THE WAY THE "COOKIES" CRUMBLE: INTERNET PRIVACY AND DATA PROTECTION IN THE TWENTY-FIRST CENTURY

*Rachel K. Zimmerman**

INTRODUCTION

Upon entering the doors of New York University School of Law, one finds the following words engraved on the wall: "Freedom and Justice Through Law." For hundreds of years, members and non-members of the legal profession have generally assumed the truth of these words. In recent years, however, circumstances have drawn into question the law's ability to assure a level of freedom and justice acceptable to the American people. This is due, in part, to the difficulty the law has had responding to technological innovation in the United States.

Privacy law, in particular, has had difficulty keeping pace with advances in technology. The changing nature of available technology presents a continuous challenge to the body of law regulating its use. From tiny hidden microphones and video cameras[1] to voice and face recognition capabilities[2] and computerized data banks,[3] technology has enabled people to gather vast amounts of information about an

---

* Candidate for J.D. degree, 2001, New York University School of Law. I would like to thank Professor Rochelle Dreyfuss for her insightful contributions, Jonathan Zimmerman for his technical advice, and Nathan Sevilla and the *Journal of Legislation and Public Policy* staff for their outstanding editorial assistance.

1. *See* Gary T. Marx, *Ethics for the New Surveillance*, *in* VISIONS OF PRIVACY: POLICY CHOICES FOR THE DIGITAL AGE 39, 40 (Colin J. Bennett & Rebecca Grant eds., 1999).

2. *See* Pattern Recognition and Image Processing Lab, Department of Computer Science and Engineering, Michigan State University, *Face Location* (last visited Feb. 21, 2001) (describing human face detection method and calling it "the first step in a fully automatic face recogni-tion system"); Pattern Recognition and Image Processing Lab, Department of Com-puter Science and Engineering, Michigan State University, *Speaker Verification*, (last visited Feb. 21, 2001) (describing mechanics of speaker verification system).

3. *See* SARA BAASE, A GIFT OF FIRE: SOCIAL, LEGAL, AND ETHICAL ISSUES IN COMPUTING 41-43 (1997) (discussing Federal government's maintenance of more

individual without his or her knowledge or consent. Furthermore, the mechanics of modern society require most people to reveal certain personal information to a variety of companies and organizations for legitimate uses. In many cases, however, once this information has been shared, the law places few restrictions on how it may be used.

The Internet has quickly emerged as yet another innovation to which the law must adapt if it is to remain the protector of freedom and justice. Along with the immense social benefits of the Internet comes a vast potential for privacy violation. For example, servers have the capacity to gather information from users visiting their sites; "cookies"[4] may be sent by Web sites to be stored on a visitor's hard drive and later be re-transmitted to the Web site should that visitor ever return, and Online Service Providers (OSPs)[5] can monitor all Web sites its customers visit and with whom they communicate via e-mail.[6] Although these wonders of modern technology may serve legitimate purposes, they also create a certain amount of insecurity regarding the personal data and information of Internet users.

This note begins in Part I by identifying the specific threats the Internet poses to personal privacy. Part II discusses whether, and for what reasons, the legislature should be concerned with these threats. Part III evaluates the effectiveness of current methods of protecting privacy. Finally, Part IV proposes a multifaceted solution that includes both constitutional and statutory remedies. The constitutional remedy suggests revising the "reasonable expectation of privacy" test to incorporate concerns about new technology prior to the development of that technology. The statutory remedy incorporates "fair information practices" and relies on European Union legislation[7] for guidance.

---

than 2000 computerized databases full of personal information and how these databases aid government agencies in profiling "potential" criminals).

4. *See* Joshua B. Sessler, Note, *Computer Cookie Control: Transaction Generated Information and Privacy Regulation on the Internet*, 5 J.L. POL'Y 627, 632-33 (1997) ("When a Web-site is visited, the server can write a file onto the user's computer hard-drive which characterized what took place at the site. In general, cookies allow sites to 'tag' their visitors with unique identifiers so they can be identified each time they visit.").

5. *See* Leonard T. Nuara et al., *What Lawyers Need to Know About the Internet*, N.J. LAW., Aug. 1999, at 10 ("To connect to the Internet . . . businesses and individuals purchase access from . . . online service providers (OSPs). . . . OSPs deliver access to the Net and provide proprietary content organized in an easy to use format. Some OSPs include America Online, Prodigy and MSN.").

6. *See* Sessler, *supra* note 4, at 631-35.

7. *See* Council Directive 95/46 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, 1995 O.J. (L 281) 31 [hereinafter Council Directive].

I
TECHNOLOGY'S DARK SIDE: THE INTERNET'S THREAT TO PERSONAL PRIVACY

As technological innovations have become more advanced, mechanisms for monitoring people's behavior without their knowledge have become increasingly prevalent. Indeed, "[n]ew multimedia communications and computing technology is potentially much more intrusive than traditional information technology because of its power to collect even more kinds of information about people, even when they are not directly aware that they are interacting with or being sensed by it."[8] Not only does this new computing technology allow the collection of more data, but it also allows collectors to do more with the data they acquire. Furthermore, the types of organizations collecting personal information are becoming more varied. While Americans have historically worried only about surreptitious monitoring by government agencies, they now need to concern themselves with the activities of private companies as well.[9]

The type of privacy invasion involved with Internet use differs from the traditional conception of privacy. When one thinks of an invasion of privacy, one usually imagines people peeping in windows or telemarketers calling during dinner. Privacy erosions on the Internet are more subtle, and most people are probably unaware they are occurring since the mechanisms developed to monitor Internet behavior have been specifically designed not to notify the user of their existence. In fact, "[t]he irony is that the unobtrusiveness of such technology both obscures and contributes to its potential for supporting invasive applications, particularly as users may not even recognize when they are online in such an environment."[10]

In today's context, privacy can be divided into four basic categories: 1) information privacy, 2) bodily privacy, 3) communications privacy, and 4) territorial privacy.[11] The primary concern when dealing

---

8. Victoria Bellotti, *Design for Privacy in Multimedia Computing and Communications Environments*, *in* TECHNOLOGY & PRIVACY: THE NEW LANDSCAPE 63, 64 (Philip E. Agre & Marc Rotenberg eds., 1997).

9. *See* Walter A. Effross, *Commercial Profiles or Suspect Classifications?: Preparing, Preventing, and Parrying Public and Private Profiling*, 1999 STAN. TECH. L. REV. VS 9, ¶ 9 (comparing and contrasting government profiling for "airline terrorists" or "drug couriers" with commercial profiling currently employed both on and off Internet in United States), *at* http://stlr.stanford.edu/STLR/Symposia/Privacy/99_VS_9/.

