



Controlling Chaos:

The Emerging Law of Privacy and Speech in Cyberspace

ERIC J. SINROD AND BARAK D. JOLISH*

CITE AS: 1999 STAN. TECH. L. REV. 1

http://stlr.stanford.edu/STLR/Articles/99_STLR_1/

INTRODUCTION

¶ 1

The Internet's¹ explosive growth has opened new avenues for communication, learning, commerce, and entertainment. Like any new medium, however, it comes with its share of problems. Over recent years public debate has focused primarily on two issues: personal privacy and the profusion of "objectionable" content online. Those concerned with privacy fear that the Internet serves as a portal through which the government, big business, or criminals can glean information about individuals' finances, habits, opinions, and even most intimate secrets. Those concerned with objectionable content argue that the medium allows children easy access to explicit pornography and violence. While many of the early users and proponents of the Internet passionately argue that its greatest value comes from its absolute freedom, the call for government intervention has grown with the Internet's gradual assimilation into the life of mainstream America. This article surveys recent developments in the controversies surrounding the role of government in online privacy regulation and in free speech issues such as censorship, "spam,"² and defamation.

* Eric J. Sinrod, a partner in the San Francisco office of Hancock Rothert & Bunshoft LLP, practices commercial litigation and Internet, information and communications law; his e-mail addresses are ejsinrod@hrblaw.com and eric@sinrodlaw.com. Barak D. Jolish is a student at Hastings College of the Law and will become an associate at the Hancock firm later in 1999; his e-mail address is jolishb@uchastings.edu.

¹ The "Internet" refers to a vast worldwide system of linked computer networks. The "World Wide Web" (or just "the Web") is the part of the Internet represented in graphical, linked "pages." "Cyberspace" refers more generally to the ethereal world of virtual reality, the Internet, the World Wide Web, and similar computer environments. See CNET.com, *CNET Glossary* (visited Jan. 10, 1999) <<http://www.cnet.com/Resources/Info/Glossary/>>. Consistent with the practice of most Internet users, this article employs these terms interchangeably to describe the online world accessible through graphical "browsers" (e.g., Netscape Navigator and Microsoft Internet Explorer).

² "Spam" is mass mailing sent over the Internet to a bulletin board, news group, or group of people. *CNET Glossary*, *supra* note 1.

I. PRIVACY

¶ 2 In survey after survey Internet users cite privacy as the most important issue facing the medium today;³ indeed, over three-quarters would go online more often if they felt that the confidentiality of their personal information and communications was secure.⁴ The fact that the Web often serves as a forum to explore intensely personal issues—sexuality and politics, for instance—only heightens these anxieties.⁵ There are also indications that privacy concerns hinder the growth of Internet commerce; fifty-seven percent of users report that Web site policies to guarantee the security of their personal data affect their decisions to make online purchases.⁶

¶ 3 The true impact of these concerns is, however, unclear. Fears about privacy have certainly not completely stifled the growth of the Internet; the number of users and volume of online sales continue to explode.⁷ It is also significant to note that millions of Americans are comfortable enough with the Internet to regularly trade stock online: Online stock brokerages now handle about twenty-five percent of all U.S. trades.⁸

A. *The Gathering and Disclosure of Private Information*

¶ 4 One of the greatest threats to online privacy is a Web site's unauthorized disclosure of its visitors' "personal identifying information," including one's name, e-mail or postal address, credit card, and Social Security numbers. Sites routinely gather such data from online registration forms, mailing lists, surveys, user profiles, and order fulfillment forms.⁹ Many Web sites also create "cookies"—small files on the user's computer that can contain any information the Web site deposits there, including the names of the pages the user visited or what the user typed.¹⁰ The Web site can then access this file to compile a dossier of an individual's interests.

¶ 5 What ultimately happens to the information Web sites collect is often difficult to discover. Sites may make direct use of or sell registration and other information

³ See Graphic, Visualization, & Usability Center (GVU), *8th WWW User Survey*, ¶ 11 (Oct. 1997) http://www.gvu.gatech.edu/user_surveys/survey-1997-10/.

⁴ See Heather Green et al., *A Little Net Privacy, Please*, Business Week Online, ¶ 3 (Mar. 16, 1998) <<http://www.businessweek.com/1998/11/b3569104.htm>>.

⁵ See, e.g., Charlene Laino, *Searching for Love over a Modem* MSNBC News, (Jun. 8, 1998) <<http://www.msnbc.msn.com/news/171418.asp>>(reporting on the growing number of women who use the anonymity of the Internet to explore questions about sexuality).

⁶ See Green et al., *supra* note 4, ¶ 3.

⁷ America Online ("AOL"), for instance, recently reported that 1.25 million of its 15 million members shopped online for the first time in the 1998 holiday season. Between November 26 and December 27, members spent an estimated \$1.2 billion shopping through AOL. See *AOL Does \$1 Billion in Retail*, WIRED NEWS (Jan. 4, 1999) <<http://www.wired.com/news/news/business/story/17116.html>>. Amazon.com's 1998 fourth-quarter sales reached \$250 million—over three and a half times its 1997 sales. See *Amazon's Holiday Bonanza*, WIRED NEWS (Jan. 5, 1999) <<http://www.wired.com/news/news/business/story/17142.html>>.

⁸ See Craig Bicknell, *E-Brokers Enjoy Their Own Run-Up*, Wired News (Dec. 22, 1998) <<http://www.wired.com/news/news/business/story/16992.html>>.

⁹ A 1997 study by the Electronic Privacy Information Center ("EPIC") found that 49 of the 100 most visited Web sites collect personal information through such methods. Electronic Privacy Information Center, *Surfer Beware: Personal Privacy and the Internet*, ¶ 8 (June 1997) <<http://www.epic.org/Reports/surfer-beware.html>>.

¹⁰ See "Cookies" in *CNET Glossary*, *supra* note 1. Used ethically, cookies are fundamentally a convenience feature. By storing information like passwords, preferences and profiles, cookies save users the time and effort necessary to re-enter this information each time they visit a web site. If the user wishes to forgo the convenience, she may configure her browser to "decline" cookies.

to market research companies or direct marketing services. Indeed, the market research firms IntelliQuests and Engage Technologies already tracking user preferences using cookies and data gathered by participating sites.¹¹ Net advertising sites DoubleClick and NetGravity also using cookies to track user movements in order to customize ads to each individual's tastes.¹²

¶ 6 Some commentators argue that these practices are no different than those used by more conventional media. For example, sweepstakes companies routinely sell information from entry forms, magazines buy and sell subscriber lists, and credit card companies provide "leads" for life insurance offerings.¹³ Though this point is well taken, it cannot be denied that the Web presents new and unique grounds for concern. First, by its very nature the Internet greatly eases and speeds the process of information gathering. Second, an Internet user may not be aware that a Web site can also covertly collect data about her habits—from where and to where she links, which pages she views, how long she stays, and what she purchases online.¹⁴

¶ 7 Of even greater potential impact on privacy is the sale of personal information to "look-up" or "individual reference" services. These services pool information into giant databases linked with data from such public sources as real property records, marriage and divorce records, birth certificates, driving records, court records, postal records, and government applications.¹⁵ These databases may also include information from non-public sources, including survey data and credit and marketing reports.¹⁶ California-based Imgis has already developed such a program.¹⁷ Such comprehensive databases do have beneficial uses; for instance, they "enable law enforcement agencies to carry out their missions, public interest groups to find missing children, banks and corporations to prevent fraud, journalists to report the news, lawyers to locate witnesses, and consumers to find lost relatives."¹⁸

¶ 8 Yet, the policies for disbursing this database information have in the past sometimes failed to ensure that personal information remains secure. For instance, two years ago, Lexis-Nexis' P-Trak service briefly allowed its general customers to obtain sensitive information—including the Social Security numbers—of others.¹⁹

¹¹ See Craig Bicknell, *Database Marketing on the Web*, WIRED NEWS (Oct. 7, 1998) <<http://www.wired.com/news/news/business/story/15456.html>>; Craig Bicknell, *For Sale: Your Tastes, Interests*, WIRED NEWS (Jun. 24, 1998) <<http://www.wired.com/news/news/business/story/13212.html>>. Both companies claim they do not match the data they gather with individual user names.

