Yale Journal of Law and Technology

Volume 1
Issue 1 *Yale Journal of Law and Technology*

Article 4

1999

LECTURE: About Privacy: Protecting the Consumer on the Global Information Infrastructure

Debra Valentine

LECTURE: About Privacy: Protecting the Consumer on the Global Information Infrastructure[+]

Debra Valentine[*]

I. INTRODUCTION

The Internet is a remarkable tool, providing millions of users easy access to a wealth of information, goods, and services. Its extraordinary growth is propelled in part by exponential growth in the online consumer market. Between early 1997 and December of that year, the number of adults online in the United States and Canada climbed from 51 to 58 million. Of those users, approximately 75% reported that they had shopped for product information on the World Wide Web and 10 million had actually purchased a product or service online. Analysts estimate that Internet advertising--which totaled approximately $ 300 million in 1996--will swell to $ 4.35 billion by the year 2000.[1]

II. THE PRIVACY CONCERN

As the Internet expands, so does the potential to acquire and exploit personal information. American businesses have always, of course, collected some information from consumers to facilitate transactions. The Internet is unique, however, in its ability to compile vast amounts of information with great efficiency at low cost. Computers log our answers to questions about personal preferences, favorite activities, family structure, Social Security number, occupation, medical history, income bracket, and credit card number.

Children are especially vulnerable. Operators of pen pal sites, chat rooms, and other sites often post or disclose identifying information about children that enables third parties to contact them offline and without permission. A recent Federal Bureau of Investigation (FBI) and Department of Justice (DOJ) investigation discovered that online services and bulletin boards are quickly becoming the most powerful resources used to contact children by those who solicit sexual activity with minors or produce child pornography.[2] Online marketers learn about family finances from children by asking them, for example, about the kinds of gifts--even stocks and bonds--that they have received.

Moreover, consumers do not always disclose their online information knowingly. The innocuous-sounding "cookie" and other computer counting mechanisms record what we buy, what we look at,

---

[+] Edited transcript of remarks delivered to the Yale Law and Technology Society on December 8, 1998

[*] B.A. Princeton University, 1976 (Phi Beta Kappa). J.D. Yale Law School, 1980 (Editor, Yale Law Journal). Law Clerk, U.S. Court of Appeals for the Third Circuit. Attorney, Office of Legal Counsel, Department of Justice, 1981-85. Associate, Partner, O'Melveny and Meyers, 1985-95. Deputy Director for Policy Planning, Federal Trade Commission (FTC), 1995-96. Assistant Director for International Antitrust, International Division, Bureau of Competition, FTC, 1996-97. General Counsel, FTC, since September 1997.

[1] See FEDERAL TRADE COMMISSION, PRIVACY ONLINE: A REPORT TO CONGRESS 3 (1998) [hereinafter PRIVACY ONLINE]. Similar predictions appear in leading business magazines. See, e.g., Alice Z. Cuneo, Online Retailers Look to Web for Holiday Magic, ADVERTISING AGE, Oct. 26, 1998, at S12 (reporting estimates that online sales could more than double from last year's level); R. Quick & T. Weber, The Lazy Man's Guide to the Holidays: Avoid the Malls with a Few Mouse Clicks, WALL ST. J. INTERACTIVE EDITION, Nov. 13, 1998.

[2] See PRIVACY ONLINE, supra note 1, at 5 n.21.

how long we look at it, and whether we've looked at it before. While firms develop extensive electronic dossiers that can be stored, sorted, shared, and sold, we often remain virtually unaware of the data's existence, extent, possessors, or future uses.

This information, and the deductions that may be drawn from it, is online gold, especially to marketers interested in sharpening their solicitations. The information reveals not only individuals' traits, but also, when aggregated, provides insights into broader social trends, preferences, and consumption patterns.[3] The value of online personal information is increased by the fact that Internet advertising (via the Web and e-mail) is relatively inexpensive and can be widely distributed instantaneously. Not surprisingly, the very prevalence, ease, and relatively low cost of collecting and disseminating this information--characteristics that distinguish the online environment from more traditional information collection methods--are also what raise privacy concerns. The ability to gather, process, and disseminate information on the Internet provides consumers with a wealth of benefits. However, some uses of personal data may be intrusive, as when private information is widely circulated; or reckless, as when inaccurate information is shared with countless people or firms; or predatory, as when the information is used to target victims for a scam or children for criminal activity.

