January 2000

Privacy on the Internet: The Evolving Legal Landscape

Debra A. Valentine

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

Part of the Law Commons

Recommended Citation
Available at: http://digitalcommons.law.scu.edu/chtlj/vol16/iss2/10
PRIVACY ON THE INTERNET: THE EVOLVING LEGAL LANDSCAPE

Prepared Remarks of

Debra A. Valentine†

TABLE OF CONTENTS
I. Introduction ................................................................................ 401
II. Privacy on the Internet—The Evolving Legal Landscape .......... 403
   A. Federal Trade Commission Act and Informational Privacy ........ 404
   B. Other Federal Statutes and Informational Privacy ....................... 408
   C. Federal Internet-Law .............................................................. 410
III. Current Federal Policy on Internet Privacy ............................... 412
IV. The U.S. Approach to Privacy Versus the E.U. Approach ........ 415
V. Conclusion .................................................................................. 417

I. INTRODUCTION

The Internet has evolved from a communications link among defense researchers into a network providing millions of users easy access to a wealth of information, goods, and services. Currently, it is estimated that well over 100 million people have access to the Internet, and the number is growing quickly. In part, the exponential growth in the on-line consumer market has propelled the Internet’s extraordinary growth. As the Federal Trade Commission (FTC or “Commission”) noted in its July 1999 report to Congress, on-line commerce tripled from approximately $3 billion in sales in 1997 to

† General Counsel of the United States Federal Trade Commission. Ms. Valentine previously served as Assistant Director for International Competition and Deputy Director for Policy Planning at the FTC. Before serving with the FTC, she was a partner at O’Melveny & Myers. Ms. Valentine graduated from Yale Law School and received her undergraduate degree from Princeton University. The views expressed here are those of the author and not necessarily of the Federal Trade Commission or any Commissioner.

approximately $9 billion in 1998.\textsuperscript{2} Annual consumer sales are projected to skyrocket from $15 billion in 1999 to $184 billion in 2004.\textsuperscript{3}

The Net is transforming not just our economy, but also our society and our notions of privacy. While the Internet provides a goldmine of information, products, and services to consumers, the Internet also is a rich source of information about consumers. Internet sites collect substantial amounts of personal information, both directly through registration pages, survey forms, order forms, and on-line contests, and indirectly through software products such as "cookies" and other types of tracking software.\textsuperscript{4}

By following consumers' on-line activities, Internet site owners and other data collectors gather significant information about visitors' personal interests and preferences. Such consumer data have proven to be extremely valuable to on-line companies—they enable on-line marketers to target products and services tailored specifically to the interests of individual consumers and permit companies to boost their revenues by selling the data or selling advertising space on their Internet sites.\textsuperscript{5} An entire industry has emerged to market a variety of software products designed to assist Internet sites in collecting and analyzing visitor data and in serving targeted advertising.\textsuperscript{6}

Ultimately, the prevalence, ease, and relatively low cost of collecting, maintaining, and disseminating personal consumer information have a Janus-faced aspect. On the one hand, the ability to gather, process, and disseminate information on the Internet provides

\begin{itemize}
  \item Actual sales for 1999 are not yet available, but the FTC has projected figures of $12 to $18 billion. See FTC'S JULY, 1999 PRIVACY REPORT, supra note 2, at 3; see also Forrester Research, Inc., Online Retail to Reach $184 Billion by 2004 as Post-Web Retail Era Unfolds (Sept. 28, 1999) <http://www.forrester.com/ER/Press/Release/0,1769,164,FF.htm>.
  \item See John Markoff, Bitter Debate On Privacy Divides Two Experts (Dec. 30, 1999) <http://www.nytimes.com/library/tech/99/12/biztech/articles/30privacy.html>. Cookie technology allows a web site server to place information about a consumer's visits to the site on the consumer's computer in a text file readable only to that web site server. The cookie assigns each consumer's computer a unique identifier so that the consumer can be recognized in later visits to the site. Advertisers are now able to assign a cookie to the computers of users who visit sites in advertising networks and to follow those users from site to site by reading information stored in that cookie at each site.
  \item See FTC'S JULY, 1999 PRIVACY REPORT, supra note 2, at 2.
  \item See id.; see also supra note 4.
\end{itemize}
consumers with a wealth of benefits (e.g., web sites can “remember” where a consumer has been and what type of products the consumer likes so that when the consumer returns to the site, she can be directed to additional products that are likely to interest her). On the other hand, darker voices are legitimately concerned that the manipulative use of information available on the Net may adversely affect privacy. Some uses of personal data can be intrusive, as when private information is widely circulated; or reckless, as when inaccurate information is widely shared with other people and companies; or predatory, as when the information is used to target victims for a scam or crime.