¹² See Kristi Coale, *DoubleClick Tries to Force Hand into Cookie Jar*, WIRED NEWS (Mar. 17, 1997) <<http://www.wired.com/news/news/technology/story/2615.html>>.

¹³ See, e.g., *Is There a Privacy Double Standard on the Web?*, CNN Interactive (Jun. 17, 1998) <<http://cnn.com/TECH/computing/9806/17/net.privacy.idg/index.html>> (an editorial by editors of the Internet site Industry Standard pointing out that the privacy issue is not unique to the Internet).

¹⁴ See Susan Stellan, *Who's Watching You Online?*, CNET News.Com (May 30, 1996) <<http://www.cnet.com/Content/Features/Dlife/Privacy/ss01.htm>> (describing the information that a Web site may discover about its visitors).

¹⁵ "Look-up services" (also called "individual reference services") are computerized database services often used to locate, identify, or verify the identity of individuals. Federal Trade Commission, *Individual Reference Services: A Report To Congress* ¶ 1 (Dec. 1997) <<http://www.ftc.gov/bcp/privacy/wkshp97/irsdoc1.htm#IndividualReferenceServices>>. Lexis-Nexis and credit reporting firms such as Equifax and Trans Union are "look-up" service providers.

¹⁶ *Id.*

¹⁷ See Craig Bicknell, *For Sale: Your Tastes, Interests*, *supra* note 11, at ¶ 27.

¹⁸ Federal Trade Commission, *supra* note 15, at ¶ 4.

¹⁹ See Rose Aguilar, *Service Pulls Social Security Numbers*, (visited Dec. 3, 1998) <<http://www.news.com/News/Item/0,4,1539,00.html>>. Note that some narrow disclosures of some information may nonetheless be illegal under existing law. The Fair Credit Reporting Act, for instance, regulates the collection and distribution of information by credit bureaus. 15 U.S.C. § 1681(1992).

Though the extent of such activity is unclear, the public record already contains accounts of companies who violate even their own posted privacy policies.

¶ 9 Simple and cheap access to personal information is a boon to criminals seeking to perpetrate identity theft and credit card fraud. Equally troubling, however, is the potential harm of legally obtained information distributed for non-criminal purposes. Employers, for example, may gain access to records of employee visits to the web sites of groups which advocate unpopular political views or sexual orientations. Indeed, as stated earlier, it is in these very areas that people feel more free to explore on the Internet than anywhere else. It is also important to note that “[g]iven the ease with which information can be gathered, aggregated, and shared, errors could be widely replicated and the harm long-lasting.”²⁰

¶ 10 Perhaps the most publicized disclosure of private online information involves the recent case of decorated US Navy Petty Officer Timothy R. McVeigh.²¹ McVeigh’s ordeal began when he sent an e-mail to a civilian Navy volunteer regarding a toy drive for the families of sailors on the naval vessel Chicago. McVeigh sent the e-mail under his America Online (“AOL”) screen name “boysrch.”²² Using the AOL “member profile directory,” the volunteer learned that “boysrch” described himself as “Tim,” a member of the military whose “marital status” was “gay.” The volunteer forwarded this information to the Navy, whose investigators in turn called AOL to ask for “boysrch’s” real name. Though the Navy investigators neither obtained a warrant nor even identified themselves,²³ an AOL representative affirmatively identified McVeigh as the customer in question.²⁴ The Navy then commenced an administrative discharge proceeding against McVeigh for “homosexual conduct.”²⁵

¶ 11 Ruling on McVeigh’s motion to enjoin his dismissal, the District Court for the District of Columbia found that the Navy’s actions were illegal under the Electronic Communications Privacy Act of 1986 (“ECPA”), which regulates the interception of private communications and access to and disclosure of stored electronic communications.²⁶ The ECPA specifically forbids the federal government from seeking information about online communications system users unless: a) it obtains a warrant issued under the Federal Rules of Criminal Procedure or state equivalent, or b) it gives prior notice to the online subscriber and then issues a subpoena or receives a court order authorizing disclosure of the information in question.²⁷ It is important to note, however, that the ECPA and the patchwork of other existing legislation do not provide the same privacy protection to sensitive personal data collected by private entities.

²⁰ See *supra* note 13 and accompanying text. For a study of the extent and effect of mistakes by credit report services, see *Mistakes Do Happen: Credit Report Errors Mean Consumers Lose*, CALPIRG (visited Dec. 3, 1998) <<http://www.pirg.org/consumer/credit/mistakes/index.htm>>.

²¹ *McVeigh v. Cohen*, 983 F. Supp. 215 (D. D.C. 1998).

²² A “screen name” is a popular AOL feature which allows a user to create several online personas (“profiles”) without disclosing his or her actual identity.

²³ The Navy paralegal who made the call only stated that he was “a third party in receipt of a fact sheet and wanted to confirm a profile sheet, [and] who it belonged to.” *McVeigh v. Cohen*, 983 F. Supp. at 217.

²⁴ *Id.* at 217.

²⁵ *Id.*

²⁶ *Id.* at 219 (citing 18 U.S.C. §§ 2510-2522, 2701-2711 (1994)).

²⁷ 18 U.S.C. § 2703 (b)(A)-(B), (c)(1)(B).

¶ 12 Though McVeigh won the right to stay in the Navy, his career was effectively over; in July of 1998, he agreed to retire in exchange for full benefits and a settlement to cover his legal fees.²⁸

B. Regulation

¶ 13 Thus far, the federal government has let the information technology industry regulate itself.²⁹ As concerns over privacy issues mount, however, states, Congress and the President have shown an increasing willingness to push the industry to adopt stronger protections. The Federal Trade Commission(FTC) and the Commerce Department lead the federal efforts to track privacy protection policies.

1. The FTC.

¶ 14 In June of 1998, the Federal Trade Commission(FTC) presented to Congress its assessment of the effectiveness of self-regulation as a means of protecting consumer privacy on the World Wide Web.³⁰ The report began by identifying “core principles of fair information practice”:

(a) that consumers be given notice of an entity’s information practices; (b) that consumers be given choice with respect to the use and dissemination of information collected from or about them; (c) that consumers be given access to information about them collected and stored by an entity; (d) that the data collector take appropriate steps to ensure the security and integrity of any information collected; (e) that fair information practice codes or guidelines should contain enforcement mechanisms to ensure compliance with these core principles; and (f) that parents play an important supervisory role of commercial transactions involving their children.³¹

¶ 15 In a 1997 survey designed to characterize U.S. commercial Web sites, the Federal Trade Commission (FTC) determined that only 14% of the 1,400 sites surveyed provided any notice of their information collection practices, and only 2% provided a comprehensive privacy policy.³² When the survey examined sites targeting children, it found that 89% directly collected personally identifiable informa-

²⁸ See *Navy, America Online Both Settle “Don’t Ask, Don’t Tell” Lawsuit*, WALL ST. J., June 15, 1998, at B13G.