III. CONSIDERATIONS REGARDING GOVERNMENTAL EFFORTS TO PROTECT CONSUMERS' ONLINE PRIVACY

Congress vested the Federal Trade Commission (FTC) with broad consumer protection and antitrust jurisdiction to promote the fair and efficient functioning of the marketplace. We view ourselves as promoting social welfare by ensuring that consumers have access to (1) high quality goods at competitive prices and (2) accurate and nondeceptive information so that they can choose wisely among the available goods. In light of the Internet's extraordinary growth, capabilities, and potential for misuse, this medium has prompted substantial FTC attention over the past three years.[4]

---

[3] See James Gleick, Like Mozart? You'll Love Madonna, N.Y. TIMES MAG., Oct. 25, 1998, at 32 ("The on-line marketers are getting to know you better than you know yourself.").

[4] In addition to the FTC's 1998 online privacy report, see PRIVACY ONLINE, supra note 1, the Commission has issued:

- FEDERAL TRADE COMMISSION, INDIVIDUAL REFERENCE SERVICES (1997)
- FEDERAL TRADE COMMISSION, PUBLIC WORKSHOP ON CONSUMER PRIVACY ON THE GLOBAL INFORMATION INFRASTRUCTURE (1996)
- FEDERAL TRADE COMMISSION, ANTICIPATING THE 21ST CENTURY: CONSUMER PROTECTION POLICY IN THE NEW HIGH-TECH, GLOBAL MARKETPLACE (1996).

Additionally, the Commission frequently has addressed online privacy issues in congressional testimony. Recent FTC testimony includes:

- Protection of Children's Privacy on the World Wide Web: Hearings Before the Subcomm. on Communications of the Senate Comm. on Commerce, Science, and Transportation, 105th Cong. (1998) [hereinafter Children's Privacy] (prepared statement by Robert Pitofsky, FTC)
- Consumer Privacy on the World Wide Web: Hearings Before the Subcomm. on Telecommunications, Trade, and Consumer Protection of the House Comm. on Commerce, 105th Cong. (1998) [hereinafter Consumer Privacy]

The FTC's goals throughout have been to prevent misuse of the Internet by protecting consumer privacy online, and to encourage effective self-regulation as the preferred approach for doing so. These efforts are based on the belief that greater protection of personal privacy will not only protect consumers but also increase their participation in the online marketplace. Interestingly, survey results consistently indicate that consumers' concerns about privacy rank as the number one reason why they refrain from using the Internet and from engaging in electronic commerce.[5] The unfortunate fact, however, is that relatively few sites have established practices that protect the privacy of collected information, or even that inform consumers of the possible uses of their data. The adoption of fair information treatment practices could also enhance market efficiency by preventing errors and misrepresentations by those who gather, circulate, and use information. These types of errors are often far less costly to avoid than to correct. For example, if a web site circulates incorrect information that someone has gone bankrupt, or reveals a child's phone number or address, the site's error can cause considerable financial or personal injury or embarrassment. This problem could be prevented with a few simple, preventative measures.

Two cautions should be addressed before discussing the FTC's specific efforts to protect online privacy. First, governmental efforts to control the exploitation of electronically gathered information raise issues about who decides what information can be gathered and used, under what circumstances, with what protections, and subject to what penalties for violations. These issues may be of constitutional magnitude, since first amendment concerns almost invariably arise when the government exercises control over the acquisition and publication of information. Our preference for industry self-regulation to protect consumers' online privacy in part reflects an appreciation of these concerns.

Second, the United States does not act alone in cyberspace. The European Union passed a directive three years ago that extensively regulates the buying and selling of personal data.[6] This directive, which took effect October 25, 1998, lays down common rules that firms must observe when collecting, holding, or transmitting personal data in their business or administrative activities. Most fundamental for firms is an obligation to collect data only for specified, legitimate purposes and to hold only data that is relevant, accurate, and up-to-date. European citizens, in turn, are guaranteed a bundle of rights: the right of access to their personal data; the right to correct any data that is

---

- Consumer Protection in Cyberspace: Combating Fraud on the Internet: Hearings Before the Subcomm. on Telecommunications, Trade, and Consumer Protection of the House Comm. on Commerce, 105th Cong. (1998) [hereinafter Cyberspace Fraud]
- Internet Privacy: Hearings Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary, 105th Cong. (1998) [hereinafter Internet Privacy]
- Internet Fraud: Hearings Before the Subcomm. on Investigations of the Governmental Affairs Committee, 105th Cong. (1998) [hereinafter Internet Fraud].

