Information Harvesting on the Internet: A Consumer's Perspective on 2001 Proposed Legislation Restricting the Use of Cookies and Information Sharing

Alexander H. Burke

Follow this and additional works at: http://lawecommons.luc.edu/lclr

Part of the Consumer Protection Law Commons

Recommended Citation


Available at: http://lawecommons.luc.edu/lclr/vol14/iss2/2
STUDENT ARTICLES

Information Harvesting on the Internet: A Consumer’s Perspective on 2001 Proposed Legislation Restricting the Use of Cookies and Information Sharing

Alexander H. Burke*

I. Introduction

Technological advances such as the Internet constantly challenge perceptions of privacy. In 1890, Louis Brandeis defined privacy as “the right to be let alone.”1 Since then, the law of privacy has developed along with technology. Indeed, Justice Scalia contemplated this very notion recently with respect to Fourth Amendment privacy rights in the recent Kyllo2 case:

It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology. For example, the technology enabling human flight has exposed to public view (and hence, we have said, to official observation) uncovered

* J.D. candidate, May 2003, Loyola University Chicago School of Law; B.A. International Relations, 1997, Colgate University. The author would like to thank his family and friends for their help and support, especially Robert Burke and Tom Burke for their insightful suggestions and comments.


portions of the house and its curtilage that once were private.\(^3\)

The \textit{Kyllo} case, which ruled that infrared technology used to look “through” exterior walls of buildings to find sources of heat was unconstitutional without a search warrant, illustrates the need for continuously developing privacy law to keep up with technology. It is time for the law to catch up with Internet information gathering technology in particular.

Before marketing technological breakthroughs, business owners were successful because they paid attention to their customers’ habits. For example, every time Alice came into his deli, Sam the butcher had just what she had ordered for the “Brady Bunch” wrapped and ready. Sam was probably able to suggest one particularly good cut of meat or another for the Bradys, and even put some cuts of meat on special knowing that there was a likely chance that Alice would be interested. Sam was able to make these suggestions because he had, over a long period of time, developed a personal relationship with the family, and through that relationship had come to understand the Brady family’s tastes and preferences. The line between “customer” and “friend” had blurred, and because of that blurring, Sam understood more about the Bradys than other local vendors who did not know the family as personally. He was successful in his job because he paid attention to his customers’ habits.

Today, with super-efficient computer data sorting and technological breakthroughs in data gathering, the methods that Sam the butcher used to determine what the Bradys might be interested in has been taken much further.\(^4\) Indeed, information gathering has become a vast industry, with companies interested in much more than whether consumers prefer ground round or ground chuck.\(^5\) This information gathering is done by nameless, faceless computer servers, rather than by a friendly face like Sam, and is capable of creating, and often is designed to create, a much more personal profile about Internet surfers than Sam likely ever imagined.

\(^3\) \textit{Id.}


\(^5\) \textit{Id.} at 1404.
The history of advertising reveals how ancient Sam’s method was compared to information gathering techniques on the Internet.6 Indeed, it was only in the late nineteenth and twentieth centuries that product marketing went so far as to design an advertising campaign for the general American consumer.7 Before then, butchers and all other types of vendors had been using Sam’s “neighborly method” of targeted advertising. With the advent of mass production and distribution, marketers soon realized that they were faced with a much larger potential customer base than ever before. This customer base was so vast that advertising became inefficient because many of the individuals it reached were not interested in the advertised products. Marketers saw that they could more effectively advertise if they targeted their campaigns toward those who were most likely to purchase their products.8

Advertisers did this originally through radio and television, choosing, for example, children’s shows during which to advertise toys, and adult shows, such as the nightly news, to show off their newest automobile style.9 Next came targeted advertisements via United States Mail, relying on zip codes to target potential consumers by specific neighborhoods.10 Luxury item advertisements could be sent, for example, to households in Beverly Hills, Chicago’s North Shore and New York’s Upper East Side, rather than to entire cities, thus making mailings more efficient. Finally, marketers began to gather information through surveys where consumers volunteered their information either in exchange for goods or services, or simply because they did not mind taking the time to do so. These practices of harvesting information, along with other aggregate sources of information such as phone books, led to telemarketing, an even more targeted form of advertising.11

The most recent frontier of information gathering happens on the Internet, which, because of software application innovations, allows information harvesting on an unprecedented scale.12 The scope

---

6 Id. at 1404-13. Of course, the neighborly method of advertising is still valid and useful.
7 Id. at 1404.
8 Id.
9 Id. at 1405.
10 Id. at 1405-06.
11 Id. at 1405.
12 Id. at 1409.
of harvesting is large both on the horizontal and vertical axis. Horizontally, Internet use and information gathering is prolific: over one-third of the American population uses the Internet, and it is nearly certain that a surfer will hit a website that is harvesting her information. On the vertical access, websites gather enormous amounts of information about every visitor, often times sharing that information with third parties. The problem is not only that the information electronically gathered is extremely detailed, but also that it is easily transferred to others, thus making the consumer more susceptible to her information being used for marketing or ominous purposes, such as identity theft.