For over five years, the FTC has actively monitored developments in e-commerce, particularly those affecting consumer privacy. The FTC has supported industry self-regulation and has taken enforcement actions as needed. The FTC also has endorsed certain legislative initiatives (e.g., the Children's Online Privacy Protection Act) to address specific on-line privacy concerns. As explained below, there is no simple choice between self-regulation or legislation as the anointed vehicle for protecting consumers’ privacy. We already have both and will continue to need both in the future.

II. PRIVACY ON THE INTERNET—THE EVOLVING LEGAL LANDSCAPE

In the United States, individual privacy, including on-line privacy, is protected through a combination of constitutional guarantees, federal and state statutes, regulations, and voluntary codes of conduct, all of which apply to the public and private sectors in different ways. Although the U.S. Constitution does not explicitly mention a right to privacy, the Supreme Court decades ago recognized a fundamental right to privacy, or the right to be left alone. The Court subsequently interpreted the Bill of Rights as creating, through a penumbra of various rights, “a right of personal privacy, or a guarantee [that] certain areas or zones of privacy [do] exist under the Constitution.” Viewed in hindsight, the federal courts have effectively acknowledged a right to privacy with respect to marital relations, procreation, contraception, family relationships,

7. See Sunstein, supra note 1, at 37; see also Glenn R. Simpson, E-Commerce Firms Start to Rethink Opposition to Privacy Regulation as Abuses, Anger Rise, WALL ST. J., Jan. 6, 2000, at A24.
child rearing, and education. In addition, a number of state constitutions specifically enumerate the right of citizens to be protected from privacy invasions.

Aside from constitutional guarantees, the U.S. legislative approach to privacy has been traditionally sectoral, that is, privacy law has developed to address particular data types and users. Historically, fear of the government's use of personal data was the primary concern. Certain statutes thus limit the use of personally identifiable data that the government maintains. Other statutes limit the government's use of personal data maintained by industry. And some statutes limit firms' use of personal data. While no single law or regulation specifically recognizes a U.S. citizen's general right to informational privacy, certain laws as applied do afford a fair amount of such privacy to consumers.

A. Federal Trade Commission Act and Informational Privacy

Section 5 of the Federal Trade Commission Act ("FTC Act") in


14. For example, the Tax Reform Act of 1976, 26 U.S.C. § 6103 (1994 & Supp. I 1995), protects the confidentiality of tax returns and return-related information and limits the dissemination of individual tax return data. Another example is the Privacy Act of 1974, 5 U.S.C. § 552a (1994), which regulates the government's creation, collection, use, and dissemination of records which can identify an individual by name or other personal information.

15. See, e.g., Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2522, 2701 (1994), as amended, which limits the circumstances under which the federal and state governments may access oral, wire, and electronic communications.


particular can protect consumers' informational privacy whenever a company collects or disseminates personal data in an unfair or deceptive manner. For example, in August 1998, the Commission brought its first on-line privacy case against GeoCities. In that case, the Commission was concerned that GeoCities, one of the most frequently visited sites on the Web, collected personal identifying information from its members, both adults and children, and misled them as to its use of that information. When visitors become members, they must fill out an on-line application that requires disclosure of certain personal identifying information and requests optional information regarding education level, income, marital status, occupation, and interests. Through the 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 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 alone maintained this identifying information from children, when in fact a third party collected and maintained it.

Ultimately, GeoCities settled the case by agreeing to disclose prominently on its web site just what information it collects, for what purpose, to whom it will be disclosed, and how consumers can inspect and, if desired, remove 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 actually is collecting and maintaining personal information. Finally, to protect children, the order requires GeoCities to obtain parental consent before collecting information from those age 12 or younger, and to delete any such information already collected, unless GeoCities obtains affirmative parental consent to retain it.