10. Bellotti, *supra* note 8, at 66.

11. *See* David Banisar & Simon Davies, *Privacy & Human Rights: An International Survey of Privacy Laws and Practice*, Global Internet Liberty Campaign, *at* http://www.gilc.org/privacy/survey/intro.html (last updated Oct. 3, 1998) ("[P]rivacy

with the Internet is information privacy, or data protection, defined as "the right of an individual to control the acquisition, disclosure, and use of personal information."[12]

When people log on to the Internet and visit Web sites, a great deal of personal information is collected through both active user participation and passive collection techniques. Web sites collect information through active user participation when, for example, users place online orders, fill out sweepstakes entry forms, or register to gain access to "members only" sites.[13] Conversely, the three most common forms of passive data collection methods include a Web site's use of cookies,[14] a direct marketing company's use of cookies,[15] and an OSP's collection of "click stream" data.[16] The sections that follow will analyze each in turn.

A. Web Sites' Use of Cookies

A "cookie" is a small text file that a Web site sends to be stored on the hard drives of visitors to the site.[17] Cookies contain informa-

---

protection is frequently seen as a way of drawing the line at how far society can intrude into a person's affairs.").

12. Sheri Hunter, *Defamation and Privacy Laws Face the Internet*, COMMS. LAW., Fall 1999, at 19; *see also* Janlori Goldman, *Privacy and Individual Empowerment in the Interactive Age*, *in* VISIONS OF PRIVACY: POLICY CHOICES FOR THE DIGITAL AGE 100 (Colin J. Bennett & Rebecca Grant eds., 1999).

13. *See What are Cookies?*, RBA WORLD PRODUCTIONS, (last visited Feb. 21, 2001) [hereinaf-ter *What are Cookies?*].

14. *See* Nelson A. Boxer, *Are Your Corporation's Cookies Private?*, CORP. COUNSELLOR, May 1999, at 1.

15. *See* Peter H. Lewis, *Battling Cookie Monsters*, N.Y. TIMES, Feb. 24, 2000, at G1 ("DoubleClick says the cookie information alone allows it to provide targeted advertisements to the computer and track them so the same tedious advertisements do not show up time after time."); Will Rodger, *Activists Charge DoubleClick Double Cross*, USATODAY.COM (June 7, 2000),

16. *See Click Stream*, WHATIS.COM, *at* http://whatis.techtarget.com/WhatIs_Definition_Page/0,4152,211794,00.html (last visited Feb. 21. 2001) ("In Web advertising, a click stream is the sequence of clicks or pages requested as a visitor explores a Web site."); *see also* Nuara, *supra* note 5, at 10.

17. *See* Boxer, *supra* note 14. Servers most commonly use the following four cookie varieties: 1) visitor cookies keep track of the number of visits made by that particular computer to the Web site; 2) preference cookies save preferences regarding the manner in which the page loads (i.e. colors, number of search results displayed, etc.); 3) shopping basket cookies assign an identification value—that remains constant as the user moves throughout the site—and save all selections to a file corresponding to that identification value; 4) tracking cookies, used primarily by direct marketing companies, assign an identification value the first time the user visits a site on which the company displays a banner ad and thereafter keep track of the other sites visited by the user assigned that value. *What are Cookies?*, *supra* note 13.

tion on varying topics; some relating to the number of visits a user makes to a particular Web site, others keeping track of a user's passwords and preferences.[18] Most Internet users do not know that a site is sending cookies because most browsers have, as their default setting, no cookie warning. Browsers generally have both the capacity to be configured to warn the user when a Web site tries to send a cookie, and a mechanism by which the user may reject the cookie. However, the default setting ensures that most users have no knowledge of how many cookies are sent to their hard drive nor from where they are sent.[19]

Cookies can betray an Internet user's privacy in two primary ways. First, cookies are stored on the user's hard drive and can be accessed at a later date.[20] Once accessed, the cookies will display a detailed list of each Web site that has been visited by that computer within a relevant time frame. Furthermore, the text of the cookie file may reveal personal information about the user, such as the user's password, e-mail address, or any other information entered while at that site.[21] An example of such a scenario occurred recently when government officials discovered that John Deutch, former head of the CIA, used his home computer to write top-secret memos.[22] In the resulting search of his CIA-issued home computer to evaluate the extent of the damage done to national security, the FBI found cookies indicating that his computer had visited adult entertainment sites, designated as "high risk" by the CIA.[23]

The second way in which cookies may affect privacy is that the servers of the Web sites who send cookies also receive the information stored on that particular cookie when a user makes a return visit to the same site.[24] Using cookies, Web sites currently have the ability to track from what site the user came, the links on which the user clicked while in the site, any purchases made, and any personal information entered. Many cookies are also able to identify the Internet protocol (IP) address[25] of the user, thus giving them the capacity to identify the

---

18. *See What are Cookies?*, *supra* note 13.

19. *See Persistent Client State: HTTP Cookies*, NETSCAPE, *at* (last visited Feb. 21, 2001).

20. *See id.*

21. *See What are Cookies?*, *supra* note 13.

22. Niles Latham, *Too Big for his Breaches: CIA Ex-Chief Free as Scientist is Jailed for Same Offense*, N.Y. POST, Mar. 8, 2000, at 10.

23. *Id.*; Vernon Loeb, *Tenet Offers 'No Excuse'; Senate Panel Hears CIA Chief on Deutch's Security Lapses*, WASH. POST, Feb. 3, 2001, at A21.

24. *See What are Cookies?*, *supra* note 13.

25. Nuara, *supra* note 5, at 10 ("IP [Internet protocol] assigns every computer on the Internet an address made up of a series of four numbers between 1 and 255 (i.e.

exact location of the computer used to access the site.[26] Once a Web site collects this personal information, it may use it in ways that violate the privacy interests of the data subject. For example, a woman could choose to purchase a pregnancy test from an online store, believing this to be a sure method of retaining anonymity in the face of such a personal matter. However, the Web site might choose to disseminate information regarding her purchase and her e-mail address to pro-life organizations that could then inundate her with messages via e-mail.

B. Direct Marketing Companies' Use of Cookies

Through the posting of "banner ads,"[27] direct marketing companies exemplify the harm information-gathering practices on the Internet could cause. One such company, DoubleClick, has been the subject of recent litigation and immense public concern.[28] DoubleClick, like many other Internet direct marketing companies, posts banner ads on the Web sites of other companies.[29] Banner ads serve a double purpose: They advertise the products of DoubleClick's clients while simultaneously gathering information, through the use of cookies, about any visitor to the site on which the banner ad is displayed.[30]

While most Web sites have only the limited capability to read cookies from a user's hard drive that the site itself sent on a previous visit, banner ads have a greater capacity to monitor users' behavior on the Internet. Banner ads may be posted on hundreds of different Web

---

255.255.100.1). Using these numbers, one computer can communicate with any other computer on the Internet and share data.").

26. Domingo R. Tan, Comment, *Personal Privacy in the Information Age: Comparison of Internet Data Protection Regulations in the United States and the European Union*, 21 LOY. L.A. INT'L & COMP. L.J. 661, 666 (1999).