Not surprisingly, consumers are concerned about these issues. A recent study showed ninety-two percent of consumers are “concerned” and sixty-seven percent are “very concerned” about the misuse of their personal information gathered online. Indeed, seventy-six percent of consumers who are generally not concerned with their privacy while off-line fear for their privacy while online. The Federal Trade Commission (“FTC” or “Commission”) believes that these fears result in fewer online sales and a net loss to Internet businesses, and therefore should be calmed. Studies estimate that $2.8 billion was lost in retail sales in 1999 because of consumer

---


17 Privacy Online, supra note 14, at 9.

18 Id.

19 Id.

20 Id.
skepticism and privacy concerns. This figure is estimated to rise to $18 billion in 2002.

This article will explore policy concerns and considerations as they relate to privacy and information harvesting and sharing on the Internet. The Background section will explain existing legislation that could affect information harvesting and sharing. The next section will examine the existing FTC self-regulatory policy and its recommendations for legislation, and explain the most relevant attempts at legislation that were proposed in 2001. Finally, this article will assess the FTC recommendations and proposed legislation, and will make regulation suggestions based on the consumer's point of view.

II. Background

A. Types of Information

Of course, some of the types of information gathered by websites are more invasive to surfers' privacy than others. This article will distinguish between three types of information, which are gathered in various ways: (1) pseudo-anonymous information; (2) personal information; and (3) sensitive personal information. The most commonly gathered of the three types is pseudo-anonymous information, which websites may gather without any user action other than visiting their website. Pseudo-anonymous information includes the unique browser identifier number assigned by that particular website, IP address, the pages within a particular website that the surfer visited, and the websites visited immediately before and after the surfer visits the collecting site. Personal information is only available to a website if the surfer gives the information out, and includes information such as the surfer's name, address, email, phone number, marital status, sex, and birth date. Sensitive personal

21 Id.
22 Id.
24 The title of this type of information came from the text of the Consumer Privacy Protection Act, H.R. 2135, 107th Cong. § 3(a)(1)-(2) (2001).
25 "IP address" refers to the service that provides the surfer Internet access, such as AOL, Earthlink or Compuserve.
information includes information such as the surfer's credit card number, bank account information, social security number, health care information and sexual preference. These different types of information may be harvested through a few common computer innovations laid forth below.

B. Technical Background

There are several ways that websites gather various types of information about their visitors. These methods vary in consumer interaction and knowledge, from the voluntary and transparent harvesting technique of asking for the information, to the invisible "gif" file that tracks mouse clicks.

1. Forms & Surveys

The most transparent way websites gather personal and sensitive personal information is to ask for it. The user knows exactly what information is being shared, and, until the time she submits the information to the site, has control over what information (other than pseudo-anonymous information) the website gathers. These forms are often placed on web pages as a condition to receiving products or services, or as conditions to entry into a sweepstakes. However, web surfers enter information into forms on the Internet at their own peril: once the information is in the website's database, the site may sell or share that information with anyone, restricted only by the privacy policy that it drafted itself, if it has a privacy policy at all.

2. Cookies

A cookie is a small text file containing a unique string of numbers or letters that is placed on an Internet surfer's computer.

---


27 Bob Tedeschi, E-COMMERCE REPORT; Internet Merchants Turn to Online Sweepstakes, N.Y. TIMES, June 19, 2000, at C11.

28 Privacy Online, supra note 14, at 34.

When a web surfer first visits a web page that uses cookie technology for serving advertisements or recording web usage, the cookie assigns the surfer’s browser a unique number. At this point the number is not associated with any other information. Then, each time the surfer visits a web page associated with the website from which that particular cookie was placed, the website that assigned the cookie will recognize the unique identifier number and associate the surfer’s present browsing with her past browsing. Websites store nothing but the small cookie file on the surfer’s computer; they use the identification number assigned to that file to associate the surfer’s browser with information previously harvested and stored on the website’s computers. Thus, cookies facilitate a passive exchange of information, creating a profile of the surfer on the website’s computer without the user necessarily knowing.

Cookies, when used alone, are capable of gathering pseudo-anonymous information only. However, when coupled with personal information gathered through registration processes and various other gathering techniques, cookies can be used to associate one flesh-and-blood web surfer and his personal information with his pseudo-anonymous information, thus converting pseudo-anonymous information into personal information. This type of association becomes even more invasive and potentially hazardous to a surfer if he makes an online purchase. This is because when the surfer enters his credit card information onto the website, the whole lot of information linked to that unique browser’s identification number converts to sensitive personal information, aggregately creating an extremely detailed profile of the user.

\[ \text{id.} \]

\[ \text{id.} \]

\[ \text{id.} \]

\[ \text{id.} \]

\[ \text{id.} \]

\[ \text{id.} \]

\[ \text{id.} \] at 297.
3. Web Bugs / Web Beacons

Action tags (commonly known as “web bugs”)\(^\text{36}\) are a close relative of cookies.\(^\text{37}\) Web bugs are extremely small “gif” files\(^\text{38}\) that are placed on a website and “attach” to the surfer’s screen.\(^\text{39}\) Because they are so small they are invisible to the surfer, yet they are powerful enough to allow third party advertisers to monitor his clicks and entries into forms throughout the site, and affiliated sites.\(^\text{40}\) Yahoo! expresses this notion well in its stated privacy policy: “Being able to access Yahoo! cookies [through web bugs] allows us to personalize your experience when you visit Yahoo! websites that are not on the yahoo.com domain (like Yahoo! GeoCities that has pages on www.geocities.com).”\(^\text{41}\) Perhaps even more invasively, web bugs may be placed within html email messages so that they let the sender of the email know if and when the messages have been opened, and whether they have been acted upon.\(^\text{42}\)

C. Federal Legislation

The federal government has not directly addressed website information harvesting of adult surfers’ information. However, there are several existing laws that are closely related to the subject. The following is a list and, in the interest of the focus and scope of this article, cursory analysis of those laws.