The comprehensive GeoCities consent agreement helped to establish some of the key elements of fair information practices that

---

18. See In re GeoCities, Inc., No. C-3849, 1999 FTC LEXIS 17 (FTC Feb. 5, 1999). Since the time of the settlement, GeoCities has become part of Yahoo!
20. The GeoKidz Club has been replaced by a kids' club called the Enchanted Forest.
protect consumers' on-line privacy. Those elements include: 1) notice of the site's privacy practices; 2) consumer choice regarding the use of information collected; 3) consumer access to correct or remove personal information; 4) safeguarding the security of information; 5) parental control over the collection and use of information gathered from children; and 6) an enforcement mechanism to ensure compliance. These are precisely the types of protections that the Commission has been urging web site operators to provide voluntarily through self-regulation.

Enforcement/Redress recognizes the principle that an enforcement mechanism is vital to ensure compliance with all the other fair information practices and to provide recourse for injured parties. A self-regulatory program that seeks to assure enforcement and redress might incorporate such

---


23. See FTC's JULY, 1999 PRIVACY REPORT, supra note 2, at 3-4. The FTC now recognizes five widely accepted principles essential for effective self-regulatory (or legislative programs) to protect privacy. These five principles are:

Notice/Awareness is the most basic principle. All web sites should disclose to consumers the site's information use and privacy protection policies such as: 1) what information is being collected; 2) who is collecting it; 3) how it will be used; 4) who might have, or will be given access to the data; 5) what passive or non-obvious, data collection methods are used by the site; 6) whether providing the requested information is mandatory or voluntary; and 7) how the data will be protected.

Choice/Consent embodies the principle that web sites should seek consumers' consent regarding any uses of the information beyond those necessary to achieve the basic purpose of the data request.

Access/Participation establishes the principle that consumers should be able to access data about themselves and to challenge the data's 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 meaningful access.

Integrity/Security reflects the principle that data collectors should ensure that the information they collect 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.
features as periodic compliance audits, neutral investigation of consumer complaints, a dispute resolution mechanism, and correction of misinformation or compensation for injured parties. These same principles also served as the foundation for the Children’s Online Privacy Protection Act that was enacted in 1998 (see infra).  

Another recent case illustrating section 5 of the FTC Act’s ability to protect informational privacy is the Commission’s action against ReverseAuction.com. ReverseAuction is an on-line site that features “Declining Price” auctions (that is, the initial, opening price of an item drops the longer the item remains up for auction) and “Wanted” auctions (that is, buyers who are looking for a particular item or service indicate how much they are willing to pay for the item or service, and sellers then try to outbid each other by offering lower prices). The Commission charged that the firm violated consumers’ privacy by harvesting consumers’ personal information from a competitor’s site and then sending deceptive spam to those consumers, soliciting their business.

In essence, it was alleged that, in promoting its new site, ReverseAuction registered with eBay.com, a competitor auction site. ReverseAuction agreed to be bound by eBay’s “User Agreement” and “Privacy Policy,” which purported to protect consumers’ privacy by prohibiting eBay users from gathering and using personal identifying information (such as names and email addresses) for unauthorized purposes such as spam. Notwithstanding that agreement, ReverseAuction harvested eBay’s users’ personal identifying information and used the data to send them spam promoting ReverseAuction’s own web site. ReverseAuction claimed that the spam recipient’s eBay user ID would expire soon, when in fact it was in no danger of expiring. By using this deceptive tactic, ReverseAuction lured eBay users to its web site where they could “re-register.” The Commission also alleged that consumers believed that eBay had provided their eBay user IDs and other information to ReverseAuction, or at least had authorized these practices. In reality, eBay had no idea that ReverseAuction was engaging in these activities. At the end of the day, those who “re-registered” their eBay user IDs at ReverseAuction’s site were simply registering with and

becoming a member of ReverseAuction.com with their eBay IDs now also serving as their ReverseAuction IDs.

