Hastings Communications and Entertainment Law Journal

Volume 21 | Number 3 Article 3

1-1-1999

The New Wave of Speech and Privacy Developments in Cyberspace

Eric J. Sinrod

Jeffrey W. Reyna

Barak D. Jolish

The New Wave of Speech and Privacy Developments in Cyberspace

by
ERIC J. SINROD*

JEFFREY W. REYNA**

BARAK D. JOLISH***

* Eric J. Sinrod, a partner in the San Francisco office of Hancock Rothert & Bunshoft LLP, practices commercial litigation and Internet, information and communications law, and can be reached at ejsinrod@hrblaw.com or eric@sinrodlaw.com.

** Jeffrey W. Reyna, an associate in the San Francisco office of Hancock Rothert & Bunshoft LLP, practices commercial litigation and Internet law, and can be reached at jwreyna@hrblaw.com.

*** Barak D. Jolish is a third-year student at the University of California Hastings College of the Law and will be joining Hancock Rothert & Bunshoft LLP as an associate in 1999. He can be reached at jolishb@uchastings.edu.

Introduction

The Internet offers myriad new avenues for human interaction that are as varied as the people who are online. The number of creative uses for the Internet has grown as the number of people on the Internet increases exponentially.[1] But, for all the people currently found online, there are many who still view the Internet with a wary eye. Concerns over personal privacy and government censorship are often at the forefront of many Internet users' minds.[2] As with any other medium of information, the Internet has the potential to be used as a tool for businesses, individuals, and government to peer into people's personal lives. Conversely, many are concerned that the Internet can also be used to deliver objectionable or obscene information to minors. These concerns fuel the ongoing debate over whether and how to regulate the Internet to protect the privacy and speech concerns implicated by its many uses.

The last half of 1998 and beginning of 1999 saw some important developments in the area of Internet regulation by government and the private sector. Much of the legislative

---

1. A 1998 survey by Network Wizards shows that the number of hosts tabulated in the Internet Domain Name System grew from roughly 25,000,000 in mid-1997 to nearly 37,000,000 by July of 1998. *See* Network Wizards, *Internet Domain Survey*, July 1998 (visited Feb. 9, 1999) <http://www.nw.com/zone/www/report/html>. With some variation, one host = one computer connected to the Internet. In recent years however, "virtual hosting" has necessitated the modification of this definition, since one computer can, in turn, have multiple domain names and IP addresses. *See* Network Wizards, *Internet Domain Survey* FAQ (visited Feb. 9, 1999) <http://www.nw.com/zone/WWW/faq.html>. "An IP address is a set of four numbers (each between 0 and 255, with some restrictions) separated by periods that uniquely identify that address on the Internet." *See* Matthew Grey, *Web Sites, Hostnames and IP Addresses, Oh my.* (visited Feb. 5, 1999) <http://www.mit.edu/people/mkgray/net/terminology.html>.

These figures only count the number of computers connected to the Internet. An estimate of the number of people using the Internet is more difficult to come by. According to one estimate, 108 million adults in the U.S. alone used the Internet during the last three months of 1998. *See* Cyberatlas, *Web Hits Growth Spurt in Q4*, (visited Feb. 9, 1999) <http://www.cyberatlas.com/big_picture/demographics/q4.html>.

2. *See* Graphic, Visualization & Usability Center (GVU), *8th WWW User Survey*, Dec. 12, 1997, <http://www.gvu.gatech.edu.user_surveys/survey-1997_10>; *A Little Net Privacy, Please*, BUSINESS WEEK ONLINE, Mar. 16, 1998 <http://www.businessweek.com/199811/ b3569104.htm>.

activity related to the Internet has focused on protecting children from exposure to objectionable material and preventing unwanted invasions into children's online privacy. At the same time, Congress, the courts, the European Community, and a coalition of Internet industry members, took several decisive steps – usually in different directions – in an effort to focus the ever-changing policy implications related to privacy and speech on the Internet. The aim of this article is to provide a brief overview of these recent developments as they fit into the ongoing policy debate on speech and privacy issues on the Internet.

