First Do Not Harm: The Problem of Spyware

Berkeley Technology Law Journal

Volume 20 | Issue 3 Article 6

June 2005

First Do Not Harm: The Problem of Spyware

Susan P. Crawford

FIRST DO NO HARM: THE PROBLEM OF SPYWARE

By Susan P. Crawford†

TABLE OF CONTENTS

I. INTRODUCTION

Online problems are popularly understood to be easily susceptible to offline legal categorizations and, thus, solutions.[1] "There is nothing new under the sun," we say to one another over and over again in the cyberlaw

---

† Assistant Professor, Cardozo School of Law. Thanks to Lorrie Cranor, David Johnson, David Post, Michael Steffen, Stewart Sterk, and participants in the University of Pittsburgh School of Law's "Where IP Meets IP: Technology and the Law" symposium convened by Michael Madison.

1. Jack Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199 (1998) (stating that no special problems are created by the Internet that have not been addressed by existing conflict of laws and jurisdiction concepts); Jack Goldsmith, *Regulation of the Internet: Three Persistent Fallacies*, 73 CHI.-KENT L. REV. 1119, 1121 (1998) (stating that the "Net is not a separate place, and Net users are not removed from our world").

arena. But spyware[2] appears to be an exception to this received world view. There is nothing quite like spyware in the "real" world. Unlike an infectious disease, some varieties of spyware can "phone home" enormous amounts of personal data. Unlike a fixed surveillance camera, some spyware can travel with you wherever you "go" online. And unlike a blackmail note, which is unambiguously bad, spyware is very difficult to define—there can be "good" and "bad" spyware applications that have the same essential characteristics. Spyware combines attributes of all three of these things. Like an infectious disease, it can be contracted without the user's knowledge and can have harmful, amplified effects inside the body of the user's computer. Like a surveillance camera, it can watch users across time without their knowledge. And like a blackmail note, some spyware installations may force users into involuntary relationships that feel oppressive.

Just as there is nothing quite like spyware in the "real" world, no existing offline legal or regulatory techniques are adequate to address this problem. We could legislatively require that users consent to particular installations of software that may watch (and report on) their activities; sue software providers under existing unfair trade practices or trespass laws;[3] or let the marketplace provide software applications that make it possible for users to protect themselves. This Article argues that only the last of these three sets of actions will have any real effect on spyware, and that software developers and major online companies have already responded to market demands for help by releasing useful spyware-combating products and services.

---

2. This Article focuses on the difficulty of defining "spyware." Spyware is generally understood as software that is installed on a user's computer (often without the user's knowledge) and monitors the activities of that computer, "phoning home" information about the user or the computer's activities, changing the user's web browsing settings (homepage, Internet connection settings), or prompting pop-up advertisements. Subsets of "spyware" include "adware" (software designed to generate advertising based on web use) and "malware" (software designed to do harm to a computer). State and federal legislators have defined "spyware" in various ways. For purposes of this Article, the term "spyware" is used to mean all of these things, except where otherwise specifically indicated. For a useful primer on the various meanings of "spyware," see CENTER FOR DEMOCRACY AND TECHNOLOGY (CDT), GHOSTS IN OUR MACHINES: BACKGROUND AND POLICY PROPOSALS ON THE "SPYWARE" PROBLEM (Nov. 2003), http://www.cdt.org/privacy/031100spyware.pdf.

3. The Federal Trade Commission has taken this route successfully. *See infra* Part II.E.3.a. This Article is focused on the first and third of the three options that I describe, and it does not explore the various litigation routes that might be available to private litigants.

Proposed legislative cures now under discussion may be worse than the diseases they are designed to counteract. Several pending or enacted bills (1) assume that legislative design of software is appropriate and (2) embrace the notion that "notice" is an effective concept in the spyware context—two legislative directions that this Article explains are bound to have negative effects on lawful innovation.

I am not claiming that legislation in this area signals the end of the civilized world or will bring a halt to the progress of science. To the extent that draft bills focus on bad behaviors rather than software design and notice, their enactment will have little effect on innovation and may in fact be helpful. I am concerned, however, that the software design and notice elements of pending spyware legislation may be exploited in the future as part of the larger power struggle between people who want to constrain what software can do and people who want to write code.

Three great industries want to constrain the writing of software and the functioning of the Internet: law enforcement, the content industry, and telecommunications companies. Having early legislative design mandates for software focused on "spyware"—something most people agree is "bad," even if they cannot precisely define it—is useful for these industries.[4] Later design mandates aimed at making tappability easier for law enforcement or copyright policing easier for the content industry or taxation easier for telecom agencies will be able to take advantage of the spy-

---

4. For example, the content community draws specific links between peer-to-peer ("p2p") applications used to facilitate filesharing and spyware. *See The Dark Side of a Bright Idea: Could Personal and National Security Risks Compromise the Potential of Peer to Peer File Sharing Networks?: Hearing Before the S. Comm. on the Judiciary*, 108th Cong. (2003) (statement of Sen. Orrin Hatch). Senator Hatch's comments at the conclusion of the hearing have been summarized as follows:

> Sen. Orrin Hatch (R-UT), the Chairman of the Committee, also focused on copyright infringement on P2P networks, and suggested that if no other way can be found to protect copyrighted works from piracy, 'destroying computers' should be permitted. . . . [Sen. Hatch said that he was] also troubled that many P2P networks require their users to install so-called 'spyware' or 'adware'—programs that monitor, collect, and report information about the Internet 'browsing' habits of a particular user.

Senate Committee Holds Hearing on P2P Networks, TECH LAW JOURNAL, June 18, 2003, http://www.techlawjournal.com/home/newsbriefs/2003/06d.asp. Some very popular p2p applications, such as eDonkey, iMesh, Kazaa, and Morpheus, bundle optional installations or installations disclosed only in lengthy license agreements that are difficult to read. Benjamin Edelman, *Comparison of Unwanted Software Installed by P2P Programs*, Mar. 7, 2005, http://www.benedelman.org/spyware/p2p. It would be very helpful to the content community to be able to outlaw p2p networks by using laws facially addressed to spyware.

ware legislative example. We need to decide what threshold of pain suffered by code writers makes us jump up and down and say "don't legislate." This Article is designed to encourage legislators to pause and consider the larger power relationships implicated by these bills before launching into further fruitless legislative efforts to end "spyware."

Part II of this Article surveys the legislative landscape as of mid-2005. Prompted by concerns over pop-up ads that were launched by third parties when users visited particular sites, the Utah legislature passed a spyware bill in 2003 that has been widely imitated in other states. Although the initial Utah bill was successfully challenged as violative of the dormant Commerce Clause, as of May 8, 2005 at least twenty-seven states were considering or had passed spyware legislation—including Utah, which had taken another stab at a bill barring unauthorized pop-up advertising. Meanwhile, there has been a great deal of spyware-related legislative energy expended at the federal level. Two spyware bills overwhelmingly passed in the House in 2004, and combined versions of those bills are likely to be supported by both houses of Congress in 2005.

All of the state bills trigger substantial dormant Commerce Clause issues and are unlikely to be found to be constitutional.[5] More importantly, however, the legislative approaches taken at both the state and federal levels have three major problems. First, many of these bills are overly regulatory, setting forth detailed design mandates and notice requirements. Second, these legislative efforts are doomed to be unsuccessful in terms of producing a reduction in spyware—just as the CAN-SPAM Act of 2003 was unsuccessful in reducing the volume of spam.[6] Third, many legislators appear to view spyware as an assault on privacy interests, a view that does not illuminate the problem of spyware. In fact, people are upset by some forms of spyware because they create oppressive, unwanted relationships, not because they violate some preexisting idealized privacy interest. Existing law directed toward remediating oppressive relationships, including both prima facie tort claims and federal statutory schemes, may adequately address spyware.

---

5. Given the state laws' focus on software content, these laws may be unconstitutional under the First Amendment as well. *See* ACLU v. Miller, 977 F. Supp. 1228 (N.D. Ga. 1997) (invalidating a state law criminalizing Internet transmissions that falsely identify the sender and holding that a state may impose content-based restrictions only to promote a "compelling state interest" and only through use of "the least restrictive means to further the articulated interest"). These statutes may not be sufficiently narrowly tailored, may sweep protected speech within their scope, and are often vague in their use of terms. *See infra* Part II.D.1.

6. *See infra* Part II.D.2.

Part III provides concrete suggestions for addressing spyware. There is no one organization with sufficient knowledge to recognize and deal with "bad" spyware. Only a technical approach—and only a particular kind of technical approach at that—will work. Technical actors need to take an "immune system" approach to spyware, dividing their efforts and experimenting in the field the same way immunity networks do. If we think of the legal system as a medical expert operating on this difficult disease, our first priority must be to wait to allow these already-emerging immunity networks to take effect, and to "do no harm" in the interim. This is a time for patience, not for the knife.

Part IV asks: what is the legal role of these immunity networks? It may be time to recognize that individuals, and their unhappy relationships with spyware, will not always be the most important actors on the legal stage. We are part of a collective technical environment that has become too difficult for us to understand or deal with as people, and too difficult for any existing legal institutions to take on effectively. As a result, individuals may need to choose to cede some control over their machines to technical networks that will help in the constant fight against oppressive adware and malware. This is not a move towards enforced similarity, as in communism. Nor is this a move towards a voting, democratic approach to software, where software that is voted "bad" becomes illegal. Instead, we should recognize that there is already in the world a third way of governing that we need to embrace as we face difficult technical warfare: competing networks. Only by allowing these networks to "represent" and protect us will we survive the coming difficulties. Such networks will provide the benefits of connection as well as the technical protections on which the spyware debate focuses.

II. THE LEGISLATIVE LANDSCAPE

Because there is so much legislative activity on the spyware front, the most useful way to discuss U.S. spyware legislation is to tell the story of the initial Utah state statute and its constitutional problems, clump the rest of the pending (or enacted) state bills into three groups (bad acts bills, notice bills, and trademark bills), and spend some time on the implications of the federal bills that will likely pass before this Article is published. If nothing else, this discussion should signal that we have not settled on a central legislative metaphor for dealing with spyware. Is spyware a type of software that does things that would surprise a user (if the user knew what was happening)? Is spyware a type of software that is automatically installed on a "protected computer" without the user being given an oppor-

tunity to refuse? Is spyware a type of software that allows the unauthorized use of trademarks in search terms (or visits to particular websites) to prompt the display of unauthorized advertisements? Is spyware anything that tracks what a user does online, whether or not the technology collects personally identifiable information? Apparently it depends which legislator is talking.

A. The Initial Utah State Statute: The Spyware Control Act

Utah's 2004 Spyware Control Act[7] was a reaction to the success of WhenU's SaveNow program in presenting pop-up ads to computers browsing the web. The SaveNow program is downloaded by users in return for obtaining a piece of freeware—a popular, free piece of software.[8] The consumer is presented with a license agreement stating that SaveNow will generate "contextual" pop-up ads. After the user clicks "I agree," the SaveNow program is installed on the user's computer and causes a directory of search terms and URLs to be saved on the user's desktop. As the user browses, his/her use of search terms and web addresses causes the presentation of pop-up ads and coupons. Although ad impressions triggered by the software are reported back to central SaveNow servers, search terms and websites visited by the particular computer are not.

1-800 Contacts, a Utah company that was unhappy that competitors' ads were triggered by the SaveNow software to appear in windows over 1-800 Contacts' site, sued WhenU, the company behind SaveNow.[9] After 1-800 Contacts gained an early victory against WhenU in that lawsuit,[10]

---

7. H.B. 323, 2004 Gen. Sess. (codified at UTAH CODE ANN. § 13-39-101 et seq.).

8. Examples include MP3 players, screensavers, file sharing applications, online games, and shopping tools.

9. 1-800 Contacts sued WhenU in federal court in New York on the theory that WhenU's advertisements infringe 1-800 Contacts' trademark and copyrights and initially prevailed. 1-800 Contacts, Inc. v. WhenU.com, Inc., 309 F. Supp. 2d 467, 472 (S.D.N.Y. 2003) (granting preliminary injunction on trademark challenge but denying the copyright challenge). The Second Circuit reversed this decision in June 2005, ruling that WhenU does not "use" 1-800 Contact's trademarks within the meaning of the Lanham Act, 153 U.S.C. § 1127 (2000), when it (1) includes 1-800 Contact's website address in an unpublished directory of terms that trigger delivery of advertising or (2) causes branded pop-up ads to appear on a computer screen next to the 1-800 Contact's website window. 1-800 Contacts, Inc. v. WhenU.com, Inc., No. 04-0026(L), 2005 U.S. App. LEXIS 12711, at *5 (2d Cir. June 27, 2005).