Individual Commissioners and Commission staff have also given congressional testimony or spoken on Internet privacy issues in other fora. All the reports, congressional statements and testimony are on the FTC's web site, as are many of the speeches. See <http://www.ftc.gov>.

[5] See PRIVACY ONLINE, supra note 1, at ii-iii, 3.

[6] Council Directive 95/46 on the Protection of Personal Data, 1995 O.J. (L281) 31.

inaccurate; the right to know where the data originated; the right to refuse use of their data for activities such as direct marketing; and the right of recourse if unlawful processing occurs.

Significant for the U.S. economy and for U.S. firms is that the directive prohibits transmitting personal data to any country that doesn't provide adequate (which roughly translates as comparable) protection. Each EU member country now is enacting its own law to implement the directive. As of October 1998, six members either had done so or had draft laws in place. It is not yet known, of course, how stringent the various national laws and policies of the EU member countries will be, how strictly they will be enforced, or how flexible their contemplated system of exemptions and special conditions for individual companies will be. Nevertheless, the directive may impose substantial restrictions on many retailers, direct marketers, and others that buy and sell personal data in the EU, or that acquire and transmit that data to the United States. The U.S. and EU are currently in negotiations to determine how best to harmonize the different approaches taken to protect personal data on each side of the Atlantic.

IV. FTC EFFORTS TO PROTECT CONSUMERS' ONLINE PRIVACY: ENFORCING EXISTING LAWS, PROMOTING INDUSTRY SELF-REGULATION, AND RECOMMENDING NEW LAWS

The FTC has a three-pronged approach to online privacy: case-by-case law enforcement; promotion of industry self-regulation; and recommendations to Congress for new legislation.[7]

A. Law Enforcement

1. Fraud and Spam

In the area of enforcement, the FTC has initiated more than 40 actions alleging that firms have used the Internet for deceptive or unlawful practices.[8] Several cases have involved businesses that send unsolicited commercial e-mail, or "spam." Beyond the sheer volume and annoyance of spam, which threatens the development of the Internet as a conduit for commerce, it is rampant with deception and fraud. The FTC receives more than 1,000 complaints a day about spam. A sampling of over 250,000 spam messages that consumers forwarded to a special FTC e-mailbox indicates that the most common schemes are business opportunity scams, which promise vast income for a small investment of money and time; chain letters, which are simply electronic versions of the old-fashioned letter schemes and every bit as illegal; strategies for making money by sending bulk e-mailings (even though the e-mail lists provided are of poor quality and most legitimate businesses do

[7] The FTC also engages in substantial consumer education efforts. These efforts are omitted, given the focus here on the activities of those who collect and disseminate information, rather than on those who supply it. See Cyberspace Fraud, supra note 4 (discussing many of the FTC's cases challenging deceptive and unfair practices on the Internet).
[8] See Cyberspace Fraud, supra note 4 (discussing many of the FTC's cases challenging deceptive and unfair practices on the Internet).

not engage in bulk e-mailings); and bogus health and diet scams that tout "scientific breakthroughs" and "miraculous cures."[9]

Although most Internet fraud is fairly traditional, the Commission has seen cases where schemes uniquely and ingeniously exploit the special nature of the Internet. In *Audiotex Connection*,[10] the Commission encountered respondents who surreptitiously disconnected consumers' modems from their Internet service provider (such as AOL) and reconnected them to the Internet through a high-priced international modem connection. Defendants claimed to offer access to free computer images, but once a consumer downloaded and activated the special viewer software, an effective hijacking allegedly ensued. The software would place an international long-distance call, routed through Moldova with long-distance rates to Moldova applying, that would continue until the consumer turned off the computer. We managed to stop the alleged scam within 31 days of learning about it, and to obtain a court order providing over 38,000 consumers with almost $ 2.75 million in redress. This case demonstrates how converging information technologies--in this case, telephone and Internet services--pose unique law enforcement concerns.