I
Blocking Access To Content And Filling Bandwidth With Spam

A. Blocking Content

While many individuals have expressed a desire to keep the Internet an open marketplace of ideas subject to minimal censorship by the government,[3] they also advocate strong protections for children to shield them from exposure to objectionable material. The initial salvo in Congressional efforts to protect children from exposure to pornographic or sexually explicit material on the Internet was the Communications Decency Act (CDA).[4] The CDA sought to outlaw the transmission of "indecent" and other sexually explicit material to children over computer networks.[5] The Act further defined indecent as that which is "patently offensive" by "contemporary community standards."[6] In a 7-2 decision, the Supreme Court in *Reno v. ACLU* (*Reno I*)[7] struck down the

3. *See, e.g., Credit Card Security Greatest Internet-Related Concern Concludes Lycos Web User Study*, Cyber Dialogue (March 5, 1998) <http://www.cyberdialogue.com/index_4.html>.

4. The Communications Decency Act, 47 U.S.C. § 223(a), (d) (1996), was signed into law by President Clinton as part of omnibus legislation that addressed the entire landscape of American communications law. *See* The Telecommunications Act of 1996, Pub. L. 104-104, 110 Stat. 56.

5. *See id.*

6. *Id.*

7. 521 U.S. 844 (1997).

Act's "indecency" provisions on the ground that they violated the First Amendment's guarantee of freedom of speech.[8]

After the *Reno I* decision, Congress returned to the drawing board and renewed its efforts to regulate Internet content by enacting the Child Online Protection Act (COPA)[9] (or "CDA II" as it is called by its opponents). COPA attached criminal and civil liability for the distribution "in interstate or foreign commerce by means of the World Wide Web . . . any communication for commercial purposes that is available to any minor and that includes any material that is harmful to minors."[10] The Act provided that a person would be considered to make a "communication for commercial purposes" "only if such person is engaged in the business of making such communication."[11] The Act further stated that a person was deemed to "engage in the business" if that person "devotes time, attention, or labor to such activities, as a regular course of such person's trade or business, with the objective of earning a profit," irrespective of whether a profit was actually made.[12] The Act than defines material that is "harmful to minors" as

> any communication, picture, image, graphic image file, article, recording, writing, or other matter of any kind that is obscene or that–
>
> (A) the average person, applying contemporary community standards, would find, taking the material as a whole and with respect to minors, is designed to appeal to, or is designed to pander to, the prurient interest;

8. *See id.* While the scope of the *Reno I* opinion has been discussed at length in other fora, a brief summary is useful here. Specifically, the Court held that material published over the Internet deserves the same high level of constitutional protection as books or magazines, as opposed to the lower level afforded to broadcast media. *See id.* at 895-97. The Court went on to state that the Internet is "the most participatory for of mass speech yet developed," and is entitled to "the highest protection from governmental intrusion." *Id.* at 892. From this perspective, the Court viewed the CDA as a content-based blanket restriction on speech that did not to provide any definition of "indecent" and omitted any requirement that "patently offensive" material lack socially redeeming value. *See id.* at 898-99. The Court also expressed concern that the decentralized nature of the Internet made it particularly difficult to apply the "community standards" test of obscenity law. *See id.*

9. 47 U.S.C. § 231 (1998).

10. *Id.* at § 231(1).

11. *Id.* at § 231(e)(2)(A).

12. *Id.* at § 231(e)(2)(B).

> (B) depicts, describes, or represents, in a manner patently offensive with respect to minors, an actual or simulated sexual act or sexual contact, an actual or simulated normal or perverted sexual act, or a lewd exhibition of the genitals or post-pubescent female breast; and
>
> (C) taken as a whole, lacks serious literary, artistic, political, or scientific value for minors.[13]

Finally, the Act provided an affirmative defense for those individuals who, in good faith, restricted access to minors through the use of a credit card, adult access card, a digital certificate that verifies a user's age, or "any other reasonable measures that are feasible under available technology."[14]

Privacy groups, including the ACLU and the Electronic Privacy Information Center (EPIC), filed suit in the U.S. District Court for the Eastern District of Pennsylvania, challenging COPA on constitutional grounds.[15] We will refer to this case as *Reno II* for purposes of this discussion.[16] On February 1, 1999, the court issued a 50-page Memorandum and Order granting plaintiffs' motion for a preliminary injunction, effectively barring enforcement of the Act until the resolution of the case, either by appeal or by a trial on the merits. Though this Memorandum is not binding precedent and is subject to appellate review or modification in further trial proceedings, it is worth discussion as yet another step towards defining the constitutional parameters of regulation of Internet speech by the government.