²⁹ President Bill Clinton and Vice-President Albert Gore’s “Framework for Global Commerce,” a document outlining the administration’s views on the future of electronic commerce, states that the “Administration supports private sector efforts now underway to implement meaningful, consumer-friendly, self-regulatory privacy regimes . . . [However, if] privacy concerns are not addressed by industry through self-regulation and technology, the Administration will face increasing pressure to play a more direct role in safeguarding consumer choice regarding privacy online.” William J. Clinton and Albert Gore, Jr., *A Framework For Global Electronic Commerce*, (visited Dec. 3, 1998) <<http://www.iitf.nist.gov/eleccomm/ecom.htm#no.1>>.

³⁰ Martha K. Landesberg et al., Federal Trade Commission, Report to Congress on Privacy Online (Jun. 4, 1998) <<http://www.ftc.gov/reports/privacy3/toc.htm>>.

³¹ *Id.* at Executive Summary <[http://www.ftc.gov/reports/privacy3/exeintro.htm#Executive Summary](http://www.ftc.gov/reports/privacy3/exeintro.htm#Executive%20Summary)>. These standards are similar to those already protecting cable subscribers in the Cable Communication Privacy Act of 1984. 47 U.S.C. § 521 (1994) <www.law.cornell.edu/uscode/47/521.html>. This statute might, in fact, already directly apply to cable Internet access providers—though its language is probably too narrow to apply to web sites.

³² Martha K. Landesberg et al., Federal Trade Commission, Report to Congress on Privacy Online, Part V.B.3.a <[http://www.ftc.gov/reports/privacy3/survey.htm#General Survey Findings](http://www.ftc.gov/reports/privacy3/survey.htm#General%20Survey%20Findings)>. Similarly, a 1997 study found that only 17 of 100 sampled sites had well-articulated privacy policies. See Electronic Privacy Information Center, *supra* note 9, ¶ 1.

tion from visitors, and that fewer than 10% provided for some form of parental control over this process.³³

¶ 16 The FTC found that the voluntary industry guidelines it examined failed to address several of the principles listed above—especially those concerning strong enforcement mechanisms. The Commission concluded that, in light of its findings and “significant consumer concerns regarding privacy online, it is evident that substantially greater incentives are needed to spur self-regulation and ensure widespread implementation of basic privacy principles.”³⁴

¶ 17 The FTC was even more forceful in its recommendations regarding children’s online privacy:

The Commission now recommends that Congress develop legislation placing parents in control of the online collection and use of personal information from their children. Such legislation would require Web sites that collect personal identifying information from children to provide actual notice to parents and obtain parental consent.³⁵

¶ 18 Heeding this advice, the 105th Congress passed the Children’s Online Privacy Protection Act of 1998 as part of a larger omnibus budget bill.³⁶ The act requires parental consent before a site can ask a child under the age of 12 to provide his or her age or address. The law also requires sites collecting information from children to explicitly disclose how they plan to use the information.

¶ 19 In testimony before the House Subcommittee on Telecommunications, Trade and Consumer Protection on July 21, 1998, FTC Chairman Robert Pitofsky suggested that the FTC may well recommend further action soon. “The commission believes that, unless industry can demonstrate that it has developed and implemented broad-based and effective self-regulatory programs by the end of [1998], additional government authority in the area would be appropriate and necessary.”³⁷

¶ 20 Finally, it is important to note that sometimes even robust privacy policies may not be sufficient to protect personal information. Indeed, a 1998 investigation by the FTC of free web page provider GeoCities concluded that the company engaged in “unfair and deceptive practices” in connection with the information it collected from individuals—including children.³⁸ According to an FTC draft complaint, GeoCities:

(i) disclosed to third parties personal identifying information collected in its member application process contrary to what had been represented to consumers by the Company; (ii) implied that there was an affiliation between the Company and a children’s club operated by a GeoCities Community

³³ Landesberg et al., *supra* note 32 at Part V.C.1, V.C.4. The FTC writes that “[t]hese practices present unique privacy and safety concerns because of the particular vulnerability of children, the immediacy and ease with which information can be collected from them, and the ability of the online medium to circumvent the traditional gatekeeping role of the parent.” *Id.* at II.C.

³⁴ *Id.* at Part VI.

³⁵ *Id.*

³⁶ This act was passed as part of Pub. L. No. 105-277 (1998), an omnibus budget package.

³⁷ Deborah Scoblionkov, *Ecommerce Gets One Last Chance*, WIRED NEWS (Jul. 21, 1998) <<http://www.wired.com/news/news/politics/story/13895.html>>. The FTC has apparently extended this deadline to March of 1999. Tom Spring, *What’s Private Enough?*, PC WORLD (Dec. 23, 1998) <<http://pcworld.com/pcworld/article/0,1510,9161,00.html>>.

³⁸ See Securities And Exchange Commission, GeoCities Form S-1 registration Statement under the Securities Act of 1933, at 14 (Jun. 12, 1998) <<http://www.sec.gov/Archives/edgar/data/1062777/0001017062-98-001328.txt>>.

Leader such that children provided personal identifying information to the club believing they were disclosing the information to GeoCities[;] and (iii) failed to disclose to consumers (including the parents of children) how the Company would use the personal identifying information it collected from those consumers and children.³⁹

GeoCities ultimately avoided FTC action by agreeing in a consent order to rectify the allegedly improper practices.⁴⁰

2. *The Commerce Department.*

¶ 21 In 1997, President Clinton ordered the Department of Commerce to report on industry self-regulation to ensure the online privacy of adults and especially children.⁴¹ Pursuant to this mandate, on June 23 and 24, 1998, the Department convened a conference on “Elements of Effective Self Regulation for the Protection of Privacy.” During the conference, Commerce Secretary William Daley reflected the administration’s general position: “[The president] is well aware that e-commerce can soon be a \$300 billion business [and] does not want to do anything that would mess up all of that success.”⁴² In November of 1998 the White House announced that Commerce Department lawyer Elliot Maxwell would take the lead in advising the administration about the Internet—including recommended privacy policies.⁴³

3. *State Action.*

¶ 22 Several states have sought to impose privacy protection of their own. The most comprehensive thus far is that of Virginia, which will consider the “Virginia Internet Policy Act” in 1999.⁴⁴ The Act was drafted by Virginia Gov. James Gilmore’s 36-member Commission on Information Technology, a body which includes representatives from both the public sector and companies such as Microsoft, AOL, and MCI-Worldcom. If adopted in its current form, the Act would require that online companies clearly post their personal information collection practices, disclose how they use the data, and let consumers opt out of giving up sensitive details. The Act also lays out an enforcement mechanism, directing the state to prosecute companies that have “deceptive policies” or violate their own guidelines.⁴⁵

4. *Industry Response.*

¶ 23 The week preceding the June 1998 Commerce Department conference saw the launch of the Online Privacy Alliance (OPA), composed of 50 large companies that

³⁹ *Id.*

⁴⁰ A copy of the settlement agreement may be found at <<http://www.ftc.gov/os/1998/9808/geoord.htm>>.