27. *See* Leslie Miller & Elizabeth Weise, *FTC Studies Web Site 'Profiling,'* USATODAY.COM (Nov. 23, 1999) ("The companies compile detailed profiles of where people surf and what they look at, even if a surfer doesn't click on single ad."), *at* www.usatoday.com

28. *See, e.g.*, *In re* DoubleClick Inc. Privacy Litigation, No. 1352, 2000 U.S. Dist. LEXIS 11148, at *2 (J.P.M.L. July 31, 2000) ("Common factual questions arise because all actions allege that DoubleClick Inc. improperly used or monitored confidential information of computer users in delivering advertisements on the Internet.").*But see* John Schwartz, *Trade Commission Drops Inquiry of DoubleClick*, N.Y. TIMES, Jan. 23, 2001, at C5 (reporting FTC conclusion that "DoubleClick never used or disclosed [personally identifiable information] for purposes other than those disclosed in its privacy policy").*See also* Rodger, *supra* note 15.

29. Hillary Appelman, *Ratings That Know What You're Looking at, and When*, N.Y. TIMES, June 7, 2000, at 37; Lewis, *supra* note 15, at G1; Rodger, *supra* note 15.

30. Appelman, *supra* note 29, at 37; Lewis, *supra* note 15, at G1; Rodger, *supra* note 15.

sites and may send their own cookies in addition to the cookie sent from the Web site itself.[31] Banner ad cookies may contain all of the same information about the user that is contained in the Web site's cookies, and they have the added capacity to read the cookies sent by other banner ads situated on different sites so long as the same direct marketing company owns both banners. In this manner, direct marketing companies like DoubleClick employ cookies to collect vast amounts of personal information from unsuspecting users.[32]

Some time ago, DoubleClick expanded its potential reach by acquiring Abacus-Direct, a company in the business of collecting and amassing a large database of personal information from a variety of sources.[33] Until this merger, DoubleClick's only information about each user pertained to his or her Internet behavior; it was not possible, nor was it attempted, to connect the users' information with any personally identifying information. Upon acquiring Abacus-Direct, DoubleClick announced a plan to match users' click stream data with personally identifiable information from Abacus-Direct files, thus creating comprehensive personal profiles of thousands of unwitting Internet users.[34] The plan to merge information met strong resistance from consumer groups and Internet users across the nation.[35] It is likely that this public outrage, combined with the threat of several lawsuits, prompted DoubleClick's recent suspension of its plan to match click stream data with personal information and led to the hiring of both a privacy officer and a chairman of a new privacy advisory board.[36]

The direct marketing companies' activities in the Internet arena suggest a vast potential for the abuse of personal information. Technologists argue that the real fear regarding such behavior is that before long, "[p]rofiling . . . could be employed to determine who gets—and who is excluded from—all kinds of opportunities like jobs, housing

---

31. Appelman, *supra* note 29, at 37; Lewis, *supra* note 15, at G1; Rodger, *supra* note 15.

32. Lewis, *supra* note 15, at G1 ("DoubleClick Inc. [has] attracted billions of dollars from investors, advertisers and Web sites, in part by using software cookies—small computer files that Web sites insert into your computer—to gather information about the online habits of tens of millions of Internet users, often without their knowledge or informed consent.").

33. *See* Schwartz, *supra* note 28, at C5.

34. *See* Lewis, *supra* note 15, at G1.

35. *See* Schwartz, *supra* note 28, at C5.

36. Nick Wingfield, *DoubleClick Is Expected to Appoint Board to Advise on Privacy Threats*, WALL ST. J., May 17, 2000, at B2.

and education."[37] The technologists' fear, however, is not a distant one. Given that a study has revealed that 46.8% of Web users visited a DoubleClick network site in December of 1998 alone, and it is estimated that by February of 2000, DoubleClick will have compiled approximately 100 million Internet profiles, the public concern over such companies' activities is well founded.[38]

C. OSPs' Use of Click Stream Data

Just as Web sites and banner ad companies collect information through the use of cookies, OSPs[39] may monitor and record their subscribers' information through the use of click stream data.[40] Because users, when they connect to the Internet using an OSP, essentially rent one of the OSP's lines for the duration of the connection, the OSP can record such information as the sites users visit and the links on which users click from each site.[41]

OSPs also have the capacity to invade their subscribers' privacy by allowing the personal information they require from their subscribers to be connected to information gathered in other areas. One example of such cross-referencing may be found in the recent case of *McVeigh v. Cohen*.[42] In this case, an officer of the U.S. Navy was discharged after his OSP, America Online (AOL), gave his superiors information allowing them to connect his name with his e-mail address after the Navy intercepted a message written from his e-mail account regarding homosexuality.[43] While it is true that the officer voluntarily gave America Online his name when he registered with the company for an e-mail address, it is also true that he expected to be able to send and receive non-harmful e-mails with a certain degree of anonymity. AOL undermined this expectation when it offered the officer's personal information to his superiors.

---

37. Steve Lohr, *Online Industry Seizes the Initiative on Privacy*, N.Y. TIMES (Oct. 11, 1999), *at* http://www.nytimes.com/library/tech/99/10/biztech/articles/11priv.html.

38. Jason Williams, *Personalization vs. Privacy: The Great Online Cookie Debate*, EDITOR & PUBLISHER, Feb. 28, 2000, at 26.

39. An OSP is a company that provides Internet service to computer users. *See* Nuara, *supra* note 5, at 10.

40. *See supra* note 16 and accompanying text.

41. *See* Nuara, *supra* note 5, at 10.

42. 983 F. Supp. 215 (D.D.C. 1998).

43. *See id.* at 217 ("Through an option available to AOL subscribers, the [Navy] volunteer searched through the 'member profile directory' to find the profile for this sender. The directory specified that 'boysrch' [the username] was an AOL subscriber named Tim who lived in Honolulu, Hawaii, worked in the military, and identified his marital status as 'gay.'").

As the above examples indicate, with the advent of the Internet came a vast potential for information privacy violations. While cookies and click stream data currently present the greatest risk to Internet users' privacy, the rapid pace of technological development in the Internet arena signals the impending arrival of new devices having a similar or greater capacity for surreptitiously gathering personal data.

II
WHY AMERICA SHOULD CARE ABOUT INTERNET PRIVACY

The aforementioned threats to personal privacy brought on by the development of the Internet present more than a topic for hypothetical discussion. These threats present a true challenge for society. Privacy on the Internet is a topic not merely of interest to American citizens who use the Internet regularly, but also to officials in countries on whose trade America relies.

A. American Citizens Care about Privacy

American citizens value their privacy and express concern over the current lack of protection afforded their personal information.[44] A society's fear of privacy invasion is highly visible in its literature. George Orwell describes what life would be like in a world with no privacy protection: "You had to live—did live, from habit that became instinct—in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized."[45] Though we do not now live in an age in which we have to worry about Orwell's "Thought Police" watching us through "telescreens" in our homes, the Internet is in many ways a peering eye into our privacy. When a user is logged on and visiting Web sites, he or she never knows who is watching and recording every move. As one author warns, "the perceived danger to privacy lies in the possibility of a website combining cookie data with registration data and then pooling this data with others to compile a detailed profile of user tastes based on online activities."[46]

Further evidence of Americans' concern for maintaining personal privacy in the Internet environment can be found in the following two examples. When Amazon.com decided to post "purchase circles" showing the book-buying habits of users from selected companies and

44. *See* BBBOnLine Privacy Program, Council of Better Business Bureaus, Inc., *at* http://www.bbbonline.org (last visited Feb. 21, 2001).