In granting plaintiffs' request for a preliminary injunction, the court in *Reno II* focused its analysis on plaintiffs' claim that COPA was unconstitutional on its face as a violation of the First Amendment rights of adults. The court

---

13. *Id.* at § 231(e)(6).

14. *Id.* at § 231(c). Age verification on adult web sites was also promoted by the drafters of the Internet Tax Freedom Act. The Act used age verification as an incentive by subjecting Web sites to potential Internet taxation if they do not adequately block access to adult content by minors through the use of age verification programs. *See* Internet Tax Freedom Act, Pub. L. No. 105-277, 112 Stat. 2681 (1998) § 1101(2) *et seq.* The Act was passed as part of the 1998 Omnibus Consolidated Appropriations Bill.

15. *See* American Civil Liberties Union v. Janet Reno, No. 98-5591 (E.D. Pa. 1998), *available at* <http://www.paed.uscourts.gov/opinions/99D0078P.html>.

16. For a sampling of the reaction to the COPA injunction, see Declan McCullagh, *Judge: COPA Went Too Far*, WIRED NEWS, Feb. 2, 1999 <http://www.wired.com/news/news/politics/story/17670.html>; *Trial Possible on Web Porn Law*, CNN INTERACTIVE, Feb. 2, 1999 <http://www.cnn.com/US/9902102/internet.decency>.

stated that "[a]s a content-based regulation of [nonobscene sexual expression], COPA is presumptively invalid and is subject to strict scrutiny. . . ."[17] According to the court, the content of such protected speech could be regulated only if such regulation is narrowly tailored as the least restrictive means to further a compelling government interest.[18] The court proceeded to analyze whether COPA survived strict scrutiny by considering: the burden on speech it imposes, whether COPA furthers a compelling government interest, and whether COPA was narrowly tailored and the least restrictive means to achieve its goals.

The court concluded that COPA imposed a burden on speech for several reasons. The court used the discussion in *Reno I*[19] regarding the prohibitively high economic burden of implementing age verification systems, as one factor in the analysis of the burden COPA imposes on speech. However, the court held that, though the economic burden imposed on Web site operators who would incur out-of-pocket expense to comply with COPA's age verification provisions or lose revenue through decreased web site traffic was certainly real, other factors weighed in favor of a finding that COPA imposed an unconstitutional burden on speech. Specifically, the court found that operators may self-censor the content of their Web sites based on the economic disincentives that COPA presented. The court also found that there is

> no way to restrict the access of minors to harmful materials in chat rooms and discussion groups, which the plaintiffs assert draw traffic to their sites, without screening all users before accessing any content, even that which is not harmful to minors, or editing all content before it is posted to exclude material that is harmful to minors . . . . This has the effect of burdening speech in these fora that is not covered by the statute.[20]

17. *Reno II* (citing Sable Communications of California, Inc. v. FCC, 492 U.S. 115, 126 (1989) and R.A.V. v. City of St. Paul, 505 U.S. 377, 381 (1992)).

18. *See id.* (*citing Sable*, 492 U.S. at 126, which states that "[i]t is not enough to show that the Government's ends are compelling; the means must be carefully tailored to achieve those ends.").

19. *See Reno I*, 117 S. Ct. at 2347.

20. *Reno II*, at Part VI.A.2.

