hon. William D. Daley, Secretary of Commerce, Remarks at the Public Workshop on Online Profiling (Nov. 8, 1999).
59. See id.
60. See id.
61. See id.
62. See Solomon, supra note 50, at 3B.
cookies and online profiling enable e-commerce and Internet advertising by remembering user names and passwords for allowing quick future visits, for controlling ad frequency, for regulating the number of times a user sees a given ad, and for delivering advertisements targeted to a user's interests. With profiling, companies can do a better job of offering the right products to the right consumers. They can do it more quickly and cost effectively.

3. What Has the European Union Done to Protect Personal Information?

The European Union adopted the Data Protection Directive ("E.U. Directive") in 1995. Effective October 25, 1998, the scope of the E.U. Directive is sweeping, including all "processing" of "personal data," with only limited exceptions. The directive defines "processing" broadly as "any operation or set of operations which is performed upon personal data, whether or not by automatic means." "Personal data" is similarly given broad construct and is defined as "any information relating to an identified or identifiable natural person ('data subject')."

a. The E.U. Directive Requirements

Pursuant to the E.U. Directive, each European Union Member State ("Member State") must adopt a strict privacy law that provides clear rights to data subjects. When collecting information from an individual, the individual's processing data (referred to in the E.U. Directive as "controllers") must disclose their identities and their purposes for processing. Data can only be processed for the announced purposes, contrary to the common U.S. practice of permitting a company to use personal data for unlimited use.

63. See id.
64. See Daley, supra note 58.
65. See id.
67. See id. art. 3.
68. Id. art. 2(b).
69. Id. art. 2(a).
71. See Council Directive 95/46, supra note 13, art. 10; see also id.
72. See Council Directive 95/46, supra note 13, art. 6(1)(b); see also Swire supra note 70.
purposes. Before data can be provided to third parties for targeted advertising, the individual must be informed and have the right to opt out at no cost. Those processing the data must also guarantee that individuals have access to their own personal data and the opportunity to correct that data. Other rules apply, with regard to “sensitive data” and require special restrictions on the processing of information about racial or ethnic origin, political opinions, or the processing of data concerning health or sex life.

b. E.U. Directive Enforcement

The E.U. Directive does not itself enforce these rights, but instead requires each Member State to promulgate a law that follows the E.U. Directive’s criteria. Actual enforcement thus takes place under the laws of each Member State. Under the E.U. Directive, each country must establish one or more data protection agencies, known as “supervisory authorities,” to help implement privacy rights. Supervisory authorities must have investigative powers and the power to engage in legal proceedings or to bring violations to the attention of judicial authorities.

According to Peter Swire, the Clinton administration’s chief counselor on privacy, supervisory authorities have usually worked informally with controllers when complaints are filed. Swire explained that in many instances, the controller explained why the practice in fact complies with applicable standards or agreed to modify the objectionable practice. Nonetheless, more formal sanctions are available and will be used under national laws, including ordering the

---

73. See Swire, supra note 70.
74. See Council Directive 95/46, supra note 13, art. 14(b); see also Swire, supra note 70.
75. See Council Directive 95/46, supra note 13, art. 12; see also Swire, supra note 70.
76. See Council Directive 95/46, supra note 13, art. 8(1); see also Swire, supra note 70.
77. See Swire, supra note 70.
78. See id. If a member state does not enact such a law, then a suit could ultimately be brought in the European Court of Justice to require such enactment. Id.
79. See id.
80. See Council Directive 95/46, supra note 13, art. 28(3); see also Swire, supra note 70.
81. See Swire, supra note 70.
82. See id.
erasure of data and bans on transfers of data to jurisdictions with weak or nonexistent privacy laws. In addition to administrative remedies, the E.U. Directive requires Member States to provide the right to a judicial remedy for breach of privacy rights.

c. Adequate Protection - Articles 25 & 26

Especially relevant to the U.S. and global e-commerce is Article 25 of the E.U. Directive, governing transfers of data out of the European Union. Article 25 allows transfers to non-Member States (e.g., the U.S.), only if that non-Member State ensures an "adequate" level of protection. The E.U. meaning of "adequacy" includes fair information practice principles, which lie at the center of the U.S. privacy debate between U.S. government officials, the European Union, private enterprise, consumers, and privacy advocates.