The proposed settlement bars ReverseAuction from making any misrepresentations about complying with another company's user agreement, privacy policy, or other provisions that govern the collection, use, or disclosure of consumers' personal identifying information. In addition, ReverseAuction is barred from making any misrepresentations about the features, terms, conditions, business practices, or privacy policies of any other company. Furthermore, the proposed settlement requires ReverseAuction to send an e-mail message to all consumers to whom it had sent spam, explaining that ReverseAuction had not intended to suggest that consumers' eBay user IDs would expire and stating that eBay did not know about and had not authorized any of ReverseAuction's actions. The e-mail will inform consumers that their names and eBay user IDs can be purged from ReverseAuction's database and their registration canceled. Finally, the proposed settlement requires ReverseAuction to post its own privacy policy on its Internet web site and maintain certain records to enable the FTC to monitor compliance with the proposed settlement.

This case illustrates both section 5 of the FTC Act's broad authority and the Commission's commitment to protecting consumers' privacy on-line whenever that privacy is threatened. Here, the FTC was able to ensure that the privacy protections assured to eBay's users were not compromised when the deceptive tactics of a competitor auction site thwarted eBay's self-regulatory efforts to protect consumers' privacy. Without actions such as this one, consumers will lose confidence about whether their privacy choices will be honored. And, because consumer confidence is critical to the development of e-commerce in general, cases such as this one are essential for fostering the continuing growth of e-trade.

B. Other Federal Statutes and Informational Privacy

In addition to the FTC Act, a few other federal statutes, such as the Fair Credit Reporting Act (FCRA), Title V of the Gramm-Leach-Bliley Act, and recently proposed regulations from the Department of Health and Human Services, provide a certain amount of informational privacy protection. While earlier statutes, particularly

the FCRA, may have been conceived for an off-line world, they function to protect the privacy of both on- and off-line consumers. Indeed, it is becoming increasingly difficult to meaningfully protect privacy without addressing concerns in both the real and virtual worlds. This will become even more true as companies begin to merge on-line and off-line consumer data and profiles.

First enacted in the 1970s, the FCRA regulates consumer reporting agencies, also known as credit bureaus, and establishes important protections for consumers with respect to the privacy of their sensitive financial information that credit bureaus hold. The FCRA allows credit bureaus to disclose consumer credit reports only to entities with specified "permissible purposes" (such as evaluating individuals for credit, insurance, employment, or other, similar purposes).\(^\text{28}\) Moreover, these disclosures can only occur under specified conditions (such as certification of need from a prospective employer or insurer). In these ways, the FCRA generally limits the disclosure of consumer reports primarily to instances where a consumer initiates a transaction, such as a loan or employment application. Of course, these processes can now occur completely on-line.

There are certain caveats associated with the FCRA. First, in contrast to credit bureaus with their rich, accurate and up-to-date data collections, individual merchants, both on- and off-line, are free to distribute any information that they collect as part of their discrete transactions or experiences with consumers.\(^\text{29}\) Second, the 1996 amendments to the FCRA include a provision that permits "affiliated" companies to share consumer reports, so long as consumers are notified and given the opportunity to prevent such sharing.\(^\text{30}\) Sharing financial information among affiliated companies may well raise special concerns in the electronic banking or electronic payments context, where detailed and sometimes sensitive information about consumers is gathered.

Congress recently enacted financial privacy provisions in Title V of the Gramm-Leach-Bliley Act, which add to the legal protections


\(^{29}\) See id. § 1681a(d)(2) ("The term ‘consumer report’ does not include (A) any report containing information solely as to transactions or experiences between the consumer and the person making the report.").

\(^{30}\) Id. § 1681a(d)(2)(A)(ii). Note, moreover, that affiliates may freely share among themselves their individual transaction and experience data without providing any notice or opportunity to object to consumers. Id. § 1681a(d)(2)(A)(ii).
available for consumers’ financial information. Under Title V, banking institutions may share personal confidential financial information with their affiliates, but not with third parties such as online marketers, unless consumers are first notified and given the option to require that the banking institution keep all information private. Even with respect to affiliated entities, Title V requires financial institutions to disclose their privacy policies to their customers, including any intent to share nonpublic personal information.

Finally in the extremely sensitive area of medical records, the Department of Health and Human Services recently issued proposed regulations establishing the first-ever national standards to protect health information that is transmitted or maintained electronically. Among other things, the proposal would require an individual’s written consent to release medical information for purposes unrelated to treatment and payment. A notable loophole in the proposed rules is that the rules would not protect health information if it is transmitted or maintained solely via traditional, paper records.