As a result, the court found that plaintiffs were likely to prove that COPA imposed a burden on speech that was otherwise protected for adults.[21]

Next, while the court found that Congress has a compelling government interest in protecting minors from harmful materials, including material that may not be considered obscene by adult standards, it found that COPA failed to use the "least restrictive means" to achieve its goal.[22] The court pointed out that even with COPA in effect, minors might be able to access harmful material on foreign Web sites, non-commercial sites, and commercial American sites that use protocols apart from http, such as ftp.[23] Moreover, the court found there was some evidence presented that Internet "filtering software" could be used as an alternate, and less restrictive means, for protecting minors from exposure to obscene material on the Internet.[24]

The decision in *Reno II* marks the second time in as many years that courts have struck down federal content-based restrictions on speech – both instances dealing with material deemed to be offensive and harmful to minors. This decision reaffirms the implication that any regulation affecting speech on the Internet, particularly any content-based prohibition on speech, must be narrowly tailored and use the least restrictive means in achieving its purpose.

B. Stopping Spammers

"Spam," also known as junk e-mail or unsolicited commercial e-mail, is an often unwelcome mass mailing to electronic bulletin boards, newsgroups, or lists of e-mail addresses harvested through a variety of means.[25] The vast

21. *See id.*

22. *See id*; *see also Reno I*, S. Ct. at 2349.

23. "Ftp" stands for "file transfer protocol," and describes a way of accessing information from the Internet by downloading files from indexes, rather than loading a Web page, which is in turn normally written in the computer language "html." For a more detailed description of these and other Internet-related terms, *see* <http://www.cnet.com/Resources/Info/Glossary/Terms>.

24. *Reno II* at Part IV.A.4. Interestingly, some in the Internet industry do not favor the alternative of using filtering software because such software has the potential to block access to a wider range of content than that prohibited by COPA. *See* Neil Munro, *The Web's Cornucopia*, THE NATIONAL LAW JOURNAL, Jan. 9, 1999, at 38.

25. *See CNET Glossary*, CNET.COM (visited June 26, 1998).

majority of spam messages are used as a form of advertising products and services ranging from "get rich quick" schemes, to phone sex lines and adult web sites, to quack health products.[26] Despite its analogy to conventional junk mail, spam differs from junk mail in fundamental ways. First, mailers of conventional junk mail have to bear the cost of paper, printing and postage, whereas spammers bear negligible costs. The costs of spam are instead borne by the ISP, or Internet Service Provider, which has to accommodate the increased volume over its system. The costs and problems associated with spam can range from having to purchase additional bandwidth and devote employee time at a cost that can range into the millions of dollars for large ISPs, to disruptions in service caused by system crashes that affect paying customers.[27]

The problem is exacerbated by the fact that no centralized system exists for identifying and dealing with unsolicited spam. A recipient of a spam message cannot make a request to be removed from a spam mailing list, and making such a request via a return e-mail often only verifies the validity of one's e-mail address to spammers for their future use. Finally, even if an individual is able to remove herself from an e-mailing list or effectively use rudimentary software to filter out spam messages, the ISP is still left with the burden and havoc spam creates on its servers.

With these problems in mind, ISPs have mounted increasing legislative lobbying efforts and court battles against spammers to try to alleviate the problem. In the area of litigation, the first notable victory in favor of ISPs and against spammers came in *CompuServe v. Cyber Promotions, Inc.*[28] Although the case ended with the parties reaching a settlement wherein Cyber Promotions agreed to cease spamming targeted at CompuServe's subscribers, the court noted that nothing in either the federal or applicable state constitutions required that a private property owner tolerate a

<http://www.cnet.com/Resources/Info/Glossary/Terms/spam.html>.

26. Coalition Against Unsolicited Commercial Email, *The Problem* (visited July 27, 1998) <http://www.cauce.org/problem.html>.

27. *See* Chris Oakes, *Well-Done Spam Cooked Pac Bell's Email*, WIRED NEWS, (visited Apr. 15, 1998) <http://www.wired.com/news/news/technology/story/11684.html>.

