CATO INSTITUTE BRIEFING PAPERS

Internet Privacy and Self-Regulation
Lessons from the Porn Wars

by Tom W. Bell

No. 65 August 9, 2001

The availability and adequacy of technical remedies ought to play a crucial role in evaluating the propriety of state action with regard to both the inhibition of Internet pornography and the promotion of Internet privacy. Legislation that would have restricted Internet speech considered indecent or harmful to minors has already faced and failed that test. Several prominent organizations dedicated to preserving civil liberties argued successfully that self-help technologies offered less-restrictive means of achieving the purported ends of such legislation, rendering it unconstitutional. Surprisingly, those same organizations have of late joined the call for subjecting another kind of speech—speech by commercial entities about Internet users—to political regulation. With regard to privacy no less than pornography, however, self-help offers Internet users a less-restrictive means of preventing the alleged harms of free speech than does state action. Indeed, a review of privacy-protecting technologies shows them to work even more effectively than the filtering and blocking software used to combat online smut. Digital self-help in defense of Internet privacy makes regulation by state authorities not only constitutionally suspect but, from the more general point of view of policy, functionally inferior.

Tom W. Bell is an associate professor at the Chapman University School of Law and an adjunct scholar at the Cato Institute. For an earlier version of this paper, see "Pornography, Privacy, and Digital Self-Help," John Marshall Journal of Computer and Information Law *(forthcoming).*

The propriety of legislation affecting either pornography or privacy should depend crucially on the availability of alternative self-help remedies.

Introduction

Pornography tends to generate social stigma. Privacy tends to alleviate it. That the two frequently coexist reflects little more than the phenomenon of shame. Pornography and privacy share a more subtle relationship in Internet law and policy, however, because the propriety of legislation affecting either pornography or privacy should depend crucially on the availability of alternative self-help remedies, such as special software or communications services, that each individual can secure for him- or herself through technical rather than political means. Legislation that attempted to restrict Internet speech considered indecent or harmful to minors has already had to face that exacting test. This paper argues that proposals to regulate Internet privacy merit similar scrutiny.

The same points that have helped strike down statutory limits on Internet speech thought harmful to its readers (because it is indecent or harmful to minors) argue against enacting new statutory limits on speech thought harmful to its subjects (i.e., privacy legislation). In both cases, self-help offers Internet users a less-restrictive means of preventing the alleged harms caused by free speech than does legislation. In both cases, the alternative offered by digital self-help makes regulation by state authorities not only constitutionally suspect but, from the more general points of view of policy and effectiveness, functionally inferior.

Admittedly, that critique might strike some readers as distinctly unfashionable. Many and diverse voices have of late called for using political means to regulate speech by commercial entities about Internet users in the name of protecting privacy. That rising chorus includes the American Civil Liberties Union, the Electronic Privacy Information Center, and the Center for Democracy and Technology. Far from advancing the case for protecting Internet privacy through new regulations, however, those same three organizations have elsewhere advanced arguments that counsel against regulatory initiatives.

Indeed, the ACLU, EPIC, and CDT successfully fought legislative attempts to regulate indecent or harmful-to-minors speech on the Internet by arguing, in relevant part, that self-help offered a less-restrictive means of achieving the same ends. It turns out that self-help has an even greater edge over legislation when it comes to Internet privacy. Internet users can protect their privacy, and—following the arguments made by the ACLU, EPIC, and CDT—the ready availability of self-help alternatives casts constitutional doubt on legislation that would censor speech alleged to violate Internet users' privacy rights. Even apart from such purely legal questions, the efficacy of self-help renders such legislation suspect from a policy point of view.

Given the range of discussions taking place about Internet privacy, the relatively narrow scope of the present paper bears emphasis. It primarily concerns the legal impact that self-help remedies ought to have on legislation that would restrict speech by commercial entities about Internet users. More generally, but secondarily, it offers a policy-based critique of legislative proposals to regulate commercial activity that does not win First Amendment protection and that affects the privacy of Internet users, such as monitoring click streams or using persistent cookies. The relative merits of trying to protect Internet privacy through direct legislation, delegation of broad authority to an existing or new agency, or some other form of state action do not matter much for this analysis, which regards all such actions as susceptible to similar criticism. The discussion herein of the First Amendment, of course, concerns the U.S. legal system, though many of the observations about law and policy might well apply to other systems. This paper does not concern state action that threatens privacy rights, issues raised by international variation in privacy regulations, or esoteric questions about the relationship between privacy and conceptions of self. It does not discuss the prospect of censoring speech by noncommercial entities about

Internet users, solely because little risk of such regulation looms. If that sort of legislation surfaces, however, the arguments set forth here should for the most part prove applicable and, indeed, apply with even more force than when restricted to the defense of commercial entities.

The Demand for Internet Privacy

Judging by what they tell pollsters, Internet users worry a great deal about privacy. A Pew survey conducted from May 19 to June 21, 2000, found 54 percent of American Internet users "very concerned" that personal information about them or their families would find its way to businesses or strangers.[1] Perhaps unsurprisingly, 86 percent of those respondents favored an "opt-in" approach to Internet privacy, under which no Internet company would use such information unless expressly authorized to do so.[2] Similarly, a Harris poll taken in March 2000 found that 56 percent of respondents claimed they would, if given the choice, always opt out of providing Web sites with personal information.[3] Eighty-eight percent said that they would prefer every Web site to ask for permission before sharing their personal information with other parties.[4]