45. GEORGE ORWELL, 1984 at 6-7 (Penguin Books 1981) (1949).

46. Charles F. Luce, Jr., *Internet Privacy: Spam and Cookies: How to Avoid Indigestion While Binging at the World Wide Automat*, COLO. LAW., Oct. 1998, at 27, 30.

universities, many users viewed this as a breach of privacy without consent and asked not to be included.[47] IBM's Chairman asked his employees for their reaction. After receiving five thousand e-mail responses (ninety percent of which expressed objections to having employee book-buying habits, even as a group, disclosed online), he asked to have IBM removed from the circles.[48]

Some consumers even resort to litigation when they feel that companies have lied to them. A user of the Quicken.com Internet site sued Quicken.com's owner, Intuit, a personal finance software company, alleging that the company disclosed personal information to advertisers. The suit alleged that Intuit failed to disclose to consumers that its Quicken.com site, which allows people to track and pay bills online, "contains a 'secret information-harvesting capacity' that 'works as a window into the Internet user's activities,' providing advertisers with the users' names, addresses, and confidential financial information."[49]

Finally, and perhaps most importantly, Internet commerce stands to decline substantially if the government fails to assure consumers that their personal information will not be subject to abuse. With an estimated 120 million Americans regularly accessing the Internet by February of 2000, and annual Internet consumer sales expected to hit $184 billion in 2004, maintaining consumer confidence in the Internet is vital to the continued strength of the American economy.[50] Surveys reveal that 64% of Americans are unlikely to trust Web sites, 90% want the right to control the use of their personal information after collection, and 50% believe the government should be responsible for regulating Internet privacy.[51] Furthermore, experts say that many of these polls contain a certain amount of bias toward trusting Web sites due to consumers' lack of awareness of the extent of privacy invasions presently taking place.[52] Jeffrey Chester, Executive Director for the Center for Media Education, said, "[i]f the public knew that profiles were being created that included a tremendous amount of data includ-

47. Lohr, *supra* note 37.

48. *See id.*

49. *See* Eric J. Sinrod, *Net Privacy Lost and Found*, UPSIDE TODAY (Mar. 14, 2000), *available at* 2000 WL 4724495; Martin Stone, *Intuit Sued for Alleged Data Disclosure*, NEWSBYTES NEWS NETWORK (Mar. 9, 2000), *available at* 2000 WL 2274379.

50. *See* Debra A. Valentine, Privacy on the Internet: The Evolving Legal Landscape, Address Before Santa Clara University (Feb. 11-12, 2000), *at* www.ftc.gov

51. *See* Miller & Weise, *supra* note 27.

52. *See* Will Rodger, *Poll: Users Wary of Net Ad Targeting*, USATODAY.COM (Nov. 5, 1999), *at* www.usatoday.com

ing psychographic profiles . . . people would have a different response."[53]

B. European Union Directive

The emphasis Americans appear to place on maintaining the privacy of their personal information exists in other countries as well. This emphasis could harm American businesses if the United States government does not respond appropriately. In 1995, the European Union enacted a directive aimed at assuring the privacy of personal information.[54] The European Union Directive has, as one of its provisions, a prohibition on the transfer of data to businesses in countries with insufficient data protection laws.[55] Although the European Union Directive went into effect in 1998, the Council postponed enforcement of the data transfer provision pending the outcome of negotiations with the United States government to resolve this issue. The United State government's proposed solution rested on so-called "safe harbor" principles that would be applicable only to businesses desiring to engage in data transfer with European Union countries.[56] Although a recent European Commission decision officially accepted the terms of one such safe harbor proposal,[57] the European Union has not looked favorably upon safe harbor proposals as a permanent solution.[58]

III
CURRENT STATE OF PRIVACY PROTECTION IN THE UNITED STATES

Throughout history, the law has gradually adapted to meet the changes occurring in the world. With the recent rapid advance of sci-

53. *Id.*
54. Council Directive, *supra* note 7.
55. *See id.* § VII.
56. *See* INT'L TRADE ADMIN., U.S. DEP'T OF COMMERCE, *International Safe Harbor Privacy Principles* (Apr. 19, 1999), *at*
57. *See* Commission Decision 2000/520/EC, 2000 O.J. (L 215) 7. The Commission decision requires that U.S. companies wishing to engage in data transfer with European Community businesses consent to follow the information privacy policies required by the Council Directive. Specifically, the companies must have provisions addressing: notice, choice, onward transfer, security, data integrity, access, and enforcement. *See id.* at 10-12. The decision also recognizes the power of the FTC and the Department of Transportation "to investigate complaints and to obtain relief against unfair or deceptive practices as well as redress for individuals in case of noncompliance with the Principles."*Id.* at 12.
58. *See* Tan, *supra* note 26, at 682-83; *see also* 2000 O.J. (L 215) 7, 9.

ence and technology, however, the law has had great difficulty keeping pace. Constitutional and statutory mechanisms for dealing with privacy issues are ill-equipped to handle the present challenges. As a result, the law has failed to provide society with a means for regulating this progress. Faced with this constantly changing atmosphere, lawmakers have relinquished their power to existing regulatory agencies poorly suited to handle this new responsibility and to the Internet industry itself.

A. Constitutional Privacy Protection

The Constitution's ability to play an integral role in the Internet privacy arena is severely constrained both by the limited nature of its privacy protections and by the fact that what protections do exist only apply to government action.[59] Specifically, the Constitution's privacy protections offer limited assistance in addressing Internet privacy because the Supreme Court's First Amendment jurisprudence does not contemplate information privacy, and the Fourth Amendment's reasonable expectation of privacy doctrine is incapable of properly evaluating privacy infringements enabled by new technology. Furthermore, although many privacy invasions do result from federal or state action, a similarly high number of invasions today are undertaken by private entities—invasions to which the Constitution does not apply.

The United States Supreme Court has determined that the Constitution, through its First and Fourth Amendments, implicitly guarantees certain fundamental privacy rights. The First Amendment right to privacy cases have focused on an individual's right to make certain personal decisions without governmental interference. For example, in *Griswold v. Connecticut*, the Court held that the choice of whether or not to use contraceptives was of such a personal nature that the government could not be permitted to interfere.[60] It is true, however, that "[t]he Supreme Court has not yet held that the right to privacy limits governmental powers relating to the collection of data concerning private individuals."[61] The Fourth Amendment protection against unreasonable search and seizure may involve data protection concepts to a greater degree. In *United States v. Katz*, the Court held that the

59. This is the main premise of the state action doctrine. The application of the state action doctrine in the context of the Fourteenth Amendment is discussed in the Civil Rights Cases, 109 U.S. 3 (1883) (striking down Civil Rights Act of 1875 on ground that Fourteenth Amendment did not empower Congress to regulate behavior of private citizens).

60. *See Griswold*, 381 U.S. at 485-86.