Where there is not adequate protection, personal information transferred from Europe to the U.S. would be permitted only under one of the exceptions in Article 26. One such exception involves unambiguous consent by the data subject to the proposed transfer. Another exception arises when the transfer is necessary for the performance of a contract, such as providing the name and address for shipping a purchase into Europe. Unless one of the

---

84. See Council Directive 95/46, supra note 13, art. 22. See also, Swire, supra note 70.
86. See id. art. 25(2). The Directive states that adequacy is assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.
88. See Mike Pramik, European View of Privacy an Issue in Data Transfer, BUS. TODAY, Jan. 11, 1999, at 3.
89. See Swire, supra note 70.
exceptions listed in Article 26 is satisfied, transfers of personal data are not permitted to countries lacking adequate privacy protection.  

E.U. officials make no secret of the fact that they regard the U.S. approach to data protection as generally inadequate. In fact, the U.S. policy of self-regulation has been a sticking point in long-running trade negotiations with Europe. Efforts to settle the dispute have involved top officials from both the U.S. and E.U., including David Aaron, the Undersecretary of Commerce for International Trade, and the European Union's top negotiator, John Mogg.

C. U.S. Adequacy: Self-Regulation or Legislation?

Since 1996, the FTC has encouraged a self-regulation approach to online privacy. It argues that as more consumers become aware of online privacy issues, they will become concerned. It follows that the private sector will respond to those concerns, just like it would be concerned with poor quality, high prices, or insufficient supply to meet consumer demand.

1. Self-Regulation

"Under [self-regulation], the incentives for industry to protect privacy are entirely financial." This model carries a key assumption that "there is no legal enforcement against a company that discloses personal information about its customers." The model subscribes to the idea that customers "can be directly attracted by a strong privacy

92. See Swire, supra note 70.
94. See Lohr, supra note 32, at C1.
95. See id.
97. See Kong, Online Privacy, supra note 7, at 1E.
98. See id.
100. Id.
protection policy or repelled by breaches of privacy." In fact, privacy concerns may become so important that they induce consumers to switch from one company to another. Therefore, a company's privacy policy becomes essential to maintaining a consumer base and "may become part of its overall marketing effort to develop brand equity and an image of quality service." As much as a good privacy policy can enhance a web site's reputation, a "bad customer experience or bad publicity about the company's privacy practices can detract from the company's total reputation for quality.

Under self-regulation, consumer preferences and publicity regarding a company's privacy policy serve as two forces that influence a company's privacy policy. "The more . . . consumers are willing to change their purchasing decisions based on the company's privacy policy, the greater the market discipline on companies." At the same time, "publicity affects customers' choices by informing them of which companies are meeting their preferences." In this regard, it may be safely assumed that the prospect of negative publicity may well encourage companies to conform to customers' preferences.

In addition to shaping a company's privacy policy, publicity may also shape consumers' preferences by raising awareness and concern about possible privacy issues. Therefore, the less consumers allow company privacy policies to dictate their purchasing decisions, and the greater the publicity surrounding a company's privacy issues, the more constrained a company will be in shaping its privacy policy in a manner that conforms to consumer preferences.

According to Orson Swindle, a commissioner with the Federal Trade Commission, "it's a competitive society, and the good businesses succeed and bad businesses fail, and one way to be labeled a bad business is start abusing your

101. Id.
102. See id.
103. Id.
104. Id.
105. See Swire, supra note 99.
106. Id.
107. Id.
108. See id.
109. See id.
customers or misusing their personal information.\textsuperscript{110}

2. Legislation

Legislation exists as an alternative to self-regulation.\textsuperscript{111} The argument here is that market forces do not adequately discipline companies and are largely or entirely ineffective at protecting the privacy of personal information.\textsuperscript{112} Consequently, individual privacy rights must be asserted through legal enforcement.\textsuperscript{113} Under this solution, privacy rules are defined by the government, whether by statute, agency regulation, or court decision.\textsuperscript{114} Designated parties, such as a government agency, a state, or the citizen being wronged, can sue to enforce those rules.\textsuperscript{115}

Enforcement under legislation seeks to achieve two goals: compensation and deterrence.\textsuperscript{116} When an individual’s privacy is violated, the individual is compensated to the extent of the violation.\textsuperscript{117} Beyond compensating the individual, legislation aims to deter companies through incentives.\textsuperscript{118} In other words, legislation gives corporations a disincentive to violate one’s privacy since the expected cost for that violation (in the form of compensatory payments plus fines) presumably exceeds the expected benefit from using the individual’s personal information in an unlawful manner.\textsuperscript{119}

D. Fair Information Practices

Over the past quarter century, government agencies in the U.S., Canada, and Europe have studied the manner in which entities collect and use personal information — their "information practices."\textsuperscript{120} As a result of those studies, safeguards have been developed to assure those practices are