What Internet users actually do about privacy sends a distinctly different message from what they say, however. The Pew survey found that 64 percent of Internet users would provide personal information if necessary to access a Web site[5] and that only 24 percent of Internet users who know about cookies[6] have configured their Web browsers to reject them.[7] The Harris poll discovered that only 19 percent of Internet users make a habit of reading Web sites' privacy notices.[8] Studying deeds rather than words, moreover, reveals decreasing concern about Internet privacy. Harris found that over two years the percentage of Internet users who refuse to register at Web sites by offering personal information has dropped from 59 percent to 46 percent.[9] More recently, the Pew study put that figure at a mere 27 percent.[10]

Nonetheless, consistent with what they say when polled (rather than what they do online) many Internet users demand stronger laws protecting online privacy. Fifty-seven percent of respondents to the Harris poll agreed, "The government should pass laws now for how personal information can be collected and used on the Internet."[11] Three-quarters of those surveyed by ABC News said it should be illegal for companies to sell information about what consumers buy on the Internet.[12]

Those results hardly reflect balanced assessments of the costs and benefits of regulating speech about Internet users, of course. Many consumers would casually approve of abolishing credit reports, too, without reckoning the resulting impact on their access to credit cards or home mortgages. And the gap between words and deeds, not to mention the various other interpretation problems that plague polls,[13] suggests that no one should consume complaints about Internet privacy without a side order of salt. Nonetheless, surveys uncovering concern about Internet privacy appear to have encouraged regulators, politicians, and activists to take action.

Impressed by such polls and impatient with the slow pace of industry self-regulation, in May 2000 the Federal Trade Commission called for new legislation protecting the privacy of Internet users.[14] Congress has already taken under consideration such bills as the Consumer Internet Privacy Enhancement Act,[15] the Consumer Privacy Protection Act,[16] and the Consumer Internet Privacy Protection Act of 1999,[17] although none has yet to pass. President Bush would likely sign those kinds of protections into law.[18] He has signaled his support of legislation giving greater privacy protection to Internet users. Regulators and politicians can count on influential activist organizations to support the call for new laws protecting Internet privacy, including, most

What Internet users actually do about privacy sends a distinctly different message from what they say.

notably for present purposes, the ACLU, EPIC, and CDT. The ACLU has called for legislation to mandate, among other things, that personal information about Internet users never be collected or distributed without their knowledge and consent; that any organization collecting personally identifiable information from Internet users inform them why it is doing so; that organizations not reuse such information for any other purpose without a user's consent; and that every Internet user have the right to examine, copy and correct personal information.[19] EPIC has advocated regulations that would impose confidentiality obligations on Internet consumer data and limit the collection of personal data to "necessary" purposes.[20] CDT's staff counsel, Deirdre Mulligan, has testified to Congress that "we must adopt legislation that incorporates into law Fair Information Practices—long-accepted principles specifying that individuals should be able to 'determine for themselves when, how, and to what extent information about them is shared.'"[21]

That the ACLU, EPIC, and CDT have good intentions about protecting the privacy of Internet users should surprise no one. That they propose remedies that would regulate speech should perhaps raise eyebrows, however. The arguments that the ACLU, EPIC, and CDT once employed in defense of indecent or harmful-to-minors speech on the Internet also apply to the restrictions that they would now impose on another type of speech: speech by commercial entities about Internet users.

That the ACLU, EPIC, and CDT have good intentions about protecting the privacy of Internet users should surprise no one. That they propose remedies that would regulate speech should perhaps raise eyebrows.

Digital Self-Help versus Regulation of Pornographic Speech

The ACLU, EPIC, and CDT successfully challenged the constitutionality of legislation restricting Internet speech classified as indecent or harmful to minors by arguing that the availability of self-help alternatives disqualified such laws as the "least restrictive means" of regulating constitutionally protected speech.[22] Those organizations have leveled the same claim against the Communications Decency Act of 1996, the Child Online Protection Act,[23] and New Mexico's[24] and New York's[25] COPA-like state laws. This part describes the application in those cases of the argument that the availability of digital self-help made legislative restrictions on Internet speech unnecessary, excessive, and, thus, unconstitutional.

Let us start with the Communications Decency Act.[26] The ACLU and EPIC joined in arguing before the Supreme Court that the CDA unconstitutionally limited indecent speech on the Internet because private filtering options offered an alternative to a state prohibition on indecent Internet speech.[27] Contrary to the government's assertion that there existed no equally effective alternative to the CDA's criminal ban on indecent speech, the plaintiffs observed that the trial court had "found that the existing software affords parents a significant option for protecting children" and that the government itself had admitted to a growing and competitive market for self-help tools.[28] The plaintiffs also cited protections available through the major commercial online services and technical standards then under development that would facilitate user-based blocking of indecent Internet speech.[29]

The CDT, in its capacity as a member of the plaintiff Citizens' Internet Empowerment Coalition, backed a similar analysis in its Supreme Court brief, which cited the availability of blocking and filtering software as proof that the CDA was "unconstitutional because there are less restrictive measures Congress could have selected that would have been much more effective in preventing minors from gaining access to indecent online material."[30] The self-help arguments used by the ACLU, EPIC, and CDT apparently proved convincing; the Supreme Court struck down the CDA because it did not offer the least-restrictive means of achieving the government's goals.[31]

The ACLU and EPIC again joined forces in challenging COPA, a statute that by targeting speech harmful to minors, rather than all types of indecent speech, aimed to avoid the overbreadth that had rendered the CDA unconstitutional. As in their earlier attack on the CDA, the ACLU and EPIC argued that the availability of self-help alternatives demonstrated the Child Online Protection Act's unconstitutionality: "There are numerous less restrictive and more effective alternatives to COPA, including user-based filtering software, that parents may use if they wish to restrict what their children view."[32] Again, the argument succeeded. The trial court granted a preliminary injunction on enforcement of the statute, observing that "blocking or filtering technology may be at least as successful as COPA would be in restricting minors' access to harmful material online without imposing the burden on constitutionally protected speech that COPA imposes on adult users or Web site operators."[33]