10. *1-800 Contacts*, 309 F. Supp. at 467. The New York district court decision (now reversed) conflicted with two earlier decisions by federal district courts in Virginia and Michigan. *See* U-Haul Int'l, Inc. v. WhenU.com, Inc., 279 F. Supp. 2d 723 (E.D. Va. 2003) (holding that WhenU pop-up advertisements do not represent trademark infringement, unfair competition, trademark dilution, or copyright infringement); Wells Fargo & Co. v. WhenU.com, Inc., 293 F. Supp. 2d 734 (E.D. Mich. 2003) (same). The

1-800-Contacts went the legislative route and urged the Utah legislature to pass a bill addressing SaveNow's tactics.[11] Although a large coalition of substantial online companies lobbied against the bill,[12] it was enacted into law in March 2004.[13] This Act barred any person from installing "spyware" on another person's computer or causing such installation.[14] Part of the bill appeared to be aimed directly at WhenU's business. The bill defined "Context Based Triggering Mechanisms" as "a software based trigger or program residing on a consumer's computer that displays an advertisement according to: (a) the current Internet website accessed by a user; or (b) the contents or characteristics of the current Internet website accessed by a user."[15] According to the bill, use of a Context Based Triggering Mechanism to display an advertisement "that partially or wholly covers or obscures paid advertising or other content on an Internet website in a way that interferes with a user's ability to view the Internet website" was

---

Gator Corporation, now owned by Claria Corp., has also been sued several times for similar actions. *See, e.g.*, *In re* Gator Corp., 259 F. Supp. 2d 1378, 1380-81 (J.P.M.L. 2003) (providing docket information for consolidated actions). *Washingtonpost. Newsweek Interactive Co., LLC. v. Gator Corp.* resulted in an injunction in favor of the website operators and eventually settled in 2003. No. 02-909-A, 2002 U.S. Dist. LEXIS 20879 (E.D. Va. July 16, 2002). The terms of the settlement have not been made public. Todd Weiss, *Online newspapers settle lawsuit with Gator Ad service*, COMPUTERWORLD, Nov. 2, 2003, http://www.computerworld.com.au/index.php/id;1502815315;relcomp;1.

11. *See Burns, Wyden Told to Focus Anti-Spyware Bill on Action, Not Technology*, 5 WASHINGTON INTERNET DAILY 57, Mar. 24, 2004 ("The Utah Bill resulted from WhenU triumphing in court over 1-800-Contacts, a Utah company that sued to stop WhenU ads from popping up over its web site.").

12. The Information Technology Association of America (ITAA), Google, Yahoo! Inc., Microsoft Corp., America Online, the Software & Information Industry Association, Oracle Corp., eBay, and Amazon.com formed an ad hoc coalition opposing the bill. *Utah Governor Mulls Spyware Bill, Industry opposes: Constitutional Issues Raised*, ECOMMERCE LAW DAILY, Mar. 12, 2004, http://subscript.bna.com/SAMPLES/ecd.nsf/0/4574a5cb36c6555985256e5500022a0b?OpenDocument.

13. The Spyware Control Act was passed by the Utah Legislature on March 3, 2004 after a twenty-six to zero vote in its favor. Utah State Legislature, H.B. 323 Fourth Substitute, http://www.le.state.ut.us/%7E2004/htmdoc/hbillhtm/HB0323S04.htm (last visited Aug. 19, 2005). The bill was signed into law by Governor Olene S. Walker on March 23, 2004. *Id.*

14. "Spyware" was defined as "software residing on a computer that monitors the computer's usage, sends information about the computer's usage to a remote computer or server, or displays or causes to be displayed an advertisement in response to the computer's usage." UTAH CODE ANN. § 13-40-102(4)(2), (b) (2004) (subsection indicators omitted).

15. *Id.* § 13-40-102(1).

illegal.[16] The bill provided for a private cause of action and set damages at $10,000 for each separate violation.[17]

Following a challenge by WhenU, a Utah state court on June 22, 2004 enjoined this Act from coming into force on dormant Commerce Clause grounds.[18] The court found that plaintiff had shown that compliance with the statute would be difficult and expensive, that the statute was vague, and that it created a risk of different penalties and mandates being applied to online companies from state to state.[19]

In early 2005, Utah introduced revisions to this Act that are driven by pop-up ad generation concerns.[20] The revised Act defines "spyware" as "software on the computer of a [Utah] user" that "collects information about an Internet website at the time the Internet website is being viewed in this state" and uses that information contemporaneously to display pop-up ads.[21] The key violation under the new Act is to display an ad in response to a particular trademark when that advertisement has been purchased by someone other than the mark owner.[22] Damages under the Act have been reduced from $10,000 per violation to $500 per each separate occurrence resulting in display of an unauthorized advertisement, plus a possibility of treble damages and attorneys' fees and costs.[23]

The revised Utah bill attempts to deal with the dormant Commerce Clause problem by applying its penalties only to spyware that is installed on the computer of a Utah resident that collects information "at the time [an] Internet website is being viewed in this state."[24] It provides a safe harbor for advertisers who "request[] information about the user's state of residence before sending the spyware or displaying a pop-up advertisement to the user" when the user says he/she does not live in Utah.[25]

---

16. *Id.* § 13-40-201.

17. *Id.* § 13-40-301(1), (2).

18. WhenU.com, Inc. v. State, No. 040907578 (3d Dist. Utah June 22, 2004), *available at* http://www.benedelman.org/spyware/whenu-utah/pi-ruling-transcript.

19. *Id.*

20. Spyware Control Act Revisions, H.B. 104, 2005 Leg., 56th Sess. (Utah 2005).

21. UTAH CODE ANN. § 13-40-102(8) (2005).

22. *Id.* § 13-40-201.

23. *Id.* §§ 13-40-301, 302.

24. It is not clear that this will be enough to solve the dormant Commerce Clause problem; after all, there is no requirement that the communication that is unlawful—here, the transmission of the software to Utah residents—take place entirely within Utah. *See* Am. Libraries Ass'n v. Pataki, 969 F. Supp. 160, 169-170 (S.D.N.Y. 1997).

25. UTAH CODE ANN. §§ 13-40-201, 202 (2005).

B. Other State Bills

1. Bad Acts

Alabama, Arkansas, Arizona, California, Illinois, Maryland, Michigan, Nebraska, New York, Rhode Island, Virginia, and Washington are considering or have enacted "bad acts laundry list" bills.[26] The bills outlaw software that deceptively "takes control" of a computer by modifying home pages, changing bookmarks, changing modem or other Internet access settings, transmitting or relaying unauthorized e-mail messages, using the computer as part of a distributed denial of service attack, or "opening multiple, sequential, stand alone advertisements" in a browser that cannot be closed without turning off the computer or closing the browser. The collection of personally identifiable information through deceptive means is also illegal under these bills, which focus on the use of keystroke loggers as well as software that gathers information about the websites visited by a user. The bills make illegal the deceptive prevention of a user's efforts to block software installations, misrepresentations that software will be uninstalled or disabled by what the user does next, and deceptive actions to disable anti-spyware software. These bills prohibit misrepresentations that software is needed for security or privacy or in order to open, view, or play a particular type of content. And the state legislatures working on these "bad acts" bills intend to continue their work. For example, the preamble to the California act states bravely that "it is the intent of the Legislature to revise the provisions in this act as needed to fully protect consumers from additional unfair and deceptive practices and to address future innovations in computer technology and practices."[27]

2. Trademark Concerns

Alaska, Indiana, Massachusetts, New Hampshire, and Tennessee, like Utah, have focused on the use of software to trigger unauthorized adver-

---

26. S.B. 122, 2005 Leg. (Ala. 2005); S.B. 2904, 2005 Leg., Reg. Sess. (Ark. 2005); H.B. 2414, 47th Leg., 1st Reg. Sess. (Ariz. 2005); CAL. BUS. & PROF. CODE § 22947 (Deering 2005) (imposing a $1000 penalty per violation); H.B. 380, 94th Gen. Ass. (Ill. 2005); H.B. 945, 2005 Leg., Reg. Sess. (Md. 2005); S.B. 151, 2005 Leg. (Mich. 2005); L.B. 316, 99th Leg., 1st Sess. (Neb. 2005); A.B. 549, 2005-2006 Reg. Sess. (N.Y. 2005); H. 6211, Gen. Ass., Jan. Sess. (R.I. 2005); H.B. 2215, 2005 Leg., Gen. Ass. (Va. 2005); H.B. 1012, 59th Leg., 2005 Reg. Sess. (Wash. 2005). For updated status of state spyware bills, see National Conference of State Legislatures, 2005 State Legislation Relating to Internet Spyware or Adware, http://www.ncsl.org/programs/lis/spyware05.htm (last visited Aug. 19, 2005).

27. CAL. BUS. & PROF. CODE § 22947.

tisements.[28] To avoid a "spyware" categorization under these bills, software that triggers the display of ads must clearly identify the name of the entity responsible for delivering the advertisement in the body of the ad itself and the ad must not be triggered by an unauthorized trademark use. "Spyware" is defined to exclude "software or data that reports to an Internet web site only information previously stored by the Internet web site on the user's computer."[29]

These bills also require user consent for "spyware" to be installed legally. Consent will require user agreement to a full, detailed, plain language license agreement that, among other things, instructs the user how to distinguish the "spyware" advertisements from other advertisements.[30] Trademark owners and website operators have a private right of action under these bills, and can seek damages of $10,000 for each violation plus treble damages and attorneys fees.[31]

3. Notice Concerns

Michigan, Pennsylvania, Oregon, Tennessee, and Texas have enacted or are considering notice bills, under which "spyware," broadly defined,[32]

---

28. S.B. 140, 24th Leg. (Alaska 2005); H.B. 1714, 2005 Reg. Sess. (Ind. 2005) (section 2 provides that "'context based triggering mechanism' means a program or software based trigger that: (1) resides on a consumer's computer; and (2) displays an advertisement according to (A) the current Internet web site accessed by a user; or (B) the contents or characteristics of the current Internet web site accessed by a user"); S.B. 273, 184th Gen. Ct. (Mass. 2005) (defining spyware as follows: "software residing on a computer that monitors the computer's usage and either sends information about the computer's usage to a remote computer or server or causes to be displayed an advertisement in response to the computer's usage, or both"); H.B. 47 (N.H. 2005); H.B. 1742, 104th Gen. Ass. (Tenn. 2005).

29. H.B. 1714, § 2.

30. *Id.*

31. *Id.*

32. A draft Michigan spyware bill states: "Spyware" means computer instructions or software installed into a computer program, computer, computer system, or computer network for any of the following purposes:

> (a) monitoring the use of a computer program, computer, computer system, or computer network.
>
> (b) sending information about the use of a computer program, computer, computer system, or computer network to a remote computer or server or data collection site or point.
>
> (c) displaying an advertisement or causing an advertisement to be displayed in response to the use of a computer program, computer, computer system, or computer network.

S.B. 1315 (Mich. 2004) § 5a(5). The Pennsylvanian counterpart defines spyware as follows:

is illegal unless a consumer has a great deal of information supplied to him or her about the software: name and contact information of the person installing it (or on whose behalf it is being installed), notice of intent to install the software and a description of how it will affect its target, a full license agreement, and a method for refusing the installation and avoiding any further contact. Oregon provides that such notices "shall be in at least 10-point boldfaced type, in immediate proximity to the space reserved for the owner to agree to the installation."[33]

C. Overarching Commerce Clause Issues with Pending State Bills

All of the state bills pose substantial dormant Commerce Clause problems. Even where the bills provide a state nexus (such as, in the Utah bill, the scope limitation to Utah residents' computers and operating when those residents are in fact in Utah), the impact of these bills will not be limited to conduct occurring within the relevant state. "[P]urely intrastate communications over the Internet" do not exist.[34] Although these state bills and acts focus on spyware that has been installed on the computers of users inside the state, that installation requires a transmission that will

---

> An executable computer program that automatically and without the control of a computer user gathers and transmits to the provider of the program or to a third party either of the following types of information:
> (1) Personal information or data of a user.
> (2) Data regarding computer usage, including, but not limited to, which Internet sites are, or have been, visited . . . .

H.B. 574 § 2 (Penn. 2005) (introduced Feb. 16, 2005); *see also* H.B. 2302, 73rd Leg. Ass., 2005 Reg. Sess. (Ore. 2005). It is worth noting that much of the Pennsylvania bill is taken up with rules about commercial e-mail, all of which should, presumably, have been preempted by CAN-SPAM. The Tennessee and Texas bills contain both "notice" and "trademark" elements. H.B. 1742, 104th Gen. Ass. (Tenn. 2005); S.B. 327, 79th Leg. (Tex. 2005).