⁴¹ See Department of Commerce, *Elements of Effective Self Regulation for the Protection of Privacy and Questions Related to Online Privacy: Notice and Request for Public Comment* (Jun. 5, 1998) <http://www.ntia.doc.gov/ntiahome/privacy/6_5_98fedreg.htm>.

⁴² Ashley Craddock, *Panel Debates Online Privacy Issues*, N.Y. TIMES ON THE WEB (Jun. 24, 1998) <<http://www.wired.com/news/news/politics/story/13223.html>>.

⁴³ See Declan McCullagh, *Net Guru Named at Commerce*, CNET NEWS.COM (Nov. 18, 1998) <<http://www.wired.com/news/news/politics/story/16351.html>>.

⁴⁴ The Governor’s Commission on Information Technology, *A Legislative Framework for the Virginia Internet Policy Act* (visited Jan. 5, 1999) <<http://www.sotech.state.va.us/intpol.htm>>.

⁴⁵ *Id.*

sell products on the Internet.⁴⁶ Headed by former FTC Commissioner Christine Varney, the OPA established privacy guidelines and pledged to “introduce and promote business-wide actions that create an environment of trust and foster the protection of individuals’ privacy online.”⁴⁷ On July 2, 1998, the OPA released its enforcement plan, which calls for Web sites to use a third-party licensing program or a membership association to monitor company compliance with company privacy policies.⁴⁸ The alliance also calls on companies to provide consumers clear and effective complaint mechanisms where violations are found, and to educate the public about Internet privacy.⁴⁹

¶ 24 Among the third-party monitoring organizations the OPA named are BBBOnLine and TRUSTe. BBBOnLine, a wholly-owned subsidiary of the Council of Better Business Bureaus, features a “privacy ‘seal’ program, which incorporates the pertinent guideposts and self-regulation requirements outlined by the Federal Trade Commission the U.S. Department of Commerce.”⁵⁰ It is important to note, however, that BBBOnLine privacy policies will apply only to online companies that sign up with the group—not to all Better Business Bureau members across the nation. 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.⁵¹

¶ 25 Many trade groups have also enacted their own privacy guidelines. The Direct Marketing Association, for instance, has instructed its 3,600 members to provide notice to their Web visitors of the personal information they were collecting and how the data would be used.⁵² Likewise, the fourteen members of the Individual Reference Services Group have “pledged to adopt self-regulatory principles governing the dissemination and use of personal data.”⁵³

¶ 26 Despite this flurry of activity, electronic privacy advocates continue to challenge the online industry’s ability to regulate itself. Their primary criticism is that even the best self-regulation plans wield weak enforcement mechanisms and penalties and thus present little assurance of member compliance.⁵⁴ On June 22, 1998, for instance, the non-profit Electronic Privacy Information Center (EPIC) released a study finding that, of the forty newest Direct Marketing Association sites, only eight had any privacy policy posted at all, and of those only three met the organization’s guidelines.⁵⁵ EPIC’s executive director also noted that the FTC questioned GeoCi-

⁴⁶ Included in this group are Netscape, America Online, AT&T, Disney, Equifax, Microsoft, and Procter & Gamble.

⁴⁷ *Online Privacy Alliance*, (visited Jul. 22, 1998) <<http://www.privacyalliance.org/>>.

⁴⁸ The timing of the OPA announcement corresponded to FTC Chairman Robert Pitofsky’s testimony to the House Commerce Committee on on-line privacy.

⁴⁹ *Online Privacy Alliance* (visited Nov 27, 1998) <<http://www.privacyalliance.org/resources/enforcement.shtml>>.

⁵⁰ *Id.*

⁵¹ See *TRUSTe* (visited Jun. 27, 1998) <http://www.truste.org/webpublishers/pub_howhtml>. The TRUSTe site features a “wizard” to help Web sites automatically generate their own privacy policy.

⁵² Direct Marketing Association, *The DMA’s Privacy Promise* (visited Jan. 5, 1999) <<http://www.the-dma.org/topframe/index7.html>>.

⁵³ See *Individual Reference Services Group* (visited June 27, 1998) <<http://www.irsg.org/>>.

⁵⁴ See Courtney Macavinta, *Net Privacy Plans Scrutinized*, Cnet News.com (Jun. 24, 1998) <<http://www.news.com/News/Item/0,4,23538,00.html?st.ne.fdmh>>.

⁵⁵ Electronic Privacy Information Center, *Surfer Beware II: Notice Is Not Enough* (Jun. 1998) <<http://www2.epic.org/reports/surfer-beware2.html>>. The DMA refutes the EPIC study, and points to its own May survey which found that 64% of leading business Web sites had privacy policies, compared to 38% in January. (*footnote continued*)

ties' privacy practices while the company was a member of TRUSTe.⁵⁶ In addition, there is a danger that only a self-selecting pool of Web sites will agree to voluntarily regulate themselves, therefore leaving other less scrupulous sites unregulated.

¶ 27 The question of online regulation thus remains very much contingent on the ability of the Internet industry to persuade its members to follow robust privacy guidelines. The industry must also convince consumers and the government that it is protecting the privacy rights of individuals.

5. *European Union Privacy Directive.*

¶ 28 Some form of government action may be necessary in response to the European Union privacy directive, which took effect October 25, 1998.⁵⁷ Adopted in 1995, the directive prohibits companies located in a European Union country from transmitting electronic data to nations that lack "adequate protection" for personal data—including potentially the U.S.⁵⁸ Though the standards for "adequate protection" remain largely unclear, this policy could potentially expose U.S. companies to liability for failing to protect European consumers' privacy—even absent an actual breach. To prevent such an outcome, the Clinton Administration has proposed a "safe harbors" system in which companies would voluntarily comply with basic privacy principles similar to those which many e-commerce Web sites already employ.⁵⁹ The outcome of U.S.-European talks on this issue is as yet unclear.

6. *Technological Solutions.*

¶ 29 Technological advances may ultimately resolve at least some of the privacy issues discussed above. The World Wide Web Consortium, a standard setting body, has proposed the Platform for Privacy Preferences, or P3P. P3P is an automated system to give users more control over the information they disclose about themselves as they surf the Web. Under the proposal, site designers would post their privacy practices in a format the user's browser would understand. Web surfers could, in turn, set browser preferences to control how much information they want to release to Web sites they visit.

¶ 30 Privacy advocates, however, are still wary. Barry Steinhardt, president of the Electronic Frontier Foundation, observed:

there are still a lot of unanswered questions about P3P and the underlying philosophy of industry self-regulation If you turn [P3P] on and say you want to be anonymous, you're going to be blocked from a lot of sites There's a question of whether this will work or [whether] there will be a consumer revolt.⁶⁰

See Courtney Macavinta, *Commerce Dept. Slams Privacy Efforts*, CNET News.com (Jun. 23, 1998) <<http://www.news.com/News/Item/0,4,23457,00.html>>.

⁵⁶ See Courtney Macavinta, *Industry Floats Plan on Privacy*, CNET News.com (Jul. 21, 1998) <<http://www.news.com/News/Item/0,4,24434,00.html?st.ne.ni.lh>>.

⁵⁷ See Council Directive 95/46, 1995 O.J. (L 281) 3.

⁵⁸ Article 26 of the Directive does allow for an exception if the entity controlling the information can demonstrate that it has taken adequate precautions to protect its privacy. The document also suggests that unspecified contractual provisions may serve to satisfy Directive requirements.