Although the third circuit affirmed the injunction on COPA's enforcement on appeal, it expressed reservations about the self-help argument. It opined that the blocking and filtering technologies cited by the trial court "do not constitute government action, and we do not consider this to be a lesser restrictive means for the government to achieve its compelling interest."[34] As explanation, the appellate court offered no more than an unsupported claim that "the parental hand should not be looked to as a substitute for a congressional mandate."[35] That seems an unjustifiably narrow interpretation of the "least restrictive means" test, however. Congress can boast of no mandate to legislate in contravention of the First Amendment, after all, and the Supreme Court has made clear that the availability of superior private alternatives can strip lawmakers of legitimate power to restrict free speech.[36] To put the matter more generally and in economic terms, lawmakers must bear the burden of justifying their actions by proof of a salient and serious market failure. Under either analysis, a full inquiry into the "least restrictive means" of correcting a problem must consider effective self-help as an alternative to state action.

Perhaps the third circuit found it suggestive that in *ACLU v. Reno* the Supreme Court, when listing possible alternatives to the CDA, included only those involving state action.[37] That supposed limitation would hardly justify limiting inquiries under the "least restrictive means" test to government action, however, since context indicates that the Supreme Court meant only to scold the legislature for failing to pass a different "provision"—not to comment on the government's failure to consider self-help remedies.[38] So far as reading judicial tea leaves goes, the Third Circuit should have pondered why the Supreme Court stated for the record: "Systems have been developed to help parents control the material that may be available on a home computer with Internet access."[39] As if to answer that question, the Supreme Court had already explained *ACLU v. Reno* in terms that cast sharp doubt on the Third Circuit's refusal to regard self-help as an alternative to state action: "The mere possibility that user-based Internet screening software would 'soon be widely available' was relevant to our rejection of an overbroad restriction of indecent cyberspeech."[40]

The ACLU has also used the self-help argument in challenging state laws similar to COPA. As proof that a New Mexico statute[41] criminalizing the dissemination of Internet speech harmful to minors failed to represent the least restrictive means of effectuating the government's interest, the ACLU cited "many alternative means that are more effective at assisting parents in limiting a minor's access to certain material if desired."[42] The trial court granted a preliminary injunction on the statute's effectiveness, noting the existence of "a wide range of mechanisms that parents can use to prevent their children from accessing material online they do not want their children to view,"[43] and the Tenth Circuit affirmed.[44] The ACLU made the same argument in its complaint[45] against a New York law that criminalized Internet speech harmful

Lawmakers must bear the burden of justifying their actions by proof of a salient and serious market failure.

to minors.[46] Here, though, the trial court granted a preliminary injunction without addressing such First Amendment claims, basing its decision solely on grounds that the act interfered with interstate commerce.[47]

Self-Help versus Regulation of Commercial Speech

Digital self-help makes unnecessary state action limiting speech that is indecent or harmful to minors. The same argument applies to state action that would limit speech by commercial entities about Internet users. Digital self-help offers more hope of protecting Internet users' privacy than it does of effectively filtering out unwanted speech, and the availability of such self-help casts doubt on the constitutionality of legislation restricting speech by commercial entities about Internet users. From the more general point of view of policy, moreover, digital self-help offers a better approach to protecting Internet privacy than does state action.

Digital self-help makes unnecessary state action limiting speech that is indecent or harmful to minors. The same argument applies to state action that would limit speech by commercial entities about Internet users.

The Efficacy of Self-Help in Protecting Internet Privacy

Digital self-help offers what may be the only viable solution to protecting Internet privacy. Consider the many types of self-help already available. Internet users who worry about cookies can simply configure their browsers to reject them—a process that takes about 15 seconds.[48] Though that will cut off access to sites that admit only registered users, advanced self-help measures can both preserve access to such sites and bar offensive cookies. More cautious Internet users can download software like AdSubtract,[49] IDcide Privacy Companion,[50] *PC Magazine*'s CookieCop,[51] Siemens' WebWasher,[52] Internet Junkbuster,[53] or Guidescope,[54] all of which offer more precise control over cookies and all of which are free of charge. Privacy Companion, to pick one, distinguishes between cookies that give you access to a particular site's personalized services and cookies that advertisers might use to track your movements across the net.[55] Internet users who demand still more privacy can buy Freedom[56] software to browse the net under disguise of a pseudonym or subscribe to Anonymizer.com's[57] or or SafeWeb.com's services[58] to become completely invisible to online merchants. In sum, then, Internet users already enjoy a variety of cheap and effective tools for protecting privacy online.[59] If consumer demand reflects poll results, moreover, entrepreneurs will have ample incentives to create tools that protect Internet privacy even more cheaply and effectively.[60]

Such privacy-protecting services differ in one crucial regard from services that try to filter out offensive speech: they work better. Because meaning depends on context, filtering software has trouble distinguishing blue-footed and winged "boobies" from the human variety. More fundamentally, no one has yet figured out how to encode in software the difficult moral reasoning that responsible parents and teachers use to raise kids right. Privacy-protecting services tackle a comparatively simple technical problem. That they will not solve it perfectly matters little; they need only protect privacy better than political action can.[61] On that count, privacy-protecting services have a great edge over filtering software. The same "least restrictive means" test that applies to other types of constitutionally protected speech also applies to speech by commercial entities about Internet consumers and ought to apply with even greater force.