\(^{38}\) These gif files take up one pixel of the user’s screen.

\(^{39}\) Chance, 165 F. Supp. 2d at 1157.

\(^{40}\) Id.


1. Children’s Online Privacy Protection Act

The Children’s Online Privacy Protection Act ("COPPA"), passed in October 1998, was one of the very first laws dealing explicitly with online privacy.\(^{43}\) It expanded the FTC’s power to curtail information gathering on the Internet.\(^{44}\) If a website is directed toward children under thirteen, or should know that its site is being used by children under thirteen, then it must comply with five key requirements: (1) notice to the surfer of what information is being harvested and how it is being used; (2) parental consent for surfers under thirteen; (3) parental review of website material and privacy practices; (4) limits on the use of games and prizes; and (5) security of information that is harvested.\(^{45}\) The scope of the act is limited in that it applies only to those websites directed toward children.\(^{46}\) COPPA serves an important purpose in that it protects children, but falls short of protecting adults’ information.

2. Electronic Communications Privacy Act

Title II of the Electronic Communications Privacy Act ("EPCA")\(^{47}\) is designed to “prevent hackers from obtaining, altering or destroying certain stored electronic communications.”\(^{48}\) It creates both criminal and civil causes of action toward this end, making it unlawful for persons to gain unauthorized access to communications facilities and their data.\(^{49}\) The relevant portion of the statute makes it unlawful to intentionally, without authorization or in excess of authority, access an information service facility and obtain access to its electronic information.\(^{50}\)


\(^{44}\) Id.


\(^{46}\) See Warmund, supra note 43, at 194-95.

\(^{47}\) 18 U.S.C. § 2701 et. seq.

\(^{48}\) In re DoubleClick Privacy Litig., 154 F. Supp. 2d 497, 507 (S.D.N.Y 2001).

\(^{49}\) Id.

\(^{50}\) 18 U.S.C. § 2701(a)(1)-(2) (2001). There are three exceptions to the ECPA’s prohibitions on access to stored communications. The ECPA does not proscribe conduct which is authorized: (1) by the party or entity providing the electronic
Plaintiffs have attempted to use the EPCA to stop advertisers from gathering their information through cookies and web bugs, but have failed because users generally contractually authorize websites to gather information. Sites that allow banner advertisements generally authorize their advertisers to access gathered information. Thus, because cookies do not actually store information (they merely identify browsers associated with information), there is no cause of action under this law that will stop third parties from obtaining personal information. Thus, although the law on its face may appear to make harvesting information through cookies and web bugs unlawful, courts have consistently held that it does not.

3. Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act of 1986 ("CFAA") is aimed at those gathering governmentally-sensitive information from others' computers. The CFAA prohibits knowing, unauthorized, or in excess of authorization, access of a computer in order to obtain information determined by the United States Government to require protection. "Access," as outlawed by the CFAA, occurs when an individual willfully communicates or attempts to communicate, deliver or transmit restricted data to anyone not entitled to receive it, or retains restricted data and fails to deliver it to the officer or employee of the United States entitled to receive it.

Although related to privacy and computer integrity, this Act is not likely to stop the kind of information harvesting with which this article is concerned. Two of the earliest cases that implemented this Act are indicative of its scope. In 1989, Hebert Zinn was the first to be convicted of a violation of the CFAA for accessing a computer with the intent to impair its availability or integrity; for purposes of unauthorized access to a computer without authorization of the owner of a computer, or exceeding authorized access to a computer; for using a computer to attempt to engage in electronic communication with any person; and for using a computer to cause an electronic communication to be sent to any person.

51 See DoubleClick, 154 F. Supp. 2d at 510-12.
52 DoubleClick, 154 F. Supp. 2d at 510-12.
53 See, e.g., id.
54 Peter Brown, Patents, Copyrights, Trademarks, and Literary Property Course Handbook Series, 637 PLI/Pat 131, 141 (Feb./Mar. 2001).
56 Id.
convicted under the Act. Zinn broke into AT&T and the Department of Defense's computer systems and was found guilty of destroying $174,000 worth of files, copying programs worth millions of dollars, and publishing passwords and information on how to violate computer security systems. Next, in 1988, a graduate student named Robert Morris released a "worm" program to go through the Internet in search of security weaknesses it could exploit. The worm was also programmed to multiply itself, and crashed over 6,000 systems costing its victims days of productivity and possibly millions of dollars. Thus, although it relates to security of online information, the CFAA has little to do with curtailing information harvesters.

