
Tom W. Bell

Follow this and additional works at: http://repository.jmls.edu/jitpl

Part of the Computer Law Commons, Internet Law Commons, Privacy Law Commons, and the Science and Technology Law Commons

Recommended Citation

http://repository.jmls.edu/jitpl/vol19/iss1/6

This Article is brought to you for free and open access by The John Marshall Institutional Repository. It has been accepted for inclusion in The John Marshall Journal of Information Technology & Privacy Law by an authorized administrator of The John Marshall Institutional Repository.
PORNOGRAPHY, PRIVACY, AND DIGITAL SELF HELP

by Tom W. Bell†

I. INTRODUCTION

Pornography tends to generate social stigma. Privacy tends to alleviate it. That the two frequently co-exist thus reflects little more than the economics 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. 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 arguments that have helped to strike down statutory limits on Internet speech thought harmful to its readers (because indecent or harmful to minors) argue against enacting new statutory limits on speech thought harmful to its subjects (because within or by commercial entities and about Internet users). In both cases, self help offers Internet users a less restrictive means of preventing the alleged harms caused by free speech than legislation does. In both cases, the alternative offered by digital self help makes regulation by state authorities not only constitutionally suspect but also, from the more general point of view of policy, 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 within or by commercial entities and about Internet users. Part II describes that rising chorus, noting in particular that its ranks include the American Civil Liberties Union ("ACLU"), the Electronic Privacy Information Center ("EPIC"), and the Center for Democracy and Technology ("CDT"). Far from advancing the case for protecting Internet privacy through new po-

† Visiting Professor, University of San Diego School of Law (‘00-‘01), Associate Professor, Chapman University School of Law. © 2000 Tom W. Bell. All rights reserved. I thank Marc Rotenberg and Jerry Kang for commenting on an early formulation of my argument, and Lee A. Hollaar for commenting on a later one, but take sole responsibility for this article as submitted for publication.
political initiatives, however, those same three organizations have elsewhere advanced arguments that counsel against it. As Part III relates, 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. Part IV summarizes the various ways in which Internet users can protect their privacy and—following the example set by the ACLU, EPIC, and CDT—argues that 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 extant volume of speech 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 within or by commercial entities and about Internet users. More generally, but secondarily, it offers a policy-based critique of legislative proposals to regulate non-speech acts of commercial entities that affect the privacy of Internet users. The relative merits of trying to protect Internet privacy via 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; it regards all as susceptible to similar criticism. The paper's discussion of the First Amendment of course concerns the U.S. legal system, though many of its observations about law and policy might well apply to other legal systems. This paper does not concern state action that threatens privacy rights, nor issues raised by international variation in privacy regulations, nor esoteric questions about the relationship between privacy and conceptions of self. It does not discuss the prospect of censoring speech within or 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.

II. THE HUE AND CRY FOR POLITICAL PROTECTION OF INTERNET USERS' PRIVACY

To judge from 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% of American Internet users "very concerned" that personal information about them or their families would find its way to
businesses or strangers. Perhaps unsurprisingly, 86% 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. Similarly, a Harris poll taken last March found that 56% of respondents claimed they would, if given the choice, always opt-out of providing Web sites with personal information. Eighty-eight percent said that they would prefer every Web site to ask for permission before sharing their personal information with other parties.

What Internet users actually do about privacy sends a distinctly different message from what they say, however. The Pew survey found that 64% of Internet users would provide personal information if necessary to access a Web site and that only 24% of Internet users who know about cookies have configured their Web browsers to reject them. The Harris poll discovered that only 19% of Internet users make a habit of reading Web sites' privacy notices. Studying deeds rather than words moreover reveals decreasing concern about Internet privacy. Harris found that over the last 2 years the percentage of Internet users who refuse to register at Web sites by offering personal information has dropped from 59% to 46%. More recently, the Pew study put that figure at a mere 27%.

Nonetheless, consistent with what they say when polled (rather than what they actually do when 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 In-
ternet.” Three-fourths of those surveyed by ABC News said it should be illegal for companies to sell information about what consumers buy on the Internet.