The Constitutionality of Regulating Commercial Entities' Speech about Internet Users

But should state action regulating speech by commercial entities about Internet consumers have to pass the "least restrictive means" test? Does such speech qualify, in other words, for the same level of constitutional protection afforded to indecent and harmful-to-minors speech? In brief: maybe it does, but that probably does not matter. Although an exhaustive answer would exceed the bounds of the present paper[62] and would

lack the guide of controlling case law,[63] this section offers a quick explanation of that conclusion.

Speech by commercial entities about Internet consumers might well qualify for protection under the "least restrictive means" test, which courts apply when strictly scrutinizing restrictions on ordinary speech—or for that matter, speech that is indecent or harmful to minors.[64] At a minimum, though, such speech would almost certainly qualify as commercial speech,[65] which is generally protected from any regulation that is "more extensive than is necessary" to serve the government's alleged interest.[66] If a regulation on commercial speech constitutes a blanket ban on truthful statements, however—a description that might well apply to extreme restrictions on speech by commercial entities about Internet consumers—the "least restrictive means" test would come back into play.[67]

State action restricting speech within or by commercial entities about Internet users looks constitutionally suspect even under the more lax test generally applicable to commercial speech. By way of distinguishing it from the more demanding "least restrictive means" test, the Tenth Circuit recently explained that in applying the "more extensive than is necessary" test:

> We do not require the government to consider every conceivable means that may restrict less speech and strike down regulations when any less restrictive means would sufficiently serve the state interest. We merely recognize the reality that the existence of an obvious and substantially less restrictive means for advancing the desired government objective indicates a lack of narrow tailoring.[68]

The large and growing number of self-help alternatives for protecting Internet privacy certainly qualifies them as obvious. Furthermore, although the ultimate determination must turn on the facts, the efficiency of existing self-help protections probably already qualifies them as less restrictive than any of the various current proposals to regulate speech by commercial entities about Internet users.

Self-Help and Public Policy in Protecting Internet Privacy

Even apart from such constitutional questions, the availability of so many efficacious means of protecting Internet privacy through self-help suggests that legislation toward the same end could not tout curing market failure as a justification.[69] Whether a great many Internet users avail themselves of such self-help measures has little bearing on that point, of course.[70] Notwithstanding talk to the contrary, actions may reveal Internet users quite willing to trade personal privacy for access to Web sites.[71] As no one has a vested right to access another's private Web site, that quid pro quo should raise no outcry. It matters most that Internet users have a realistic choice between preserving and sacrificing their privacy.[72] Judging by what they tell pollsters, moreover, an overwhelming majority of Americans think that Internet users—not government or industry—should bear the primary responsibility for exercising that choice.[73]

Legislation protecting Internet privacy offers little benefit. Moreover, the potential costs of such legislation are high. The Children's Online Privacy Protection Act of 1998[74] does not give much encouragement on that count, as it has increased legal uncertainty,[75] raised the expense of providing online services,[76] and even forced some companies out of the market for young Internet users.[77] A more comprehensive statute, covering not just the privacy of children but also that of adults, might well generate more comprehensive problems.

The prospect of having government agencies enforce such a statute should not engender much optimism. Notwithstanding federal law[78] and a specific White House edict to the contrary,[79] federal agencies have largely failed to implement privacy protections on

An overwhelming majority of Americans think that Internet users—not government or industry—should bear the primary responsibility for exercising choice.

State and federal Web sites routinely fall short of the same privacy-protection standards that activists would have government impose on private actors.

their own Web sites.[80] A privacy audit by the General Accounting Office found that the privacy policies of only 46 of the 70 federal agencies it surveyed fulfilled applicable requirements.[81] More generally, a recent study showed that state and federal Web sites routinely fall short of the same privacy-protection standards that activists would have government impose on private actors.[82] Though one might argue that government agents quite naturally enforce privacy laws less vigorously against themselves than against other citizens,[83] somehow that excuse does not give much comfort.

As a matter of public policy as well as constitutional law, politicians should invoke state power only to correct manifest failures of market and other nonpolitical mechanisms to alleviate serious national problems. Even then, lawmakers should do so only if the all-too-likely risks of government failure do not threaten to cancel out the putative gains of state action.[84] The benefits, in brief, must outweigh the costs. Proposals to pass laws protecting Internet users' privacy merit skepticism.[85]

Conclusion

The availability of speech-filtering programs has already powerfully affected responses to Internet pornography. The advent of tools such as cookie-control software and anonymizing networks now presents a similar challenge to the law and policy on Internet privacy. In each case, the availability of self-help alternatives renders state action suspect on constitutional and policy grounds. The same activist organizations that argue against legislation restricting Internet speech that is indecent or harmful to minors should reconsider their demands for privacy legislation that would restrict speech by commercial entities about Internet users. Politicians and regulators should likewise question the wisdom of trying to mandate privacy protections that Internet users can easily obtain on their own.

This paper began by noting that pornography and privacy share bonds based in shame: what the former heightens, the latter lessens. It has argued that Internet law and policy should take account of a more significant relationship between pornography and privacy, one based in the common role that digital self-help should play in evaluating state action directed toward either of them. Even under that analysis, however, one might well conclude that shame still bonds Internet pornography and Internet privacy. For it would indeed prove a shame, with regard to either, if lawmakers ignored the alternatives offered by digital self-help and instead enacted unconstitutional, unnecessary, and unjustified regulations.

Notes

1. Susannah Fox, *Trust and Privacy Online: Why Americans Want to Rewrite the Rules,* Pew Internet & American Life Project, 2000, http://www.pewinternet.org/reports/toc.asp?Report=19.