⁵⁹ International Trade Administration Electronic Commerce Taskforce letter to industry representatives (visited Jan. 6, 1999) <<http://www.ita.doc.gov/ecom/menu.htm#Safe>>.

⁶⁰ *Id.*

The P3P scheme also requires a certain level of computer literacy to successfully edit the preferences for the desired level of protection.

¶ 31 The future of P3P is uncertain, especially as one of the Consortium's former members has filed a patent for the technology. The company apparently plans to license technology at an annual royalty rate of one percent of all revenues directly associated with the technology (with a \$50,000 minimum for companies with revenues of over \$2.5 million).⁶¹ Thus far the Consortium failed to meet its goal of introducing P3P into the market by April of 1998,⁶² and indeed it will not be included in Internet Explorer 5.0, the next version of Microsoft's browser.

II. SPEECH

A. Censorship

¶ 32 Americans differ as to the appropriate level of censorship on the Internet. In a recent survey, only 30% of Internet users reported that they were "very" or "extremely" concerned about pornography on the Web. Indeed, 70% of users instead expressed concern about the "desire of special interest groups to restrict what is available over the Internet" and about "government censorship of what is available on the Internet."⁶³ This contrasts somewhat with a May, 1997 poll of the general population in which 80% of respondents agreed that "the government should take steps to control access to pornographic or sexually explicit material on the Internet to protect children and teens under 18 years of age." These differences are likely to moderate as more members of the general population become Internet users.

¶ 33 Perhaps responding to the latter concerns, in 1996 President Clinton signed the Communications Decency Act (CDA)⁶⁴ into law as part of omnibus legislation affecting the entire landscape of American communications law. The CDA outlawed the transmission of "indecent" and other sexually explicit materials to minors over computer networks. The Act defined indecency as that which is "patently offensive" by "contemporary community standards."

¶ 34 The United States Supreme Court's 1997 decision in *Reno v. ACLU* down the "indecent" provisions of the CDA, holding that they violated the First Amendment's guarantee of freedom of speech.⁶⁵ The Court held that the government must grant the Internet the same level of protection as books or magazines (a level significantly higher than that granted to speech on television or over the telephone). The decision agreed with the lower federal court's conclusion that the Internet is "the most participatory form of mass speech yet developed," and is entitled to "the highest protection from governmental intrusion."⁶⁶ In that context, the CDA was viewed as a "content-based blanket restriction on speech" that "fail[ed] to provide any definition of 'indecent' and omit[ted] any requirement that 'patently offensive'

⁶¹ InterMind, *Patent Information for W3C Members* <http://www.intermind.com/W3CMembers/licensing_letter.htm>.

⁶² World Wide Web Consortium, *Comments to the Federal Trade Commission's Bureau of Consumer Protection Workshop on Consumer Information Privacy* (Jun. 10-13, 1997), <<http://www.ftc.gov/bcp/privacy/wkshp97/comments2/w3c-ftc.htm>>.

⁶³ Madeline Mooney and Tracy Pozil, *Credit Card Security Greatest Internet-Related Concern Concludes Lycos Web User Study* (Mar. 5, 1998) <<http://www.cyberdialogue.com/press/releases/aius3.html>>.

⁶⁴ 47 U.S.C. § 223(a), (d)(1996).

⁶⁵ 117 S.Ct. 2329 (1997).

⁶⁶ *Id.* at 2340.

material lack socially redeeming value.”⁶⁷ Moreover, the Act “neither limit[ed] its broad categorical prohibitions to particular times [and places] nor base[d] them on an evaluation by an agency familiar with the medium’s unique characteristics.” Ultimately, the CDA’s “burden on adult speech [was] unacceptable if less restrictive alternatives would be at least as effective in achieving the Act’s legitimate purposes The Government [did] not prove[] otherwise.”⁶⁸ The Supreme Court also pointed out that the decentralized nature of the Internet made it difficult to apply the “community standards” test for obscenity law. Ultimately, the *Reno* decision suggests that any legislation affecting the Internet must be narrowly tailored so as to fall within the standards of liberal as well as conservative communities.⁶⁹

¶ 35 In spite of this setback, the political forces behind the CDA continued to push for regulation of adult material on the Internet. In 1997, Rep. Mike Oxley (R-Ohio) introduced the Child Online Protection Act (“COPA”), which President Clinton signed into law as part of a \$500-billion federal budget bill for fiscal 1999.⁷⁰ Called “CDA II” by its critics, COPA requires commercial website operators who offer material which is “harmful to minors” to verify that each of their visitors is an adult. The act mandates they do this by requiring a credit card number, adult access code, or similar measures. Violators face up to \$50,000 in fines and six months in prison per offense.

¶ 36 The same coalition of civil liberties groups, news publishers and online merchants that challenged the Communications Decency Act in *Reno* have challenged COPA in a federal district court in Philadelphia.⁷¹ In their complaint, the *ACLU v. Reno* plaintiffs argue that the COPA age-verification provisions place an undue burden on constitutionally protected Web sites and would prevent adults from surfing the Internet anonymously. 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.⁷²

¶ 37 In reaching its decision, the *Reno II* court again focused on the law’s impact on the First Amendment rights of adults. First, the court found that “as a content-based regulation of [nonobscene sexual expression], COPA is presumptively invalid and is subject to strict scrutiny.”⁷³ The government could thus regulate the content of such speech only if its regulation was narrowly tailored as the least restrictive

⁶⁷ *Id.* at 2331.

⁶⁸ *Id.* at 2332.

⁶⁹ *See id.* at 2348. The *Reno* case provides an interesting contrast to *United States v. Thomas*, where the federal government brought charges in Tennessee against a California couple who posted sexually explicit material on a members-only electronic bulletin board service (BBS). The Tennessee federal court applied Memphis community standards and convicted the California couple of obscenity violations, and the Sixth Circuit affirmed. The *Thomas* court stressed the fact that the defendants very easily could have controlled access to the BBS by refusing to give its phone number to people in jurisdictions in which the defendants did not wish to provide service. In contrast, it is not possible to exercise this control once material is posted on the seamless and global Internet. 74 F.3d 701 (6th Cir. 1996).

⁷⁰ Pub. L. No. 105-277 (1998).

⁷¹ *American Civil Liberties Union v. Reno*, No. 98-5591 (E.D. Pa. filed Oct. 22, 1998) available at <<http://www.paed.uscourts.gov/opinions/99D0078P.HTM>>.

⁷² *Id.*

⁷³ *Id.* (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)).

means to further a compelling government interest.⁷⁴ 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.⁷⁵ 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 on-line using protocols apart from http such as ftp.⁷⁶ 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.⁷⁷

¶ 38 The court also found that COPA imposed an undue burden on speech because plaintiffs may self-censor the content of their Web sites to avoid the costs of age verification systems.⁷⁸ Finally, the court noted that there is

no way to restrict 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.⁷⁹

¶ 39 1997 also saw several state attempts to regulate Internet speech. New York, for instance, passed a COPA-like law making it a crime to engage in online communications which are “harmful to minors.”⁸⁰ Yet, in what is perhaps a demonstration of the difficulties these “state CDAs” face, the court in *American Libraries Association v. Pataki* soundly rejected the New York statute.⁸¹ The *Pataki* court based its reasoning on the interstate commerce effects of the New York law.