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. And the gap between words and deeds, not to mention the various other epistemic problems that plague polls, 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, the Federal Trade Commission called last May for new legislation protecting the privacy of Internet users. Congress has already taken under consideration such bills as the Consumer Internet Privacy Enhancement Act, the Consumer Privacy Protection Act, and the Consumer Internet Privacy Protection Act of 1999. Should he get the opportunity to do so, the next president would likely sign those


12. Consider, for instance, how poor questions give poor results. Pew pollsters predictably discovered that only 15% 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, supra n. 1, at 22. An ABC News poll taken last January pressed respondents to give an objective description of their everyday concerns, however, and found that 57% 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, supra n. 11, at ¶ 7.


14. Sen. 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).

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

16. H.R. Res. 313, 106th Cong. § 102 (1999) (imposing on interactive service providers a duty with regard to a personally identifiable information of obtaining the subject's affirm-
sort of protections into law; both Al Gore and George W. Bush have come out in 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 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 and that it not reuse such information for any other purpose absent a user's affirmative consent, and that every Internet user have the right to examine, copy, and correct personal information about him or her. EPIC has advocated regulations that would impose confidentiality obligations on Internet consumer data and limit the collection of personal data to "necessary" purposes. 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

17. See William Safire, Stop Cookie-Pushers, N.Y. Times, A27 (June 15, 2000) (reporting that Al Gore, when asked by editors of New York Times whether he supported legislation protecting Internet privacy, replied, "I don't think an unfair burden should be placed on the users of the Internet to affirmatively go out and protect their own privacy [and] I think there should be procedures commonly accepted which protect them more or less automatically unless they the Internet users take affirmative steps to surrender their privacy.").


19. ACLU, 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, Section IV <http://www.aclu.org/congress/1070698a.html> (July 6, 1998).

shared."  

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 within or by commercial entities and about Internet users.

III. HOW DIGITAL SELF HELP ARGUED AGAINST REGULATION OF INDECENT OR HARMFUL-TO-MINORS SPEECH

The ACLU, EPIC, and CDT have successfully challenged the constitutionality of legislation restricting Internet speech classified as indecent or harmful-to-minors by arguing, *inter alia*, that the availability of self-help alternatives disqualified each such law as the least restrictive means of regulating constitutionally protected speech. They have leveled that claim against the Communications Decency Act of 1996 ("CDA"), the Child Online Protection Act ("COPA"), and New Mexico's and New York's 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.

We start with the CDA. 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. 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


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


27. *Brief for Appellee, CEIC at II.B.3, ACLU v. Reno*, 521 U.S. 844 (1997) <http://www.aclu.org/court/renovaclu.html> (accessed Sept. 27, 2000). Both the ACLU and EPIC were named parties to the litigation and signed the brief. *Id.*
software affords parents a significant option for protecting children,” and
the government itself had admitted to a growing and effective 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’ In-
ternet 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 re-
strictive measures Congress could have selected that would have been
much more effective in preventing minors from gaining access to inde-
cent online material.”30 The self-help arguments employed 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 demon-
strated COPA’s unconstitutionality. “There are numerous less restric-
tive 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

28. Id.
29. Id.
32. Brief Of Plaintiffs-Appellees, ACLU, EPIC, et. al at Summary of Argument, ACLU
www.aclu.org/court/acluvrenoiimotion.html>). See also id. at 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 pre-
vent children from accessing chat rooms and to block access to Web sites and dis-
cussion 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 pro-
grams are not perfect, both because they fail to screen all inappropriate material
and because they block valuable Web sites. However, a voluntary decision by con-
cerned parents to use these products for their children constitutes a far less re-
strictive alternative than COPA’s imposition of criminal penalties for protected
speech among adults.
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."