\textsuperscript{110} Kong, Online Privacy, supra note 7, at 1E.
\textsuperscript{111} See Swire, supra note 99.
\textsuperscript{112} See id.
\textsuperscript{113} See id.
\textsuperscript{114} See id.
\textsuperscript{115} See id.
\textsuperscript{116} See id.
\textsuperscript{117} See Swire, supra note 99.
\textsuperscript{118} See id.
\textsuperscript{119} See id.
\textsuperscript{120} See FTC, PRIVACY ONLINE: A REPORT TO CONGRESS (1998) (Fair information practice principles were first articulated in a comprehensive manner in the United States Department of Health, Education and Welfare's seminal 1973 report entitled RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS.).
fair and provide adequate privacy protection. In a report to
Congress, the FTC identified the core principles required to
assure those information practices are fair and provide
adequate privacy protection. Those fair information
practice principles are: (1) Notice/Awareness, (2)
Choice/Consent, (3) Access/Participation, (4)
Integrity/Security, and (5) Enforcement/Redress. The U.S.
encourages web sites to incorporate these principles into their
privacy polices but have had limited success thus far
convincing web sites to provide this level of protection.

Of the principles, Notice/Awareness is touted as the most
fundamental: consumers must be given notice of a company's
information practices before personal information is collected
from them. Without notice, a consumer cannot make an
informed decision as to whether and to what extent he should
disclose personal information. All other principles are
rendered meaningless unless consumers have notice of an
entity's information practices and his or her rights with
respect thereto.

The Choice/Consent principle requires that consumers be
given options with respect to whether and how personal
information collected from them may be used. Specifically,
the principle relates to secondary uses of information, i.e.,
uses beyond those necessary to complete the contemplated

121. See id.
122. See id.
123. Such principles can be either procedural or substantive. Procedural
principles address how personal information is collected and used by governing
the methods by which data collectors and data providers interact. These
principles ensure that consumers have notice of, and consented to, an entity's
information practices. Substantive principles, by contrast, impose substantive
limitations on the collection and use of personal information, regardless of
consumer consent, by requiring that only certain information be collected and
that such information only be used in certain ways. See THE PRIVACY
PROTECTION STUDY COMMISSION, PERSONAL PRIVACY IN AN INFORMATION
125. See REPORT, supra note 7, at 7-8. Two industry-funded surveys of
commercial web sites conducted during the week of March 8, 1999 showed that
only 10% or 22% of companies, depending on the study, addressed all five
substantive fair information practice principles.
126. See id. at 3.
127. See id.
128. See id.
129. See id.
With respect to Choice/Consent, the consumer has historically been given two options: "opt-in" or "opt-out." Web sites adopting the opt-in approach require affirmative steps by the consumer to allow the collection and use of information, i.e., the consumer would need to choose to be on a company's general mailing list or marketing list sold to third parties. Opt-out web sites require the user to take affirmative steps to prevent the collection and use of his information. The key distinction between the two practices (and a topic of much debate) is in the default setting. In other words, if the consumer takes no affirmative steps, what happens to his or her personal information?

The Access/Participation principle requires giving consumers reasonable access to information collected about them and allows them to contest that data's accuracy and completeness. This principle demands that access be timely and user-friendly. It also demands that the means be in place to verify and send corrections to all data recipients.

The Integrity/Security principle requires that companies take reasonable steps to assure that information collected from consumers is accurate and secure from unauthorized use. Both managerial and technical measures are taken to protect against loss and the unauthorized access, destruction, use, or disclosure of the personal data. Included in managerial measures are internal organizational measures that limit employee access to data and ensure that those employees with access do not use the data for unauthorized purposes. Technical security measures to prevent unauthorized access include: encryption in data transmission and storage of data, limits on access through use of passwords, and data storage on secure servers that are

130. See id. at 9.
131. See FTC, PRIVACY ONLINE: A REPORT TO CONGRESS 9 (June 1998).
132. See id.
133. See id.
134. See id.
135. See REPORT, supra note 7, at 3.
136. See FTC, PRIVACY ONLINE: A REPORT TO CONGRESS 9 (June 1998).
137. See id.
138. See REPORT, supra note 7, at 3-4.
139. See FTC, PRIVACY ONLINE: A REPORT TO CONGRESS 10 (June 1998).
140. See id.
141. A server is a host computer on a network that holds information (e.g., web sites) and responds to requests for information from it (e.g., links to another web site). See Netlingo Homepage (visited Jan. 20, 2000)
located within an adequate firewall\textsuperscript{142} and do not allow remote access.\textsuperscript{143}

Finally, the effectiveness of the substantive fair information practice principles depends upon implementation of the Enforcement/Redress principle.\textsuperscript{144} This principle requires governmental or self-regulatory mechanisms to impose sanctions for noncompliance with fair information practices, and without it, the substantive principles are merely suggestive rather than prescriptive.\textsuperscript{145}