2. Ibid.

3. "Harris Poll: A Growing Threat," *Business Week Online,* March 20, 2000, http://www.businessweek.com/2000/00_12/b3673010.htm. The story reports results of a Harris Interactive telephone survey of 1,014 adults—presumably from the United States—between March 2 and March 6, 2000. The story does not specify the poll's margin of error.

4. Ibid.

5. Fox, p. 6.

6. A cookie is a "message given to a Web browser by a Web server. The browser stores the message in a text file called cookie.txt. The message is then sent back to the server each time the browser requests a page from the server." *Webopedia,* http://webopedia.internet.com/TERM/c/cookie.html.

7. Fox, p. 8.

8. "Harris Poll," p. 2. This figure comes from multiplying the 55 percent of respondents who said they had "seen a privacy notice or other explanation of how personal information collected by that site will be used" by the 35 percent who responded "always" to the question, "If you have

seen a privacy notice, how often do you read the information contained in the privacy notice?"

9. Ibid., p. 9.

10. Fox, p. 9. This figure comes from multiplying the 45 percent of Internet users who have not provided real personal information to a site by the 61 percent of that group who report that they categorically refuse to offer that information.

11. "Harris Poll," p. 16.

12. Daniel Merkle, "Internet Invasion," *ABCNews.com*, February 3, 2000, http://www.abcnews.go.com/onair/DailyNews/poll000203.html. The survey was conducted by telephone from January 21 to January 26, 2000, among a random national sample of 1,006 adults, by International Communications Research of Media, and had a three-point margin of error.

13. Consider how poor questions give poor results. Pew pollsters predictably discovered that only 15 percent of Americans described themselves as "not too" or "not at all" concerned about businesses or strangers obtaining personal information about them or their families. Fox, p. 22. An ABC News poll taken last January pressed respondents to give an objective description of their everyday concerns, however, and found that 57 percent of respondents admitted that they "don't spend much time worrying that computers and other types of technology are being used to invade their privacy." See also Merkle.

14. Federal Trade Commission, "Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress," May 2000, pp. 36–38, http://www.ftc.gov/reports/privacy2000/privacy2000.pdf. The majority report did not discuss consumer self-help, though Commissioner Orson Swindle, dissenting, did (p. 65).

15. S. Res. 2928, 106th Cong. §2(a) (2000) (requiring commercial Web sites to give notice before collecting personally identifiable information and allowing the subjects of that information to forbid its use for marketing purposes or its distribution to third parties).

16. S. Res. 2606, 106th Cong. §102 (2000) (requiring service providers and commercial Web sites to give notice and obtain consent before collecting, using, or disclosing personally identifiable information and giving the subjects of that information the right to review and correct it).

17. H.R. Res. 313, 106th Cong. §2(a)(1) (1999) (imposing on interactive service providers a duty with regard to personally identifiable information to obtain the subject's consent before transferring the information to a third party and giving subjects the right to review and correct such information).

18. Lisa M. Bowman, "ZDNN Q&A with George W. Bush," *ZDNet News,* June 21, 2000, http://www.zdnet.com/zdnn/stories/bursts/0,7407,2591588,00.html. ZD: "Should the government legislate online privacy?" GWB: "I think there ought to be laws here that say a company cannot use my information without my permission to do so."

19. American Civil Liberties Union, Comments to Office of International Affairs, National Telecommunications and Information Administration, Re: Elements of Effective Self-Regulation for the Protection of Privacy and Questions Related to Online Privacy, 2000, §4, http://www.aclu.org/congress/l00698a.html.

20. Electronic Privacy Information Center, "Need for Enforceable Privacy Codes," in Comments of Electronic Privacy Information Center before the FTC in re Public Workshop on Consumer Information Privacy Incorporating: Data Base Study, April 15, 1997, http://www.epic.org/privacy/internet/ftc/epic_comments_497.html. See also Comments of Andrew Shen on behalf of EPIC in re Online Profiling Project, P994809/Docket No. 990811219-9219, http://www.ftc.gov/bcp/profiling/comments/shen.htm (calling for regulation of online profiling).

21. Deirdre Mulligan, Prepared statement before the Subcommittee on Courts and Intellectual Property of the House Committee on the Judiciary, Oversight Hearing on Privacy and Electronic Communications, May 18, 2000, http://www.cdt.org/testimony/000518mulligan.shtml.

22. *Sable Communications, Inc., v. FCC,* 492 U.S. 115, 126 (1989) (explaining that government must also show that it has a compelling interest to regulate such speech).

23. 47 U.S.C.S. § 231 (Lexis Supp. 2000).

24. N.M. Stat. Ann. § 30-37-3.2(A) (2000) (criminalizing the dissemination by computer of material harmful to minors).

25. N.Y. Penal § 235.21(3) (Consol.1999).

26. 47 U.S.C.S. § 223 (Lexis Supp. 2000).

27. Brief for appellees at II.B.2, *American Civil Liberties Union v. Reno,* 521 U.S. 844 (1997). Both the ACLU and EPIC were named parties to the litigation and signed the brief.

28. Ibid.

29. Ibid.

30. Brief for appellee, CEIC at III.C., *American Civil Liberties Union v. Reno,* 521 U.S. 844.

31. *American Civil Liberties Union v. Reno,* 521 U.S. 844.