61. 3 RONALD D. ROTUNDA & JOHN E. NOWAK, TREATISE ON CONSTITUTIONAL LAW: SUBSTANCE AND PROCEDURE § 18.30 (3d ed. 1999).

Fourth Amendment protects information that a person subjectively expects to remain private if that belief is one society accepts as reasonable.[62]

This reasonable expectation of privacy test fails to fully protect most personal information, however, because people share the information for varied purposes. In many circumstances, once this information is shared, even if it was originally disclosed for a very limited purpose, the subject can no longer be said to have a reasonable expectation that it will remain private. The recent holding of a federal court in Virginia in *United States v. Hambrick*[63] provides an example of the way courts apply, and will likely continue to apply, the reasonable expectation test to Internet matters. The court held that an Internet user had no reasonable expectation of privacy in the personal account information his OSP revealed to government investigators.[64] The court based its holding on the fact that the information was freely given to the provider to begin with, so it could not be considered inherently private information. Furthermore, since the court found that Congress had not legislatively determined it to be reasonable to rely on an OSP to keep such information private, it declined to do so of its own accord.[65]

One theory that has been advanced to encourage courts to respond to abusive data collection practices with constitutional privacy protection is the "information aggregation theory." This theory was attempted in both *Nader v. General Motors*[66] and *Tureen v. Equifax, Inc.*,[67] and met a different result in each suit. In *Nader*, the court suggested that there could be some basis for finding a privacy violation using a theory of information aggregation. Even if data is made public in small amounts and for specific, limited purposes to companies, privacy may still be violated by the unauthorized aggregation of information from several unrelated sources to be used for purposes unrelated to those for which the data was collected.[68] In *Tureen*, how-

62. *See Katz*, 389 U.S. at 351-52 ("What a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.") (citations omitted).

63. 55 F. Supp. 2d 504 (W.D. Va. 1999).

64. *Id.* at 507-08.

65. *See id.* at 507.

66. 255 N.E.2d 765 (N.Y. 1970).

67. 571 F.2d 411 (8th Cir. 1978); *see also* Sessler, *supra* note 4, at 631-35.

68. *See Nader*, 255 N.E.2d at 772 (Breitel, J., concurring).

ever, a different court failed to find a violation of privacy on the basis of information aggregation principles.[69]

Thus, while the Supreme Court has read implied rights to privacy into the First and Fourth Amendments to the Constitution, these rights offer little comfort to Internet users. The implied privacy rights do not extend to information freely given, even if it is given for a legitimate purpose and later put to unauthorized use. Furthermore, the Constitution can only protect citizens from the government, not from private individuals or entities.

B. Statutory Privacy Protection

In evaluating the current state of privacy legislation, one must first examine the laws Congress has enacted over the years to address privacy concerns. Privacy legislation in the United States presently resembles a patchwork quilt, with Congress addressing specific problems as they arise.[70] Many of the laws were enacted "in response to technological changes that were perceived as threatening an area of individual privacy."[71] Such laws fall far short of providing a comprehensive system of information privacy protection.

One example of Congress's historical tendency to respond to a novel issue only after discovering pertinent abuses can be found in the circumstances of Judge Bork's Supreme Court nomination hearings before Congress. During Judge Bork's testimony, members of Congress questioned him regarding information they possessed describing his video rental patterns. This information had been obtained legally by simply asking his local video store to provide a record (which all similar establishments routinely keep) of his video rentals.[72] As a result of public concern over this event, Congress enacted the Video Privacy Protection Act of 1988.[73]

Current legislation provides at least minimal protection for personal information held by credit reporting agencies, federal agencies, financial institutions, cable providers, and video stores.[74] Unfortunately, there exists no conceptual framework underlying these amorphous regulations. As explained above, each statute is drafted in response to the specific problems Congress chooses to address after

69. *See Tureen*, 571 F.2d at 416.
70. *See* Tan, *supra* note 26, at 671.
71. PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 5 (1995).
72. *See* Sessler, *supra* note 4, at 663.
73. 18 U.S.C. § 2710 (1994).
74. *See* REGAN, *supra* note 71, at 6.

these problems have had a large and noticeable public impact. Congress's piecemeal privacy legislation addressing data protection has included such acts as the Electronic Communications Privacy Act,[75] the Tax Reform Act,[76] the Freedom of Information Act,[77] the Right to Financial Privacy Act,[78] the Fair Credit Reporting Act,[79] the Cable Communications Privacy Act,[80] the Telephone Consumer Protection Act,[81] and the Federal Records Act.[82]

Of the above, the statute that appears to be the most comprehensive in protecting privacy rights on the Internet is the Electronic Communications Privacy Act (ECPA). Though still a prime example of the sectoral approach to privacy legislation in the United States, the ECPA significantly affects Internet privacy in that it currently forbids providers of Internet service from revealing the contents of electronic communications. Unfortunately, as one critical scholar has noted:

> Although this may seem to bar communication providers from peddling personal information in the marketplace, such privacy protections are illusory. The . . . bar applies solely to the contents of communications, not to transactional records, which may be freely disclosed to anyone "other than a governmental entity."
>
> Unfortunately, the line is not bright between the contents of a communication and the transactional data about that communication. . . . The legislative history adds little light, except to make clear that "contents" do not include "the identity of the parties or the existence of the communication."[83]

Therefore, the threats posed by cookies and click stream data remain unaffected.

C. Regulatory Agencies' Role in Privacy Protection

Congress has attempted to fill part of the void left by its failure to enact appropriate legislation by delegating the responsibility to the Federal Trade Commission (FTC). Unfortunately, the FTC was not created for such a task and does not have the expertise or authority to effectively monitor or enforce privacy issues on the Internet. Further-

75. 18 U.S.C. §§ 2510–2521, 2701–2711 (1994 & Supp. IV 1999).
76. 26 U.S.C. § 6103 (1994 & Supp. IV 1999).
77. 5 U.S.C. § 552 (1994).
78. 12 U.S.C. §§ 3401–3422 (1994).
79. 15 U.S.C. § 1681a (1994 & Supp. IV).
80. 47 U.S.C. § 551 (1994).
81. 47 U.S.C. § 227 (Supp. IV 1994).
82. 44 U.S.C. §§ 2101–2118 (1994).
83. Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1234-35 (1998).

more, the FTC has many other duties and is thus unable to commit sufficient resources to the protection of individuals' privacy on the Internet.[84]

It is worth noting, however, the FTC's effective role, albeit limited, in the Internet privacy arena. The FTC experienced some success in dealing with Internet regulation in the GeoCities matter.[85] In 1998, the FTC brought action against GeoCities, a popular Internet portal, for violating express promises made to users in its voluntarily adopted privacy policy. In a 1998 consent order, GeoCities agreed to several conditions, including the following: GeoCities will not misrepresent the purposes for which it collects personal identifying information; GeoCities will post a privacy notice on its Web site; and GeoCities will notify members of what information it currently has and allow them to delete their personal information from all databases.[86] Unfortunately, it took a great amount of express fraud and misbehavior for the FTC to justify its involvement in the GeoCities matter—an approach that leaves no protection for many privacy concerns. Furthermore, since GeoCities' privacy policy stated that private information would not be released to third parties, GeoCities itself could have easily avoided a confrontation with the FTC if it had merely posted no privacy policy at all.