E. Privacy Seal Programs

The emergence of online privacy seal programs is the private sector's attempt at providing adequate protection of personal information through a self-regulatory approach.\textsuperscript{146} These programs require their licensees to abide by codes of online information practices and to submit to various types of compliance monitoring in order to display a proprietary privacy seal on their web sites.\textsuperscript{147} Seal programs offer an easy way for consumers to identify web sites that follow specified information practice principles, and for online businesses to demonstrate compliance with those principles.\textsuperscript{148} Of the privacy seal programs currently in existence, three of the most widely used are: TRUSTe, BBBOnLine, and CPA WebTrust.\textsuperscript{149}

1. TRUSTe

TRUSTe, an independent, non-profit organization was founded by the Electronic Frontier Foundation (EFF) and CommerceNet Consortium and launched in June 1997.\textsuperscript{150} TRUSTe issues its branded online seal, or "trustmark," to

\begin{itemize}
  \item \textsuperscript{142} A firewall is a device that protects a private network from the public part. It is designed to keep unauthorized outsiders from tampering with a computer system, therefore increasing a server's security. See Netlingo Homepage (visited Jan. 20, 2000) <http://www.netlingo.com>.
  \item \textsuperscript{143} Remote access is access to information from a location that is not within a company's firewall.
  \item \textsuperscript{144} See REPORT, supra note 7, at 4.
  \item \textsuperscript{145} See FTC, PRIVACY ONLINE: A REPORT TO CONGRESS 10 (June 1998).
  \item \textsuperscript{146} See REPORT, supra note 7, at 9.
  \item \textsuperscript{147} See id.
  \item \textsuperscript{148} See id.
  \item \textsuperscript{149} See id. at 9-12.
\end{itemize}
web sites that disclose what personal information is being
gathered, how it will be used, with whom it will be shared,
and whether the user has an option to control its
dissemination.151 An individual or company who licenses a
trustmark also submits to monitoring and oversight by
TRUSTe, as well as a complaint resolution procedure.152

The TRUSTe program includes third-party monitoring
and periodic reviews of licensees' information practices to
ensure compliance with program requirements. . . . These
reviews include 'web site reviews,' in which TRUSTe
examines and monitors changes in licensees' privacy
statements and tracks unique identifiers in licensees' databases (a practice known as 'seeding') to determine
whether consumers' requests to be removed from those
databases are being honored.153

"On-Site reviews" involve a third-party auditing firm
which may be called, should TRUSTe have reason to believe
that a licensee is not in compliance with the terms of the
license agreement.154 By January 12, 2000, TRUSTe had
awarded one thousand privacy seals.155

2. BBBOnLine

BBBOnLine, a subsidiary of the Council of Better
Business Bureaus, launched its privacy seal program for
online business in March 1999.156 In order to be awarded the
BBBOnLine Privacy Seal, applicants must take appropriate
steps to ensure that their information management practices
comply with their privacy policies and any applicable
BBBOnLine Privacy Program requirements.157 Most notable
among the privacy requirements is that the policy must
disclose: the collector(s) of the information,158 the type and
intended use of the individually identifiable information
being collected,159 the choices individuals have about the way

151. See id.
152. See REPORT, supra note 7.
153. Id.
154. See id.
156. See FTC, REPORT, supra note 7.
158. See id.
159. See id.
such information is used and to whom it is disclosed, and any individually identifiable information collected at the site which is shared with third parties and choices available to users with regard to this information.

3. CPA WebTrust

The American Institute of Certified Public Accountants ("CPA") and the Canadian Institute of Chartered Accounts created CPA WebTrust in September 1997. The privacy seal program mandates that certified public accountants award the CPA WebTrust seal to web sites who conduct quarterly audits to ensure compliance with the program's standards. While CPA WebTrust is primarily designed to disclose business practices and assure consumers of a web site's transaction integrity, it does have an information protection component. The requirement with regard to information protection is that the entity maintain effective controls to provide reasonable assurance that private customer information obtained through e-commerce is protected from uses not related to the entity's business. Twenty-seven web sites to date have passed the WebTrust examination conducted by a licensed CPA or chartered accountant, and are periodically examined by a WebTrust licensed CPA to ensure compliance with the above mentioned principles.

F. Recent Steps by the FTC

In November 1999, the FTC and the Department of Commerce held a public workshop on online profiling. The workshop was held to better understand the technology behind online profiling and consisted of panelists from both

160. See id.
161. See id.
162. See REPORT, supra note 7.
163. See id.
164. See id.
168. See Daley, supra note 58.
private industry and privacy advocacy groups. The workshop aimed to educate government officials and the public about the benefits and risks of the technologies behind online profiling and their implications for consumer privacy.