28. 962 F. Supp. 1015 (S.D. Ohio 1997).

trespass "whenever the trespasser is a speaker, or the distributor of written speech, who is unsatisfied with the fora which may be available on public property, and who thus attempts to carry his message to private property against the will of the owner."[29]

In late 1998, ISPs scored another victory against spammers in *America Online, Inc. v. LCGM, Inc.*[30] In this instance, America Online (AOL) sued several spammers to stop a practice that the court found included the sending of over 300,000 unsolicited spam messages to AOL subscribers on a daily basis.[31] AOL based its case on several theories, including: false designation under the Lanham Act[32] where the spammers used the "aol.com" designation in their spam e-mail headers;[33] dilution of a service mark under the Lanham Act;[34] exceeding the terms of AOL's access agreement by harvesting AOL subscribers' e-mail addresses in violation of the Computer Fraud and Abuse Act;[35] impairing computer facilities by "intentionally accessing a protected computer without authorization . . . caus[ing] damage," which is also a violation of the Computer Fraud and Abuse Act;[36] in addition to violations of Virginia common law and statutory law.

Though the court declined to rule on the issue of the extent of damages suffered by AOL as a result of the spammers' actions, the court did immediately enjoin the defendants from "further distributing unsolicited bulk e-mail messages to AOL members," prohibited them from further

29. *Id.* at 1027.

30. 1998 U.S. Dist. LEXIS 20144.

31. *See id.* at *7.

32. The Lanham Act at 15 U.S.C. § 1125(a)(1) of makes it unlawful to use in commerce:

> any false designation of origin . . . which –
>
> (A) is likely to cause confusion, or to cause mistake, or to deceive as to the affiliation, connection, or association of such person with another person, or as to the origin, sponsorship, or approval of his or her goods, services, or commercial activities by another person . . . .

Other courts have held that the sending of spam constitutes a violation of this section of the Lanham Act. *See* America Online, Inc. v. IMS, 24 F. Supp. 2d 548 (E.D. Va. 1998); Hotmail Corp. v. Van Money Pie, Inc., 1998 U.S. Dist. LEXIS 10729 (N.D. Cal. 1998).

33. *See AOL*, 1998 U.S. Dist. Lexis 20144.

34. 15 U.S.C. § 1125(c)(1).

35. 18 U.S.C. § 1030(a)(2)(C).

36. 18 U.S.C. § 1030(a)(5)(C).

using the "aol.com" header or harvesting the e-mail addresses of AOL members, and ordered them to terminate any outstanding AOL memberships.[37]

Though some of the spamming practices at issue in the *AOL* case are uncommon, particularly with respect to the unlawful appropriation of AOL's trade name, the case presents a prime example of the development of the law to deal with emerging problems presented by the Internet. Internet Service Providers are increasingly deploying myriad tools to combat what by all accounts is a potentially disruptive marketing practice that affects not only the ISPs' business, but the subscribers' rights to unfettered access to the Internet without interruption or unsolicited advertising.

II
Private Vs. Public Regulation Of Information Mining: Addressing Internet Privacy

Information about the habits, preferences, buying capacity, and other demographics of Internet users is a hot commodity. How valuable is it? So valuable that online marketers have recently announced a program whereby they will give consumers for *free* a new personal computer and Internet service.[38] Well, not really *free*. In exchange for the sub - $1,000 PC and the Internet access usually valued at around $20 per month, the customer will provide a questionnaire full of detailed demographic data, including age, income, marital status, and information about personal tastes and interests.[39] In addition, the company will "monitor which Internet sites the users visit."[40] This enterprise is the latest spin on continuing efforts by Internet marketers to gather and disclose private information about Internet users (read: potential Internet *consumers*).

---

37. *AOL*, 1998 U.S. Dist. Lexis 20144.

38. *See Web entrepreneur to give away PCs, make money on ads*, CNN INTERACTIVE, Feb. 8, 1999 <http://www.cnn.com/tech/computing/9902/08/freepc.reut/>; *see also* Craig Bicknell, *For Sale: Your Tastes, Interests*, WIRED NEWS, June 24, 1998 <http://www.wired.com/news/news/politics/privacy/ story/13212.html> (outlining plans to sell/trade information gathered from Internet user's habits online).