4. Gramm-Leach-Bliley Act

The Financial Modernization Act, more commonly known as the Gramm-Leach-Bliley Act ("GLBA"), creates notice requirements and restricts financial institutions' abilities to disclose nonpublic personal information about consumers to nonaffiliated third parties. The GLBA states that financial institutions have obligations to respect the privacy of their customers and to protect the security and confidentiality of those customers' nonpublic personal information. The GLBA orders the FTC, Securities and Exchange Commission, and Federal Reserve to issue regulations that: (1) insure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of such records; and (3) protect against unauthorized access to or use of

57 Brown, supra note 54, at 141.
58 Id.
59 Id.
60 Id.
62 15 U.S.C.A. § 6809(3). The entities covered include, but are not limited to, mortgage lenders, "pay day" lenders, finance companies, mortgage brokers, account servicers, check cashers, wire transferors, travel agencies operated in connection with financial services, collection agencies, credit counselors and other financial advisors, tax preparation firms, non-federally insured credit unions, and investment advisors that are not required to register with the Securities and Exchange Commission.
such records or information that could result in substantial harm or inconvenience to any customer.\textsuperscript{64}

The GLBA applies to information gathered by financial institutions on the Internet through forms, cookies and web bugs.\textsuperscript{65} As implemented, the GLBA does permit financial institutions to share this nonpublic personal information with their affiliates.\textsuperscript{66} However, financial institutions are permitted to share nonpublic personal information with third parties only if proper notice has been given to the consumer whose information will be shared.\textsuperscript{67} The consumer has to opt-out of information sharing, which requires that he be aware of the financial institution's policies through the notice he received pursuant to the GLBA.\textsuperscript{68}

5. Health Insurance Portability and Accountability Act

In 1996, Congress addressed the issue of privacy of health information in the Health Insurance Portability and Accountability Act ("HIPAA") of 1996.\textsuperscript{69} HIPAA required the Department of Health and Human Services ("HHS") to promulgate regulations to govern the privacy of all medical records.\textsuperscript{70} HHS issued regulations that, among other things, require authorization for all information uses and disclosures beyond those necessary for treatment, payment, or health care operation, including information sharing for marketing purposes.\textsuperscript{71}

\footnotesize{\textsuperscript{64} Id.}

\footnotesize{\textsuperscript{65} Martin Hsia, Intellectual Property And Technology Law In The Internet Age, 5-Nov. HAW. B.J. 4, 9 (2001).}

\footnotesize{\textsuperscript{66} See Solove, supra note 4, at 1443 (useful deconstructions of the GLBA and HIPAA).}

\footnotesize{\textsuperscript{67} 15 U.S.C. § 6802(a).}

\footnotesize{\textsuperscript{68} 15 U.S.C. § 6802(b).}


\footnotesize{\textsuperscript{70} 110 Stat. at 2033-34.}

\footnotesize{\textsuperscript{71} 45 C.F.R. § 164.508 (2001).}
D. The Current Self-Regulatory Environment

1. FTC Power

The FTC’s power to regulate data collection online is derived from Section five of the Federal Trade Commission Act (“FTC Act”), and from COPAA, discussed above. The FTC Act prohibits unfair and deceptive commercial practices affecting commerce. It allows the FTC to seek injunctive and equitable relief, including redress for violations, and authorizes the Commission to act in order to enforce certain fair information practices. Thus, if a website posts a privacy statement and violates its own stated policy, it will have committed an unfair information practice and will be held liable under the FTC Act. The Commission’s power with respect to harvesting adults’ information stops there, however, because whether or not to have a privacy statement at all is still up to the website.

2. Seal Programs

The online industry’s primary self-regulatory technique is implemented through “seal programs.” Seal programs allow websites that comply with their own FTC-approved privacy policies to post a trademark-type seal on their site, signifying to consumers that they implement privacy policies approved by a seal program. The idea is to create an industry-wide standard of reliability so that consumers may browse with confidence, knowing that their personal information is being gathered in a responsible manner. The seal program was the

---

73 Privacy Online, supra note 14, at 33.
75 Id.
76 Privacy Online, supra note 14, at 33.
77 Id.
78 Id. at 6.
79 Id.
80 Id.
website industry’s way of circumventing what they consider “costly” legislation.\textsuperscript{81}

However, there are flaws in these programs. First, many approved websites have multiple privacy policies that relate to different portions of their site.\textsuperscript{82} Thus, information related to a financial transaction may be stored, but not shared, while information gathered from a sweepstakes entry may be shared without discretion.\textsuperscript{83} These practices may fit within the website’s privacy policy, but these policies may be too difficult to understand for consumers.\textsuperscript{84}

Second, sites may promise never to share a surfer’s information with others, but have links to other websites that may not have privacy policies at all. For example, Yahoo! states in its privacy policy that there may be ad banners on their site, over which surfers have no control, that use cookies, and that “[i]f you want to prevent a third-party ad server from sending and reading cookies on your computer, currently you must visit each ad network’s website individually and opt-out (if they offer this capability).”\textsuperscript{85}

Finally, seal programs are funded by license fees from their members,\textsuperscript{86} and depend on relicensing in order to continue existing.\textsuperscript{87} This circular relationship is common among self-regulatory environments, and the Internet community is a fine example of its failure. As Marc Rotenberg, Director of the Electronic Privacy Information Center (“EPIC”) commented: “Simply stated, our policy is backward. We impose government controls on techniques to protect privacy, where market-based solutions are preferable. And we leave

\begin{footnotes}

\textsuperscript{82} \textit{Privacy Online}, supra note 14, at 21.