32. Brief of plaintiffs-appellees, ACLU, EPIC, et al. at Summary of Argument, *American Civil Liberties Union v. Reno* , Case No. 99-1324 (3rd Cir. 1999), http://www.aclu.org/court/acluvrenoii_motion.html. See also ibid., § V.C. (citations omitted):

> COPA is not the least restrictive means of achieving defendant's asserted interest. The record showed that many alternative means are more effective at assisting parents in limiting minors' access to certain material if desired. Commercial online services like America Online and Prodigy Internet provide features to prevent children from accessing chat rooms and to block access to Web sites and discussion groups based on keywords, subject matter, or specific discussion groups. Online users can also purchase special software applications, known as user-based blocking programs, that block access to certain resources, prevent children from giving personal information to strangers by e-mail or in chat rooms, and keep a log of all online activity that occurs on the home computer. User-based blocking programs are not perfect, both because they fail to screen all inappropriate material and because they block valuable Web sites. However, a voluntary decision by concerned parents to use these products for their children constitutes a far less restrictive alternative than COPA's imposition of criminal penalties for protected speech among adults.

33. *American Civil Liberties Union v. Reno,* 31 F. Supp.2d, pp. 473, 497 (E.D. Pa. 1999), affirmed, 217 F.3d 162 (3rd Cir. 2000).

34. *American Civil Liberties Union v. Reno,* 217 F.3d, p. 171 (3rd Cir. 2000).

35. Ibid., p. 181.

36. See *Consolidated Edison Co. of New York v. Public Service Commission of New York,* 447 U.S. 530, 542 (1980) (holding unconstitutional a ban on utility bill inserts on grounds that customers "may escape exposure to objectionable material simply by transferring the bill insert from envelope to wastebasket."); *Erznoznik v. Jacksonville,* 422 U.S. 205, 210–11 (1975) (striking down as unconstitutional an ordinance prohibiting indecent drive-in movies on grounds that passers-by must bear the burden of looking away); *Cohen v. California,* 403 U.S. 15, 21 (1971) (reversing as unconstitutional a conviction based on public display of "Fuck the Draft" on grounds that offended parties "could effectively avoid further bombardment of their sensibilities simply by averting their eyes"). The Court has extended similar protection even to commercial speech. See *Bolger v. Youngs Drug Products Corporation,* 463 U.S. 60, 73–74 (1983) (holding ban on offensive mail unconstitutional on grounds that parents could effectively limit children's access to it).

37. *Reno v. American Civil Liberties Union,* 521 U.S. 844, 879 (stating that less restrictive alternatives included "requiring that indecent material be 'tagged' in a way that facilitates parental control of material coming into their homes, making exceptions for messages with artistic or educational value, providing some tolerance for parental choice, and regulating some portions of the Internet—such as commercial Web sites—differently than others, such as chat rooms"). But see Malla A. Pollack, "Opt-in Government: Using the Internet to Empower Choice—Privacy Application," *Catholic University Law Review* 52 (forthcoming)(proposing that were the Supreme Court to revisit that list, it might now add Professor Pollack's suggestion: "The Federal government should set up a private zone on the Internet by setting up a search engine which will link only to sites providing the highest level of privacy").

38. *Reno,* 521 U.S., p. 879.

39. Ibid., pp. 854–55.

40. *U.S. v. Playboy Entertainment Group,* 529 U.S. 803, 120 S. Ct. 1887, quoting *Reno,* 521 U.S., pp. 876–77.

41. N.M. Stat. Ann.

42. Complaint for Declaratory and Injunctive Relief, ¶ 91; see also *ACLU v. Johnson,* 4 F. Supp. 2d 1024 (D.N.M. 1998)(2000), http://www.aclu.org/court/acluvjohnson_complaint.html.

43. Ibid., p. 1033.

44. Ibid.

45. Complaint for Declaratory and Injunctive Relief, *American Library Ass'n v. Pataki,* 969 F. Supp. 160, 183 (S.D.N.Y. 1997), http://www.aclu.org/court/nycdacomplaint.html (arguing, inter alia, that software filters provide a less restrictive alternative to New York statute forbidding Internet speech harmful to children). The ACLU was a plaintiff in the case.

46. N.Y. Penal Laws § 235.21(3) (Consol. 1999).

47. *Pataki,* pp, 183–84.

48. See "Stopping Cookies in IE3 + Netscape," http://www.cookiecentral.com/stopcm.htm (describing how to configure a variety of browsers so as to reject cookies); see also David Whalen, "The Unofficial Cookie FAQ," http://www.cookiecentral.com/faq; and "How Web Servers' Cookies Threaten Your Privacy," http://www.junkbusters.com/ht/en/cookies.html.

49. AdSubtract, "We Subtract the Ads!" http://www.adsubtract.com. Individual consumers can download and use AdSubtract SE free of charge or pay $29.95 for AdSubtract Pro. Both versions block ads and cookies.

50. "Get the Idcide Privacy Companion," http://www.idcide.com/html/Support/faq.htm. Privacy Companion blocks persistent cookies, in particular those that go to external sites, and costs nothing to download and use.

51. Mark Sweeny, "Accept Cookies by Site," *PC Magazine,* February 1, 2000, http://www.zdnet.com/pcmag/stories/solutions/0,8224,2430351,00.htm. CookieCop version 1.2 filters cookies by site and can be downloaded and used free of charge.

52. WebWasher, "Welcome to WebWasher," http://www.webwasher.com. WebWasher is available for home and educational use free of charge. It filters both cookies and ads—including, in particular, Web bugs.

53. Junkbusters, "Bust the Junk out of Your Web Browsing," http://www.junkbusters.com/ht/en/ijb.html (offering free download of Internet Junkbuster and claiming that the software stops unauthorized cookies and prevents the disclosure of other information about browsing behavior).