Another development came in December 1999, when the FTC announced the establishment of the Federal Trade Commission Advisory Committee on Online Access and Security. Having outlined five core fair information practice principles in their 1998 Report to Congress, the FTC noted in its follow-up report that Access/Participation and Integrity/Security are important privacy safeguards that face a number of implementation issues. The Committee was established to consider the parameters of reasonable access to personal information, adequate security measures to protect such information, and to present options for implementation of these fair information practices with the costs and benefits of each option.

The FTC's establishment of an Advisory Committee on Online Access and Security was a clear step toward identifying the more granular details of implementing fair information practice principles. The Committee issued its report in May 2000, and in a major policy shift, came to the conclusion that consumer confidence in using the Internet will increase if the FTC regulates how businesses use personal information collected online. Their studies led them to find that legislation is necessary to ensure Internet privacy protections and that "industry alone [has] not been sufficient."

In their report, the Commission recommended legislation

---

169. See id.
170. See id.
172. See id.; see also FTC, PRIVACY ONLINE: A REPORT TO CONGRESS (June 1998).
173. See FTC, Advisory Committee, supra note 171.
requiring adherence to fair information practice principles.\textsuperscript{176} They suggested requiring commercial web sites to notify visitors of what information is collected about them and how it will be used, to give visitors the option to choose whether information can be shared, and to give access to review information collected by a site as well as the security of that information.\textsuperscript{177} While the FTC voted to forward the privacy recommendations to Congress, the vote to issue the report was three to two, with Commissioner Orson Swindle dissenting.\textsuperscript{178} It is clear the FTC is not settled on the issue.

G. Legislative Options

Despite the FTC's recent efforts to educate itself and the public about online profiling, legislation remains a viable alternative to self-regulation. Over fifty bills resided in the 106th Congress addressing online privacy.\textsuperscript{179} Of those, two stand out as being representative of the sort of legislation that might replace the current self-regulatory approach toward online profiling.\textsuperscript{180}

1. Electronic Privacy Bill of Rights Act of 1999

Designed to prevent unfair and deceptive practices in the collection and use of personal information, Senator Edward Markey introduced the Electronic Privacy Bill of Rights Act of 1999 in November 1999.\textsuperscript{181} Senator Markey's bill covers all five of the fair information practice principles\textsuperscript{182} and allows the FTC to provide incentives for web sites to self-regulate and implement the protections afforded individuals by the Act.\textsuperscript{183} Violations of this bill would be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act.\textsuperscript{184}

\textsuperscript{176} See id.
\textsuperscript{177} See FAIR INFORMATION PRACTICES, supra note 174, at 36-38.
\textsuperscript{178} See Kong, supra note 7, at 1E.
\textsuperscript{179} See Associated Press, supra note 174.
\textsuperscript{180} See H.R. 3321, 106th Cong. (1999); S. 809, 106th Cong. (1999).
\textsuperscript{181} H.R. 3321.
\textsuperscript{182} H.R. 3321 § 3(b).
\textsuperscript{183} H.R. 3321 § 4(b)(1).
\textsuperscript{184} H.R. 3321 § 3(c).
2. Online Privacy Protection Act of 1999

Senator Conrad Burns introduced the second approach, the Online Privacy Protection Act of 1999, in April 1999. Senator Burns's bill makes it unlawful for an operator of a website to collect, use or disclose personal information concerning an individual in a manner that violates regulations to be prescribed by the FTC. The FTC regulations would be required to incorporate all five fair information practice principles. Under the bill, states are authorized to enforce such regulations by bringing actions on behalf of residents.

III. IDENTIFICATION OF THE PROBLEM

One source of insight into the adequacy of personal data protection has been the E.U. "Working Party on the Protection of Individuals with regard to the Processing of Personal Data" ("Working Party"). The Working Party issued an opinion regarding the level of U.S. data protection in January 1999, at which time the Working Party Commissioners took the view that voluntary self-regulation could not be relied upon to provide adequate protection in all cases for personal data transferred from the European Union. The Working Party opinion responded to the introduction of a set of "safe harbor" principles which would serve as an agreed "benchmark" standard of protection. The Working Party has since maintained the view, initially expressed in that January 1999 Opinion, that in terms of

185. See S. 809.
186. Individuals age 13 and above were not covered by the Children's Online Privacy Protection Act of 1998.
187. S. 809.
188. See S. 809.
189. See S. 809.
190. The Working Party is composed of a representative of the supervisory authority or authorities for each Member State, along with a representative of the Commission and a representative for any authority or authorities established for European Community institutions. See also, Council Directive No. 95/46, supra note 13, art. 29.
194. See id.
ONLINE PROFILING

substantive content, "any acceptable set of 'Safe Harbor' principles must, as a minimum requirement, include all the principles set out in the OECD Privacy Guidelines,"\textsuperscript{195} i.e., the fair information practice principles.