33. H.B. 2302, 73rd Leg. Ass., 2005 Reg. Sess. (Ore. 2005) § 2(3).

34. *See Am. Libraries Ass'n*, 969 F. Supp. at 171 (striking down a New York statute that prohibited online dissemination of harmful materials to minors because it did not require that the communication take place entirely within New York state and there was no way to limit the reach of the statute to New York); People v. Foley, 692 N.Y.S.2d 248, 256 (N.Y. App. Div. 1999) (holding that a New York statute criminalizing the dissemination of indecent material to minors through the Internet in order to lure minors to engage in sexual activity passed dormant commerce clause analysis); People v. Lipsitz, 663 N.Y.S.2d 468, 475 (N.Y. Sup. Ct. 1997) (holding that the application of New York consumer protection laws to New York business pursuant to Internet solicitations was proper under the dormant Commerce Clause). The Supreme Court has decided that state regulatory schemes that permit in-state wineries to ship alcohol to consumers but restrict the ability of out-of-state wineries to do the same are unconstitutional under the 21st Amendment and the dormant Commerce Clause. Granholm v. Heald, 125 S. Ct. 1885 (2005).

have come—necessarily—from out of state. Thus, because these statutes may impose burdens on out-of-state communications that are not necessarily unlawful, their constitutionality is suspect.[35] Web publishers and software developers cannot effectively prevent the flow of information to any given state.[36] State regulations may burden interstate commerce "when a statute . . . has the practical effect of requiring out-of-state commerce to be conducted at the regulating state's direction,"[37] and these state statutes have precisely this effect. Moreover, and perhaps more importantly, imposing state regulations in this area will subject the Internet to inconsistent regulations, something that is likely to make a reviewing court uncomfortable.[38]

---

35. *See* Am. Booksellers Found. v. Dean, 342 F.3d 96, 104 (2d Cir. 2003) (holding a state statute concerning dissemination of material harmful to minors unconstitutional under the dormant Commerce Clause and First Amendment); ACLU v. Johnson, 194 F.3d 1149, 1160-63 (10th Cir. 1999) (same); PSINet v. Chapman, 167 F. Supp. 2d 878, 882, 891 (W.D. Va. 2001) (same); Cyberspace Commc'ns, Inc. v. Engler, 55 F. Supp. 2d 737, 739-40, 751-52 (E.D. Mich. 1999) (same), *aff'd*, 238 F.3d 420 (6th Cir. 2000); *cf.* People v. Hsu, 99 Cal. Rptr. 2d 184 (Cal. Ct. App. 2000) (finding a state statute criminalizing pedophile activity constitutional because it included an intent requirement and prohibiting transmission of harmful material to seduce minors would not burden any legitimate commerce).

36. It is a matter of scholarly dispute whether technology now exists that could enable websites to determine, in an accurate and cost-effective fashion, where their visitors are coming from. *Compare* Joel Reidenberg, *Technology and Internet Jurisdiction,* 153 U. PA. L. REV. (forthcoming 2005) ("Commercial pressures and the dynamic nature of the Internet have resulted in geolocation and the re-creation of geographic origin and destination."), *and* Michael A. Geist, *Is There a There There? Toward Greater Certainty for Internet Jurisdiction*, 16 BERKELEY TECH. L.J. 1345, 1401 (2001) (pointing to the efficacy of geolocation technologies), *with* Andrea M. Matwyshyn, *Of Nodes and Power Laws: A Network Theory Approach to Internet Jurisdiction Through Data Privacy*, 98 NW. U. L. REV. 493, 520 (2004) ("Geolocation technologies, while demonstrating relatively high levels of accuracy for marketing purposes, are still imperfect, both for the Internet and other forms of Network Communications; they do not offer adequate levels of certainty for jurisdiction purposes to be mandated as the tool of choice for jurisdictional determinations. For example, the European Union believes that geolocation technologies are inadequate tools for the purpose of assessing value-added tax on e-commerce." (citations omitted)). I consider the best-regarded free geolocation service, NetGeo, out of date and increasingly inaccurate, while the services that are more accurate (Akamai Edgescape, Digital Envoy, and Quova Geopoint) cater to large enterprises and charge steep monthly subscription fees.

37. Brown & Williamson Tobacco Corp. v. Pataki, 320 F.3d 200, 208-09 (2d Cir. 2003) (citations omitted).

38. *See Am. Booksellers Found.*, 342 F.3d at 104 ("[A]t the same time that the internet's geographic reach increases Vermont's interest in regulating out-of-state conduct, it makes state regulation impracticable. We think it likely that the internet will soon be seen as falling within the class of subjects that are protected from State

D. Federal Bills

The 108th Congress was a time of great legislative activity on the subject of spyware, and the 109th is proving to be a similarly active period. Although no bills have passed in either the House or the Senate as of the time of the preparation of this Article, it is very likely that spyware legislation will pass later this year. Bills on the list, each of which is discussed below, include the SPY ACT, the I-SPY ACT, and the SPY-BLOCK Act.

1. SPY ACT

The House bill in the lead as of May 2005, H.R.29 (The Securely Protect Yourself Against Cyber Trespass Act (SPY ACT)), which preempts state legislation on these issues, is both a "laundry list of bad acts" bill and a notice bill.[39] The SPY ACT, which passed in the House on May 23, 2005, contains a list of "bad acts" that is very similar to the lists set forth in the Alabama, Arkansas, Arizona, California, Illinois, Michigan, Ne-

---

regulation because they 'imperatively demand[ ] a single uniform rule.'") (quoting Cooley v. Bd. of Wardens, 53 U.S. 299, 319 (1851)). On the other hand, *Pike v. Bruce Church, Inc.*, requires that "[w]here the statute regulates even-handedly to effectuate a legitimate local public interest, and its effects on interstate commerce are only incidental, it will be upheld unless the burden imposed on such commerce is clearly excessive in relation to the putative local benefits". 397 U.S. 137, 142 (1970). Some commentators have argued that the Pataki approach to dormant Commerce Clause issues is overreaching and insufficiently nuanced. *See generally* Jack L. Goldsmith and Alan O. Sykes, *The Internet and the Dormant Commerce Clause*, 110 YALE L. J. 785, 787 (2001) ("The dormant Commerce Clause, properly understood, leaves states with much more flexibility to regulate Internet transactions than is commonly thought."); Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199, 1212 (1998) (spillover effects of local regulations are "a commonplace consequence of the unilateral application of any particular law to transnational activity in our increasingly interconnected world"); Michael W. Loudenslager, *Allowing Another Policeman on the Information Superhighway: State Interests and Federalism on the Internet in the Face of the Dormant Commerce Clause*, 17 BYU J. PUB. L. 191 (2003) (stating that deference to state police powers requires narrower reading of dormant Commerce Clause).

39. A 2004 version of the The SPY ACT passed the House in October 2004 by a vote of 399-1. Andrew Noyes, *Spyware Bill OK'd by House Commerce Committee*, 6 WASHINGTON INTERNET DAILY 47, Mar. 10, 2005. Its sponsor, Representative Mary Bono of California, reintroduced the SPY ACT in January 2005. The Subcommittee on Commerce, Trade, and Consumer Protection reported out H.R. 29 on Feb. 16, 2005. On March 4, 2005, an amended version of the bill was proposed by the Commerce Committee, and on May 23, 2005, the bill passed in the House. GovTrack.us, 109th Congress: Securely Protect Yourself Against Cyber Trespass Act, http://www.govtrack.us/congress/bill.xpd?bill=h109-29 (last visited Aug. 29, 2005). Chairman Barton of Texas has vowed to get H.R. 29 to the President's desk during 2005. *See* Michael Grebb, *Revised Spyware Bill Moves Ahead*, WIRED NEWS, Mar. 10, 2005, http://www.wired.com/news/politics/0,1283,66848,00.html.

braska, New York, Rhode Island, Virginia, and Washington proposed (or passed) bills: unauthorized "taking control" of the computer, modifying settings of the computer without authorization, modem hijacking, using the computer as part of a network of computers to cause damage, delivering uncloseable advertisements, collecting personally identifiable information by keystroke logging, phishing, and rendering security software inoperable.[40]

The SPY ACT "notice" provisions are far more complicated than those found in most of the state level bills.[41] The Act begins by creating the term Information Collection Program (ICP). According to the Act, an ICP is computer software that collects personally identifiable information and sends it on to anyone else, or uses it to show an advertisement. The bill contains a list of specific information that is considered "personally identifiable."[42] Next, the Act goes on to include in the definition of an ICP computer software that collects information about webpages accessed by a computer[43] (whether or not personally identifiable) and uses it to show advertisements. This is potentially a very broad category of code. HTML code, Java script, noncommercial applications, and very localized search functions that show ads based on pages visited within a site or search terms employed within a particular application might all fall within this definition.[44]

To this broad category of software, the SPY ACT applies an opt-in notice and consent provision, making it illegal to transmit an ICP to or execute an ICP on a computer unless the ICP (1) provides notice (including

---

40. *See supra* note 26.

41. Florida has introduced S.B. 2162, 2005 Leg., Reg. Sess. (Fla. 2005), and Georgia has introduced S.B. 127, 2004-05 Reg. Sess. (Ga. 2005), both of which appear to be very closely modeled on the SPY ACT.

42. SPY ACT § 10 (including specific information, like name, physical address, e-mail address, phone number, SSN, tax ID number, passport number, driver's license number, credit card number, access code, password, and date of birth).

43. The SPY ACT potentially covers all devices that compute around the world. *See infra* note 50.

44. Section 3(b)(2) of the SPY ACT states that computer software that would otherwise be considered an ICP will not be if the only information collected has to do with pages within a particular site and the information is not made available to people other than (i) the provider of the website accessed or (ii) a party authorized to facilitate the display or functionality of webpages within the site accessed. The only permitted advertising delivered to or displayed on the computer using this information is advertising on pages within that particular site. It is not clear how the SPY ACT will deal with information feeds or new technologies (including communication clients of various kinds) whose outputs do not map clearly onto "websites" or "pages."

specific English-language disclosures) and (2) includes functions listed in the bill.

The notice provisions in the SPY ACT require that ICP notices be clearly distinguished from any other information visually presented at the same time on the computer, and that they contain particular required texts in English, for example, "This program will collect and transmit information about you. Do you accept?" or "This program will collect information about Webpages you access and will use that information to display advertising on your computer. Do you accept?"[45] The notice also must provide a description of the types of information to be collected and sent by the ICP, an explanation of the purpose for these actions, and identify the ICP by name. After the user has consented to execution of the ICP, if the program is used to collect or transmit materially different information, a second notice must be sent and a second consent must be obtained. The Federal Trade Commission (FTC) is commanded to issue regulations on these notice subjects.[46] The FTC is not, however, provided with additional funding for this drafting work.[47]

---

45. The required notices may not communicate effectively to the 10 percent of Americans who do not speak English. US CENSUS BUREAU, LANGUAGE USE AND ENGLISH-SPEAKING ABILITY: 2000, Oct. 2003, http://www.census.gov/prod/2003pubs/c2kbr-29.pdf. Moreover, because the SPY ACT potentially affects devices around the globe, *see infra* note 50, Chinese notices may be more appropriate.

46. The SPY ACT is under the jurisdiction of the House Commerce Committee, which has been fiercely fighting for control over Internet-related issues with the Committee on the Judiciary for several years. *See, e.g.*, *House Commerce and Judiciary Committees Vie for High Tech Leadership*, TECH LAW JOURNAL, June 15, 1999, http://www.techlawjournal.com/intelpro/19990616a.htm. The Commerce Committee has jurisdiction over the FTC, and thus is interested in making spyware a deception issue subject to FTC rulemaking. Rep. Barton of Texas, who chairs the House Commerce Committee, has made clear that spyware legislation is his top priority. Because Rep. Barton is also in charge of rewriting the Telecommunications Act, it would be politically unwise for large online companies to challenge his spyware agenda, as it may adversely effect their telecommunications interests as well. For an exploration of the implications of the turf war between the Judiciary and Commerce committees, see John M. deFigueiredo, *Committee Jurisdiction and Internet Intellectual Property Protection*, May 2002, http://itc.mit.edu/itel/docs/2002/defigueiredo_0502.pdf (describing jurisdictional turf wars between committees over continuing and new issues can have a profound impact on the behavior of legislators and the outcomes of policies).