Congress has also given the FTC the secondary duty of reporting annually on the state of Internet privacy and recommending to Congress what action to take. In its 1998 report, the Federal Trade Commission recommended that Congress pursue legislation to protect the privacy of children online,[87] and presented a four-part legislative model[88] "that Congress could consider in the event that then-nascent self-regulatory efforts did not result in widespread implementation of

84. *See* Jonathan P. Cody, *Protecting Privacy Over the Internet: Has the Time Come to Abandon Self-Regulation?*, 48 CATH. U. L. REV. 1183, 1228 (1999).

85. *See* Valentine, *supra* note 50 (describing first online privacy case where "the Commission was concerned that GeoCities, one of the Web's most frequently visited sites, collected personal identifying information from its members, both adults and children, and misled them as to its use of that information").

86. *See id.*

87. *See* MARTHA K. LANDENSBERG ET AL., FEDERAL TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS 4-6 (1998), *at* http://www.ftc.gov

88. *See Privacy in Cyberspace: Hearings Before the Subcomm. on Telecommunications, Trade, and Consumer Protection of the House Comm. on Commerce*, 106th Cong. 308-09 (1998) (prepared statement of Hon. Robert Pitofsky, Chairman, the Federal Trade Comm'n), *microformed on* CIS No. 99-H271-12, *available at* http://www.ftc.gov

self-regulatory protections."[89] The model presented in 1998 would have "require[d] operators to: 1) provide notice to consumers on how their personal information is used; 2) give consumers a choice about whether and how their information is used; 3) provide security for personal information collected; and 4) allow consumers access to their own information to promote accuracy."[90] The 1999 Report, however, took the opposite stance, recommending no legislation and instead suggesting continued reliance on industry self-regulation.[91]

In formulating its 1999 Report, the FTC relied on studies revealing that, although 93% of surveyed Web sites collected personal information from customers, 66% made some form of disclosure about the Web site's information practices.[92] Based on this data, the FTC concluded that, unlike in 1998, when effective self-regulation had not yet taken hold, "[i]n the ensuing year there have been important developments both in the growth of the Internet as a commercial marketplace and in consumers' and industry's responses to the privacy issues posed by the online collection of personal information."[93]

Unfortunately, while it may be true that 66% of Web sites provided *some* notice regarding their use of personal information, few sites provided users with the protections envisioned by a true system of information privacy protection.[94] The FTC, in choosing a self-regulatory model that required only some notice, lowered the standards to a point that makes it difficult to believe that any Web site surveyed did not comply. These findings may not suggest better industry self-regulation; they may merely suggest that the FTC is using more lenient testing requirements and is choosing to put its confidence in industry rather than the legislature.

The FTC conducted another survey of Web sites in February and March of 2000.[95] Recognizing "that online privacy continues to pre-

89. *See* MARTHA K. LANDESBERG & LAURA MAZZARELLA, FEDERAL TRADE COMM'N, SELF-REGULATION AND PRIVACY ONLINE: A REPORT TO CONGRESS 15 n.4 (1999), [hereinafter 1999 REPORT].

90. Hunter, *supra* note 12, at 20.

91. 1999 REPORT, *supra* note 89, at 12 ("[T]he Commission believes that legislation to address online privacy is not appropriate at this time.").

92. *See id.* at 7.

93. *Id.* at 1.

94. FTC Commissioner Sheila F. Anthony was "dismayed [that] . . . only 10 to 20 percent of [the surveyed] sites have privacy disclosures implementing the four basic substantive fair information practices."*Id.* at 22; *see also supra* text accompanying note 90.

95. *See* FEDERAL TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE: A REPORT TO CONGRESS (2000), [hereinafter 2000 REPORT].

sent an enormous public policy challenge" and that the 2000 survey demonstrated "that industry efforts alone have not been sufficient," the 2000 Report recommends that Congress enact legislation setting forth "a basic level of privacy protection for consumer-oriented commercial Web sites."[96] Specifically, the FTC recommends that this legislation require Web sites to comply with the widely accepted fair information practice principles of notice, choice, access, and security.[97] While Congress has yet to act definitively upon the FTC's recommendations, the 2000 Report does signal a step in the right direction.

D. Industry Self-Regulation

For lack of a better approach and due to strong industry pressure, the federal government's policy toward the Internet privacy issue over the last several years has been to allow the industry to self-regulate.[98] This hands-off approach is due in part to a fear that imposing formal regulation on Internet companies will stifle their potential for economic success. While some studies recently determined that self-regulation presents a viable option for dealing with Internet privacy concerns, the methodology employed in reaching this conclusion allowed companies substantial leeway in defining "privacy policy."[99] Therefore, though this method appears to have achieved some degree of success over the past few years, many sites remain without any privacy policy at all, and the majority of those that have policies provide only a fraction of the protection recommended by fair information practices.[100] Furthermore, of the sites that do have policies, many are accessible only if the user notices tiny print hidden at the bottom of the Web page. Since many consumers feel that they need only concern themselves with a site's privacy policy if they are making a purchase and revealing such information as a credit card number, most users do not notice or read the privacy policies of the majority of the sites they visit.[101]

---

96. *Id*. at ii, iii.
97. *See id*. at iii.
98. *See Electronic Communication Privacy Policy Disclosure: Hearing Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary*, 106th Cong. 37 (1999) (prepared statement of Marc Rotenberg, Director, Electronic Privacy Information Center), *microformed on* CIS No. 00-H-521-85, *available at* 570 PLI/Pat 1093.
99. *See id.* at 41.
100. *See* 1999 REPORT, *supra* note 89, at 7.
101. Ben Hammer, *A Surprise in Every Package*, THESTANDARD.COM (Mar. 6, 2000) (describing seldom read privacy policies of major Web sites including

The only step in the right direction has been the fairly recent emergence of a few independent organizations offering privacy certification or "seal" programs for Web sites. For example, the Better Business Bureau's Privacy Program "features verification, monitoring and review, consumer dispute resolution, a compliance seal, enforcement mechanisms and an educational component."[102] The problem, however, with optional seal programs such as BBB*Online*[103] and Truste[104] is that each Internet company has complete discretion regarding the decision to enlist in a privacy program. Furthermore, although the programs claim to have enforcement mechanisms, the most they can do is remove a company from the program, publicize the company's violation, or refer the company to government enforcement agencies such as the FTC.[105] Most of these programs intend to address information explicitly gathered by companies when users, for example, order products, enter contests, register for services, or join mailing lists, and do not address the situation of Web sites' servers surreptitiously sending cookies.[106] Thus, while these programs offer some security to Internet users, it is far from the sort that could be assured by comprehensive federal legislation.