54. Guidescope, "Take Control of the Web: Surf Faster, Safer and Easier" http://www.guidescope.com/home. Guidescope blocks ads, Web bugs, and referrer information, thereby protecting its users against distribution of certain types of information about their browsing activities. Individual consumers can download and use Guidescope free of charge.

55. Idcide, "Get the Idcide," http://www.idcide.com/html/Support/faq.htm. In its "medium privacy" mode, Privacy Companion allows you to receive personalized services from the site you are visiting while blocking tracking by external sites. IDcide's patent-pending technology is designed to distinguish between persistent cookies sent to the site you are visiting and persistent cookies that are sent to external sites. The medium privacy protection mode prevents the external cookies from being set while allowing the site you are visiting to set cookies.

56. Freedom Internet Privacy and Security Software, "How Freedom Works," http://www.freedom.net/info/how.html (describes how Freedom software uses encryption and a private network to allow users to browse the Web using untraceable online pseudonyms). Freedom software costs $49.95.

57. Anonymizer.com, "Online Privacy Services," http://www.anonymizer.com/services/paidSurf.html (explains that the Anonymizer service provides anonymous surfing and "safe cookies" to protect user's privacy). Anonymizer allows unlimited free use of its service, albeit of a less functional version than the premium service enjoyed by customers paying $5 per month.

58 SafeWeb, http://www.safeweb.com (explains that the SafeWeb service provides anonymous surfing and protection from "profiling" cookies). SafeWeb allows unlimited free use of its service.

59. U.S. Senate Judiciary Committee, "Know the Rules Use the Tools—Privacy in the Digital Age: A Resource for Internet Users," 2000, pp. 10–21, http://judiciary.senate.gov/privacy.htm (catalogs various self-help technologies for protecting privacy); see also Fox p. 10 (reporting survey results on Internet privacy). Although the present survey has emphasized digital tools, those tools do not exhaust the range of self-help methods for protecting Internet privacy. People sorely worried about their privacy on the Internet could of course simply stop using it. Less drastically, and probably more commonly, they might lie about personal information when asked by a Web site to register. Pew pollsters found that 24 percent of Internet users reported having given false personal information to a Web site. See Randy Cohen, "The Ethicist," *New York Times Magazine,* June 4, 2000 (gives amusing advice on how to ameliorate the apparent immorality of that self-help method by typing in your protest: "'This question is intrusive.' You'll gain access to the site, and the proprietor will understand your objection and have a chance to change his ways"). See Plaintiff's Second Amended Verified Original Petition and Application for Temporary Restraining Order and Temporary Injunction, *Universal Image Inc. v. Yahoo, Inc.,* No. 99-13839-A18, 20 (County Ct., Dallas County, Tex., filed Jan. 18, 2000), http://legal.web.aol.com/decisions/dlpriv/univtro2.pdf. To judge from one somewhat extraordinary complaint, Internet users aggravated that Web sites use cookies could even bring suit for trespass, theft, and criminal stalking.

60. But see Ann Bartow, "Our Data, Ourselves: Privacy, Propertization, and Gender," *University of San Francisco Law Review* 34 (2000): 679 (states that average Web users might be able to implement some types of self-help but worries that Web sites will condition access on receipt of private information); Prepared Remarks of Debra A. Valentine, general counsel of the FTC, *Computer and High Technology Law Journal 16* (2000): 417 (complains that such "self-help requires considerable consumer education and sophistication and may well fail to protect consumers against surreptitious privacy invasions or identity theft").

61. See *Playboy,* p. 1892. ("It is no response that voluntary blocking requires a consumer to take action, or may be inconvenient, or may not go perfectly every time").

62. See generally, Eugene Volokh, "Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking about You," *Stanford Law Review* 52 (2000): 1049 (provides a more complete application of First Amendment principles to proposed information privacy); see also Julie A. Cohen, "Examined Lives: Information Privacy and the Subject as Object," *Stanford Law Review* 52 (2000): 1409–23 (discussing First Amendment as it relates to data privacy); and Solveig Singleton, "Privacy as Censorship: A Skeptical View of Proposals to Regulate Privacy in the Private Sector," Cato Institute Policy Analysis no. 295, January 22, 1998, http://www.cato.org/pubs/pas/pa-295.html.

63. A. Michael Froomkin, "The Death of Privacy?" *Stanford Law Review* 52 (2000): 1521 (states that government's ability to regulate privately generated speech relating to commerce is surprisingly unlitigated).

64. Volokh, pp. 1080–84 (discussing the commercial speech doctrine). But see Cohen, p. 1418 (stating that the "accumulation, use, and market exchange of personally identifiable data . . . aren't really 'speech' at all"). Cohen admits, however, that extant case law has treated such acts as commercial speech (p. 1410).

65. See generally, *U.S. West, Inc. v. FCC,* 182 F.3d 1224 (10th Cir. 1999), cert den sub nom; and *Competition Policy Inst. v. U S West, Inc.*, 120 S. Ct. 2215 (2000) (treating speech within or by commercial entities and about telephone users as commercial speech).

66. *Central Hudson Gas & Electric Corp. v. Public Service Commission of New York*, 447 U.S. 557, 566 (1980).

67. *44 Liquormart, Inc. v. Rhode Island,* 517 U.S. 484, 507–08 (1996).

68. *U.S. West,* p. 1238. But see *Trans Union Corp. v. FTC,* 2001 U.S. App. LEXIS 6241, *22-*23 (D.C. Cir. 2001) (No. 00-1141) (denying petition to review FTC determination that Fair Credit Reporting Act barred sale of names and addresses for target marketing purposes). *Trans Union* stands on shaky ground. The court stretched *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.,* 472 U.S. 749 (1985)—a case concerning injurious falsehoods—to find that the target marketing lists in question warranted "reduced constitutional protection." *Trans Union,* 2001 LEXIS at *23, quoting *Dun & Bradstreet,* p. 762, n. 8. Notably, only three justices signed on to that portion of *Dun & Bradstreet,* and even they emphasized that they did not intend to "leave all credit reporting subject to reduced First Amendment protection."