39. *See id.*

40. *Over 500,000 apply for free PCs*, MSNBC.COM, Feb. 10, 1999 <http://www.msnbc.com/news/239946.asp>.

Web sites routinely gather data from visitors using online registration forms, mailing lists, surveys, user profiles, and other fulfillment forms.[41] In addition, Web sites have the ability to *covertly* collect information about the habits of their users. Any Web site can discover, for instance, visitors' e-mail addresses, from where and to where they link, which pages they view, how long they stay, and what they purchase online.[42] The range of things done with this information is unclear, but at a minimum, this information has been collected, used and/or sold for purposes of targeted marketing. In 1998, the Federal Trade Commission investigated GeoCities, for "unfair and deceptive practices" associated with the disclosure of information collected from individuals, including children.[43] Another well-documented case dealing with the gathering and disclosure of private information involved AOL's unauthorized disclosure of personal information about US Navy Petty Officer Timothy R. McVeigh (including information about his stated marital status) to the Navy without a warrant.[44] This disclosure effectively terminated Officer McVeigh's illustrious Navy career based on the Navy's "don't ask, don't tell" policy on gays in the military.[45]

These examples illustrate the different ways an individual's privacy can be compromised on the Internet, by private and government entities alike. Policymakers from both U.S. and foreign governments have undertaken various efforts to secure the privacy of Internet users through legislation aimed at protecting the online privacy of both adults and children. At the same time, an Internet industry

41. A 1997 study by the Electronic Privacy Information Center (EPIC) found that 49 of the top 100 most visited Web sites collect personal information through such methods. *See* EPIC, *Surfer Beware: Personal Privacy and the Internet*, (visited June 1997) <http://www.epic.org/reports/surfer-beware.html>.

42. *See* CENTER FOR DEMOCRACY AND TECHNOLOGY, "*Who's Watching You?*" <http://www.13x.com/cgbin/cdt/snoop.pl> (for a demonstration of the types of information a Web site may discover about its visitors.).

43. *See GeoCities Form S-1 Registration Statement under the Securities Act of 1933*, Securities and Exchange Commission, June 12, 1998 <http://www.sec.gov/Archives/edgar/data/1062777/000101706298001328.txt>. The Federal Trade Commission eventually settled with GeoCities. *Id.*

44. McVeigh v. Cohen, 983 F. Supp. 215 (D. D.C. 1998).

45. *Id.*

coalition, the Online Privacy Alliance, has recently released a "White Paper" outlining its positions on Internet privacy, with a heavy emphasis on industry self-regulation. These different approaches are discussed in turn.

A. Online Privacy For Children

The protection of children always has been of paramount concern in the public policy debate on government regulation of the Internet. In addition to the series of Congressional proposals meant to protect minors from access to obscene content on the Internet, Congress has recently enacted legislation aimed at protecting children's online privacy. The Children's Online Privacy Protection Act (COPPA) was enacted by Congress in October of 1998.[46]

In essence, COPPA strictly governs the circumstances under which Internet marketers or web sites gather and use data from children.[47] The Act requires that the Federal Trade Commission promulgate regulations that "require the operator of any website or online service directed to children that collects personal information from children or the operator of a website or online service that has actual knowledge that it is collecting personal information from a child" to provide notice of the nature of such data collection, the uses for the data, and the data disclosure practices.[48] The Act further requires that such online service or website "obtain verifiable parental consent for the collection, use, or disclosure of personal information from children."[49] Such

46. The Children's Online Privacy Protection Act (COPPA) was enacted as Title XIII, sections 1301 through 1308, of the 1999 Omnibus Appropriations Bill, and was codified at 15 U.S.C. §§ 6501-6506.

47. COPPA defines "child" as "an individual under the age of 13." 15 U.S.C.§ 6501(1).

48. 15 U.S.C. § 6502(b)(1)(A).