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." 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." 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 the availability of superior private alternatives can strip lawmakers of legitimate power to restrict free speech. 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 the Supreme Court in *ACLU v. Reno* when listing possible alternatives to the CDA, included only those involving state action. That supposed intimation

---

35. Id. at 181.
36. See Consol. Edison Co. of New York v. Pub. Serv. Comm'n 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. Jacksonvile*, 422 U.S. 205, 210-11 (1975) (striking down as unconstitutional an ordinance prohibiting indecent drive-in movies on grounds that passersbys must bear the burden of looking away); *Cohen v. California*, 403 U.S. 205, 210-11 (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 Drugs Products Corp.*, 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. ACLU*, 521 U.S. at 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
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 government for failing to pass a different provision—not to comment on the government’s failure to consider self-help remedies.\textsuperscript{38} So far as reading judicial tea leaves goes, the Third Circuit might have found it more fruitful to ponder 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.”\textsuperscript{39} As if to answer that question, the Supreme Court recently explained \textit{ACLU v. Reno} in terms that cast sharp doubt on the third circuit’s refusal to regard self help as an alternative state action: “[T]he 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.”\textsuperscript{40}

The ACLU has also employed the self-help argument in challenging state laws similar to COPA. As proof that a New Mexico statute\textsuperscript{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.”\textsuperscript{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,”\textsuperscript{43} and the Tenth Circuit affirmed.\textsuperscript{44} The ACLU made the same argument in its complaint\textsuperscript{45} against a New York law that criminalized Internet speech harm-
ful to minors. Here, though, the trial court granted a preliminary injunction without addressing such First Amendment claims, basing its decision solely on grounds the act interfered with interstate commerce.

IV. WHY DIGITAL SELF HELP ARGUES AGAINST REGULATION OF COMMERCIAL ENTITIES’ SPEECH ABOUT INTERNET USERS

Given the demonstration above that the availability of digital self help argues against state action limiting indecent or harmful-to-minors speech, this Part pits the same argument against state action that would limit speech within or by commercial entities and about Internet users. The parallel holds up nicely. 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 within or by commercial entities and 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 state action does.

A. THE EFFICACY OF SELF HELP IN PROTECTING INTERNET PRIVACY

Digital self help offers a quite—and perhaps 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. Though that will cut off access to sites that admit only registered users, more advanced self help measures can both preserve access to such sites and bar offensive cookies. More cautious Internet users can, for instance, download software like AdSubtract, IDCide Privacy Companion, PC Magazine’s CookieCop, Siemens’ WebWasher, In-
ternet Junkbuster, all of which offer more precise control over cookies and all of which come 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 Internet.55 Internet users who demand still more privacy can buy Freedom software to browse under disguise of a pseudonym or subscribe to Anonymizer.com's services 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.58 If consumer demand reflects poll re-

52. Webwasher, Welcome to Webwasher <www.webwasher.com> (accessed Oct. 27, 2000). WebWasher is available for home and educational use free of charge. Id. It filters both cookies and ads—including, in particular, web bugs. Id.
54. Guidescope, Take Control of the Web Surf Faster, Safer, & Easier ¶ 1 <http://www.guidescope.com> (accessed July 1, 2000). Guidescope blocks ads, web bugs, and referrer information, thereby protecting its users against distribution of certain types of information about their browsing activities. Id. Individual consumers can download and use Guidescope free of charge. Id.
55. Get the Idcide, supra n. 50, at ¶ 3 <http://www.idcide.com/html/Support/faq.htm> (accessed Nov. 5, 2000). 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. Id. 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 the external sites. Id. The Medium Privacy protection mode prevents the external cookies from being set while allowing the site you are visiting to set cookies. Id.
58. See generally U.S. Sen. Jud. Comm., Know the Rules Use the Tools—Privacy in the Digital Age: A Resource for Internet Users 10-21 <http://www.senate.gov/-judiciary/privacy.htm> (2000) (cataloging various self-help technologies for protecting privacy); see also Fox, supra n. 1, at 10 (reporting survey results on Internet Privacy). Although the present survey has emphasized digital tools, that does not exhaust the range of self-help methods for protecting Internet privacy. Id. 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 when asked by a Web site to register by offering personal information. Pew pollsters found that 24% of Internet users reported having given false personal information
sults, moreover, entrepreneurs will have ample incentives to create tools that protect Internet privacy even more cheaply and effectively.