First, the Act represents an unconstitutional projection of New York law into conduct that occurs wholly outside New York. Second, the Act is invalid because although protecting children from indecent material is a legitimate and indisputably worthy subject of state legislation, the burdens on interstate commerce resulting from the Act clearly exceed any local benefit derived from it. Finally, the Internet is one of those areas of commerce that must be marked off as a national preserve to protect users from inconsistent legislation that, taken to its most extreme, could paralyze development of the Internet altogether. Thus, the Commerce Clause ordains that only Congress can legislate in this area, subject, of course, to whatever limitations other provisions of the Constitution (such as the First Amendment) may require.⁸²

⁷⁴ *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.”).

⁷⁵ *Id.*; see also *Reno v. ACLU I*, 117 S.Ct. at 2349.

⁷⁶ *Id.*

⁷⁷ *Id.*

⁷⁸ *Id.*

⁷⁹ *Id.*

⁸⁰ N.Y. Penal Law § 235.20(6) (1997).

⁸¹ 969 F. Supp. 160 (S.D.N.Y. 1997).

⁸² *Id.* at 182.

¶ 40 Others concerned with children’s access to indecent materials have taken less expansive approaches. For instance, in early 1997 the White House requested that online content providers adopt “ratings” to alert Internet users of possibly objectionable content.⁸³ Indeed, an upcoming release of Netscape’s browser will offer users the option of excluding sites of a certain rating, such as adult content sites.⁸⁴ Certain Internet providers have also embraced the use of commercially available “filtering” programs that allow parents to control what types of content their children can access.⁸⁵ In fact, two bills in the 105th Congress would have required Internet service providers to make filtering software available to all subscribers.⁸⁶

¶ 41 Many public libraries and schools have already installed Internet filters on their computers. Legislation and the threat of lawsuits partially have driven this growth.⁸⁷ The California Assembly, for example, considered a bill in 1997 that would require all public libraries that receive state funds to adopt a policy prohibiting minors from accessing “harmful” matter on library Internet terminals.⁸⁸ Senate Bill 97,⁸⁹ sponsored by Senator John McCain (R-Ariz.), would require that schools and public libraries receiving federal Internet grants to install as-yet-unspecified blocking and filtering software on any and all public-use computers so as to shield minors from “inappropriate” material.

¶ 42 Some free speech advocates have expressed concern that content filters may block important and valuable information along with the obscene and violent. An EPIC survey found that one “family-friendly” search engine blocked access to almost 90 percent of materials containing even innocuous terms such as the “American Red Cross” and the “San Diego Zoo.”⁹⁰ The Censorware Project found that another filter had blocked “gay-themed” sites even though they contained no nudity, violence, or obscenity.⁹¹ Civil liberties organizations are especially wary of filters in government institutions like public libraries.⁹²

¶ 43 On Nov. 23, 1998, Virginia Federal District Court Judge Leonie Brinkema ruled that a Virginia public library’s Internet filtering policy violated the First Amend-

⁸³ See *Online News Producers Oppose Site-content Ratings*, CNN INTERACTIVE (Aug. 29, 1997) <<http://cnn.com/TECH/9708/29/Internet.ratings/>> (discussing online news producers’ refusal of the White House request to adopt a rating system).

⁸⁴ See *Netscape Readies Communicator Upgrade to Version 4.5*, CNN INTERACTIVE (Jun. 18, 1998) <<http://cnn.com/TECH/computing/9806/18/netscape.upgrade.idg/>> (discussing Netscape’s upgrade which allows the user to exclude certain sites).

⁸⁵ There are a variety of filters on the market, including Cybersitter and Net Nanny. Companies like America Online, Inc. and Walt Disney Co. have released their own tools for parents who wish to screen Internet content.

⁸⁶ See H.R. 774, 105th Cong. (1997) (Rep. Zoe Lofgren’s (D-Cal.) Internet Freedom and Child Protection Act of 1997); H.B. 1180, 105th Cong. (1997) (Rep. Joseph McDade’s (R-Pa.) Family-Friendly Internet Access Act of 1997).

⁸⁷ See Janet Kornblum, *Post-CDA Filtering Under Fire*, CNET NEWS.COM (Jul. 3, 1997) <<http://www.news.com/News/Item/0,4,12158,00.html>> (discussing the filter controversy and the CDA); see also American Civil Liberties Union, *Censorship In a Box*, (visited Jun. 26, 1998) <<http://www.aclu.org/issues/cyber/box.html>> [hereinafter ACLU] (discussing the appropriateness and constitutionality of mandatory filters in public libraries).

⁸⁸ A.B. Res. 1793 (Cal. 1997).

⁸⁹ S. 97, 106th Cong. (1999).

⁹⁰ *Faulty Filters: How Content Filters Block Access to Kid-Friendly Information on the Internet* (visited Jan. 5, 1999) <<http://www2.epic.org/reports/filter-report.html>>.

⁹¹ The Censorware Project, *Blacklisted by Cyber Patrol* (visited Jan. 5, 1999) <<http://www.censorware.org/reports/cyberpatrol/ada-yoyo.html>>.

⁹² See ACLU, *supra* note 87.

ment.⁹³ In making this ruling, Judge Brinkema held the policy in question was subject to strict scrutiny; the county thus had to prove that its policy was necessary to serve a compelling state interest, and that it was narrowly drawn to achieve that end.⁹⁴ In examining the evidence before her, the Judge found that the county's citation of isolated complaints in other libraries was not sufficient to establish that the regulation was necessary. She also found that the policy was not narrowly tailored, and cited three less restrictive means that the county had not tested: privacy screens around Internet terminals, library staff monitoring of Internet use, and the installation of filtering software on only some Internet terminals designated for minors' use.

¶ 44 Judge Brinkema also ruled that the library's filtering policy was over-inclusive "because, on its face, it limits the access of all patrons, adult and juvenile, to material deemed fit for juveniles."⁹⁵ She noted that the U.S. Supreme Court in *Reno* similarly ruled that the attempt by the Communications Decency Act to shield children from Internet pornography was unconstitutional in that its broad scope suppressed a large amount of constitutionally protected adult speech.

¶ 45 Judge Brinkema finally ruled that the library's filtering policy was an unconstitutional prior restraint because "it includes neither sufficient standards nor adequate procedural safeguards" to allow for prior judicial determinations before material is censored.⁹⁶ The judge was particularly troubled that the library would abdicate the responsibility of censoring speech to a private party—the software filter publisher.

¶ 46 In an interesting twist on the library filtering issue, the Pacific Justice Institute, a religious-rights group, recently represented the mother of a 12-year-old boy in a suit designed to compel the City of Livermore, California to *install* Internet filters in its libraries.⁹⁷ In its first incarnation, the suit contended that the library wasted public funds and created a public nuisance by allowing minors—like the plaintiff's son—to access images of "seminude and nude women positioned in sexually alluring and explicit poses." The court dismissed this complaint on Oct. 21, 1998, ruling that a portion of the CDA that survived *Reno* immunizes providers of Internet access from responsibility for material which others transmit. The Judge also rejected later arguments that, by providing unfiltered Internet access, the library was essentially providing pornography and therefore violating the constitutional rights of children.⁹⁸

¶ 47 Ultimately, it is unclear whether U.S. laws aimed at regulating Internet content will have a major substantive effect. The Internet, after all, is a global network, and Americans may access a Web site based in Amsterdam as easily as one based in Ak-

⁹³ *Mainstream Loudoun v. Loudoun County Libraries*, 24 F. Supp. 2d 522 (E.D. Va. 1998).