In the most recent opinion (adopted in December 1999), the Working Party reiterated this view and concluded that the proposed "Safe Harbor" arrangements remained unsatisfactory.\textsuperscript{196} How long until the American public and the E.U. tire of the self-regulatory efforts and demand proper protection of personal data? In light of the inadequate protection that self-regulation provides, my proposal is for Congress to adopt legislation in line with fair information practice principles such that online profiling may continue, but only with the consent of the consumer.

IV. ANALYSIS

A. Limitations of Self-Regulation and Legislation

In theory, either self-regulation or legislation could lead to optimal protection of privacy, but both are subject to market and government limitations.\textsuperscript{197} The most glaring limitation with regard to self-regulation is the fact that the ability of consumers to learn about and monitor a company's privacy policies is restricted.\textsuperscript{198} Customers may adopt strategies such as reporting different middle initials to each company and checking those names with each unsolicited letter or email, but in reality such efforts are costly in both time and effort.\textsuperscript{199} Opponents argue that because consumers will not be able to effectively monitor a company's use of


\textsuperscript{196}. See Opinion 7/99, supra note 195.

\textsuperscript{197}. See Swire, Protection of Personal Info., supra note 99.

\textsuperscript{198}. See id.

\textsuperscript{199}. See id.
personal information, it follows that they will not be able to discipline the company efficiently in the marketplace.200

Advocates of the self-regulation framework argue that legislation is limited by administrative costs and lack of flexibility.201 Costs include the expense of drafting, administering, and enforcing the rules.202 The assertion is that no matter how these functions are allocated between the branches of government, taxpayer funds are usually needed, and the amount of funding can be substantial.203

Of particular concern is the lack of flexibility of government rules.204 Government rules are hard to change, even when consensus exists in the agency and policy community that such a change is appropriate.205 This is true particularly during periods of rapid technological and market changes.206 The present day sees the uses of personal data undergoing just this sort of rapid change and arguably rules promulgated under today’s assumptions will make less sense when the technical and economic realities change.207

B. The U.S. Self-regulatory Approach Has Not Worked

Jupiter Communications estimates that consumers spent $7 billion dollars online during the 1999 holiday season, up from $3.1 billion for the same period in 1998.208 With online profiling on the rise too,209 concerns about privacy protection are at the forefront of the public agenda.210

When the FTC released its 1998 report to Congress,211 there were indications that industry leaders committed themselves to working toward self-regulatory solutions.212 At

200. See id.
201. See id.
202. See id.
204. See id.
205. See id.
206. See id.
207. See id.
209. See Kong, Online Profiling, supra note 8, at C1.
210. See Solomon, supra note 50, at 3B.
211. See FTC, PRIVACY ONLINE: A REPORT TO CONGRESS (June 1998).
212. See Prepared Statement of the Federal Trade Commission on “Self-Regulation and Privacy Online,” before the Subcommittee on Communication of
that point, the FTC had concluded that an effective self-regulatory system had not yet emerged, but was willing to defer judgment on the need for legislation. In its 1999 Report, the FTC further conceded that much remained to be done to ensure the widespread adoption and implementation of fair information collection practices.

Supporting this concession were two industry-funded surveys of commercial web sites. The surveys clearly suggested that despite self-regulation and the attention online privacy has received, web sites were not adopting fair information practice principles. Only 10% of the sites in the GIPPS sample and only 22% of the sites in the OPA study implemented all five substantive fair information practice principles.

The May 2000 Report discloses the results of a more recent survey that indicates little change since the 1999 Report to Congress. According to the survey, only 20% of web sites in a random sample of 335 web sites collecting personal information implement all five fair information practice principles. And of 91 of the 100 busiest web sites, 42% implement such principles.

Other surveys tell a similar story. Seventy-one percent of U.S. households with access to the Internet say the possibility that their personal details might become available to third parties discourages them from making online purchases. Seventy percent of respondents in another recent national

---


213. See REPORT, supra note 7, at 4.
214. See Prepared Statement, supra note 212.
215. See id.
216. See REPORT, supra note 7, at 8.
217. See id.
218. See id. at 7 (the Georgetown Internet Privacy Policy Survey ("GIPPS") reporting findings on the information practices of 361 web sites drawn from a list of the 7,500 busiest servers on the Web).
219. See Culnan, supra note 16.
220. See Prepared Statement, supra note 212.
221. Conducted during the months of February and March 2000.
222. See FAIR INFORMATION PRACTICES, supra note 174.
223. See id.
survey reported that they were uncomfortable providing personal information to businesses online.\(^{225}\) Also, 87% of U.S. respondents in yet another recent survey of Internet users stated that they were somewhat or very concerned about threats to their privacy online.\(^{226}\)

When asked if he thought that privacy seal programs effectively protected consumers' privacy and would eliminate the need for legislation, Orson Swindle, a commissioner with the FTC replied in the negative saying, "We've got a long way to go."\(^{227}\) In light of the statistics and FTC statements regarding the status of self-regulation, it can reasonably be inferred that self-regulation and privacy seal programs are not working.