47. The SPY ACT's anointing of the FTC as the drafter of spyware rules is reminiscent of the FTC's adventures in children's online privacy under the Children's Online Privacy Protection Act (COPPA) of 2000. I have noted that despite expending enormous energy drafting rules under that statute, the FTC has brought very few cases. There is evidence that some providers of legitimate interactive services for children went out of business rather than attempt to comply with the burdensome consent requirements of the rules. *See* Ben Charny, *The Cost of COPPA: Kids' Site Stops Talking*, ZDNET,

Under the SPY ACT, all ICPs must allow the program to be disabled easily by a user, and they must ensure that any triggered advertisement is accompanied by the name or logo of the ICP. "Embedded advertisements" (an undefined term) are excepted from the latter requirement. The FTC may make rules about these functions, but is not required to do so. The SPY ACT provides for fines of up to $3 million for "patterns or practices" that violate the "bad acts" provisions, and sunsets at the end of 2010.

2. I-SPY ACT of 2005

The House Judiciary Committee introduced its own bill, H.R. 744 or the Internet Spyware (I-SPY) Prevention Act of 2005, which passed in the House on May 23, 2005. The bill avoids the regulatory approach of the SPY ACT, instead focusing on penalties for actual harm to computers.[48] It imposes up to a two-year prison sentence on anyone who uses spyware to intentionally break into a computer and either alter the computer's security settings, or obtain personal information with the intent to defraud or injure a person or with the intent to damage a computer. Additionally, it imposes up to a five-year prison sentence on anyone who uses software to intentionally break into a computer and uses that software in furtherance of another federal crime.

3. SPY BLOCK Act

The Senate is considering S. 687, or the Software Principles Yielding Better Levels of Consumer Knowledge Act (SPY BLOCK Act), co-

---

Sept. 12, 2000, http://news.zdnet.com/2100-9595_22-523848.html?legacy=zdnn; Carrie Kirby, *Youth Privacy Net Law Takes Effect, Many Web Site Operators Worry They'll Lose Money on Children's Market*, SAN FRANCISCO CHRONICLE, Apr. 21, 2000, at B1, *available at* http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2000/04/21/BU102542.DTL; Electronic Privacy Information Center, *The Children's Online Privacy Protection Act*, http://www.epic.org/privacy/kids (last visited Aug. 19, 2005) (stating that critics have claimed that the methods outlined by the FTC for verification—sending/faxing printed forms, supplement of credit card numbers, calling toll-free numbers, and forwarding digital signatures through e-mail—are inadequate to protect personal information, as well as prohibitively costly and cumbersome. Consequently, children may manipulate information to access these websites, and that online businesses may eliminate children-focused sites).

48. I-SPY uses the same broad definition of protected computers found in the SPY ACT—any "electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device . . . which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States." 18 U.S.C.A. § 1030(e) (West 2005).

sponsored by Senator Burns of Montana and Senator Wyden of Oregon. This bill has "bad act" elements, but goes beyond the bad acts explored by state legislation to outlaw very general deceptive software acts: it is unlawful under the SPY BLOCK Act to cause the installation of software[49] on a computer[50] in a manner that conceals the fact of the installation of the software from the user, prevents the user from having an opportunity to grant or withhold consent to the installation, or is the result of inducing the user to consent to the installation by means of a misrepresentation; it is also unlawful to cause the installation of software that prevents uninstall efforts. Given the definitions of "software" and "computer" under the SPY BLOCK Act, it could potentially cover software associated with routing communications across the Internet.

The SPY BLOCK Act states that ads prompted by software are unlawful if they are displayed "without a label or other reasonable means of identifying to the user of the computer, each time such an advertisement is displayed, which software caused the advertisement's delivery."[51] The Act also contains some language that appears to be trying to make unlawful any software installation that would surprise an end user:

> (a) It is unlawful for a person . . . to— (1) cause the installation on that computer of software that includes a surreptitious information collection feature; . . .
>
> (c). . . the term "surreptitious information collection feature" means a feature of software that—
>
> (1) collects information about a user of a protected computer or the use of a protected computer by that user, and transmits such information to any other person or computer—
>
> (A) [automatically]
>
> (B) [invisibly] and
>
> (C) for purposes other than—(i) facilitating the proper technical functioning of a capability, function, or service that an authorized user of the computer has knowingly used, executed, or enabled . . .
>
> (2)...without prior notification that—(A) clearly and conspicuously discloses to an authorized user of the computer the type of information the software will collect and the types of ways the

49. Under the SPY BLOCK Act, "the term 'software' means any program designed to cause a computer to perform a desired function or functions." S. 687, 109th Cong. § 13(9) (2005).

50. As in the other federal pieces of legislation, "computer" is defined very broadly to include all computers around the world. *Id.* § 12(8).

51. *Id.* § 4(a).

> information may be used and distributed" has not been provided.[52]

The FTC is given authority to promulgate rules for notifications that software will have to provide in order to avoid being categorized as a "surreptitious information collection feature."[53] Preemption provided by the SPY BLOCK Act is narrower than in the other federal bills, and covers only state legislation or regulation that deals with software installed or used to collect information or present ads, or prescribes specific methods for providing notification before the installation of software on a computer.[54]

It is likely that the Senate will pass the SPY BLOCK Act with a criminal amendment. The differences among the SPY BLOCK, I-SPY, and SPY ACT bills will be worked out in conference committee meetings. These bills are marching towards passage with virtually no opposition, which is not surprising because it is difficult to lobby against a bill labeled as fixing the problem of "spyware."

E. Implications of Pending Legislation

1. Implication One: Design Mandates

To the extent these bills deal with deceptive "bad acts" that are widely viewed as harmful spying, they are likely duplicative of existing unfair trade practices laws and unlikely to pose problems for future innovation. The I-SPY ACT falls within this category, as do the "bad acts" bills (including the first section of the SPY ACT) that focus on software that deceptively "takes control" of a computer or uses keystroke loggers. Because the deceptive use of software is outlawed under these bills, not the software itself, they may have the salutary effect of pushing the FTC to bring cases against clearly bad actors. But bills that broaden the definition of "spyware" to include software that gathers information about the websites visited by a user, or software that somehow surprises a user (as in the pending SPY BLOCK Act), or software that triggers contextual ads or web content based on user activity or use of unauthorized search terms (as in the revised Utah bill and the other state "trademark" bills), and require "notice" to be given to consumers before such software can be legally used, constitute technical design mandates focused on the software itself rather than legislation about deceptive behavior.

---

52. *Id.* § 3.
53. *Id.* § 7(b).
54. *Id.* § 10.

For example, under the proposed SPY ACT, all "information collection programs" must provide "notice" and include required functions in order to be considered lawful.[55] Information collection programs are broadly defined to include software that "collects information regarding the Web pages accessed using the computer" and "uses such information to deliver advertising to, or display advertising on, the computer."[56] In order to avoid falling into the hole of "spyware" liability, software meeting these broad definitions must provide elaborate disclosures in English and obtain consent from users. Similarly, the SPY BLOCK Act makes illegal "surreptitious information collection features" that without notice to the user collect information and use it for purposes that might surprise the user, and outlaws software that causes ads to be displayed without labels of various kinds. All of the "trademark" state bills and "notice" bills require notices and labels for liability to be avoided. Broadly stated, because these pending bills require functions, labels, and notices to be applied to software, whether or not the software coder feels it is a good idea to have such notices in place or the advertiser wants a label plastered on its ad, they are design mandates.

In conversation, people will say clearly that they think "spyware" is bad. We can all agree that the kinds of bad acts addressed by these bills constitute behavior that should be punished. Deceptive hijacking of the browser function, deceptive phishing, and deceptive installation of software are all things we can be confident are wrong. These provisions will not slow the course of innovation. But defining "spyware" in terms of broad categories of functions plus absence of "notice" (and clickthrough "assent") is a step legislatures should not take lightly, for several reasons.

First, the definition could be over-inclusive. Many of these broadly defined functions are in fact things that users now and in the future may want to have happen invisibly. For example, Yahoo! is offering a deeply contextual search function—Y!Q—that users can place on their own websites.[57] When text is highlighted on that page, and the search function is triggered, the search results respond to the text in context on the page. What if Y!Q also included ad results in exchange for the free service? Would that be "spyware" under one of these bills? Would users then have to see only labeled ads, or respond to notices in order to get the search function at all?

---

55. SPY ACT, 108th Cong. § 3 (2004).

56. *Id.*

57. *See* Yahoo! Search Help: Y!Q Search, http://help.yahoo.com/help/us/ysearch-/yq/index.html (last visited Aug. 30, 2005).

Similarly, Google is now offering an updated version of the popular Google Toolbar that allows users to highlight text on any webpage and be sent directly to another site—even though the author of the webpage did not insert a link in the underlying text.[58] In effect, Google is adding its own links to pages, starting initially with U.S. addresses as the highlighted text that goes to Google-chosen maps. Google tracks and logs the information gathered through this process, including pages visited, searches chosen, form information filled-in, and the IP address of the visitor, and can link that information to whatever a Google registrant has done with his or her Gmail account. Google can then use this information to trigger highly-focused ads that are presented to the user in Gmail or other contextually relevant places.[59] Would a user be surprised by this functionality? Should the Google Toolbar-generated ads be accompanied by various labels that make it clear what software triggered these ads? What if the user's use of the Google Toolbar generated just a drop of data in an ocean of other Google-gathered information that triggered these ads?[60]

SideStep, which bills itself as "the traveler's search engine," accompanies users as they shop for travel services online. When a user is about to

---

58. Anita Hamilton, *Google Tricks*, TIME MAGAZINE, Mar. 7, 2005, http://www.time.com/time/archive/preview/0,10987,1032364,00.html.

59. In 2004, Google filed a declaratory judgment action against American Blind based on American Blind's threats of suit arising out of Google's keyword advertising practices. Google, Inc. v. Am. Blind & Wallpaper Factory, Inc., No. C03-5340, 2004 U.S. Dist. LEXIS 27601 (N.D. Cal. Apr. 8, 2004). In March 2005, the Northern District refused to grant Google's motion to dismiss American Blind's trademark infringement and dilution claims, stating that American Blind might be able to show actionable trademark "use" based on purchase of keywords by Google advertisers. Google, Inc. v. Am. Blind & Wallpaper Factory, Inc., No. C 03-05340 JF, 2005 U.S. Dist. LEXIS 6228 (March 30, 2005). Judge Brinkema of the Eastern District of Virginia recently issued a decision concerning Google's use of keywords to trigger advertisements. Geico v. Google, Inc., No. 1:04cv507 (E.D. Va. Aug. 8, 2005) (holding that while mere use of keywords to trigger advertisements does not constitute trademark infringement, advertisements that reference trademarks in their headings or text may infringement trademarks).

60. eBay also has a toolbar that knows where you are on the eBay network of sites (including PayPal) at all times, and where you are when you have left that network. The eBay toolbar also includes an "Account Guard" feature that warns users (using colors) when they are on potentially fraudulent—spoofed—eBay or PayPal sites, and when they are on non-eBay sites. Users can report sites that they believe to be spoof sites, and that information will be reviewed by eBay and made part of the toolbar functioning if the tip is found to be accurate. Regarding this issue, eBay's Frequently Asked Questions states that the eBay toolbar is not spyware. eBay Frequently Asked Questions, eBay Toolbar With Account Guard, http://pages.ebay.com/help/announcement/4.html (last visited Aug. 30, 2005).

purchase a plane ticket, a narrow SideStep box slides out from the side of the user's screen, letting the user know that better deals on the same trip are available from different companies.[61] Many more SideStep-like applications will emerge in the months and years to come, accompanying users to provide comparison shopping and trust/verification services. Some of these services may not provide notices of any kind, and may be installed invisibly when a user elects a particular network of relationships or chooses a particular provider of online access. These applications will help users understand and organize the overwhelming wealth of information available online. They will certainly be tracking what users see and what users' preferences are, and they will have extensive information about users' offline activities. Will we call these applications "spyware," and claim that they are unlawful if they do not communicate particular prescribed notices and labels? Many of these applications are or will be free, and users want to continue having access to helpful free software.[62]

Cookies, text files that are sent by a webserver to a user's browser, are generally not considered spyware because they can only be read by the site that sent them. Thus, cookies do not track user activity across their entire web experience. But many major websites allow network advertisers, like DoubleClick and AvenueA, to place cookies on users' browsers and collate the information gathered for purposes of targeted advertising. The more sites that are served by these network advertisers, the richer and more sophisticated their databases of user activities become. Are these so-called "third party cookies" spyware that should be unlawful without notices and labels? Are users (or computers) harmed by well-targeted ads?[63]

Second, requiring these broad categories of sometimes-helpful software to provide notices (and obtain traceable consent to these notices) and include required functions, such as uninstallation features and readily-available information links, will greatly constrain the freedom of software designers. I am not arguing that facially unlawful software that does nothing but perform intrusive bad acts (like spreading viruses, or installing

---

61. *See* SideStep: The Traveler's Search Engine, http://www.SideStep.com/html/about_SideStep/main.html (last visited Aug. 19, 2005).