⁹⁴ As in *ACLU v. Reno*, Judge Brinkema reasoned that plaintiffs were adults entitled to full First Amendment protection. Judge Brinkema also rejected the county's argument that the library's policies need only survive the intermediate-scrutiny standard pertaining to a non-public forum. She found that the county's intent in establishing the library, the extent of its use and the very nature of the institution demonstrated that it is open to the public for the very type of expressive activity the Internet delivers. Judge Brinkema concluded that because the library's filtering policy is a content-based regulation in a limited public forum, it is subject to the more rigorous strict-scrutiny standard. *Id.*

⁹⁵ *Id.* at 567.

⁹⁶ *Id.* at 559 (quoting *Baltimore Boulevard, Inc. v. Prince George's County*, 58 F.3d 988, 993-94 (4th Cir. 1995)).

⁹⁷ *Kathleen R. v. Livermore*, No. 015266-4 (Alameda County Sup. Ct. filed May 28, 1998).

⁹⁸ *Judge Says Library Can Provide Unfiltered Internet Access*, CNN INTERACTIVE (Jan. 15, 1999) <<http://cn.com/TECH/computing/9901/15/library.netporn.ap/index.html>>.

ron. Thus, even if legal barriers drive some U.S.-based adult sites out of business, similar sites in other countries remain only mouse clicks away from desktops in America.

B. Spam

¶ 48 “Spam” (also called “junk e-mail” and “unsolicited commercial e-mail” (“UCE”)), is an unwelcome mass mailing to electronic bulletin boards, newsgroups or lists of e-mail addresses.⁹⁹ Most spam messages advertise products or services like phone sex lines, adult web sites, “miracle” health products, and “get rich quick” schemes.¹⁰⁰ It is estimated that roughly half of unsolicited commercial e-mail messages contain fraudulent or deceptive content.¹⁰¹ Although many compare spam to postal junk mail, the two differ in several fundamental ways. First, while junk-mailers must pay for mailing lists, postage, paper and envelopes, spammers’ costs are negligible; spammers pay pennies per name to purchase e-mail or newsgroup lists, and can even “harvest” the information themselves with software that gathers e-mail addresses from newsgroup postings and the Web. Many spammers also use free e-mail accounts to disseminate their messages.¹⁰² Ultimately, in fact, spam recipients bear most of the cost of the advertisement; according to one estimate \$2 of the average consumer’s monthly ISP bill ultimately goes to handling spam-related expenses.¹⁰³ Many Internet service providers (“ISPs”) report that spam accounts for anywhere between five and thirty percent of their e-mail volume; consequently, they must spend millions of dollars each month on extra bandwidth and employee time to accommodate and control this load.¹⁰⁴ Spikes in the volume of spam have even caused several major ISPs to crash, disrupting service to paying customers.¹⁰⁵

¶ 49 Second, there is no centralized process for identifying the source of the spam. Therefore, recipients cannot request to be removed from spam lists as they can from conventional mailing lists. Because many people respond to spam with angry reply messages, spammers often hide their own identities by using other ISP names

⁹⁹ See *CNET Glossary*, CNET.COM (visited Jun. 26, 1998) <<http://www.cnet.com/Resources/Info/Glossary/Terms/spam.html>> (defining the term “spam”).

¹⁰⁰ See *About the Problem*, Coalition Against Unsolicited Commercial Email (visited July 27, 1998) <<http://www.cauce.org/problem.html>> (discussing spam’s threat to the viability of the Internet).

¹⁰¹ The Ad-Hoc Working Group on Unsolicited Commercial Email, *Report to the Federal Trade Commission of the Ad-Hoc Working Group on Unsolicited Commercial Email* (visited July 27, 1998) <<http://www.cdt.org/spam/>> (addressing the problems of unsolicited email).

¹⁰² *Id.* This “cost-shifting” is similar to that of “junk faxes,” which became widespread after the popularization of the fax machine. The federal government killed the junk fax industry overnight with the Telephone Consumer Protection Act of 1991 (“TCPA”), which allows consumers to collect up to \$500 for every violation of the Act’s ban on “any material advertising the commercial availability or quality of any property, goods, or services which is transmitted to any person without that person’s prior express invitation or permission.” 47 U.S.C.A. § 227 (1991). Because most spam is also sent over telephone lines, the language of the TCPA is potentially broad enough to cover it. Though discussed, as of yet, the TCPA has not been used to prohibit e-mail spam.

¹⁰³ See Neal Weinberg, *A Day in the Life of a Spammer*, CNN INTERACTIVE (Jun. 29, 1998) <<http://cnn.com/TECH/computing/9806/29/spammer.idg/index.html>> (discussing the costs of spam to ISPs and consumers).

¹⁰⁴ *Id.*

¹⁰⁵ In March of 1998, for instance, an unprecedented load of spam over the course of four days caused sporadic disruption of Pacific Bell’s Internet Services to its more than 175,000 California customers. See Chris Oakes, *Well-Done Spam Cooked Pac Bell’s Email*, WIRED NEWS (April 15, 1998) <<http://www.wired.com/news/technology/story/11684.html>>.

in their return addresses. This strategy does the additional harm of exposing innocent ISPs to the wrath of angry spam recipients.¹⁰⁶

¶ 50 Certain commercially available software programs can filter spam messages from ISP computers or home e-mail accounts. At best, however, such software offers only a partial solution, and the burden for avoiding spam still falls on the recipient. Spam filters do not, for instance, reduce the cost and space required to administer the spam that enters the system (even if it is later eliminated). These programs also sometimes fail to defeat spammers' increasingly sophisticated techniques to evade filtering.

¶ 51 Though members of the 105th Congress introduced several bills to help control spam, none was enacted into law.¹⁰⁷ State legislatures were, however, more successful. California, for instance, enacted laws requiring unsolicited bulk e-mailers to appropriately label the subject line of messages selling goods and services.¹⁰⁸ Thus, for instance, adult-oriented spam would have to be labeled "ADV:ADLT." The state also requires that spammers set up a toll-free telephone number or accurate return e-mail address so that recipients can request to be taken off a spam list. Additional new statutes allow any e-mail provider to sue spammers for trespass on their computer systems, and to recover losses caused by network clogs or crashes. The law finally makes it a crime to "knowingly and without permission us[e] the Internet domain name of another individual, corporation, or entity" to send bulk e-mail.

¶ 52 The State of Washington's anti-spam law allows recipients of unsolicited commercial e-mail to collect \$500 in damages for each occurrence, while Internet service providers may collect up to \$1,000.¹⁰⁹ This law also prohibits the use of a third party's domain name, the misrepresentation of message origin, and the use of a false or misleading subject line in commercial e-mail messages. However, the law applies only to e-mail sent from or received in the State of Washington, illustrating

¹⁰⁶ Courts, however, are beginning to respond to this particular problem. In June, 1998, Northern District of California Judge James Ware permanently enjoined spammers from using the name of Microsoft's e-mail service, Hotmail, in spam return addresses. See Chris Oakes, *Hotmail Bags Spammers*, WIRED NEWS (June 16, 1998) <<http://www.wired.com/news/news/politics/story/13016.html>>.