C. Technology-Based Solutions

The web user can take steps without assistance from the marketplace or the government. One such method would be to disable the Web browser's setting for accepting cookies.\(^{228}\) While turning off cookies will stop one's online profile from growing so rapidly, it may prevent the user from entering into certain web sites that require the use of cookies.\(^{229}\) Hotmail.com, for example, will not allow access if the browser's cookie setting is disabled.

The web user can also install software that notifies the user when a web site or third party attempts to send him a cookie.\(^{230}\) These cookie alerts give the user the option to accept or reject a particular cookie, and provide the name of the company that is doing the collection. While these home remedies may temporarily ease online privacy concerns, they merely allow one to identify the company collecting information and give that person the option to say "no." The


\(^{227}\) See Kong, Online Privacy, supra note 7, at 1E.

\(^{228}\) Both Microsoft's Internet Explorer 5.0 and Netscape's Navigator 4.04 offer this ability.

\(^{229}\) See supra note 4.

\(^{230}\) Microsoft's Internet Explorer 5.0 notifies users of this fact as they change the cookie setting.

\(^{231}\) McAfee's Guard Dog and eSafe Protect are two examples.
browser setting and software programs should in no way be understood as a means for solving the greater issue of privacy.

D. A Closer Look at Legislation

The FTC adopted self-regulation believing that it was the least intrusive and most efficient means to ensure fair information practices online.\(^2\) Despite the efforts of the FTC and private industry, a commitment to fair information practice principles is needed. While government regulation is usually touted as a last resort, only to be used if the private sector fails,\(^3\) the marketplace has had ample opportunity to demonstrate the superiority of self-regulation. It appears that the experiment has failed.

While both Senator Markey's and Senator Burns's bills reflect fair information practices, only Senator Markey's bill outlines specific guidelines based upon the fair information practice principles.\(^4\) Senator Burns's bill does not identify guidelines and instead entrusts the FTC to prescribe regulations to protect the privacy of personal information. Because Senator Markey's Electronic Privacy Bill of Rights Act of 1999 is the more complete of the two, the adoption of the Act would attain "adequacy" in the eyes of the E.U. and renew consumer confidence in the online marketplace.

1. Senator Markey's Bill

The Electronic Privacy Bill of Rights Act of 1999\(^5\) would require operators of any web site or online service that collects personal information to implement a framework of privacy protections that reflects the fair information practice principles.\(^6\)

Satisfying the Notice/Awareness principle, "[the Act] requires clear and conspicuous notice on the web site of the specific types of personal information collected by the operator, how the operator uses such information, and the operator's disclosure practices for such information."\(^7\)

---

232. See Prepared Statement, supra note 212.
235. See id.
236. See H.R. 3321 § 3(b).
Addressing Choice/Consent, the Act requires the operator of such a web site to provide a clear and explicit online method by which an individual grants or denies consent to the collection and use of the information disclosed by the web site.\(^{238}\)

Incorporating Access/Participation into the Act, it requires that the “operator of such a web site provide individuals, upon request, access to personal information pertaining to them.”\(^{239}\) The Act would also require the web site to disclose “whether any personal information pertaining to such individual has been reused, disclosed, or sold and to whom.”\(^{240}\)

Addressing the last of the substantive principles, Integrity/Security, the Act “requires the operator of such a web site to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected.”\(^{241}\)

There are two ways to accomplish the Enforcement/Redress principle. The Act permits states to bring civil actions on behalf of the residents of the state, and also gives individuals a private right of action.\(^{242}\) Willful and knowing violations increase the amount of damages recoverable.\(^{243}\) While the Act mandates fair government enforcement procedures, it also combines incentives for effective self-regulation.\(^{244}\) Under the Act, the FTC would provide incentives for self-regulation by operators to implement the protections afforded individuals by the Act.\(^{245}\)

### 2. The Bill in Light of the E.U. Directive

The Act not only reflects fair information practice principles, but also satisfies the other E.U. criteria for adequate protection of personal information. In an effort to assist the U.S. with its self-regulatory approach, a 1998 E.U. Working Party document clarified how the E.U. would