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 bare-chested 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 software 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. On that count, privacy-protecting services have a great edge over filtering software. Insofar as the same least restrictive means test that applies to other types of constitutionally protected speech applies to speech within or by commercial entities and about Internet consumers, then, it ought to apply with even greater force.

B. THE CONSTITUTIONALITY OF REGULATING COMMERCIAL ENTITIES' SPEECH ABOUT INTERNET USERS

But should state action regulating speech within or by commercial entities and 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 very brief: maybe it does but probably it does not matter. Although an exhaustive answer would exceed the bounds of the present

to a Web site. Id. See Randy Cohen, The Ethicist, N.Y. Times Mag. 37 (June 4, 2000) (giving amusing advice on how to ameliorate the apparent immorality of that self-help method, "type 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 PI's 2c Amend. Verified Original Pet. and Application for T.R.O. and Temp. Inj., Universal Image Inc. v. Yahoo, Inc., No. 99-13839-A18, 20 (County Ct., Dallas County, Tex., filed Jan. 18, 2000). 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.

59. See supra pt. II (discussing poll results).
60. But see Ann Bartow, Our Data, Ourselves: Privacy, Propertization, and Gender, 34 U.S.F.L. REV. 633, 679 (2000) (allowing that average Web users might be able to implement some types of self-help but worrying that Web sites will condition access on receipt of private information); Prepared Remarks of Debra A. Valentine, General Counsel of the FTC, 16 Comp. & High Tech. L. J. 401, 417 (2000) (complaining 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 U.S. v. Playboy Ent. Group, 529 U.S. 803, 120 S.Ct. 1878, 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.").
paper and would at all events proceed without the guide of controlling case law, this subpart offers a quick explanation of that conclusion.

Speech within or by commercial entities and about Internet consumers might well qualify for protection under the least restrictive means test, which courts apply when strictly scrutinizing restrictions on ordinary—or for that matter indecent or harmful-to-minors—speech. At a minimum, though, it would almost certainly qualify as commercial speech, which courts generally protect from any regulation that is “more extensive than is necessary” to serve the government’s alleged interest. 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 within or by commercial entities and about Internet consumers—the least restrictive means test would come back into play.

State action restricting speech within or by commercial entities and 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.”

The large and growing number of self-help alternatives for protecting Internet privacy certainly qualifies them as obvious. Although the ultimate

---


63. A. Michael Froomkin, The Death of Privacy? 52 Stan. L. Rev. 1461, 1521 (2000) (stating that government’s ability to regulate privately generated speech relating to commerce is surprisingly unlitigated).

64. See Volokh, supra n. 62, at 1080-84 (discussing the commercial speech doctrine). But see Cohen, supra n. 62, at 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. Id. at 1410.

65. See generally U.S. West, Inc. v. FCC, 182 F.3d 1224 (10th Cir. 1999), cert den. sub nom., 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).


68. U.S. West, 182 F.3d at 1238 n. 11.
mate determination must turn on the facts, the efficacy and minimal expense of extant self-help protections probably also already qualifies them as less restrictive than any of the various current proposals to regulate speech within or by commercial entities and about Internet users.69

C. SELF HELP AND PUBLIC POLICY IN PROTECTING INTERNET PRIVACY

Even apart from such constitutional questions, the availability of so many and so efficacious means of protecting Internet privacy through self-help suggests that legislation toward the same end could not tout curing market failure as justification.70 Whether a great many Internet users avail themselves of such self-help measures has little bearing on that point, of course.71 Notwithstanding cheap talk to the contrary, actions may reveal Internet users quite willing to trade personal privacy for access to Web sites.72 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 or sacrificing their privacy.73 To judge from what they tell pollsters, moreover, an overwhelming majority of Americans think that Internet users—not government, not industry—should bear the primary responsibility for exercising that choice.74

That legislation protecting Internet privacy offers little benefit would not cause much concern were its potential costs not so high. The