¹⁰⁷ Representative Chris Smith's (R-N.J.) H.R. 1748, the Netizen Protection Act of 1997, would expressly extend the Telephone Consumer Protection Act of 1991 prohibition against "junk faxes" to cover unsolicited commercial e-mail. Recipients of unwanted spam would be able to obtain \$500 from a spammer for each spam message. Damages would be tripled if the court finds that the spammer "willfully" or "knowingly" violated the law.

The Senate already has passed spam legislation as part of S. 1618, a bill designed to prohibit long-distance phone companies from "slamming" (switching customers' long-distance carriers without their consent). A last-minute amendment to the bill would set aside the blanket prohibition in favor of a requirement that all commercial unsolicited e-mail contain the actual name, postal address, e-mail address and phone number of the sender. It also would mandate that spammers create a system through which junk e-mail recipients could request that they be removed from e-mail lists. The FTC would have authority to investigate violations of these standards and to impose civil fines of up to \$15,000.

In August 1998, the House Telecommunications Subcommittee approved H.R. 3888, the House equivalent of S. 1618. The House and Senate provisions differ only as to where in the message the sender must identify his or her message as spam. In the Senate bill, the spammer must include such an identification in the subject header, thus enabling ISPs and individuals to easily filter out such e-mail. The House bill, however, requires identification only in the body of the message, making it much more likely that a user would have to open the spam before realizing what it is.

¹⁰⁸ Cal Bus. & Prof. Code § 17538.4 (West 1998); Cal Bus. & Prof Code § 17538.45 (West 1999).

¹⁰⁹ 1998 Wa. ALS 149; 1998 Wa. Ch. 149; 1997 Wa. HB 2752.; see also Ed Murrieta, *Spam Law Bares Teeth*, WIRED NEWS (Jul. 16, 1998) <<http://www.wired.com/news/news/politics/story/13783.html>>.

the limits of state regulation. In spite of this obstacle, Washington's attorney general has brought at least one action under the law,¹¹⁰ as have two private citizens.¹¹¹

¶ 53

In an interesting development, the Direct Marketing Association (DMA) recently met with representatives of several anti-spam organizations, including the Coalition Against Unsolicited Commercial Email (CAUCE), Rodney Joffe, proprietor of the SAFEeps e-mail preference service, and Paul Vixie, founder of the Mail Abuse Prevention System.¹¹² The DMA persuaded the anti-spam groups to agree to a proposal for a system similar to the one now in place for paper junk mail. Under the proposal, the DMA would fund a third party database to allow users of the Internet to register their "no spam" e-mail addresses. The DMA would support legislation requiring spammers to respect the preference of those in the database.¹¹³

¶ 54

ISPs have been attempting to block and filter out spam messages, and are pushing for solutions and legislation to control the problem. Spammers, led by Cyber Promotions, Inc., have objected that this blocking interferes with their right to free speech. In *CompuServe Incorporated v. Cyber Promotions, Inc.*,¹¹⁴ the court addressed this issue and concluded that nothing in either the federal or applicable state constitutions required that a private property owner tolerate a 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."¹¹⁵ Under a consent decree, Cyber Promotions ultimately agreed to cease sending unsolicited e-mails to CompuServe subscribers. The court rejected Cyber Promotions' argument that CompuServe was exercising powers that are traditionally the exclusive prerogative of the state.¹¹⁶

C. Defamation.

¶ 55

The Internet has made it cheap and easy to distribute potentially defamatory material to millions of people. There are several models for liability, depending on the nature of web sites. A web site may be a "publisher" of information, and therefore responsible for its editorial decisions and content. Sites such as CNN Interactive, the OPA and others mentioned in this article appear to fall into this category. A site may be a "distributor," which under traditional law is not liable for the material of others unless it knows or has reason to know of the defamatory character of the content. Finally, a site may be a common carrier, which acts solely as a transmitter of information and bears no liability for content. The majority of web sites probably would be characterized as publications because their creators exercise editorial control over their content.

¹¹⁰ Deborah Scoblionkov, *Washington Nabs a Spammer*, CNET NEWS.COM (Jul. 16, 1998) <<http://www.news.com/News/Item/0,4,24294,00.html>>.

¹¹¹ Janet Kornblum, *Settlement in First Antispam Law*, WIRED NEWS (Oct. 23, 1998) <<http://www.news.com/News/Item/0,4,24294,00.html>>; see also *Engst v. Knight*, No. 98-2-17831-1 (Wash. filed Jul. 17, 1998) <<http://www.tidbits.com/anti-spam/complaint.html>>.

¹¹² Courtney Macavinta, *Opposed Groups Agree on Antispam Strategy*, CNET NEWS.COM (Dec. 7, 1998) <<http://www.news.com/News/Item/0,4,29626,00.html>>.

¹¹³ *Id.*

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

¹¹⁵ *Id.* at 1027 (quoting *Tillman v. Distribution Sys. Of America*, 648 N.Y.S.2d 630, 635 (1996)).

¹¹⁶ *Id.* at 1025-27.

¶ 56 ISPs and web sites that host web forums are good examples of the distributor model, as most conduct at least a cursory editorial screening to keep vulgarity, obscenity, and extreme incivility off of their sites. In *Zeran v. America Online, Inc.*, the federal trial and appellate courts defined ISP liability in such cases.¹¹⁷ In the weeks following the bombing of the Alfred P. Murrah Federal Building in Oklahoma City, Oklahoma, anonymous individuals attached plaintiff Kenneth M. Zeran's name and telephone number to a series of AOL electronic "bulletin board" advertisements for T-shirts with slogans such as "Finally, a day care center that keeps the kids quiet—Oklahoma 1995." Zeran sued AOL for allowing these notices to remain and reappear on AOL's "bulletin board" despite his prompt complaints. Both the U.S. District Court in Virginia and the Fourth Circuit Court of Appeals ruled that AOL was not liable for postings on its bulletin boards—decisions which the Supreme Court refused to review. In their rulings, the courts cited a so-called "good Samaritan" provision of the Telecommunications Act of 1996, which directs that interactive computer services should not be "treated as the publisher or speaker" of content posted by a third party just because the provider takes voluntary, good-faith measures to remove obscene, lewd, harassing, or otherwise objectionable material.¹¹⁸

CONCLUSION

¶ 57 Government's role in regulating the Internet is both delicate and complex; too much regulation may stifle growth and innovation, while too little may make the medium an anarchic "wild west" too frightening for most Americans. The fact that no one is quite sure how the Internet will evolve makes this process even more difficult. In this context, the halting, often cautious government approach may be the most practical; as the problems which face the expanding Internet become clearer, legislative solutions will likewise become more adept at striking this crucial balance.

¹¹⁷ 958 F. Supp. 1124 (E.D. Va. Mar. 21, 1997), *aff'd*, 129 F.3d 327 (4th Cir. 1997), *cert. denied*, 118 S.Ct. 2341 (June 22, 1998).

¹¹⁸ The Supreme Court did not strike the good Samaritan provision when it declared unconstitutional several elements of the Telecommunication Act of 1996 in *Reno v. ACLU*, 521 U.S. 844, 117 S. Ct. 2329 (1997).

Note that the CDA and the court's interpretation overrule the earlier cases of *Cubby v. CompuServe*, 776 F. Supp. 135 (S.D.N.Y. 1991) (finding ISP liable for defamatory content if ISP monitors content and fails to remove defamatory material) and *Stratton Oakmount v. Prodigy Services Co.*, 23 Media L. Rep (BNA) 1794 (N.Y. Sup. Ct. 1995).