DoubleClick, iVillage, Microsoft, and BarnesandNoble.com), *at*

102. COUNCIL OF BETTER BUSINESS BUREAUS, INC., *About the Privacy Program*, BBBONLINE, *at* http://www.bbbonline.org (last visited Feb. 24, 2001). BBBOnLine has also issued a "Code of Online Business Practices" that includes, as one of its tenets, adherence to a privacy policy respectful of information practices. BBBOnLine recommends a privacy policy that includes the following:

> Online advertisers should post and adhere to a privacy policy that is open, transparent, and meets generally accepted fair information principles including providing notice as to what personal information the online advertiser collects, uses, and discloses; what choices customers have with regard to the business' collection, use and, disclosure of that information; what access customers have to the information; what security measures are taken to protect the information, and what enforcement and redress mechanisms are in place to remedy any violations of the policy. The privacy policy should be easy to find and understand and be available prior to or at the time the customer provides any personally identifiable information.

COUNCIL OF BETTER BUSINESS BUREAUS, INC., BBBONLINE, CODE OF ONLINE BUSINESS PRACTICES 13, *at* http://www.bbbonline.org (last visited Feb. 24, 2001).

103. BBBOnLine, *at* http://www.bbbonline.org (last visited Feb. 24, 2001).

104. TRUSTe, *at* (last visited Feb. 24, 2001).

105. *See* COUNCIL OF BETTER BUSINESS BUREAUS, INC., *How the BBBOnLine Privacy Program Works*, BBBONLINE, *at* http://www.bbonline.org (last visited Feb. 24, 2001).

106. COUNCIL OF BETTER BUSINESS BUREAUS, INC., BBBONLINE, CODE OF ONLINE BUSINESS PRACTICES 13, *at* http://www.bbbonline.org (last visited Feb. 24, 2001).

IV
PROPOSED SOLUTIONS

A. A Revised Reasonable Expectation of Privacy Test

With respect to the limited role for Constitutional protection in the area of Internet privacy, a minor alteration of the reasonable expectation of privacy test could aid its ability to deal with rapid technological change. One notable scholar has commented:

> The "reasonable expectation" test has proven particularly troublesome in the information privacy context. The Court has continually held that individuals have no privacy interest in information divulged to the private sector, even though modern society leaves citizens no option but to disclose to others, where, for example, disclosure is a condition of participation in society.[107]

The paradox of the Internet is that in order to continue to harness its full potential, users must forfeit additional layers of privacy. Paul Schwartz expressed a similar sentiment in a 1995 law review article in which he wrote that technology has the "silent ability . . . to erode our expectation of privacy."[108] For this reason, the traditional reasonable expectation of privacy standard in *Katz* no longer provides an acceptable mechanism for determining when a privacy violation has occurred.

The law views the Internet as a public domain, and under traditional common law principles, what one exposes to public view cannot be considered private. While it is true that the Internet is, in some respects, public, it is not at all clear that individual users believe that their Internet activity is exposed to public view. In fact, many of the new Internet shopping sites rely on their customers' desire for privacy in their Internet transactions.[109] The rapid technological development occurring all over the world requires that we adopt a new test; a test measuring not current expectations, but the expectations a reasonable person would have about the privacy protections of any new technology prior to the development of that technology. A forward-looking method for determining privacy protections for all future innovations would enable society's expectations to define technology rather than allowing technology to define these expectations.

---

107. Goldman, *supra* note 12, at 105.

108. Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 573 (1995).

109. *See, e.g.*, Shopinprivate.com, *at* http://www.shopinprivate.com (last visited Feb. 24, 2001) (offering variety of personal products such as pregnancy testing kits, contraceptives, and feminine hygiene products that many people would be embarrassed to be seen purchasing at regular stores).

B. A Statutory Scheme Incorporating Fair Information Practices

Since the proposed alterations to the reasonable expectation of privacy test would only have an effect on privacy invasions by federal or state government officials, more is required to protect Internet users' privacy in the modern world. To address potential privacy invasions by private entities, a comprehensive and appropriate statutory scheme must be put in place. Furthermore, effective methods for enforcing such a scheme must be developed.

While it is true that Congress has primarily looked to industry self-regulation to address concerns with Internet privacy,[110] recent events have called into question the strength of Congress's reliance on this remedy. Specifically, Congress recently formed at least one new committee charged with examining Internet privacy issues. The Congressional Privacy Caucus is a bi-partisan group planning to "study online privacy-related issues and introduce legislation if it is needed."[111] Furthermore, several bills have been proposed in both the House of Representatives and the Senate to address specific areas of Internet privacy.

Congressman Green from Texas recently introduced the Consumer Online Privacy and Disclosure Act that, if enacted, would require the FTC "to prescribe regulations to protect the privacy of personal information collected from and about individuals on the Internet, [and] to provide greater individual control over the collection and use of that information."[112] While this bill succeeds in addressing the protection of transaction-generated information and provides mechanisms for enforcement, it fails to incorporate all aspects of fair information practices[113] and only applies to data containing personal information.[114] Furthermore, this bill provides incomplete protection in calling for regulations requiring consumers to opt out of having their information disclosed "for purposes unrelated to those for which such information was obtained or described in the notice," rather than allowing consumers to opt in.[115] Senator Torricelli from New Jersey

---

110. *See supra* Part III.D.

111. *See* Michele Masterson, *Privacy Fuels Gov't Efforts: Growing Internet Privacy Concerns Spur Politicians to Introduce New Legislation* (Mar. 9, 2000),

112. H.R. 5430, 106th Cong. pmbl. (2000).

113. *See id*. For example, the bill makes no provision for consumer access to information. *See id*.

114. *See id*. (defining "Personal information"as including "(A) first and last name;

(B) home and other physical address; (C) e-mail address; (D) social security number; (E) telephone number").

115. *Id.* § 2(b)(1)(A)(ii).

has proposed legislation addressing Internet privacy with an opt-in requirement.[116] The Torricelli bill, however, has been criticized by those who say that "targeting cookies may be the wrong way to go about protecting privacy."[117] The Torricelli bill, like the other proposals, does not provide comprehensive privacy protection but rather represents merely another patch on the privacy quilt.

Congress's patchwork of legislation on the issue of privacy results, in part, from the fact that its only true Constitutional authority for such legislation derives from the Interstate Commerce Clause.[118] Thus, Congress must ground each piece of legislation in principles of interstate commerce. For example, the Fair Credit Reporting Act[119] is within Congress's authority given that credit reporting companies in the United States today conduct almost all of their business across state lines. Similarly, cable providers are subject to federal legislation[120] because the television industry is inextricably bound up in interstate commerce.

The fact that the Internet is comprised of a network of data routes through many states[121] makes it an appropriate area for federal legislation. Almost every data transfer or collection that occurs today implicates interstate commerce. In fact, it would be almost impossible to imagine a situation in which personal data would be acquired and transmitted to third parties without some effect on interstate commerce. This does not mean that a legislative remedy will be any less of a patch than all other privacy legislation. It is true, however, that with a little care and thought, Congress could adopt a broader, comprehensive data protection scheme without exceeding the bounds of its authority. Therefore, if Congress were to examine and embrace data protection principles such as those used by the European Union in its Directive, it could achieve a vastly more comprehensive system of privacy protection than that which is currently in place.