49. 15 U.S.C. § 6502(b)(1)(A)(ii). The Act defines "verifiable parental consent" as:

> any reasonable effort (taking into consideration the available technology), including a request for authorization for future collection, use, and disclosure described in the notice, to ensure that a parent of a child receives notice of the operator's personal information collection, use, and disclosure practices, and authorizes the collection, use, and disclosure, as applicable, of personal information and the subsequent use of that information *before that information is collected from that child.*

15 U.S.C. § 6501(9) (emphasis added).

parental notification and consent must be obtained *before* the information is collected from the child.[50]

The Act has wide-ranging implications for the privacy interests of children who use the Internet. For example, if a web site does not first obtain "verifiable parental consent," it cannot set any information-gathering "cookies" on the child's computer, nor can the site ask the child any questions about his or her toy or video game preferences. Though the Act only applies to the gathering and disclosure of information about children by commercial web sites,[51] it nevertheless provides both children and parents a strong line of defense against the unwanted gathering and disclosure of information about children who are using the Internet.

B. European Community Privacy Directive And U.S. Response

Contrasted with this narrow approach to privacy protection, the European Community has taken a much broader approach toward protecting the online privacy of all individuals in its member states. The European Community has taken aggressive steps toward safeguarding the privacy rights of individuals with respect to the processing of personal data. With this objective in mind, the European Parliament and the Council of the European Union enacted the "European Community Privacy Directive," which became effective on October 25, 1998.[52] The Directive treats the protection of personal privacy with respect to personal data a "fundamental right."[53] To achieve the goal of protecting personal data, the Directive provides:

Member States shall provide that personal data may be processed only if:

(a) the data subject has unambiguously given his consent; or

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to

50. 15 U.S.C. § 6501(9).

51. 15 U.S.C. § 2601(2)(A) (website must be maintained for a "commercial purpose" in order to be covered by the Act).

52. The full title of the directive is "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." The complete text of the Directive can be found by searching <http://europa.eu.int> for "Document 395L0046."

53. *See* Directive 95/46/EC, Article 1.

> take steps at the request of the data subject prior to entering into a contract; or
>
> (c) processing is necessary for compliance with a legal obligation to which the controller is subject; or
>
> (d) processing is necessary in order to protect the vital interests of the data subject; or
>
> (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
>
> (f) processing in necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1.[54]

Therefore, unless the Internet user "unambiguously" gives consent for the use of personal data, or another narrow exception applies, the Web site is barred from using or collecting that data.[55] Given the global nature of the Internet, this Directive could have wide-ranging implications for American Internet companies. Article 25 of the Directive explicitly restricts the transfer of data to third countries unless that country guarantees "an adequate level of protection" is afforded to personal data.[56] Based on the current state of American privacy law, it is uncertain whether the transfer of personal data between the U.S. and the European Community would satisfy the requirements of Article 25.

In an effort to comply with the European Community Privacy Directive, and in particular Article 25, the United States Department of Commerce, pursuant to discussions with the European Commission, has promulgated a set of "safe harbor" principles that would apply to American companies that voluntarily comply.[57] The safe harbor

---

54. Directive 95/46/EC, Article 7.

55. An exception is provided if the processing of data is done solely in the interests of "journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression." Directive 95/46/EC, Article 9.

56. Directive 95/46/EC, Article 25.

57. *See* U.S. DEPT. OF COMMERCE, INT'L TRADE ADMIN., INTERNATIONAL SAFE HARBOR PRIVACY PRINCIPLES, Nov. 3, 1998 draft, available at <http://www.epic.org/provacy/intl/doc-safeharbor-1198.html>.

provisions essentially state that, in order to comply, an organization must:

> (1) provide notice about its information collection practices in clear and conspicuous language;
>
> (2) "give individuals the opportunity to choose . . . whether and how personal information they provide is used". . .
>
> (3) be "given the opportunity to choose whether and the manner in which a third party uses the personal information they provide". . .
>
> (4)"take reasonable measures to assure" the reliability of information for its intended use and "take reasonable precautions to protect [the information] from loss, misuse, unauthorized access or disclosure, alteration, or destruction.";
>
> (5) keep complete, accurate and current data records and ensure they are kept only for the purpose it has been gathered;
>
> (6) give individuals "reasonable access" to such information and allow them to amend or correct the information in case it is inaccurate; and
>
> (7) include effective enforcement mechanisms for the principles outlined above, including giving individuals recourse for enforcing these directives.[58]