\(^{238}\) See H.R. 3321 § 3(b)(1)(B)(i).
\(^{239}\) H.R. 3321 § 3(b)(1)(D)(i).
\(^{241}\) H.R. 3321 § 3(b)(1)(E).
\(^{242}\) See H.R. 3321 §§ 5, 7(a).
\(^{243}\) See H.R. 3321 § 7(b).
\(^{244}\) See H.R. 3321 § 4(b)(1).
\(^{245}\) See H.R. 3321 § 4(b)(1).
evaluate the effectiveness of a self-regulatory instrument.²⁴⁶

The document explains that for a self-regulatory instrument
to be considered a valid ingredient of "adequate protection" it
must be binding on all the members to whom personal data is
transferred and provide for adequate safeguards if data is
passed on to non-members.²⁴⁷ The plan must also include the
tour substantive fair information practice principles,²⁴⁸ must
have mechanisms which effectively ensure a good level of
general compliance,²⁴⁹ and a data subject must be able to
obtain a remedy for his problem and compensation as
appropriate.²⁵⁰

The Act addresses all of the E.U.'s criteria for evaluation.
If enacted, the Act would be binding on all web sites collecting
personal information with few exceptions.²⁵¹ By allowing a
civil and private right of action, the Act would also ensure a
good level of general compliance.²⁵² Remedies are also
available via the Act, through an injunction, monetary
damages, or both.²⁵³

V. PROPOSAL

To the extent that the U.S. desires to qualify as an
"adequate" provider of personal data protection and thereby
comply with the E.U. Directive, and also regain the
confidence of its consumers, the U.S. must adopt legislation.
Senator Markey's bill should be adopted since it is the most
complete bill in Congress and outlines specific guidelines
based upon the fair information practice principles. Adoption
of the Act would not only attain "adequacy" in the eyes of the
E.U., but would also renew consumer confidence in the online
marketplace. As technology advances in the area of online
profiling, a certain framework of protection is needed, one
that will not hinder innovation. Giving consumers choices
and the ability to take some control over who collects their

²⁴⁷. See id.
²⁴⁸. See id.
²⁴⁹. See id.
²⁵⁰. See id.
²⁵². See H.R. 3321, §§ 5, 7(a) ("Under civil actions, the State may enjoin that
practice at issue; enforce compliance with the rule; obtain damage, restitution,
or other compensation on behalf of residents of the State; or obtain such other
relief as the court may consider to be appropriate").
²⁵³. See H.R. 3321, §§ 5, 7(a).
personal information and how they use it will not cause technology to suffer because the means of collection are not being addressed in the bill. The Electronic Privacy Bill of Rights Act of 1999 merely gives the consumer control over his own personal information.

VI. CONCLUSION

As more people get online and e-commerce becomes an easier and more efficient means for shopping, concerns about online privacy will continue to escalate. "Notwithstanding the substantial benefits that consumers may receive through online profiling, consumers care deeply about the privacy of their personal information," and their voices of concern are becoming louder as they begin to understand just how much information about them is gathered.254

The European Union has already adopted legislation to protect personal information and requires the U.S. to take certain "adequate" steps to ensure the privacy of Europeans who do business with U.S. companies.255 Because of the global nature of e-commerce and the potential revenue that might be realized by a global market, the U.S. cannot afford to ignore the E.U. Directive.256 The U.S. response has been to approach online privacy with self-regulation, believing that market forces will make web sites comply with consumer demands for protection of their personal information.257 However, web sites have been reluctant to give consumers the choices and access to personal information that the E.U., privacy advocates, and consumers demand.258

Because self-regulatory efforts have been largely unsuccessful, adoption of Senator Markey's Electronic Privacy Bill of Rights Act of 1999 is the appropriate measure to take. Designing the bill around fair information practice principles and providing incentives for self-regulation, the bill would not only attain "adequacy" in the eyes of the E.U., but would also renew consumer confidence in the online marketplace. Lastly, because the bill does not address the means for collection and consumers may opt-in to receive targeted

254. REPORT, supra note 7, at 2.
256. See McLymont, supra note 14, at 1A.
257. See Kong, Online Privacy, supra note 7, at 1E.
258. See Culnan, supra note 16.
advertisements, technological advancement in online profiling will continue and will not suffer as a result.

As stated by the Secretary of the U.S. Department of Commerce, Hon. William D. Daley, "If a web firm fails to protect consumers' privacy, if they fail to disclose, if they fail to give consumers choice, I guarantee you that government will be forced to step in."259 That time is now, and Senator Markey's bill is the answer.

259. Daley, supra note 58.