Data protection laws, as they exist in other countries, are based on the idea that people maintain an interest in their personal informa-

116. Secure Online Communication Enforcement Act of 2000, S. 2063, 106th Cong. (2000).

117. *See* Patricia Jacobus, *"Cookies"Targeted as Congress, Advocates Address Net Privacy*, CNET.COM (Feb. 11, 2000), *at* https://www.cnet.com/tech/services-and-software/cookies-targeted-as-congress-advocates-address-net-privacy/

118. *See* U.S. CONST. art. I, § 8, cl. 3 (stating that "Congress shall have Power . . . [t]o regulate Commerce . . . among the several states").

119. 15 U.S.C. § 1681 (1994 & Supp. IV).

120. *See* 47 U.S.C. § 551 (1994 & Supp. IV).

121. *See* Nuara, *supra* note 5, at 9-10.

tion even after they have revealed it to a company.[122] Just because people reveal certain personal information to a company or organization for a particular purpose, that does not mean that the company can take that information and use it beyond the purpose for which the information was originally collected. People should be able to govern how their information is used, or at least be informed clearly of how the organization intends to use their information, as well as whether, and under what circumstances, that information will be revealed to third parties. If we, as a society, wish to continue to advance in the technological revolution, we must allay people's fears about the Internet.

Protecting privacy on the Internet requires developing a comprehensive scheme to address information privacy in all sectors. Information privacy consists of the following two components: 1) the right to "shield ourselves . . . from the prying eyes of others" and 2) "the right to control information about oneself, even after divulging it to others."[123] The tools of fair information practices effectively address both concerns and must be adequately implemented in American privacy legislation if the loss of this crucial aspect of personal privacy is to be averted.

The privacy paradigm of fair information practices includes the following tenets: 1) people should be aware of records that are kept; secret gathering or storing of information is unacceptable;[124] 2) people should be able to access and revise their personal information;[125] 3) information gatherers should be limited in their ability to collect personal information (collection should be relevant to uses and records should be correct);[126] 4) the use of the information both by the record keepers themselves and by third parties should be limited;[127] 5) disclosure of personal information should be limited to those instances in which consent has been secured;[128] 6) provisions should be made to ensure the security of personal information;[129] and 7) record keepers should be held accountable for failure to comply with these aforementioned principles.[130]

---

122. *See* Robert Gellman, *Does Privacy Law Work?*, *in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 193, 196-98 (Philip E. Agre & Marc Rotenberg eds., 1997).
123. Goldman, *supra* note 12, at 101.
124. *See* Gellman, *supra* note 122, at 196.
125. *See id*. at 197.
126. *See id*. at 197-98.
127. *See id*. at 197.
128. *See id*. at 198.
129. *See id*. at 200.
130. *See id*.

Legislation incorporating all the above principles will not, as some argue, interfere with Internet commerce. Rather, by engendering the confidence of Internet consumers, such a law would aid in maintaining the current rate of expansion of Internet commerce in the United States. People are becoming increasingly conscious of the issue of Internet privacy and, as awareness increases, commerce will decrease if serious action to remedy the present problem is not taken.

C. European Union Directive

The European Union Directive incorporates all of the principles of fair information practices outlined above and provides an ideal model for any country struggling to develop a system of comprehensive privacy legislation.[131] The European Union Directive requires the following regarding personal data: 1) that it be processed fairly and lawfully; 2) that it be collected and processed only in a manner compatible with a legitimate purpose; 3) that it be not excessively collected for irrelevant purposes; 4) that it be kept accurate and current; and 5) that it be kept only so long as necessary to fulfill the legitimate purpose for which they were collected.[132] Furthermore, the Directive allows for processing of personal data only where the following circumstances exist: 1) the subject has consented; 2) it is necessary for performance of a contract to which the subject is a party; 3) it is necessary for compliance with a legal obligation; 4) it is necessary to protect the vital interests of the data subject; 5) it is necessary to protect the public interest or is carried out according to official authority; and 6) it is necessary for legitimate interests.[133] Data subjects are also to be given the right to access and correct any misinformation, as well as the right to object to the processing of information pertaining to them.[134] Companies processing personal data must have adequate security systems to prevent the unauthorized accessing or altering of information by third parties.[135] Additionally, as discussed above, the Directive also contains a prohibition on transferring data to entities in countries whose laws do not provide adequate protection for personal data, except under certain circumstances.[136]

Instead of continuing to negotiate with the European Union over safe harbor principles to avoid being shut out of data transfers, the

131. *See generally* Council Directive, *supra* note 7.
132. *See id.* § I.
133. *See id.* § II.
134. *See id.* §§ V–VI.
135. *See id.* § VII, art. 17.
136. *See id.* ch. IV, art. 25.

United States should seek the European Union's aid and assistance in developing our own system of national data protection legislation. If we have this vision, it will transform our patchwork system of responding to specific issues into a jurisprudence capable of dealing with new issues as technology expands and develops.

D. Practical Considerations

The road to achieving a proper system of privacy protection in the United States will not be an easy one, but with guidance from successful countries and a focus on meeting users' needs, we will someday achieve this goal. In the meantime, Americans should strive to better inform themselves about what Internet companies are doing with their personal data and exercise their right not to use Web sites that violate their privacy. Consumers can choose to sign up with an OSP that promises to keep personal information private and secure to avoid the dissemination of click stream data. Furthermore, Internet users can configure their browsers to warn them when Web sites attempt to send cookies, can refuse to accept these cookies when sent, and can delete existing cookies from their hard drives.

CONCLUSION

Internet users in the United States presently face a very serious threat to their personal privacy. Cookies, banner ads, and click stream data collect personal information from Internet users without their knowledge or consent, and those in possession of this information face no obstacles to using it for inappropriate purposes. This information may be sold to third parties in its raw form or used to create profiles based on a person's Internet usage. We are not far from a time when companies will be able to connect a particular person with his or her profile, thus allowing unimaginable abuses of personal privacy.

Internet commerce, a driving force in our economy over the last several years, could be threatened if privacy protection is not assured. While most Americans are unaware of the extent to which such events occur, or even that they occur at all, many still express a strong desire to maintain their privacy while surfing the Internet. Furthermore, the European Union Directive threatens to put an end to all data transfers between European Union countries and the United States if the current state of affairs persists.

Constitutional interpretations have yet to adequately address information privacy. Existing privacy legislation provides remedial measures in a piecemeal manner covering some sectors but not others.

Since the Internet is so new, no existing legislation effectively protects Internet users from the dangers inherent in cookies and the collection of click stream data. Furthermore, the two approaches Congress has relied upon, regulation by the FTC and industry self-regulation, are ill-suited to deal effectively with the Internet privacy problem.

To protect Internet users' privacy and maintain consumer confidence, the Supreme Court should alter its interpretation of constitutional privacy, and Congress should enact comprehensive data protection legislation. The reasonable expectation of privacy test should be reinterpreted so that it anticipates the threats to consumers from new technology. Furthermore, a comprehensive system of data protection legislation based on the principles of fair information practices and modeled on the European Union Directive will engender consumer confidence in the economy, thereby enabling the legal system to stay one step ahead of newly developed technology rather than two steps behind.