\textsuperscript{83} \textit{Id.} at 22.

\textsuperscript{84} \textit{Id.}


\textsuperscript{87} See \textit{id.}
\end{footnotes}
privacy problems to the market, where government involvement is required.\textsuperscript{88}

III. FTC Recommendations

In response to public and Congressional concern, the FTC has been examining consumer privacy on the Internet and the availability of sensitive personal identifying information through computerized database services since 1995.\textsuperscript{89} The FTC found that information in those databases was being used by “individual reference” or “look-up” services to locate, identify or verify the identity of individuals.\textsuperscript{90} Gleaned from various public and proprietary sources, information available through the services ranged from personal information, \textit{e.g.}, name and phone number, to sensitive personal information, \textit{e.g.}, driving records, criminal and civil court records, property records, and licensing records.\textsuperscript{91} The Commission also determined that public access to this type of information confers a number of benefits and dangers on users of these services and on society.\textsuperscript{92} The look-up services enable law enforcement agencies to do their jobs more efficiently, help parents find missing children, aid journalists in reporting news, and help consumers do important tasks such as find lost relatives.\textsuperscript{93} However, the increasing availability of this information poses various risks of harm to consumers’ privacy and financial interests, including the possibility of increasing incidences of identity theft.\textsuperscript{94}


\textsuperscript{90} Id.

\textsuperscript{91} Id.

\textsuperscript{92} Id.

\textsuperscript{93} Id.

\textsuperscript{94} Id.
In May 2000, the FTC put out its third report in three years to Congress on the status of online privacy and fair information practices in the electronic marketplace. In its 200-page report, the Commission recommended that Congress pass legislation because self-regulatory efforts had, in essence, failed. The Commission’s recommendations look much like the guidelines that it promulgated for seal programs.

The recommendation calls for legislation that embraces core privacy principles developed through extensive research and collaboration from the United States, Canada, and Europe. These core principles of privacy protection are: (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security.

---

95 See generally Privacy Online, supra note 14, at 5.
96 Id.
97 Id. at 36.
98 Privacy Online, supra note 14, at 4 n.25. The FTC description of where these principles came from appears to be comprehensive and is quoted here:


99 Id. at 7.
A. Notice / Awareness

The FTC recommends that websites should be required to provide "clear and conspicuous" notice of their information practices.\(^{100}\) Adequate notice would include: (1) what information websites collect; (2) how they collect it; (3) how they use it; (4) what sort of access and choice they give surfers to amend or delete that information; (5) what sort of security they provide for the information; (6) their practices relating to sharing the information with third parties; and (7) whether other entities are collecting information through their site.\(^{101}\)

B. Choice / Consent

The Commission recommends that websites be required to offer surfers choices as to how their information is used beyond the scope of the original purpose of the data collecting. Thus, if it was collected to complete a transaction, the consumer would have a choice as to whether the website may use it for marketing purposes.\(^{102}\) These choices would allow the surfer to curtail both the website's internal use as well as affiliate/third party use of the information.

C. Access / Participation

The FTC also recommends a mandate that surfers be given "reasonable access" to the information that a website has gathered about them, and a reasonable opportunity to review the information and correct inaccuracies or delete items.\(^{103}\) The use of a reasonable standard here refers to a desired balance between consumers' right to access versus the websites' costs in providing that access.\(^{104}\)

\(^{100}\) Id. at 36.
\(^{101}\) Id.
\(^{102}\) Id.
\(^{103}\) Id. at 37.
\(^{104}\) Id. at 29.
D. Integrity / Security

Websites would be required to take "reasonable steps" in order to ensure that the information collected will be protected.\footnote{Id. at 37.} The adequacy of security under this recommendation also refers to the tension between having one's personal information free from theft or accidental disclosure while it's in the website's hands, and the costs of providing such protection.\footnote{Id. at 32.}

IV. 2001 Proposed Legislation

Although the FTC's four corners of privacy recommendations were fairly clear, Congress has not chosen to implement them in a straightforward way. Out of over fifty privacy related bills that emerged in the 2001 Congressional session,\footnote{Schwartz, supra note 42, at A1.} five were aimed primarily toward online privacy, each taking different stands on the issues raised by the FTC recommendation.\footnote{Privacy Act of 2001, S. 1055, 107th Cong. (2001); Online Privacy Protection Act of 2001, H.R. 89, 107th Cong. (2001); Consumer Internet Privacy Enhancement Act, H.R. 237, 107th Cong. (2001); Consumer Online Privacy and Disclosure Act, H.R. 347, 107th Cong. (2001); Consumer Privacy Protection Act, H.R. 2135, 107th Cong. (2001).} This is a rather large number of bills, considering that websites have banded together to form a powerful lobbying consortium called the Online Privacy Alliance.\footnote{See Privacy Alliance, at http://www.privacyalliance.org (member companies include Microsoft, AOL/Time Warner, AT&T, PricewaterhouseCoopers, Sun Microsystems and Yahoo!) (last visited Mar. 1, 2002).} The five bills are outlined below.