C. Federal Internet-Law

Specific federal protections for consumer privacy on the Internet are fairly limited. Most notably, the Children’s Online Privacy Protection Act (COPPA) requires that operators of web sites directed to children under 13 or who knowingly collect personal information from children under 13 must: (1) provide parents notice of their information practices; (2) obtain prior, verifiable parental consent for the collection, use, and/or disclosure of personal information from children (with certain limited exceptions); (3) upon request, provide a parent with the ability to review the personal information collected from his/her child; (4) upon request, provide a parent with the opportunity to prevent the further use of personal information that has already been collected, or the future collection of personal information from that child; (5) limit collection of personal information for a child’s on-line participation in a game, prize offer, or other activity to information that is reasonably necessary for the activity; and (6) establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of the personal

32. See Id. at 1437.
information collected.\textsuperscript{34} COPPA directs the Commission to adopt regulations implementing these requirements, and on November 3, 1999, the Commission published its final rule incorporating and explaining COPPA's privacy protections.\textsuperscript{35} The rule provides a safe harbor for operators who follow Commission-approved self-regulatory guidelines. Moreover, the Commission retains its authority under section 5 of the FTC Act to investigate and enforce against any child-related information practices that are deceptive or unfair.\textsuperscript{36}

COPPA is a classic example of federal legislation aimed at protecting a particular privacy problem—children's information privacy on the Internet. The lack of much additional federal legislation protecting Internet privacy stems from several sources. First, there is no consensus that one general approach solves all privacy problems. Some believe that firms should always seek consumers' consent before sharing their personal data (the opt-in advocates). Others believe that it is more efficient and beneficial for all involved if firms are allowed to share consumers' personal data so long as they notify consumers and enable them to prevent such sharing before it occurs (the opt-out advocates). Alternatively, it may prove most desirable to have opt-in (affirmative consent) rules for certain types of sensitive data sharing (\textit{e.g.}, medical information) and opt-out rules when less sensitive data is being shared or when there is a broad consensus that such sharing is useful for both consumers and firms.

Second, there is a general reluctance to create a plethora of national or state laws for an inherently global technological environment. There is a legitimate concern that an explosion of various sovereigns' laws regulating the Net would only create conflicts of laws rather than resolve issues of privacy invasion. In addition, there has been at least a tentative conclusion that existing

\begin{footnotes}
\item \textsuperscript{34} 15 U.S.C.A. §§ 6501-6506 (West Supp. 1999).
\item \textsuperscript{36} The FTC did precisely this with the Young Investor web site, which allegedly falsely represented that personal information collected from children in a survey would be maintained anonymously. The case eventually settled. \textit{See Young Investor Website Settles FTC Charges} (May 6, 1999) \langle http://www.ftc.gov/opa/1999/9905/younginvestor.htm \rangle.
\end{footnotes}
laws, such as section 5 of the FTC Act, combined with self-regulation, may be adequate to protect personal informational privacy on the Net. But that tentative consensus may be falling apart, as businesses and consumers recognize the serious harm that hackers, fraud artists and sheer mistakes can wreak with personal financial and identifying information. Moreover, businesses are beginning to worry about the specter of different state law standards as legislators attempt to respond to citizens’ concerns about identity theft and privacy invasions.37

III. CURRENT FEDERAL POLICY ON INTERNET PRIVACY

The choice of either legislating privacy on the Net or fostering self-regulation is a false one. In fact, we already have both. However, there are legitimate reasons why federal policy regarding privacy on the Internet thus far has favored a self-regulating cyberspace marketplace.

Given the rapidly evolving nature of the Internet and computer technology, self-regulation is the least intrusive and may be the most efficient means to ensure fair information practices.38 Voluntary codes are by definition developed and adopted by those with the greatest expertise about and sensitivity to industry practices and conditions. And self-regulatory codes can be revised when necessary, more promptly than legislative codes. This allows firms to respond quickly to the rapid evolution of the Internet and computer technology and to employ emerging technologies to protect consumers' privacy. Moreover, when regulation is voluntarily-adopted, compliance tends to be broader, and enforcement more prompt than when a legislature or agency imposes its mandate. And self-regulation wholly avoids many of the First Amendment issues associated with governmental regulation. Finally, where an industry can regulate itself, the government need not devote as many of its limited resources to the task.