2. Cramming: VOAA, Online Communications

Another kind of fraud, cramming, also warrants discussion. Even though it does not necessarily involve misuse of the Internet, it uses communications technologies to invade consumers' privacy, misuse personal information, and undermine consumers' choices. Cramming is the practice of including charges on telephone bills for goods or service that the consumer did not order. It exploits new telephone technologies and the deregulated telephone billing system, which is becoming a convenient alternative to more conventional billing and collection systems, such as credit cards and checks. Telephone local exchange carriers can now include on their bills charges for goods and services--such as Internet or cable television use--that are only peripheral, or even unrelated, to telephone services. Crammers, however, take advantage of the fact that this new billing service has not yet developed the fraud detection and consumer protection mechanisms of more established systems.[11] Moreover, this billing system lacks the specific statutory protections that, for example, the Truth in Lending Act[12] provides for consumers who use bankcards and other credit cards. Unfortunately, because specific consumer safeguards have not yet developed, many items or services

[9] See Federal Trade Commission, FTC UNVEILS "DIRTY DOZEN SPAM SCAMS," FTC NEWS RELEASE, July 14, 1998 (available at <http://www.ftc.gov>). Other common spam scams are: work-at-home schemes; promises of easy money or ways to "get rich quick;" free gift offers used as lures for membership payments and pyramid schemes; investment opportunities; cable descrambler kits (which seldom work and are illegal); guaranteed loans or credit on easy terms; credit repair; and vacation prize promotions.
One notable aspect of this law enforcement effort is that consumers forwarded spam they received to the FTC via the Internet, thus using the Internet to help protect their privacy and to prevent deceptive conduct.
[10] FTC v. Audiotex Connection, No. CV-97-0726 (D.H.) (E.D.N.Y., filed Feb. 13, 1997).
[11] For example, bankcard systems require access to a bankcard number, which is unique, has a limited period of validity, and is not widely available to the public through such conveniences as telephone books or Directory Assistance. Bankcard systems also monitor spending patterns and merchant accounts for indications of fraud.
[12] Truth in Lending Act (TILA) Pub. L. No. 90-321, 82 Stat. 146 (codified as amended in scattered sections of 15 U.S.C.) (1968).

on telephone bills are not adequately explained or depicted to permit consumers to know when they have been crammed or how they may challenge disputed charges.

Complaints about cramming are increasing rapidly. In the past year, the FTC received over 9000 complaints about mystery charges on phone bills. Many times, when consumers reveal personal identifying information, disclose their telephone numbers, or simply use their own computers and telephones, they leave themselves open to cramming. For cramming to work, all the unscrupulous vendor needs is the consumer's telephone number. The vendor can acquire this simply by inducing the consumer to disclose the number voluntarily. In one recent case, the *Veterans of America Association* ("VOAA") acquired consumers' phone numbers by conducting sweepstakes and prize promotion scams in malls, convention centers, and fairgrounds at which consumers wrote their names and phone numbers on sweepstakes entry forms.[13] Without the consumer's knowledge, VOAA treated the act of entering the sweepstakes as ordering VOAA's voicemail services. VOAA then passed the claimed charges on to a billing aggregator, a firm that operates as an intermediary between the vendor and the local telephone exchange company (LEC). Once VOAA's billing aggregator processed the telephone billing data from the entry forms, combined with VOAA's voicemail charge, into the necessary electronic format needed by the local exchange company, the local exchange company included a $ 4.95 monthly charge for voicemail services on the victim's bill. The FTC obtained a preliminary injunction against these alleged unlawful practices. Although the litigation is still continuing, we estimate that the VOAA scam alone cost consumers in excess of $ 2 million.

Alternatively, the scam vendor can induce the consumer to call him and then capture the number from which the call originates with an Automatic Number Identification (ANI) system, a system similar to "caller ID." A firm called Online Communications ("Online") used this scheme. In that case, Online allegedly ran newspaper advertisements offering free matching services with local singles.[14] All the customer had to do was call an 800 number and tell the Online representative the kind of person the customer wanted to meet. Using an ANI system, Online then captured the telephone number from which the customer was calling. Shortly thereafter, an Online representative purporting to be a "local single" placed a return call to that captured number, without telling the recipient that the call was being billed as a collect call from Deerfield, Florida at $ 3.99 per minute. Online's billing aggregator then took the billing information that Online captured when consumers called Online's toll-free numbers, combined it with the collect call charges, and forwarded the electronic data to the local telephone exchange companies to include in consumers' phone bills. Neither Online nor its billing aggregator took any steps to determine whether the person who actually made the initial 800 call was the subscriber for the line that was billed. Because of the shortcomings of ANI as a basis for billing, subscribers were charged hundreds of dollars on their phone bills for audio entertainment services they had neither ordered nor authorized. The

[13] See FTC v. Hold Billing Servs., Ltd., No. SA-98-CA-0629 (W.D. Tex., filed July 15, 1998).
[14] See FTC v. Int'l Telemedia Assocs., Inc., No. 1-98-CV-1935 (N.D. Ga., filed July 10, 1998).