62. *See* 2005 Spyware Study, May 12, 2005, http://www.networkadvertising.org/spyware-forum/2005_Consumer_Spyware_Survey_NAI_051205.pdf (reporting national survey of 2000 Internet users and showing most people download free software and do not want new anti-spyware laws to prevent them from being able to download such software).

63. Updating virus control requires "spyware," and parental controls (settings that a user can alter to block particular kinds of content from being accessed by members of a household) raise some of the same concerns. Both require "monitoring" of the use of a computer; both might surprise users; neither is malicious.

Trojan horses, or changing a PC's settings) should be legal. I am saying, however, that new software applications with both "spying" and "serving" elements may be developed. Right now, enhanced search toolbars and third-party cookies both spy and serve. It is unclear what will happen next in the world of legitimate software development—and requiring particular features and the provision and tracking of "notice" will inevitably constrain some developers from doing inventive things that users might like.[64]

Indeed, it may be that laws mandating particular forms of code (and the application of labels and notices to this code) are unconstitutional. We can *protect* code (from copyright and patent infringement and from circumvention),[65] and *prevent* code by law from being exported (if it uses an encryption algorithm that exceeds certain limits),[66] but only when the government is acting as a customer (or funder) can it *mandate* that code have particular attributes.[67] Otherwise, design mandates become government-facilitated upstream censorship—something that is inconsistent with free speech values.

Requiring the use of particular labels and notices is arguably a violation of the First Amendment right "to refrain from speaking at all."[68] As the Supreme Court put it in *Riley v. National Federation of the Blind of North Carolina*, "Mandating speech that a speaker would not otherwise make necessarily alters the content of the speech. We therefore consider

64. The use of voluntary privacy notices has had good effects on data practices in the U.S., because such statements give the FTC and its state counterparts ways to attack data practices that do not match the promises made in these privacy notices. Professor Pam Samuelson has suggested that, similarly, mandatory notices for digital rights management (DRM) might have good effects for consumers. Pam Samuelson, A Notice Requirement for DMCA Anti-Circumvention Rules, paper presented at Modest Proposals 2.0 Conference at Cardozo Law School (Feb. 24-25, 2005). But mandatory notices, either for DRM or for software that some legislatures would consider "spyware" would raise constitutional concerns as well as pose threats to innovation. *See supra* II.D.i.

65. Digital Millennium Copyright Act, 17 U.S.C. §§ 1201-1205 (2005); Dennis S. Karjala, *Distinguishing Patent and Copyright Subject Matter*, 35 CONN. L. REV. 439 (2003).

66. Export controls on commercial encryption products are administered by the Bureau of Industry and Security of the U.S. Department of Commerce. 15 C.F.R. pts. 730-74 (2004).

67. *Compare* U.S. v. Am. Library Ass'n, 539 U.S. 194 (2003) (discussing Children's Internet Protection Act, requiring public libraries to use Internet filters as a condition of receiving federal funding, not violative of First Amendment), *with* Ashcroft v. ACLU, 124 S. Ct. 2783 (2004) (discussing the Child Online Protection Act and holding that imposing fines and prison terms for knowingly posting web content that is harmful to minors for "commercial purposes" is likely unconstitutional because it is not the least restrictive means available to protect children).

68. Wooley v. Maynard, 430 U.S. 705, 714 (1977).

[such legislation] as a content-based regulation of speech."[69] Although it is true that commercial speech receives less protection than noncommercial speech,[70] and that disclosures can be required to keep commercial speech from being deceptive,[71] it is not at all clear that software is commercial speech.

The Supreme Court provided three factors that identify commercial speech when existing in combination: (1) advertisement; (2) mentioning a specific product by name; and (3) economically-motivated speech.[72] Software transmitted to users and networks does not necessarily meet this standard. Source code has been held to be expressive and thus protected by the First Amendment.[73] Sweeping online "notice" and "consent" laws do not seem adequately tailored to address problems with data privacy when offline data practices are left untouched—under either the intermediate scrutiny applied to commercial speech or the strict scrutiny applied to pure speech.[74] And even if software is commercial speech, spyware is not necessarily misleading or part of an illegal activity—the threshold inquiry for regulation of commercial speech under *Central Hudson Gas & Electric Corp. v. Public Service Commission*.[75] As the Court has said, "Our recent decisions involving commercial speech have been grounded in the faith that the free flow of commercial information is valuable enough to justify imposing on would-be regulators the costs of distinguishing the truthful from the false, the helpful from the misleading, and the harmless from the harmful."[76]

---

69. 487 U.S. 781, 795 (1988); *see also* Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049 (2000).

70. Ohralik v. Ohio State Bar Ass'n, 436 U.S. 447, 456 (1978).

71. Zauderer v. Office of Disciplinary Counsel, 471 U.S. 626, 651 (1985).

72. Bolger v. Youngs Drug Prods. Corp., 463 U.S. 60, 66-67 (1983) (striking down ban on mailings of contraceptive ads).

73. Junger v. Daley, 209 F.3d 481, 485 (6th Cir. 2000).

74. Boos v. Barry, 485 U.S. 312, 321 (1988) (applying the strict scrutiny standard, which requires the government to show a compelling interest in restricting the speech and that the restriction is necessary and narrowly tailored to achieve that end); Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Commc'n, 447 U.S. 557, 564 (1980) (stating that under intermediate scrutiny, regulation must not be more extensive than necessary to serve that interest).

75. 447 U.S. at 564.

76. *Zauderer*, 471 U.S. at 646.

Third, users[77] may not actually want to know everything that their machines are doing. Since the demise of the command line, the graphical user interface has been piling abstractions on top of abstractions and hiding more and more functionality from the user.[78] HTML, after all, is itself an invisible function of computer software, telling the browser how to render particular code visible to the user. It is code transmitted to and executed within the user's browser without the user's permission or knowledge. JavaScript, similarly, is used by web designers to make HTML pages more dynamic. It is also sent to the client as text and executed in the browser without the user's permission or knowledge. Several of the pending bills (including the SPY ACT) suggest that computer software that collects information about webpages accessed by the computer, or that is executed or installed without the user's knowledge, is potentially spyware that requires notice and consent. How much of this approval process do users want to be involved in? Would users like to know every time something "happens" inside their computer, and give approval to it?[79] Probably not. Users who set their browsers to "not accept cookies without permission" end up having terrible usage experiences, because they have to click to agree over and over again in order to sustain a single session on a single website.

Fourth, insisting on "notice and consent" for broadly-defined "spyware" will lead to a hopelessly impoverished and meaningless regime. No one will understand what a "yes" click means, and most people will simply click through as much as possible in order to be allowed to continue the session. If a "yes" is answered to the question "do you consent to the collection of information about your web browsing session," then that "yes" does not signal that the user understands how that collected informa-

77. Although policy discussions surrounding the spyware bills concern "users" and "consumers," the bills deal with electronic devices generally (worldwide) and "authorized users" of those devices. These "authorized users" could be systems administrators or network operators.

78. *See generally* M. MITCHELL WALDROP, THE DREAM MACHINE: J.C.R. LICKLIDER AND THE REVOLUTION THAT MADE COMPUTING PERSONAL (2001).

79. Perhaps for this reason, a recent revision of the SPY ACT exempts particular kinds of "computer software" from the notice provisions of the bill. If the software is (a) only collecting information about what pages have been accessed inside a particular website, (b) does not send information to someone other than the website operator, and (c) does not prompt advertising other than ads on the webpages within that particular website, it will not be considered an ICP. E-mail from David Cavicke, General Counsel and Chief Counsel for Commerce Trade and Consumer Protection, House Committee on Energy and Commerce (Mar. 11, 2005, 17:46:26) (on file with the author). This language is designed to exempt "HTML and Java when either performs ordinary functions like constructing Web pages," according to House staff. *Id.*

tion may be used from that moment to the end of time. It would be impossible to explain the consequences of a single "yes" without writing a novel and sending it for approval to the user. To the extent these "yes" clicks represent assent to a contract of adhesion, that contract will rise and fall based on its reasonableness, not on the presence or absence of a user's click.[80] In effect, the government will be requiring users to click helplessly along, assenting to something they do not understand over and over again.[81] This is more like forced speech ("CLICK! CLICK!") than consumer protection. Labeling generated ads to signal what software generated them is also a largely meaningless pursuit. Why will this information make any difference to the consumer? Wouldn't the consumer be happier managing his/her own user experience by using tools that block pop-ups, rather than gathering over and over again the empty knowledge of the ad's origin?

In sum, these design mandate elements of the pending legislative efforts should be understood for what they really are: reflections of an overall desire to control the online world. Although this set of issues is coming up in a context that many find "easy"—as there are few lobbyists for spyware—enacting these technical mandates should not be easy steps for legislators to take. There is in the world today an enormous push for control over the Internet generally[82] that uses fear of online threats to fuel its progress. In the copyright wars, we see a drive for technical mandates constraining devices (the broadcast flag) and requiring notices and redesigns of general purpose software that might be used for copyright infringement.[83] Staff to senators have said that software should be subject to a regime similar to products liability law, and be redesigned to avoid the risk of infringement and labeled to warn users of the potential for such risks.[84]

---

80. *See* ProCD, Inc. v. Zeidenberg, 86 F.3d 1447 (7th Cir. 1996) (holding that a software licensor can bind purchasers by: (1) providing notice of a license to a consumer at the moment of licensing, and (2) providing the license terms and conditions following the moment of license); M/S Bremen v. Zapata Off-Shore Co., 407 U.S. 1 (1972); Carnival Cruise Lines, Inc. v. Shute, 499 U.S. 595 (1991).

81. And if software manufacturers are providing notice and collecting consent, how will they know who consented to what without collecting and maintaining a great deal of personally-identifiable information? The privacy implications of these bills have not been explored—at least not publicly.

82. *See* Susan P. Crawford, *The Biology of the Broadcast Flag,* 25 HASTINGS COMM. & ENT. L.J. 603 (2003); Susan P. Crawford, *Shortness of Vision: Regulatory Ambition in the Digital Age*, FORDHAM L. REV. (forthcoming 2005).

83. *See* MGM Studios, Inc. v. Grokster, Ltd., 125 S. Ct. 2764, 2780-81 (2005).

84. Tom Sydnor, S. Comm. on the Judiciary staff member for Sen. Orrin Hatch, Public Statement at The Modest Proposals 2.0 Conference at Cardozo Law School (Feb. 25, 2005).

Similarly, the FBI would like to subject new online applications to pre-approval regimes, to ensure that they are easily tappable by law enforcement (and redesigned if they are not).[85] And the telecommunications industry would like to see broad application of "consumer privacy" mandates to IP-enabled services,[86] including required notices, labels, and all the rest. Notices, labels, and design mandates for software designated as "spyware" fit into this larger desire by incumbents for control over the high-tech industry, and represent a first crucial step down this path.

This may sound like an overstatement. "Why, no," you say to yourself. "There are no black helicopters here. All we're trying to do is lessen the scourge of spyware. Surely you can't suggest that great incumbent industries—law enforcement, content, and telecommunications—are behind this legislative effort so as to gain further control over software development."

I agree that consumer protection is a key goal for lawmaking, and I am confident that most legislators are being pushed by their relatives to do something about spyware. But this spyware battle presents an opportunity for specific design power to be asserted over code in a way we have not yet seen.[87] I would not be concerned if the legislation under consideration dealt only with "bad acts" that most people agree constitute spying. Taking this step seems wholly appropriate, and not worth an alarmist response. The insertion of notice and labeling mandates, by contrast, raises red flags and signals a shift in our understanding of what code is.

If code needs notice and labeling, it must be something that otherwise could be subject to product liability claims for failure to warn.[88] But because direct physical injury is not caused by software, it should not be

---

85. Joint Reply Comments of Industry and Public Interest, *In re* Communications Assistance for Law Enforcement Act and Broadband Access and Services, ET Docket No. 04-295 (FCC Dec. 21, 2004).

86. In re IP-Enabled Servs., 19 F.C.C.R. 4863 (proposed Feb. 12, 2004).

87. *See* A. Michael Froomkin, *The Metaphor is the Key: Cryptography, The Clipper Chip, and The Constitution*, 143 U. PA. L. REV. 709, 718-34 (1995) (describing uses of encryption technology to protect communications and provide data security).