Whether these self-regulatory principles governing the transmission, accumulation, and storage of personal information will be effective in protecting the privacy of Internet users' personal data is yet to be seen. If the Internet industry adheres to these principles, they would become a substantial first step toward safeguarding privacy in personal data collected from individuals on the Internet. At a minimum, adherence to these "safe harbor" provisions is likely to minimize any liability under Directive 95/46/EC for American companies who are in voluntary compliance and transact business with European consumers over the Internet.

C. The Response From Private Industry

In response to both the public's concern over Internet privacy, and increasing Congressional willingness to enact regulatory legislation in this arena, the Online Privacy Alliance (OPA) has promulgated several online privacy proposals.[59] OPA takes a decidedly self-regulatory approach to

58. *Id.*

59. The Online Privacy Alliance is an industry group describing itself as "an

protecting individuals' online privacy.[60] The Alliance has released two primary policy statements regarding self-regulation of online privacy by its member organizations. The first of these calls for Web sites to use a third-party licensing program or a membership association to monitor company compliance with company privacy policies. Among the third-party monitoring organizations the OPA named are BBBOnLine[61]and TRUSTe.[62] Both sites provide a version of a privacy seal that can be placed on a website, and which indicates that the website adheres to each respective organization's privacy guidelines. The alliance released its second major policy statement on November 19, 1998. It analyses of the OPA's position regarding a multi-layered approach to online privacy, where self-regulation takes the helm, while governmental regulation and private civil actions take a secondary role.[63]

Such efforts at industry self-regulation have faced strong skepticism from privacy and civil rights organizations. For example, the Electronic Privacy Information Center has noted that GeoCities was a member of TRUSTe even during FTC enforcement actions against GeoCities based on its information disclosure practices.[64] The question of online self-regulation remains very much contingent on the ability of the Internet industry to persuade its members to follow robust

---

alliance of global companies and associations committed to promoting privacy online." *See* Online Privacy Alliance (visted, Nov. 19, 1998) <http://www.privacyalliance.org>.

60. *See id.* (Mission Statement).

61. BBBOnLine is a wholly-owned subsidiary of the Better Business Bureau, and features a privacy "seal' program which "incorporates the pertinent guideposts and self-regulation requirements outlined by the Federal Trade Commission and the Department of Commerce." *BBBOnLine Privacy Program Created to Enhance User Trust on the Internet*, BBBONLINE, June 22, 1998, <http://www.bbbonline.org/bolprivacy.shtml>._It is important to note that not all Better Business Bureau members will be required to comply with the program, only those members who sign up with BBBOnLine.

62. TRUSTe has been running its "trustmark" seal program since 1997. A "trustmark" signifies that a Web site has made a commitment to disclose its privacy practices. *See* TRUSTe, (visited June 27, 1998) <http://www.truste.org/useds/program.html>.

63. *See* Legal Framework White Paper, Submitted with the Comments of the Online Privacy Alliance On the Draft International Safe Harbor Principles, Nov. 19, 1998, available at <http://www.privacyalliance.org>.

64. *See Industry Floats Plan on Privacy*, CNET NEWS, July 21, 1998 <http://www.news.com/News/Item/0,4,24434,00.html?st.ne.ni.lh>.

privacy guidelines. In addition, the online industry must also convince consumers concerned about Internet privacy, and the government, that it is protecting the privacy rights of all individuals.

III
Conclusion

The incredible and continuing growth of the Internet has led to many new and innovative ways to share information across national borders. The growth of this information exchange has brought with it the ability of individuals, governments and corporations to collect, use and even sell personal information about Internet users. It has also led to growing willingness on the part of parents and governments to implement measures intended to block minors' access to objectionable content. These measures often run head-on into constitutional limitations. Recent legal and policy developments in the search to address these concerns merit continued attention in a manner that is mindful of the Internet's promise and potential perils.