Commission obtained a court order temporarily restraining both Online and its billing aggregator, freezing Online's assets, and appointing a temporary receiver to manage Online's business.[15]

The FTC is currently in the process of determining whether to modify its 900-Number Rule,[16] which governs the pay-per-call industry, to encompass cramming. If it does, cramming violations will be subject to civil penalties of up to $ 11,000 per violation.[17]

3. Privacy: GeoCities

This past August, the Commission resolved a precedent-setting Internet privacy case.[18] Our concern was that GeoCities, one of the World Wide Web's most frequently visited sites, collected personal identifying information from its members, both children and adults, and misled them as to its use. GeoCities offers its members free and fee-based personal home pages, and links its members' home pages into a virtual community of themed neighborhoods. For visitors to become members, they must fill out an online application that requires disclosure of certain personal identifying information. The registration also requests optional information regarding education level, income, marital status, occupation, and interests. Through this registration process, GeoCities created a database rich with target markets for advertisers. The Commission alleged in its complaint that GeoCities falsely represented that the mandatory identifying information would be used only to provide members with information regarding advertising offers, products, and services that they requested, and that the optional information that members provided would not be released to third parties without permission. In addition, GeoCities collected personal identifying information from children, for whom it promotes a GeoKidz Club that offers activities, contests, and games. The FTC charged that GeoCities misrepresented that it maintained this identifying information, when, in fact, a third party collected and maintained it.

GeoCities settled the case by agreeing to disclose prominently on its Web site just what information it is collecting, for what purpose, to whom it will be disclosed, and how consumers can inspect and, if desired, remove their personal information. In addition, GeoCities must offer members an opportunity to delete their personal information from the databases of third parties. The consent order also prohibits GeoCities from misrepresenting who is sponsoring the various activities offered on its Web site and who is actually collecting and maintaining personal information. Finally, to protect children, the order requires GeoCities to obtain parental consent before collecting

---

[15] In another FTC case associated with cramming, the defendants allegedly sent look-alike telephone bills charging for audio entertainment services that the telephone line subscribers had not purchased. See FTC v. Interactive Audiotext Servs., Inc., No. 98-3049 (C.D. Cal., filed Apr. 22, 1998).

[16] Trade Regulation Rule Pursuant to the Telephone Disclosure and Dispute Resolution Act ("900-Number Rule"), 16 C.F.R. § 308 (1993). See also 47 C.F.R. §§ 64.1505-.1515 (1993) (FCC rule governing conduct of common carriers in the 900-number industry).

[17] See 16 C.F.R. § 1.98 (1998) (publishing inflation adjustment to 15 U.S.C. § 45(m) pursuant to the Federal Civil Penalties Inflation Adjustment Act, as amended by Pub. L. No. 104-134, § 31,001(s), 110 Stat. 1321 (reprinted in 28 U.S.C. § 2461 note)).

[18] GeoCities: Analysis to Aid Public Comment, 63 Fed. Reg. 44,624 (1998) (acceptance of consent agreement subject to final approval); see also Federal Trade Commission, Internet Site Agrees to Settle FTC Charges of Deceptively Collecting Personal Information in Agency's First Internet Privacy Case, FTC NEWS RELEASE, Aug. 13, 1998 (available at <http://www.ftc.gov>).

identifying information from children age twelve or younger, and to delete any such information already collected unless GeoCities obtains affirmative parental consent to retain it.

The comprehensive GeoCities consent agreement establishes five key elements that, taken together, can provide substantial protection for personal information gathered online: notice of the site's privacy practices; consumer choice regarding the use of any information collected; consumer access to correct or remove personal information; provisions to safeguard the security of the information; and parental control over the collection and use of information gathered from children. These are precisely the types of protections that the Commission has been urging Web site operators to provide voluntarily through self-regulation.

B. Self-Regulation

1. Benefits of Self-Regulation

The Commission believes that self-regulation offers the best means of protecting consumers' online privacy, for several reasons. First, self-regulation avoids many of the first amendment and related legal issues associated with governmental regulation. Second, voluntary codes are, by definition, developed and adopted by those with the greatest expertise about and sensitivity to industry practices and conditions. Third, self-regulatory codes often can be formulated, and revised when necessary, more promptly than can legislative codes. This allows firms to respond quickly to the rapidly evolving nature of the Internet and computer technology and to employ emerging technologies to protect consumer privacy. Fourth, when regulation is voluntarily-adopted, compliance tends to be broader, and enforcement more prompt, than when a legislature or agency imposes a detailed mandate. Finally, where an industry can regulate itself, the government need not devote as many of its limited resources to the task. The encouragement of self-regulation, therefore, is often an efficient and effective way for an agency to leverage its enforcement budget.