88. RESTATEMENT (THIRD) OF TORTS: PRODUCTS LIABILITY § 2 (1998) breaks down the definition into three distinct areas: (1) Manufacturing Defects—when the product departs from its intended design, even if all possible care was exercised; (2) Design Defects—when the foreseeable risks of harm posed by the product could have been reduced or avoided by the adoption of a reasonable alternative design, and failure to use the alternative design renders the product not reasonably safe; and (3) Inadequate Instructions or Warnings Defects—when the foreseeable risks of harm posed by the product could have been reduced or avoided by reasonable instructions or warnings, and their omission renders the product not reasonably safe. The design defects approach seems to have been adopted with respect to code, at least in dicta, by Judge Posner in the *Aimster* decision. In re Aimster Copyright Litig., 334 F.3d 643 (7th Cir. 2003).

treated under a products liability regime—which traditionally focuses on tangible rather than intangible products. When we think of "products" whose manufacturers should be liable for "failure to warn," we think of chairs, or power tools, and so does the Restatement (Second) of Torts.[89] Software is much more like speech than it is a product.[90] It is not clear that rendering code subject to "failure to warn" standards would improve the quality of software.[91] And it would undoubtedly constrain what new code is allowed to do, limit user experiences, and lead to a flurry of inexplicable notices and labels[92] that might drive people away from the online world.

Because legislation is primarily a one-way ratchet,[93] should "spyware" notice and labeling bills pass legislatures will be in the business of demanding more and different notices and labels: "This software may permit copies to be made. WARNING." or "This software allows you to meet

---

89. RESTATEMENT (SECOND) OF TORTS § 402A (1979) (providing the framework for products liability law); *see also* Winter v. G.P. Putnam's Sons, 938 F.2d 1033, 1034 (9th Cir. 1991) ("The purposes served by products liability law . . . are focused on the tangible world . . . .").

90. The Magnuson-Moss Warranty—Federal Trade Commission Improvements Act, 15 U.S.C. §§ 2301-2312 (2000), which establishes minimum standards for consumer product warranties, may apply to software sold to consumers. I attended an FTC workshop in October 2000 at which the applicability of Magnuson-Moss to software was discussed, and there was no answer as to whether it did or did not.

91. *See* Jeffrey Neuberger & Maureen Garde, *Information Security Vulnerabilities: Should We Litigate or Mitigate?*, 21 Andrews Computer & Internet Litig. Rep. 13 (Mar. 2004) ("On the face of events, it appears that limiting liability for software defects may have been part of the solution to the Y2K problem. . . . Perhaps the economic resources that would have been devoted to litigating Y2K issues went instead to mitigating Y2K problems.").

92. Compare the experience of consumers with required financial privacy notices under Title V of the Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-6809 (2000). That Act requires that financial institutions provide certain disclosures regarding their privacy policies and provide opt-out opportunities before releasing information about individuals to third parties. Most experts agree that these notices are viewed by consumers as meaningless, and there is no evidence that the existence of these notices has led to increased privacy. And at least one "readability consultant" has concluded that consumers are unable to read and understand these notices. Mark Hochhauser, *Lost in the Fine Print: Readability of Financial Privacy Notices*, PRIVACY RIGHTS CLEARINGHOUSE, July 2001, http://www.privacyrights.org/ar/GLB-Reading.htm.

93. For example, in the Uniting and Strengthening America by Providing Appropriate Tools required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Pub. L. No. 107-56, 115 Stat. 272, Congress made substantial changes to the 1978 Foreign Intelligence Surveillance Act (FISA), Pub. L. No. 95-511, 92 Stat. 1783. Although there is a sunset provision for these FISA changes in § 224 of the Patriot Act scheduled for December 31, 2005, it is very unlikely that we will return to pre-9/11 standards for foreign intelligence surveillance.

strangers and converse with them. Do you REALLY WANT TO DO THIS?"

2. *Implication Two: Lack of Efficacy*

Even with all the elements of the previously discussed approaches addressing spyware—notices, design mandates, and bad acts—written into legislative language, will federal spyware legislation work? The clear answer is "no." Although legitimate software distributors who routinely comply with law will provide notices and constrain their design efforts, rogue spyware sources will simply move offshore and continue their deceptive work, or stay in the U.S. and design around the rules. This has been our experience to date with the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act)[94] legislation of mid-December 2003.[95]

The most important element of CAN-SPAM, like the pending federal spyware bills, is that it preempts state anti-spam measures that are not directly related to fraud or deception.[96] Several states (most notably, California, with an "opt-in" bill that was scheduled to take effect on January 1, 2004) had enacted statutes that were extremely restrictive, and CAN-SPAM was designed to avoid the complexities of complying with fifty different state laws.

CAN-SPAM does not outlaw the sending of unsolicited commercial e-mail. Instead, it prohibits some fraudulent and misleading practices (such as misleading header information), requires senders to label their messages as commercial, and requires that senders give recipients a means to opt out of communications.[97] The labeling scheme of CAN-SPAM requires that senders provide in each message a "clear and conspicuous identification that the message is an advertisement or solicitation."[98] The Act is enforced by the FTC,[99] criminal prosecutions (with penalties ranging up to five

94. Pub. L. No. 108-187, 117 Stat. 2699.

95. *See* Press Release, The White House, Fact Sheet: President Bush Signs Anti-Spam Law (Dec. 16, 2003), http://www.whitehouse.gov/news/releases/2003/12/2003 1216-4.html; Tom Zeller, *Law Barring Junk E-Mail Allows a Flood Instead*, N.Y. TIMES, Feb. 1, 2005, at A2.

96. *See* 15 U.S.C. § 7708(b) (Supp. 2004).

97. CAN-SPAM Act, § 5(a)(3).

98. *Id.* § 5(a)(5)(A)(i).

99. *Id.* § 7(a).

years in prison),[100] actions by state attorneys general,[101] and suits by ISPs.[102]

Unsolicited e-mail on the Internet has actually increased since the passage of CAN-SPAM, and now amounts to 80 percent or more of all e-mail sent, up from 60 percent during the period before the law went into effect.[103] It appears that the greatest impact of CAN-SPAM has been to cause legitimate businesses heartaches as they try to avoid falling into some of the ambiguous traps that statute creates. Spammers, meanwhile, have changed their tactics since CAN-SPAM was enacted, and are now using "zombies networks" (computers hijacked with trojan horse programs, according to PC World) to send spam.[104] Nearly half of the world's spam is said to come from the U.S.[105] CAN-SPAM has neither made it easier to find spammers nor decreased the amount of spam.

Some may argue that CAN-SPAM was a toothless alternative to state opt-in bills, such as the California measure that CAN-SPAM was designed to preempt, and that federal spyware legislation could be made more effective than CAN-SPAM.[106] Spyware relationships leave a direct money trail that can be more easily followed than spam operations, making it potentially easier to police than spam. But both CAN-SPAM and the spyware bills attempt to do the same thing: control the flow of bits through law, in a world in which it is very difficult both to tell who is responsible for which bits and to locate these sources physically for enforcement purposes.

---

100. *See, e.g.*, Associated Press, *Spam senders convicted in first felony case*, Nov. 3, 2004, http://www.msnbc.msn.com/id/6401091 (noting that the court sentenced spammers to nine years in prison plus fines).

101. CAN-SPAM Act, § 7(f).

102. *Id.* § 7(g).

103. Zeller, *supra* note 95; Grant Gross, *Is CAN-SPAM Working? One year After it Went Into Effect, Many Say The Nation's Antispam Law is Ineffective*, PC WORLD, Dec. 28, 2004, http://www.pcworld.com/news/Article/0,aid,119058,00.asp (reporting Postini claim that legitimate nonspam e-mail was down to 12 percent in December 2004 and MX Logic claim that 25 percent of all e-mail was legitimate as of November 2004).

104. Gross, *supra* note 103.

105. Dan Ilet, *U.S. Leads the Dirty Dozen Spammers*, CNET NEWS.COM, Dec. 24, 2004, http://news.com.com/U.S.+leads+the+dirty+dozen+spammers/2100-7349_3-5503344.html.

106. Chris Hoofnagle of the Electronic Privacy Information Center made this point at a February 19, 2005 conference, "Real Law and Online Rights," sponsored by the Virginia Journal of Law and Technology at the University of Virginia. Hoofnagle has argued that the past decade of self-regulation has led to the spyware epidemic. Chris Jay Hoofnagle, *Privacy Self-Regulation: A Decade of Disappointment*, EPIC.ORG, Mar. 4, 2005, http://www.epic.org/reports/decadedisappoint.html.

Additionally, none of the spyware bills that are under consideration create any new funding for agency enforcement of their mandates. Real spyware—the truly harmful kind, not the broadly defined kind—comes from people who are completely dedicated to breaking the law. Without enforcement funding, and with the real difficulties involved in finding and prosecuting spyware sources, the spyware picture is unlikely to be changed by new federal laws. And international spyware sources will, of course, be completely unaffected.

3. *Implication Three: A Complicated Relationship With Existing Laws*

In response to the spyware epidemic, some have strongly suggested that spyware be addressed as a privacy issue.[107] In connection with pending federal spyware bills, and at the urging of legislators, public advocacy groups have testified in favor of "baseline" privacy legislation, whereby fair information practices[108] (including notice, consent, access, and security) would be required of all U.S. online participants.[109]

---

107. *See* Editorial, *The Spies in Your Computer*, N.Y. TIMES, February 18, 2004, at A1 (arguing that "Congress will miss the point [in spyware legislation] if it regulates specific varieties of spyware, only to watch the programs mutate into forms that evade a narrowly tailored law. A better solution, as proposed recently by the Center for Democracy and Technology, is to develop privacy standards that protect computer users from all programs that covertly collect information that rightfully belongs to the user").

108. An exhaustive discussion of the history and meaning of the phrase "fair information practices" is beyond the scope of this Article. *See generally* Secretary's Advisory Comm. on Automated Personal Data Systems, U.S. Dep't. of Health, Educ. & Welfare, *Records, Computers, and the Rights of Citizens* viii (1973) (stating five principles of fair information practices: no data record-keeping systems should be secret; access should be by subject; information obtained for one purpose should not be used for another purpose without consent; correction should be by subject; reliability and security of data is required); ORGANISATION FOR ECONOMIC CO-OPERATION AND DEV., RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA, Sept. 23, 1980, O.E.C.D. Doc. C(80)58 Final, *reprinted in* 20 I.L.M. 422 (1981) (stating eight similar principles); Council Directive 95/46 of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) (granting right of access to personal data, right to know where data originated, right for inaccurate data to be rectified, right of recourse in the event of unlawful processing, and right to withhold permission to use data in certain circumstances).

109. *See, e.g.*, *Combating Spyware: H.R. 29, the SPY ACT: Hearing Before the H. Comm. on Energy and Commerce*, 109th Cong. (2005) (testimony of Ari Schwartz, Associate Director, CDT), *available at* http://www.cdt.org/testimony/20050126schwartz.pdf; *Spyware: Hearing Before the S. Subcomm. on Communications of the Comm. on Commerce, Science, and Transportation*, 108th Cong. (2004) (prepared

This approach looks at spyware from the wrong end of the telescope. Although the scope of any constitutional "right to privacy" is hotly disputed,[110] such rights are fundamentally grounded in notions of property.[111] People have a right to privacy in their houses and effects, because a man's home is his castle.[112] When the subject for "privacy" is data about interactions between a user and his/her computer, or interactions between a computer and online resources,[113] it is very difficult to define the "property"

---

statement of Jerry Berman, President, CDT), *available at* http://www.cdt.org/testimony/20040323berman.pdf ("Fundamental to the issue of spyware is the overarching concern about online Internet privacy. Legislation to address the collection and sharing of information on the Internet would resolve many of the privacy issues raised by spyware.").

110. *See* Kyllo v. United States, 533 U.S. 27, 40 (2001) (stating that when "the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant"); Village of Belle Terre v. Boraas, 416 U.S. 1, 13 (1974) (Marshall, J., dissenting) (holding that an ordinance restricting "single-family" houses to those in which "persons related by blood, adoption, or marriage" live infringes upon "fundamental" First Amendment rights of privacy and freedom of association); Katz v. United States, 389 U.S. 347, 351-52 (1967) (overruling *Olmstead* and stating that "the Fourth Amendment protects people not places. . . . [W]hat [an individual] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."); Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting) (identifying a right of privacy and describing it as "the right to be let alone" in response to majority opinion that held that the government's use of wiretap without a search warrant did not violate the Fourth Amendment because no physical intrusion into the home where the calls were made); Louis Brandeis & Samuel Warren, *The Right of Privacy*, 4 HARV. L. REV. 193 (1890) (stating that the law should create a right to privacy protecting private facts).

111. Brandeis and Warren explored this right of property:

> That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. . . . Thus, in very early times, the law gave a remedy only for physical interference with life and property, for trespasses vi et armis. Then the "right to life" served only to protect the subject from battery in its various forms; liberty meant freedom from actual restraint; and the right to property secured to the individual his lands and his cattle. . . . Gradually, the scope of these legal rights broadened; and now the right to life has come to mean the right to enjoy life—the right to be let alone; the right to liberty secures the exercise of extensive civil privileges; and the term "property" has grown to compromise every form of possession—intangible, as well as tangible.