69. Fred H. Cate, "Privacy and Telecommunications," *Wake Forest Law Review* 33 (1998): 47 ("The most effective protection for information privacy is individual responsibility and action.").

70. But see Froomkin, pp. 1502–06 (arguing that because consumers suffer from privacy myopia, they sell their data too often and too cheaply). Citing a dearth of empirical data, Froomkin admits to assuming a consumer's aggravation over others' profiles of him will outweigh the aggregate value of the goods and services won by his various small sacrifices of personal information. Here, as with other markets, however, why would their revealed preferences not tell us all we need to know about what consumers, as a class, really want?

71. John Schwartz, "'Opting-in': A Privacy Paradox," *Washington Post,* September 3, 2000, p. H1 (describing LifeMinders Inc., a service that has persuaded 18 million Internet users to offer it personal information such as the birth dates of their family and friends, the vehicles they drive, and the names of their pets, which information it openly resells to third parties, all in return for receiving reminders of upcoming events, pet care tips, targeted advertising, and so forth).

72. Cohen, pp. 1393–96 (critiquing the legitimacy of choice in nonpolitical contexts about personal privacy).

73. Fox, p. 28. When Pew pollsters asked, "Who should have the MOST say over how Internet companies track people's activities online and use personal information?" 68 percent of respondents replied "People who use Web sites." Only 19 percent of respondents chose the federal government and only 6 percent chose Internet companies.

74. 15 U.S.C.A. §6502 (West 2000).

75. Lynne Burke, "Contending with COPPA Confusion," *Wired News,* August 23, 2000, http://

www.wired.com/news/politics/0,1283,38332,00.html (quoting Alex Bentacur, vice president of girl's clothing site 100percentgirls.com, "The law, which we support completely, is so unclear").

76. Carolyn Duffy Marsan, "Net Privacy Law Costs a Bundle," *CNN.com,* May 16, 2000, http://www.cnn.com/2000/TECH/computing/05/16/privacy.bill.idg/index.htm (relating high costs of complying with COPPA and effects on market).

77. Tamara Loomis, "Lawyers Wrestle with Online Privacy," *New York Law Journal,* July 13, 2000, http://www.nylj.com/stories/00/07/071300a4.htm (relating that some companies have left the market rather than incur costs of complying with COPPA).

78. 5 U.S.C.A. § 552a (West 2000) (specifying limits on power of federal agencies to collect and use information about individuals); see also Marc Rotenberg, "Letter to Congressional Leaders Outlines Risks of Web Tracking Technologies," June 22, 2000, http://www.epic.org/privacy/internet/cookiegate_pr.html (suggesting that use of cookies by federal agencies violates Privacy Act).

79. Jacob J. Lew, Memorandum for the Heads of Executive Departments and Agencies, Re: Privacy Policies and Data Collection on Federal Web Sites , June 22, 2000, http://www.whitehouse.gov/omb/memoranda/m00-13.html (forbidding use of cookies by federal Web sites absent clear and conspicuous notice, compelling need to gather data, appropriate and publicly disclosed privacy safeguards for handling collected information, and personal approval by agency head).

80. Declan McCullagh, "Feds' Hands Caught in Cookie Jar," *Wired News,* June 30, 2000, http://www.wired.com/news/politics/0,1283,37314,00.html (reporting dozens of federal Web sites continued to violate the White House's privacy directive by continuing to use "cookies" on their Web sites).

81. U.S. General Accounting Office, "Internet Privacy: Agencies' Efforts to Implement OMB's Privacy Policy," 11 (GAO/GGD-00-191) September 2000, http://www.gao.gov/new.items/gg00191.pdf (assessing conformity with Office of Management and Budget requirements). It has also been reported that nearly half of federal Web sites collecting personal information failed to post privacy policies, thereby arguably violating OMB requirements. .

82. See Darrell West, "Assessing E-Government: The Internet, Democracy, and Service Delivery by State and Federal Governments," September 2000, http://www.brown.edu/Departments/Taubman_Center/polreports/egovtreport00.html (reporting that of 1,716 state government sites, 36 federal sites, and 61 federal court sites, only 5 percent had a security policy and only 7 percent a privacy policy).

83. McCullagh (quoting Erick Gustafson, director of technology policy at Citizens for a Sound Economy, on failure of federal agencies to follow White House directives and Privacy Act of 1974). ("It's typical. Governments think the rules don't apply to them. They're historically the worst offenders of privacy and the rights of citizens.")

84. Pollack (describing the inefficiencies inherent in government regulation).

85. Fred H. Cate, "Principles of Internet Privacy," *Connecticut Law Review* 32 (2000): 889–91 (enunciating reasons for preferring private, market-based solutions to Internet privacy).

Published by the Cato Institute, Cato Briefing Papers is a regular series evaluating government policies and offering proposals for reform. Nothing in Cato Briefing Papers should be construed as necessarily reflecting the views of the Cato Institute or as an attempt to aid or hinder the passage of any bill before Congress. Additional copies of Cato Briefing Papers are $2.00 each ($1.00 in bulk). To order, or for a complete listing of available studies, write the Cato Institute, 1000 Massachusetts Avenue, N.W., Washington, D.C. 20001, call (202) 842-0200 or fax (202) 842-3490. Contact the Cato Institute for reprint permission.