Self-regulatory efforts may sometimes lapse into a vehicle for exclusionary or collusive conduct. Government vigilance is therefore appropriate, especially where business rivals with incentives to restrain competition are involved in the process. Nonetheless, code-setting efforts, properly conducted, can be pro-competitive by increasing consumer confidence, stimulating demand, and lowering costs. In the case of the Internet, if the private sector adopts principles incorporating widely-accepted information treatment practices that respect consumer privacy, and if it creates an effective enforcement mechanism, this self-regulation likely will offer pro-competitive benefits as well as afford consumers adequate privacy protection.

2. Desirable Attributes of Self-Regulation for Consumers' Online Privacy

Having addressed privacy and technology issues in many contexts and having reviewed government studies done here and abroad, the FTC now recognizes five widely accepted principles--plus two

additional ones when children are involved--that we believe are essential for effective self-regulatory or legislative programs to protect privacy.[19]

a. Notice/Awareness

The most basic of the principles is notice. Web sites should disclose to consumers the site's information use and privacy protection practices. Absent such notice, a consumer cannot make an informed choice about whether--and to what extent--to disclose personal information. Critical factors to include in this notice are: what information is being collected; who is collecting it; how it will be used; who might have, or be given, access to the data; what passive, or non-obvious, data collection methods are used by the site; whether providing requested information is mandatory or voluntary; and how the data will be protected.

b. Choice/Consent

Web sites should seek consumers' consent regarding any uses of the information beyond those necessary to achieve the basic purposes of the data request. Such additional uses might include, for example, the sale of the data to direct marketers or to firms that aggregate and sell information about individuals. There are three basic kinds of consent: "opt-in," which prohibits the Web site from collecting and using personal data unless the consumer affirmatively permits it; "opt-out," which allows the Web site to collect and use the data unless the consumer takes affirmative steps to prevent it; and selective choice, which permits consumers to limit their consent to certain kinds of data or uses.

c. Access/Participation

A consumer should be able to access data about himself or herself and to challenge its accuracy or completeness. Timely and inexpensive access, a means for consumers to verify the information recorded in the site's database, and a method to correct information or add objections to the file, are essential for ensuring the accuracy of data.

d. Integrity/Security

The data collector should ensure that the information is secure and accurate. For example, the collector should use only reputable sources of data, should cross-check data where possible and take steps to secure the data against loss or unauthorized access.

e. Enforcement/Redress

An enforcement mechanism is necessary to ensure compliance with the other principles and to provide recourse for injured parties. A self-regulatory program that seeks to assure enforcement and redress might incorporate such features as periodic compliance audits, neutral investigation of

[19] See PRIVACY ONLINE, supra note 1, at 7-14; see also Consumer Privacy on the World Wide Web: Hearings Before the Subcomm. on Telecommunications, Trade, And Consumer Protection of the House Comm. on Commerce, 105th Cong. (1998).

consumer complaints, a dispute resolution mechanism, and correction of misinformation or compensation for injured parties. Government might also enforce fair information treatment practices through legislation allowing for private remedies, government enforcement either civilly or criminally, or a combination of these mechanisms.

3. Additional Protections for Children

Where information is collected from children twelve years old or under, the Commission believes that two additional protections are advisable.

a. Opt-in Consent or Prior Parental Approval

As a general rule (with a few pragmatic exceptions), sites should obtain prior parental approval before collecting information from young children if that information will enable someone to contact the child offline.

b. Opt-out Consent for Continued Use

At any time a child's parents should be able to direct the site not to collect further data from the child, and not to use or retain in retrievable form any information that it already has collected.

4. Individual Reference Services

One area where the Commission's efforts to promote self-regulation have achieved some notable success involves the "individual reference service" or "look-up service" industry. These firms are computerized database services that collect and sell personal identifying information, which they glean from a variety of public and non-public sources.

The information collected often is far broader than the typical personal identifying information. For example, motor vehicle records and driver's licenses may disclose the subject's Social Security number, aliases, physical characteristics or infirmities, and alcohol abuse. Similarly, real estate and professional licensing records may disclose asset ownership, employment, credit history, medical problems, marital status, and civil judgments or criminal convictions. Some look-up services now have records on more than 150 million people. While the existence and preservation of this information is a fact of modern life, its compilation in a single storehouse can pose a disquieting threat to privacy.