Brandeis & Warren, *supra* note 110, at 193.

112. *Id.*; *Kyllo*, 533 U.S. at 40; *Olmstead*, 277 U.S. at 478.

113. Although the preceding discussion should make clear that not all of the pending sypware bills are the same, or even similar, many of them go far beyond requiring

that is being impinged on and should be protected as "private,"[114] either through constitutional protection or common law tort claims. The key, defining characteristics of property are exclusive ownership and the ability to exclude (or invite) others. Do you "own" streams of data (created by your interactions by others) about your online transactions and experiences? Do you expect to be able to consent to, correct, and "remove" these streams of data that you "own"? Physically separable personal information is very different to conceptualize, much less protect.

More importantly, focusing on notions of inevitably property-based privacy misses the forest for the trees. The reason people are upset by spyware is that it creates oppressive, unwanted relationships through, for example, hijacking their browsers, or using their PC for an attack on others, or flashing unwanted pop-up ads. Users' instinctive worry is not that spyware violates some preexisting idealized control over particular pieces of data they "own" or could possibly define in advance in some clean, sterile way. As soon as a user goes online, he or she is thrust into an interactive data flow experience that is largely invisible to them. There is no castle; there are no walls; there is nothing to draw a line around and say "this is private." Users want many of these data flows to be invisible to them (or would want this if they suddenly had to control and authorize every data exchange). What is troublesome is bad interactions—oppressive, unreasonable relationships that bother the user.

Now that we have identified users' actual concerns about spyware, we discover that existing federal and state laws and court-created doctrines directed toward addressing oppressive relationships may already adequately address users' legal issues.

a) Federal Law

There are several federal laws addressing computer privacy. The federal Computer Fraud and Abuse Act (CFAA) already makes unauthorized

---

restraints on the use or collection of personally identifiable information to constraining the use or collection of use data generally. *E.g.*, SPY ACT, H.R. 29, 109th Cong. § 3(B)(1)(b) (2005) (covering "computer software that. . . (2)(A) collects information regarding the Web pages accessed using the computer; and (B) uses such information to deliver advertising to, or display advertising on, the computer").

114. *But see* Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1377 (2000) (stating that meaningful autonomy requires a degree of freedom from monitoring, scrutiny, and categorization by others); Daniel Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1091-92 (2002) (discussing need for ad hoc, contextual conceptions of privacy).

computer intrusions illegal.[115] The CFAA has proven to be a broad and flexible statute, under which anyone who obtains information from a computer or causes damage or obtains anything of value can be sued.[116] All spyware could potentially be reached by a claim under the CFAA, as long as the code caused (or would have caused) aggregated losses over a one-year period of at least $5,000.[117] Repeated, intentional spyware activity is likely to meet this threshold.[118]

The Electronic Communications Privacy Act (ECPA)[119] made it a crime and a statutory tort to intercept electronic communications, to disclose intercepted communications, or to use intercepted communications.[120] ECPA also made criminal (and tortious) any unauthorized access to "stored electronic communications."[121] To the extent that spyware is installed without user consent—which is often the case—ECPA may provide a cause of action against its source.

The FTC has already brought litigation against spyware sources under Section 5 of the Federal Trade Commission Act, which outlaws unfair or deceptive trade practices.[122] In October 2004, the FTC sought and obtained a federal court injunction against Seismic Entertainment Produc-

115. 18 U.S.C. § 1030 (2000). The central offense under the CFAA is the abuse of a computer to obtain information. Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1128-29 (W.D. Wash. 2000) (involving an employer who sued a competitor under the CFAA for hiring away employees to improperly gain information).

116. Civil causes of action under the CFAA are available against the violator for compensatory damages and injunctive relief. 18 U.S.C. § 1030(g) (2000); *see* Pac. Aerospace & Elecs., Inc. v. Taylor, 295 F. Supp. 2d 1188, 1196 (E.D. Wash. 2003) (stating that employers "are increasingly taking advantage of the CFAA's civil remedies to sue former employees and their new companies who seek a competitive edge through wrongful use of information from the former employer's computer system").

117. 18 U.S.C. § 1030(g).

118. *See, e.g.*, Four Seasons Hotels & Resorts B.V. v. Consorcio Barr, S.A., 267 F. Supp. 2d 1268 (S.D. Fla. 2003) (holding that a hotel licensee violated the CFAA by intentionally attempting to access the licensor's protected computers without authorization, spoofing the licensor's computers, causing congestion on the licensor's VPN device, and obtaining information of value in the form of confidential customer and financial data).

119. Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.).

120. 18 U.S.C. § 2510 (1994).

121. *Id.* §§ 2701-10.

122. These provisions prohibit unfair or deceptive acts or practices in or affecting commerce. 15 U.S.C. § 45(a) (2000).

tions, Inc., Smartbot.net, Inc., and Sanford Wallace,[123] after alleging that these actors had installed software code onto users' computers without authorization that changed those users' home pages, downloaded and installed various other programs, caused an incessant stream of pop-up messages to be displayed, and triggered ads for defendants' "anti-spyware" programs. Defendants did not contest the agency's factual allegations, but argued that their actions were "accepted marketing practices used by reputable companies."[124] The FTC alleged that defendants' actions were "unfair."[125] The court agreed with this assessment and granted an injunction—adding that it thought defendants' actions were "deceptive" as well as "unfair."[126] Thus, the FTC been successful proceeding against "spyware" purveyors under its existing powers.

b) State law

Deceptive trade practices acts based on the Uniform Deceptive Trade Practices Act model have been adopted in many states.[127] California's unfair competition law imposes civil liability for "any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising,"[128] and provides standing for citizens that can show harm by such unfair practices to bring claims even where the conduct alleged is a violation of a statute that does not provide for a private right of action.[129] These acts broadly prohibit unfair or deceptive conduct in commerce, and thus could be used by states in connection with spyware activities in just the same way that the FTC has used its authority.

---

123. FTC v. Seismic Entm't Prods., Inc., No. 04-337-JD, 2004 U.S. Dist. LEXIS 2278 (D.N.H. Oct. 21, 2004), *available at* http://www.cdt.org/privacy/spyware/spywiper/20041021seismicruling.pdf.

124. *Id.* at *11.

125. Under the FTC Act, an act or practice is unfair if it: (1) causes or is likely to cause substantial injury to consumers; (2) the injury to consumers is not outweighed by any countervailing benefits; and (3) the injury is not reasonably avoidable by consumers. *See* 15 U.S.C. § 45(n) (2000).

126. "The affected users were not notified of the defendants' activities and did not know what had caused the problems with their computers, making the defendants' activities both deceptive and unfair." *Seismic Entm't Prods., Inc.*, 2004 U.S. Dist. LEXIS at *9-*10.

127. For example, Colorado, Delaware, Georgia, Hawaii, Illinois, Maine, Minnesota, Nebraska, New Mexico, Ohio, Oklahoma, Oregon. *See* Legal Information Institute, Uniform Business and Financial Laws Locator, http://www.law.cornell.edu/uniform/vol7.html#dectr (last visited Aug. 29, 2005).

128. CAL. BUS. & PROF. CODE § 17200 (Deering 2005).

129. *See* CAL. BUS. & PROF. CODE §17204 (Deering 2005); Barquis v. Merchants Collection Ass'n of Oakland, Inc., 496 P.2d 817, 828 (Cal. 1972).

If deception is difficult to prove, there is an even broader state law approach to spyware that captures the essence of the spyware violation: prima facie tort. Although not widely used (and in fact often denigrated), this tort addresses unjustified actions that are intended to harm another—or, in other words, the creation of an oppressive relationship.[130] The prima facie tort requires (1) an injury to another and (2) culpable conduct on the part of the actor that is (3) unjustifiable under the circumstances.[131] All other specific intentional torts are instantiations of the general principle stated in the prima facie tort.[132] In the absence of a mature, specific, clearly-delineated "spyware" intentional tort (or even an intentional tort that clearly applies to spyware), the prima facie tort will provide courts with a role in redressing oppressive relationships created by code.[133] Involving courts in creating a common law of spyware—deciding which oppressive relationships are harmful enough to merit judicial censure—will allow for a much more nuanced approach to spyware than is possible through legislation.

As outlined in the previous two subsections, both federal and state legal frameworks already exist that address the concerns that are driving the current push for spyware legislation. Litigation based on these existing

---

130. *See* RESTATEMENT (SECOND) OF TORTS § 870 (1979) ("One who intentionally causes injury to another is subject to liability to the other for that injury, if his conduct is generally culpable and not justifiable under the circumstances. This liability may be imposed although the actor's conduct does not come within a traditional category of tort liability."). Prima facie tort is recognized in Missouri, New Mexico, and New York. *See* Bandag of Springfield, Inc. v. Bandag, Inc., 662 S.W.2d 546, 553 (Mo. Ct. App. 1983); Schmitz v. Smentowski, 785 P.2d 726, 739 (N.M. 1990); Beavers v. Johnson Controls World Servs., Inc, 901 P.2d 761 (N.M. Ct. App. 1995); Curiano v. Suozzi, 469 N.E.2d 1324, 1327 (N.Y. 1984); Bd. of Educ. v. Farmingdale Classroom Teachers Ass'n, 343 N.E.2d 278 (N.Y. 1975).

131. ATI, Inc. v. Ruder & Finn, Inc., 368 N.E.2d 1230, 1232 (N.Y. 1977).

132. As for conduct intentionally causing harm, however, it has traditionally been assumed that the several established intentional torts developed separately and independently and not in accordance with any unifying principle. This Section purports to supply that unifying principle and to explain the basis for the development of the more recently created intentional torts. More than that, it is intended to serve as a guide for determining when liability should be imposed for harm that was intentionally inflicted, even though the conduct does not come within the requirements of one of the well established and named intentional torts.

RESTATEMENT (SECOND) OF TORTS § 870 cmt. a.

133. *See* Porter v. Crawford & Co., 611 S.W.2d 265, 269 (Mo. Ct. App. 1980) (noting that Justice Holmes introduced the prima facie tort doctrine in this country).

laws may be a better solution to spyware than legislation—particularly "notice" and "labeling" legislation.

But even litigation's effect on spyware will be greatly constrained by interdependencies, jurisdictional tangles, and technical realities that are beyond the scope of any court. Spyware purveyors are certainly not necessarily based in the U.S., and spyware often reaches consumers through highly complex chains of affiliates whose relationships are very difficult to parse.[134] Without an attorney's-fee recovery mechanism, many lawyers are unwilling to take on the expense of litigating against spyware sources, and prosecutors often lack the resources to investigate technical spyware cases.

III. THE TECHNICAL LANDSCAPE

Given that both legislation and litigation are unlikely to be up to the task of definitively solving the spyware problem, what should we do? There is no one legal institution with sufficient knowledge to recognize and fix the infinite varieties and functionalities of "bad" spyware in advance. Legal minds simply cannot design a sufficient attack on spyware. This Part suggests that legal systems can instead encourage deference to the development of technical immune networks, and points to areas for possible future work.

The informational properties of the immune system are remarkable. Although the networks that make up the human immune system are distributed throughout the body, the system is able to distinguish between "self" and "nonself" quickly and retain this information in "memory." It can thus tell the difference between harmful microbes (foreign materials or "antigens") and the body. Special types of white blood cells (lymphocytes) recognize foreign material by forming molecular bonds between these foreign materials and receptors on the surface of the lymphocyte. In effect, immune system detectors bind to particular (foreign) short chains of amino acids—thus recognizing the pattern encoded by these short chains.[135] These detectors are highly specific, so each recognizes only a limited

134. *Combating Spyware: H.R. 29, the SPY ACT: Hearing Before the H. Comm. on Energy and Commerce*, 109th Cong. (2005) (testimony of Ari Schwartz, Associate Director, CDT), *available at* http://www.cdt.org/testimony/20050126schwartz.pdf (noting that spyware download process is "sustained through a nearly impenetrable web of affiliate relationships that is used to deflect accountability and frustrate law enforcement").

135. Stephanie Forrest & Steven Hofmeyr, *Immunology as Information Processing*, *in* DESIGN PRINCIPLES FOR IMMUNE SYSTEM & OTHER DISTRIBUTED AUTONOMOUS SYSTEMS (L.A. Segal & I.R. Cohen eds. 2000).

number of foreign chains.[136] Some lymphocytes (those that mature in the thymus gland) actually attack and destroy cells that are recognized as foreign; others mark the foreign cells for destruction. This distributed system is error-tolerant, dynamic, self-protecting, and adaptable.[137] Lymphocytes that bind too strongly with "self" cells are selected out, so that the remaining cells will be able to recognize abnormal peptides. Once lymphocytes have encountered and destroyed a particular organism, they carry out resistance to that organism for some time—they remember their enemies. They also "learn" new foreign materials through the development of new receptors. Through a complex interaction among decentralized molecules, cells, and organs, acting independently but communicating, the system is able to protect individuals from outside and internal enemies.