69. See infra Part II.
70. Fred H. Cate, Privacy and Telecommunications, 33 Wake Forest L. Rev. 1, 47 (1998) "[T]he most effective protection for information privacy is individual responsibility and action." Id.
71. But see Froomkin, supra n. 63, at 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, Professor Froomkin admits to assuming that 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. Id. Here as with regard to other markets, however, why would not their revealed preferences not tell us all we need to know about what consumers, as a class, really want?
72. See John Schwartz, 'Opting-in': A Privacy Paradox, Washington Post H01 (Sept. 3, 2000) (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).
73. But see Cohen, supra n. 62, at 1393-96 (critiquing the legitimacy of choice in non-political contexts about personal privacy).
74. Fox, supra n. 1 When Pew pollsters asked "who should have the MOST say over how Internet companies track people's activities online and use personal information," 68% of respondents replied "People who use Web sites." Id. Only 19% of respondents chose the federal government and only 6% chose Internet companies. Id. at 28.
Children's Online Privacy Protection Act of 1998 ("COPPA")\(^{75}\) does not give much encouragement on that count, as it has increased legal uncertainty,\(^{76}\) raised the expense of providing online services,\(^{77}\) and even forced some companies out of the market for young Internet users.\(^{78}\) A more comprehensive statute, covering not just the privacy of children but also of adults, might well generate more comprehensive problems.

Nor should the prospect of having government agencies enforce such a statute engender much optimism. Notwithstanding federal law\(^{79}\) and a specific White House edict to the contrary,\(^{80}\) federal agencies have largely failed to implement privacy protections on their own Web sites.\(^{81}\) 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.\(^{82}\) 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 ac-

---


76. See Lynne Burke, Contending with COPPA Confusion, Wired News <http://www.wired.com/news/politics/0,1283,38332,00.html> (Aug. 23, 2000) (quoting Alex Bentacur, vice president of girl’s clothing site 100percentgirls.com, “[T]he law, which we support completely, is so unclear.”).


78. See Tamara Loomis, Lawyers Wrestle With Online Privacy, N.Y.L.J., <http://www.nylj.com/stories/00/07/071300a4.htm> (Thursday, July 13, 2000) (relating that some companies have left the market rather than incur costs of complying with COPPA).


80. Jacob J. Lew, Memorandum for the Heads of Executive Departments and Agencies, Re: Privacy Policies and Data Collection On Federal Web Sites <http://www.whitehouse.gov/omb/memoranda/m00-13.html> (June 22, 2000) (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).


82. U.S. General Accounting Office, Internet Privacy: Agencies’ Efforts to Implement OMB’s Privacy Policy 11 (GAO/GGD-00-191) <http://www.gao.gov/new.items/gg00191.pdf> (Sept. 2000) (assessing conformity with OMB requirements). It has been reported that nearly half of federal Web sites collecting personal information failed to post privacy policies, thereby arguably violating OMB requirements. Id. at 17.
Though one might argue that government agents quite naturally enforce privacy-protecting laws less vigorously against themselves than against us citizens, somehow that excuse does not give much comfort.

As a matter not only of constitutional law but also of public policy, politicians should invoke state power only to correct manifest failures of market and other non-political mechanisms to correct serious national problems. Even then, law makers 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. The benefits, in brief, must outweigh the costs. Proposals to pass laws protecting Internet users' privacy merit skepticism on both counts.

V. CONCLUSION

The availability of speech-filtering programs has already powerfully affected responses to Internet pornography. The advent of tools like cookie-control software and anonymizing networks now presents a similar challenge to the law and policy of 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 pressed that argument against legislation restricting indecent or harmful-to-minors Internet speech should thus reconsider their demands for legislation that would restrict speech within or by commercial entities and 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 of course argued that Internet law and policy should take account of a more significant relationship between pornography and privacy, one

83. See Darrell West, Assessing E-Government: The Internet, Democracy, and Service Delivery by State and Federal Governments <http://www.brown.edu/Departments/Taubman_Center/poreports/egovreport00.html> (Sept. 2000) (reporting that of 1,716 state government sites, 36 federal sites and 61 federal court sites, only 5% had a security policy and only 7% had a privacy policy).


85. See Pollack, supra note 37 (describing the inefficiencies inherent in government regulation).

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 law makers ignored the alternatives offered by digital self help and instead enacted unconstitutional, unnecessary, and unjustified regulations.