A. Privacy Act of 2001

entity to a non-affiliated third party unless prescribed procedures for notice and opportunity to restrict such disclosure have been followed.\footnote{S. 1055.} Sufficient notice would include statements: (A) describing the identity of the commercial entity collecting the personally identifiable information; (B) identifying the types of personally identifiable information that are being collected on the individual; (C) explaining how the commercial entity may use the information; (D) describing the categories of potential recipients of the information; (E) explaining whether the individual is required to provide personally identifiable information in order to do business with the website; and (F) explaining how the individual may opt-out of having his information used or sold.\footnote{S. 1055 § 101(b)(1)(A)-(E).}

The notice described above must be given in the medium that the information was taken (e.g., on the Internet), and must be provided prior to the sale or use of the personally identifiable information, allowing a reasonable time for the surfer to choose to opt-out of its being shared.\footnote{S. 1055 § 101(b)(2)-(3).} The choice of opting out of the sale or use of information must be administered through “easy to use” accessible and available means.\footnote{S. 1055 § 101(c)(1).} An opt-out is considered permanent. However, if an individual does not opt-out of information collection and later decides that he does not want that information shared, he may opt-out at that time and the website must stop using and selling the information from that time on.\footnote{S. 1055 § 101(c)(3).} Senator Feinstein’s bill does not address security as it pertains to the possibility of websites losing or inadvertently leaking the information they collected.\footnote{See generally S. 1055 § 101. The bill also \[a\]mends Federal criminal law to prohibit the display, sale, or purchase of social security numbers without the affirmatively expressed consent of the individual. Exempts certain public records containing social security numbers from such prohibition. Amends the Social Security Act to prohibit the use of social security account numbers on: (1) checks issued for payment by governmental agencies; and (2) driver’s licenses or motor vehicle registration. Prohibits a commercial entity from requiring disclosure of an individual’s social security number in order to obtain goods or services. Imposes civil monetary penalties for}
read twice and was then referred to the Committee on the Judiciary, where it has since been dormant.\textsuperscript{117}

\section*{B. Online Privacy Protection Act of 2001}

The first bill introduced to the House of Representatives was the Online Privacy Protection Act of 2001 on January 3, 2001.\textsuperscript{118} The bill, sponsored by Representative Rodney P. Frelinghuysen,\textsuperscript{119} orders the FTC to prescribe limitations on the disclosure by an information recipient of consumer information, with certain exceptions such as information necessary to transactions, information gathered pursuant to a legitimate business activity, or where required by law.\textsuperscript{120} The bill provides that notice must be clear and conspicuous and must notify the surfer of the identity of the website operator, what personal information is collected by the operator, how the operator uses the information, and what information may be shared with other

\begin{itemize}
\item misuse of a social security number.
\item Amends the Gramm-Leach-Bliley Act to make conforming limitations upon financial industry sale and sharing of non-public personal financial information.
\item Sets forth prohibitions against the selling or marketing of protected health information by specified entities.
\item Amends the Driver's Privacy Protection Act relating to proscriptions against release and use of certain personal information from State motor vehicle records to expand the definition of such personal information, and to include "highly restricted personal information" among such proscriptions.
\item Empowers State Attorneys General to enforce this Act.
\item Establishes Federal injunctive authority regarding any violation of this Act.
\end{itemize}


\textsuperscript{119} Id.

companies. The bill requires a "meaningful and simple" process whereby surfers may access a description of the information collected, consent to its release, and choose to limit the disclosure of the information for purposes unrelated to those for which such information was obtained. Finally, the bill mandates reasonable security measures for the information. The Consumer Privacy Protection Act of 2001 implements these principles by making violations constitute unfair or deceptive practices within the purview of the FTC Act. The Online Privacy Protection Act of 2001 was referred to the House Committee on Energy and Commerce on January 3, 2001, and was then referred to the Subcommittee on Commerce, Trade and Consumer Protection on February 7, 2001.

C. Consumer Internet Privacy Enhancement Act

On January 20, 2001, Representatives Anna Eshoo and Christopher Cannon introduced the Consumer Internet Privacy Enhancement Act. This Act makes it unlawful for a commercial website to collect personally identifiable information from a website user unless the operator provides both notice and choice to limit the sharing of that information. Notice must include: (A) the identity of the operator of the website and any third parties the operator knowingly permits to collect personally identifiable information from users through the website; (B) the types of personally identifiable information that may be collected online by the website and the categories of information the website may collect in connection with the surfer's visit; (C) a description of how the operator uses the information gathered, including a statement as to whether the information may be sold, distributed, disclosed, or otherwise made available to third parties for marketing purposes; (D) a description of the categories of potential recipients of any such personally identifiable information; (E) whether the user is required to provide personally identifiable information in order to use the website and any