Self-regulatory efforts, of course, may fail—they may not be rigorously implemented or enforced, or they may lapse into a vehicle for exclusionary or collusive conduct among rivals. Businesses may be reluctant to disclose to consumers what they do with personal data, simply to avoid having to compete for customers based on how firms protect personal data. Government vigilance is therefore appropriate


and necessary, especially where business rivals, who have an incentive to restrain competition, are involved in the process.

The Commission's numerous activities to monitor industry efforts to protect consumers' privacy include public workshops, Commission Task Forces, creation of an Advisory Group, and surveys of web sites' privacy practices. The Commission's most recent workshop, jointly sponsored by the U.S. Department of Commerce, focused on on-line profiling. This workshop examined the use of "cookies" and other types of tracking software—and even methods of combining this information with personal information collected directly from consumers or contained in other databases—to create targeted, user-profile based advertising campaigns. Some maintain that no personally identifiable information is collected by this profiling—at most the profile is of the browser or the computer hardware without a street, e-mail address or name attached. But consumer groups and privacy advocates have raised concerns about these practices, primarily because many consumers are unaware that software can be used to create on-line profiles about them. Privacy advocates believe that consumers should at least be given notice that such profiling is occurring and given the choice of whether an on-line profile can be created, maintained, and used. I confess to having some sympathy with that position.

The Commission has also used Task Forces to grapple with various Internet privacy issues such as understanding the costs and benefits of implementing fair information practices on-line. The costs and benefits of granting consumer access to their on-line information and guaranteeing the security of personal information have been particularly contentious. Indeed, the benefits and costs are interrelated insofar as increased access to information, at least with today's technology, tends to undermine the security and integrity of the data.

To better address this dilemma, the Commission recently announced the establishment of the Advisory Committee on Online Access and Security ("Advisory Committee"). The Advisory Committee is to examine what constitutes reasonable access to personal information, including whether the extent of access provided by web sites should vary, depending upon the sensitivity of the


personal information collected and/or the purpose for which such information is collected. It will consider whether consumers should be provided access to enhancements to personal information (e.g., inferences about their preferences or purchasing habits). Other issues are whether appropriate and feasible methods exist for verifying the identity of individuals seeking access and whether the difficulty and costs of retrieving consumers' data should be considered. Finally, the Advisory Committee will consider whether a reasonable fee should be assessed for access and whether limits should be placed on the frequency of requests for access.

On the security side, the Advisory Committee will consider how to define appropriate standards for evaluating the measures taken by web sites to protect the security of personal information. That is, it will consider what may constitute reasonable steps to assure the integrity of this information and what measures should be undertaken to protect against its unauthorized use or disclosure. By May 2000, the Advisory Committee will prepare a written report presenting options for implementing these fair information practices along with the costs and benefits of each option.41

Finally, the Commission continues to monitor through surveys the progress of firms' privacy efforts and to assess whether self-regulatory programs are in fact fulfilling their promise. The results of past surveys of commercial web sites suggest that on-line businesses are increasingly providing more notice of their information practices. The Commission's 1998 survey found that only 14% of the sites surveyed posted any disclosure regarding their information practices, and even fewer—2%—posted a comprehensive privacy policy. The "most popular" web sites performed better—71% had posted an information disclosure practice or notice.42 A year later, two other, independent surveys found that 66% of 361 busy web sites surveyed posted at least one disclosure about their information practices, while 93% of the 100 top web sites did.43 Unfortunately, these same surveys found that very few sites (10% to 22%) posted disclosures

41. The report or excerpts from the report should be available in May 2000 at <http://www.ftc.gov>.
42. See FTC's JULY, 1999 PRIVACY REPORT, supra note 2, at 4.
covering all the substantive fair information practice principles. Thus, major challenges remain for effective self-regulation.

In March 2000, Commission staff conducted a new Internet survey to assess the progress that commercial web sites have made in implementing all of the fair information practices (notice, choice, access, security, and enforcement), and went beneath the surface to determine whether on-line privacy practices are adequate for enabling consumers to exercise choice about how their personal information is collected and shared. Commission staff analyzed what information a domain collects; whether a privacy policy is posted and what it covers; whether a recognized seal is posted; and whether third party advertisers attempt to place cookies on the site's visitors' computers. The staff hopes to issue its findings in a report by mid-summer.