Convenient access to this information about individuals through look-up services undoubtedly confers a myriad of benefits to users and society. Look-up services enable law enforcement agencies to locate witnesses, help public interest groups to find missing children, and aid banks in preventing fraud. But the information, if inaccurate, insecurely maintained, or unwisely distributed, may expose

individuals to fraud, embarrassment, prejudice, computer hacking, and other problems. Perhaps most troubling is the increasing misuse of this information for identity theft.[20]

Look-up services are not new. Recently, however, their capabilities have burgeoned because the Internet and computer technology have made it easier and less expensive than ever to aggregate, access, and manipulate previously unimaginable quantities of richly-detailed information. Not only is data increasingly available in electronic form, but computer processing speeds have increased, data storage costs have dropped, and data from multiple sources can be combined more easily to create new information products. In turn, it is far easier and less expensive than it was to purchase reference reports, especially when they are acquired online.

In June 1997, the Federal Trade Commission held a workshop regarding the individual reference service industry. Thereafter, Commission staff engaged in an ongoing dialogue with industry members known as the Individual Reference Service Group (IRSG), who were crafting a set of self-regulatory principles to address privacy and related concerns.[21] This effort was largely successful. The IRSG Principles incorporate most of the controls that we and the public believe are necessary or desirable for preventing data misuse.

First, the IRSG Principles limit access to sensitive information by placing restrictions on the availability of nonpublic information. The Principles adopt a three-tier customer category scheme that makes less information available to customers who have the least rationale for access to such information. For example, signatories to the IRSG Principles have agreed not to disclose Social Security numbers or mothers' maiden names, which are readily used for identity theft and other types of fraud, to the general public. Customers who have greater access to non-public data are subject to greater controls--both in the initial screening of those customers and in limiting the permissible uses of the data they acquire.

Second, the IRSG Principles monitor use and maintain some general audit trails of collected data, requiring signatories to take measures to prevent misuse of all non-public information. Third, signatories must provide consumers with access to personal information, a means for correcting inaccuracies, and an opportunity to opt out of general distribution of non-public personal data. Fourth and most important, the Principles require an independent third party to review annually the signatories' compliance with these controls, with the results to be made public.

The signatories to the IRSG Principles include the vast majority of the industry that supplies personal information to commercial users: look-up services, the three national credit agencies, and some information vendors. That the vast majority has agreed to annual compliance reviews is a truly innovative self-regulatory measure in the information practices area. Moreover, since the signatories have agreed not to do business with non-signatories that do not comply with the IRSG Principles,

---

[20] Recent research shows that consumers are particularly concerned about the sale of their Social Security numbers and other personal identifiers. Anecdotal evidence also indicates that increasing access to sensitive identifying information poses risks of unlawful uses. Whether initially obtained by an unscrupulous employee, scam artist, computer hacker, or Internet surfer, such information in the wrong hands can have severe repercussions, including identity theft.

[21] See INDIVIDUAL REFERENCE SERVICES, supra note 4 (describing the industry and IRSG Principles).

the program has the potential to guide not just the signatories' practices, but those of the industry's customers and suppliers as well.

The IRSG Principles are concededly not perfect. For example, they provide scant protections for the use of public information, and no opportunity for consumers to review these public records and correct transcription and other mistakes.

Overall, however, the IRSG Principles go a long way toward ensuring that information about individuals is being collected, disseminated and used responsibly, and with a minimum of risk.

5. Limited FTC Success in Promoting Self-Regulation to Achieve Online Privacy

Despite the potential benefits of self-regulatory programs, the Commission has not been as successful as it would have liked in urging the online industry to regulate its information practices. Let me review a few statistics from a survey of over 1400 web sites that we included in our June 1998 report to Congress regarding online privacy.[22] Although 85% of the surveyed web sites collect personal information from consumers, only 14% provide any notice regarding their information practices, and only 2% do so by means of a comprehensive privacy policy. The news with respect to children's web sites is somewhat more encouraging. While 89% of children's sites surveyed collect information from children, 54% provide some minimal disclosure of their information practices. However, just 23% of the sites tell children to get their parent's permission before providing personal information, 7% advise parents of the site's information practices, and fewer than 10% allow for any parental control over the information's collection and use.[23] Shockingly, only 1% obtain parental permission before collecting personal information from children.[24]

Given that the vast majority of online businesses have yet to adopt even the most fundamental fair information practice--simple notice--it is not surprising that the Commission concluded that "effective industry self-regulation with respect to the online collection, use, and dissemination of personal information has not yet taken hold."[25]