121 H.R. 89 § 2(b)(1)(A).
122 H.R. 89 § 2(b)(1)(B).
123 H.R. 89 § 2(b)(1)(C).
124 H.R. 89 § 6(d).
126 H.R. 237 § 2(a)(1)-(2).
other consequences of failure to provide that information; (F) a general
description of what steps the operator takes to protect the security of
personally identifiable information collected online by that operator;
(G) a description of the means by which a web surfer may elect not to
have his personally identifiable information used by the operator for
marketing purposes, or sold, distributed, disclosed, or otherwise made
available to a third party, except for information related to the
provision of the product or service provided by the website or
information required to be disclosed by law; and finally, (H) the
address or telephone number at which the user may contact the
website operator about its information practices and also an electronic
means of contacting the operator.127 This bill also allocates
enforcement authority among certain federal agencies and the FTC,
allows states attorneys general a cause of action, and mandates that a
study be done on online privacy.128 On January 20, 2001 the
Consumer Internet Privacy Enhancement Act was referred to the
House Committee on Energy and Commerce, and was subsequently
referred to the Subcommittee on Commerce, Trade and Consumer
Protection on February 14, 2001.129

D. Consumer Online Privacy and Disclosure Act

The Consumer Online Privacy and Disclosure Act,
promulgated by Representative Gene Green on January 31, 2001,
makes it unlawful for an operator of a website or online service to
collect, use, or disclose personal information concerning an individual
in a manner that violates regulations to be prescribed by the FTC.130
The Act mandates that the regulations require websites to protect the

127 H.R. 237 § 2(b).
128 H.R. 237 § 3(b)(1)-(6).
129 Bill Summary Congressional Research Service (CRS) of the Library of
Congress' Objective Summary for Consumer Internet Privacy Enhancement Act,
2002).
130 Consumer Online Privacy and Disclosure Act, H.R. 347, 107th Cong. §
confidentiality, security, and integrity of personal information they collect.\textsuperscript{131}

This bill has a specific prohibition of online profiling that bans websites from: (1) correlating IP address information with personal information, absent a pre-existing business relationship; (2) allowing third parties to attach persistent cookies that track Internet activity as a means of developing a personal profile on an individual without allowing the individual to opt-out of such attachment; and (3) selling transactional information as a means to satisfy creditors in the case of insolvency.\textsuperscript{132} This proposal also provides for enforcement through the FTC Act,\textsuperscript{133} and through a private right of action.\textsuperscript{134} On January 31, 2001 this bill was referred to the House Committee on Energy and Commerce, and then again referred to the Subcommittee on Commerce, Trade and Consumer Protection on February 14, 2001.

E. Consumer Privacy Protection Act

The Consumer Privacy Protection Act, introduced by Representative Tom Sawyer on July 12, 2001,\textsuperscript{135} mandates that information recipients shall not share with any other person "personal information" collected or obtained from or about a consumer unless the consumer has been given clear and concise notice of the extent and circumstances under which such a disclosure may occur, and the consumer has given his tacit or affirmative consent.\textsuperscript{136} Personal information includes the consumer's name, address, phone number and email address.\textsuperscript{137} The bill also prohibits websites from requiring consumers, as a condition to entering into or completing a transaction, to provide personal information that is not necessary to complete the


\textsuperscript{132} H.R. 347 § 1(a)(2)-(3).

\textsuperscript{133} H.R. 347 § 4(d).

\textsuperscript{134} H.R. 347 § 5.


\textsuperscript{136} H.R. 2135 § 3(a)(1)-(2).

\textsuperscript{137} H.R. 2135 § 10(4).
transaction,\textsuperscript{138} and prohibits websites from refusing to enter into a transaction because a consumer has not allowed disclosure of his personal information.\textsuperscript{139} The bill requires affirmative consent for sensitive information,\textsuperscript{140} such as a consumer’s social security number or financial information.\textsuperscript{141}

Additionally, the Consumer Privacy Protection Act deems violations as unfair or deceptive practices within the purview of the FTC Act.\textsuperscript{142} Finally, Representative Sawyer’s bill authorizes consumers and state attorneys general to pursue violations in Federal District Court.\textsuperscript{143} This bill was introduced on June 12, 2001, and was referred to Committee on Energy and Commerce. On June 18, 2001, the bill was then referred to the Subcommittee on Commerce, Trade and Consumer Protection. It has been dormant since.\textsuperscript{144}

In its report, the Commission decided that self-regulation does not work because too few websites have voluntarily joined the “seal” programs designed to curtail their own actions.\textsuperscript{145} From a consumer perspective, however, the FTC recommendations and proposed legislation do not go far enough.

V. Analysis

One cannot blame Sam the butcher or Internet advertisers for aiming advertising efforts at those customers who were most likely to be interested in their products. The difference between sharing information as Sam might with his neighbor and digitally sharing, however, is that digital sharing is more conducive to exploitation and

\textsuperscript{138} H.R. 2135 §3(b).
\textsuperscript{139} H.R. 2135 §3(c).
\textsuperscript{140} H.R. 2135 § 3(a)(1)-(2).
\textsuperscript{141} H.R. 2135 §10(5).
\textsuperscript{142} H.R. 2135 §5(a)-(b).
\textsuperscript{143} H.R. 2135 §§ 7-8.
\textsuperscript{145} See generally Privacy Online, supra note 14, at 36.
misuse. At the same time, the type of information gathered by websites is extremely helpful to the marketing and advertising industries. Privacy, however, should not be sacrificed for dollars won by websites through information harvesting.