If self-regulation is to succeed, another critical issue is how to create incentives to encourage the development of privacy-enhancing technologies that will give consumers more control over how and when their personal data is collected and used. One such technology is the World Wide Web Consortium's "Platform for Privacy Preferences" (P3P). The P3P platform would enable web sites to present their privacy policies in such a way that consumers' computers could automatically "read" the policies and automatically "release" information to sites that conform to consumers' pre-programmed choices on acceptable privacy policies. The P3P protocol, however, is still in the drafting stage.

IV. THE U.S. APPROACH TO PRIVACY VERSUS THE E.U. APPROACH

The U.S. approach to protecting consumer privacy on-line—
relying significantly on industry self-regulation with a minimum of legislative and administrative mandates—differs from that of the European Union (E.U.), which relies more on legislative protections. In particular, the E.U. passed a Directive in 1995 that extensively regulates the buying and selling of personal data.\footnote{DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 24 OCTOBER 1995 ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA AND ON THE FREE MOVEMENT OF SUCH DATA (visited Mar. 27, 2000) <http://europa.eu.int/eur-lex/en/lil/dat/1995/en_395Loo46.html>; see also OECD, GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDE R FLOWS OF PERSONAL DATA (visited Mar. 28, 2000) <http://www.oecd.org/dst/it/it/secure/prod/PRIV-EN.htm>.} The Directive, which took effect on October 25, 1998, specifies 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 are relevant, accurate, and up-to-date. European citizens, in turn, are guaranteed a bundle of rights—a right of access to their personal data; a right to correct any data that are inaccurate; a right to refuse use of their data for activities such as direct marketing; and a right of recourse if unlawful processing occurs.

Significant for the U.S. is that the Directive prohibits the transfer of personal data to any country that does not provide “adequate” (meaning “comparable”) protection. Each E.U. member country has been enacting its own laws to implement the Directive. It is still too early to know how stringent the various E.U. member states’ laws and policies 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 U.S. subsidiaries who buy and sell personal data in the E.U., or on firms that acquire and transmit personal data to the United States.

The U.S. and the E.U. are currently in negotiations to determine how best to harmonize their different approaches to protect personal data. They have been working on developing “safe harbors” that establish a set of criteria which, if met, would allow U.S. companies to do business with European citizens or firms.\footnote{See U.S. DEPARTMENT OF COMMERCE, Draft, INTERNATIONAL SAFE HARBOR PRIVACY PRINCIPLES (Nov. 15, 1999) <http://www.ita.doc.gov/tdlcom/Principles1199.html>.} These “safe harbors” would require U.S. firms to provide: (1) notice of their information practices; (2) choice as to whether and how personal information may be disclosed to third parties; (3) onward transfer of
personal data to third parties, consistent with the notice and choice provided; (4) security for personal data, whether at its creation, maintenance, use, or transmission; (5) access by individuals to the information that a firm holds about them and the ability to correct, amend, or delete inaccurate information; and (6) enforcement mechanisms to assure compliance with the foregoing principles and recourse for injured persons. Most recently, U.S. and E.U. delegates met in December to try and complete the negotiations on the safe harbors, but the December meeting ended without any definitive conclusions.

V. CONCLUSION

Like the ever-evolving Internet, the legal landscape that applies to the Internet is in motion and will be for years to come. One way to cope with such an ever-changing scene is to allow self-regulation to develop and change along with it. But industry self-regulation may only gradually develop effective enforcement mechanisms and may ultimately provide inadequate protection against highly motivated hackers or fraud artists. Another way is to empower citizens with technology that helps protect their privacy and permits them to assert control over how their personal data are used. But self-help requires considerable consumer education and sophistication and may well fail to protect consumers against surreptitious privacy invasions or identity theft. Finally, legislation may establish protection against specific fraudulent abuses, or for specific groups, such as children, or may even create useful minimum criteria like those established in the Children’s Online Privacy Protection Act. But the legislative process can be slow and cumbersome and may lag behind or interfere with technological developments. Thus, neither pure self-regulation, nor consumer education and technological empowerment, nor legislation alone can be the answer. All are needed to ensure meaningful privacy protection on the evolving Net.