C. Legislation

In its June 1998 report to Congress, the Commission acknowledged that the federal government currently has limited authority over the collection and dissemination of online personal data. Although the FTC's authority to challenge unfair or deceptive conduct[26] provides a basis for some enforcement against particular information practices, the Commission lacks the unambiguous authority to require firms across-the-board to adopt fair privacy practices, or to act whenever necessary to protect children's online privacy.[27] For these reasons, and because an effective system

[22] See PRIVACY ONLINE, supra note 1.
[23] See id. at ii.
[24] See id. at 37.
[25] Id. at ii.
[26] See 15 U.S.C. § 45 (1994).
[27] See Children's Privacy, supra note 4, at 4;. See also Letter from Jodie Bernstein, Director, Bureau of Consumer Protection, Federal Trade Commission, to Kathryn C. Montgomery, President, and Jeffrey A. Chester, Executive

of self-regulation has not emerged yet, the Commission urged Congress in June to adopt legislation protecting children's online privacy.[28] Congress did so in the Children's Online Privacy Protection Act of 1998.[29] The Commission also believes that unless industry demonstrates that it has developed and implemented "broad-based and effective" self-regulatory programs by year's end, additional governmental authority in this area is not only appropriate but also necessary.[30]

The bill that Congress passed protecting children's online privacy closely tracks the Commission's recommendations. It is designed to place parents in control of the online collection and use of personal information from their children, but recognizes that a marketer's responsibility varies with the age of the child from whom information is sought. The legislation has three main aspects: substantive protections, FTC interpretive rules, and a safe harbor provision.

1. Substantive Protections

The new law's substantive protections mirror those already discussed--they provide for notice to parents of children under thirteen, consumer choice about how their child's data will be used, consumer access to their child's data, and security.

A key component is an "opt-in" requirement that requires parental consent before sites may collect information from children under thirteen. In addition, the bill grants broad opt-out rights that allow parents the opportunity, at any time, to prevent sites from (1) gathering further information from their child, (2) using previously-collected information, or (3) retaining that information in retrievable form. As a further protection, site operators and online service providers may not condition a child's participation in a game or other activity on the disclosure of more personal information than is reasonably necessary to engage in that activity. The bill also specifies several situations in which consent is not necessary, such as where the information is needed to contact the parents or to respond to a single request from the child and then is not retained in retrievable form.

2. Regulation

The law also requires the FTC to promulgate and enforce regulations that incorporate and flesh out the statute's substantive provisions. In addition, any state may enforce these FTC regulations by bringing a *parens patriae* action on behalf of its residents for an injunction, damages, restitution, or other appropriate relief.

3. Safe Harbor

Director, Center for Media Education (July 15, 1997) (regarding "Petition Requesting Investigation of and Enforcement Action Against SpectraCom, Inc."). As summarized in Children's Privacy, the letter states that "it is a deceptive practice to expressly or impliedly misrepresent the purpose for which personal identifying information is being collected from children . . . [and] that it is likely to be an unfair practice to collect personal identifying information from children and sell or otherwise disclose that information to third parties without providing parents with adequate notice and a prior opportunity to control the collection and use of the information." Children's Privacy, supra note 4, at 7 n.23 (emphasis in original).

[28] See PRIVACY ONLINE, supra note 1, at 40-43.

[29] See Children's Online Privacy Protection Act, Pub. L. No. 105-277, 112 Stat. 2681 (1998).

[30] See Consumer Privacy, supra note 4, at 4.

An important feature of the new statute is that Congress directed the Commission to provide incentives for self-regulation through the use of a "safe harbor." Under this approach, an industry group may submit proposed guidelines to the Commission for review and approval. The agency then has 180 days to evaluate the self-regulatory proposal in light of conditions within the industry and the nature and sensitivity of the collected information. If the Commission certifies that the proposed guidelines are in compliance with the FTC's regulations, qualifying entities that adhere to the guidelines will enjoy safe harbor protection from liability.

V. CONCLUSION

Cynics might suggest that seeking privacy in a cyberspace world has all the promise of looking for a unicorn in a forest. I disagree. Unlike the situation with unicorns, privacy is not a ²yes or no² proposition, but instead exists on a spectrum, and you can preserve it to a greater or lesser degree. In my view, the Commission's law enforcement, self-regulatory, and legislative activities have increased privacy protections for consumers, with great benefits for them and little cost to businesses.