Legislation should aim at stopping the possibility of exploitation and misuse of consumer information. For example, imagine a twenty-five year old graduate student who decides to use Yahoo! as his primary Internet portal. A portal is a website that is designed to provide numerous services to users such that they do not have to leave the site for much of their browsing. The hypothetical student uses the Yahoo! search engine, shops and generally looks to Yahoo! first when he wants to make an online transaction. If Yahoo!, or any other portal, were to take full advantage of data gathering and compiling, it could conceivably create the following profile on an individual user:

1) IP Address, websites visited before and after each time the user visits the portal or an affiliate (gathered automatically).

2) Full Name, date of birth, email address (entered as a condition of gaining access to the site’s content).

3) Street address, telephone number (entered as required information while purchasing stereo speakers on the website’s auction page).

4) Sex, marital status, race, dating preferences, sexual orientation (entered voluntarily while signing up for an online singles chat room).

---

146 Steven A. Hetcher, Norm Proselytizers Create a Privacy Entitlement in Cyberspace, 16 BERKLEY TECH. L.J. 877, 897-904 (2001).

147 Id.


149 Yahoo! asks every user registering for their first name, last name, Email Address, Zip Code, Gender, Industry, Occupation. https://edit.my.yahoo.com/config/register (last visited Mar. 1, 2002). Yahoo! uses cookies so that it may “access your information when you ‘sign in,’ so that we can provide you with customized content, such as My Yahoo!” http://privacy.yahoo.com/privacy/us/cookies/details.html (last visited Mar. 1, 2002).


5) Possible health status (gleaned from frequent searches on the website’s search engine or online health advice column).  

6) Vacation plans; including dates, destination city, hotel, and other arrangements (based on online booking through the portal’s travel agent feature).

7) Clothing preferences and sizes (based on purchases made from partners of the portal site).

8) Close friends and business contacts (based on frequent email and chatting with particular email addresses and screen names).

9) Work experience, universities attended, job skills, hobbies (based on voluntary submission of resume to portal’s online resume bank).

10) Social security number, information about your assets and income (required for Yahoo! bill paying).

---


157 The Yahoo! privacy page states that

Yahoo! collects nonpublic personal information, such as your name, address, and social security number, and information about your assets, and income, from you when you apply for, register for, or use a financial product or service. **** Yahoo! may collect nonpublic personal information about you from our business partners, such as information that you provide to them on applications or other forms. **** Yahoo! may also collect nonpublic personal information about your transactions with us, our business partners, or others such as information regarding your use of the financial products and services that we offer or information necessary to provide those products and services to you. **** In addition, Yahoo! automatically receives and records information on our server logs from your browser including your IP address, Yahoo! cookie information and the page you requested. (Emphasis added).

If this information were unfairly exploited or misused by Yahoo! or an affiliate, the effect on the consumer would be devastating. Federal law should protect the consumer from having his information gathered and sold. This author has three regulatory suggestions for where FTC non-regulation and Congress’ legislative attempts have generally fallen short.

The first advocates a more prolific choice for surfers. Most websites that allow third parties to gather information disclaim any liability for ad banners and other affiliated third-party links that appear on their site. Consumers should have the choice of a one-click opt-out of non-necessary personal and sensitive personal information gathering by websites and their affiliates. This would ensure that consumers have a true choice as to whether their information is harvested. Websites may depend on revenue derived from their affiliates, but this should not be allowed at privacy’s expense. After all, web users surf in order to view and interact with content on the Internet, not to see what interesting advertisement a website will put onto a banner next.

Second, legislation should mandate that all links from a website that refer a user to another website clearly identify that they do so on the link itself. It would be possible to do this without affecting the nature of the website environment by creating a small universal symbol indicating that a graphical link is taking the surfer out of the scope of the website, and therefore the site’s privacy statement. Similarly, disclosure of the site to which the browser will go for text links could easily be disclosed on the link itself. This notice would be in plain view every time the surfer sees links that may jeopardize his privacy by taking him outside of the scope of the website’s privacy policy.

Third, legislation should address the problem that consumers have no real assurance that their information will not be resold once information has been shared. Privacy statements should clearly indicate to the surfer whether the website’s agreements with third parties provide that the information will not be resold. This would curb the dissemination of personal information, and keep consumers in control.

VI. Conclusion

While it would be nice for surfers to be able to have the kind of relationship with website operators that the Bradys had with Sam the butcher, it simply cannot happen. Not because websites are inherently impersonal (indeed, the Internet is perhaps most powerful when used as a communication device), but because websites choose to operate that way, sacrificing personal relations for gathering the most attention, visitors and data possible. Toward this end, websites have created an industry that is based on the absence of regulation, and technologically uninformed web surfers who do not understand that their information is being harvested and shared. This information reaping for the purpose of sharing must be stopped through tougher legislation than has been proposed in the first session of the 107th Congress. Consumers should be aware of what information they are giving out, to whom, and feel secure that a nameless, faceless third party will not contact them as a result of what they believed was secure surfing. Sam the butcher, who believes in trust, would have it no other way.