Because it is able to respond in a fine-grained, highly parallel, distributed, decentralized, and coordinated way to enormous varieties of foreign materials, the idea of the human immune system provides a fascinating analogous physiological solution to the spyware problem.[138] Like antigens, spyware comes in a multitude of forms. No centralized command-and-control "inoculation" system could ever deal with spyware, because the learning/feedback loops would be simply too slow and too clumsy, and it would fail to deal with intruders it had never seen before.[139] An immune system can "learn" about particular foreign patterns—invading bits—and then remember what it learns.[140] It solves by swarming.

---

136. Stephanie Forrest & Steven Hofmeyr, *John Holland's Invisible Hand: An Artificial Immune System* (1999), http://www.cs.unm.edu/~steveah (presented at the Festschrift held in honor of John Holland).

137. *Id.*

138. Computer scientists know this well, and have been working comfortably with this metaphor for some time. *See* Forrest & Hofmeyr, *supra* note 136. The idea of an immunity network rather than a legal structure as a solution for a hard problem is new to lawyers, however. We are more used to hierarchies.

139. An FTC Report states, "Because the digital fingerprint [used by spyware scanner programs to identify spyware] is only developed after a spyware program is discovered and analyzed, there is a lag time between the distribution of a spyware program and the ability of anti-spyware programs to detect it." FTC, SPYWARE WORKSHOP REPORT, MONITORING SOFTWARE ON YOUR PC: SPYWARE, ADWARE, AND OTHER SOFTWARE 14 (March 2005), http://www.ftc.gov/os/2005/03/050307spywarerpt.pdf.

140. When the immune system encounters a new pathogen, it might take three weeks or so to clear the initial infection. Steven Hofmeyr, An Immunological Model of Distributed Detection and Its Application to Computer Security 30 (1999) (unpublished Ph.D. dissertation, University of New Mexico) (on file with author). But later invasions by the same pathogen will be reacted to much more quickly—indeed, there may be no evidence of a re-infection. *Id.* A classic example of immune system memory is the system's reaction to measles. *Id.*

A network built like an immune system would allow for a great deal of redundancy and simultaneously reduce local complexity, leaving less for individual machines/users to know. It would observe user-network interactions; learn the code paths that each application uses during its normal operations ("self"); develop a profile of each application's behavior and then block anything that falls outside that profile and is likely to do serious harm ("harmful non-self");[141] tell the human later what has been blocked (which, as "good" spam filters have taught us, is much better than simply blocking the material invisibly); log the event; minimize harm to the rest of the life going on inside the network; and allow creation of metainformation that will help other users. It would also operate in a completely decentralized fashion. The immune system, after all, is made up of millions of agents that act completely locally.

As just one existing example, Sana Security, founded by Steven Hofmeyr, is building computer security schemes that are based on immunity ideas.[142] Sana's software can "learn and take care of itself."[143] It "installs on the operating system and takes a snapshot of how the uninfected machine normally works."[144] Then "it waits and watches for anomalies to normal computing behavior and takes action against any deviation that could harm the PC or alter its normal operation."[145] The operation of this

141. Not all pathogens are harmful, and eliminating non-harmful pathogens might actually harm the human body. *Id.* at 1. The same is likely true of code.

142. *See* Sana Security, http://www.sanasecurity.com (last visited Aug. 19, 2005). Computer scientists have been talking about software in biological terms for some time. *See, e.g.*, Stephanie Forrest et. al, *Computation in the Wild*, *in* THE INTERNET AS A LARGE-SCALE COMPLEX SYSTEM (K. Park & W. Willinger eds. forthcoming), *available at* http://crypto.stanford.edu/portia/pubs/articles/FBGA1917099772.html (claiming that networked computer systems can be better understood, controlled, and developed when viewed from the perspective of living systems).

143. John Verity, *Computing*, MIT TECH. REV., Oct. 2003, http://www.techreview.com/Articles/03/10/tr100computing1003.asp; Dan Neel, *Sana Gives Desktop PCs Autoimmunity*, SECURITYPIPELINE.COM, Oct. 25, 2004, http://www.securitypipeline.com/news/51200074.

144. Neel, *supra* note 143.

145. *Id.* A recent article about watching botnets (networks of compromised machines that can be instructed remotely by an attacker) described the creation of "honeypots" that perform many of the same functions. THE HONEYNET PROJECT AND RESEARCH ALLIANCE, *Know Your Enemy: Tracking Botnets: Using Honeynets to Learn More About Bots*, Mar. 13, 2005, http://www.honeynet.org/papers/bots. These honeypots "actively participate in networks (e.g. by crawling the web, idling in IRC channels, or using P2P-networks) or modify honeypots so that they capture malware and send it to anti-virus vendors for further analysis." *Id.* There are, however, also legal risks of monitoring networks:

software may initially be annoying, until we teach it what we want it to allow. Like a young student, it may begin with many questions.

If Sana can do this, any other company can too. It is very likely that "immunity networks" will soon be available to us (either on our own desktops or within our own networks) that will learn our hard drives and watch for anomalies.[146] In small ways, these networks are already developing. Some excellent tools are already available to combat spyware, including Microsoft Anti-Spyware, Spybot Search and Destroy, Lavasoft's AdAware, CounterSpy from Sunbelt Software, and Computer Associate's eTrust PestPatrol. Sites like spywarewarrior.com and securitypipeline.com will help us figure out which networks to join or adopt.[147]

Very early versions of immunity networks already exist, in the form of updated Symantec or Norton client applications. To some extent, these applications learn from their environment and watch for events to which they should respond. But I suggest that these applications are primitives. They are not decentralized or peer-created. They rely on updated authoritative blacklists of undesirable bits and applications. Significantly, ISPs

---

> For honeynet deployments in the U.S., consider three legal issues: first, ensure that you are in compliance with the laws that restrict your right to monitor the activities of users on your system. Second, recognize and address the risk that attackers will misuse your honeynet to commit crimes, or store and distribute contraband. Third, consider the possibility that your honeynet will be used to attack other systems, and the potential liability you could face for resulting damage. Your lawyer may identify other legal issues as well. If you deploy a honeynet outside the U.S., look to the applicable laws of the jurisdiction in which you will operate. Designing and implementing your honeynet with attention to these concerns can help you stay out of legal trouble.

THE HONEYNET PROJECT, KNOW YOUR ENEMY 252 (2004).

146. Cisco is already doing this. *See Core Elements of the Cisco Self-Defending Network Strategy* (Cisco Self-Defending Network, White Paper 2005), http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns413/networking_solutions_white_paper0900aecd80247914.shtml. It has introduced its own "adaptive security" program, which relies on "network-based, multi-layered, application-oriented, IP-dependent, worm mitigation, dynamic trust" elements. *Id.* Its plan is for all network hardware and software on the backbone and within enterprises to be coordinated to provide security against spyware and other security threats. *Id.* Although enterprise network security is a classic subject, Cisco may have larger plans for "the Internet" itself.

147. Microsoft recently introduced its own anti-spyware program, available to Windows XP and Windows 2000 users for free download through July 2005. Microsoft Windows AntiSpyware (Beta), http://www.microsoft.com/athome/security/spyware/software/default.mspx (last visited Aug. 19, 2005). This event marks an enormous step forward because Windows operating systems run on more than 90 percent of computers worldwide.

like Earthlink and AOL are already competing on the basis of their ability to protect users from spyware,[148] and many ISPs spend up to 40 percent of their customer service resources responding to spyware-related inquiries.[149]

All of these things, taken together, will provide a solution to oppressive spyware. They will take the self-conscious form of immunity networks when users affirmatively tie their online access and communications to the use by themselves *and others they communicate with* of spyware protections that learn. We will eventually leave the ISP model of "membership" (which is based only on commodity connectivity rather than valuable learning/reaction services provided by network administrators) and move towards participation in immunity networks.[150] (These networks may map to the outlines of current ISPs for the foreseeable future, but with the rise of wireless mesh services ISPs as a business category may diminish in importance as the years go by.)[151] Groups of machines and people will cluster together, looking for companionship as well as security, and to join one of these networks will be to buy into a set of practices governing many different kinds of interactions.

We should wait for these steps to take effect, rather than plunging towards legislative solutions that are likely to cause more troubles than they solve. Law should now look at technology problems the way modern doctors look at health care: "do no harm," "do not give antibiotics when you

148. EarthLink offers a free software suite to its users that blocks spyware, spam, and viruses. Earthlink TotalAccess, http://www.earthlink.net/software (last visited Aug. 19, 2005). AOL claims it is the first ISP to offer automated spyware detection. Paul Roberts, *AOL Goes After Spyware*, PC WORLD, Jan. 6, 2004, http://www.pcworld.com/news/Article/0,aid,114106,00.asp.

149. Jim Thompson, *Malware Returns*, ISP-PLANET, May 27, 2005, http://www.isp-planet.com/business/2005/spyware.html.

150. I believe that the ISP intermediary business model, under which ISPs provide commodity connectivity to upstream networks, is already under enormous pressure, and that in the coming years, we will see great consolidation in the ISP marketplace. This is already happening in India. *See* Joji Thomas Philip, *80% ISPs fall off infobahn*, BUSINESS STANDARD, June 14, 2005, http://www.business-standard.com/iceworld/storypage.php?hpFlag=Y&chklogin=N&autono=191508&leftnm=lmnu9&leftindx=9&lselect=0 (reporting that 80 percent of India's 700 private ISPs have gone out of business in the last four years). Surviving ISPs will have to reinvent themselves as much more meaningful businesses, and immunity provisions may provide a useful path towards solvency.

151. *See* Microsoft Networking Research Group, *Self-Organizing Neighborhood Wireless Mesh Networks*, http://www.research.microsoft.com/mesh (last visited Aug. 19, 2005) (describing the topology of "community-based multi-hop wireless networks," in which every member of the network contributes packet-routing resources). Traditional broadband providers (DSL, cable, satellite, T1) will still be needed to get these packets to the public Internet, but the intermediary role of the local ISP may disappear in time.

are only dealing with a virus," and "help the body develop its own defenses." Congress, like an HMO, should approve (or defer to) treatments, fund research, regulate use of highly, facially dangerous substances, and otherwise get out of the way. Much is already being done without legislative involvement.

IV. THE IMPLICATIONS OF TECHNICAL IMMUNITY NETWORKS

The set of problems that we lump together as "spyware" (a set that is itself full of ever-increasing variety) is a particular expression of the world's complexity. We have opened ourselves to communication, and it is too much for us (or at least for our relatives) to deal with. No human being, and no legal institution, can single-handedly take on this problem.

I have suggested in this Article that the only real solutions to spyware are technical in nature, and that these technical solutions will come in the form of immunity networks. This suggestion leads me to guess that our focus on individual privacy and our obsession with global interconnectivity may both become inappropriate or irrelevant as the Internet changes. It may be time to recognize that individuals, and their unhappy relationships with spyware, will not always be the most important actors in this technical environment. It may be that individuals need to choose to cede some control over their individual machines to networks that will help in the constant fight against oppressive spyware and malware.[152]

I am emphatically not suggesting that membership in an immunity network be mandated by statute. Rather, it may be that some of the ultimate connectivity providers (the entities that make it possible to reach the public Internet) will mandate as a condition of service that individuals sign up for one of several immunity providers. It may become more expensive for individuals who have not joined such a network to be online.

This is not a move towards enforced similarity, as in communism. Nor is this a move towards a voting, democratic approach to software, where software that is voted "bad" becomes illegal. Instead, we need to recog-

152. The P3P lesson tells us that even with some controls ceded, users can be given opportunities to reverse or override decisions made by (and defaults set by) machines and networks. P3P, or Platform for Privacy Preferences, automatically compares a consumer's privacy preferences with a website's privacy policy and alerts the consumer to any discrepancies. *See* Platform for Privacy Preferences (P3P) Project, http://www.w3.org/P3P (last visited Aug. 19, 2005). Of course, even if we cede some of our autonomy to immunity networks, and establish clear boundaries between them, we will never, ever win the battle against "spyware." We will experience local emergencies, great ups and downs, and periods of calm, but we will never be completely at peace.

nize that there is already in the world a third way of governing that we need to begin to embrace as we face difficult technical warfare: competing networks. Such networks may be more flexible than any presumptively uniform law, although such flexibility will be possible only if: (1) exit from and entry into these networks is truly voluntary, and (2) adequate competition among networks exists.

Only by allowing these networks to "represent" and protect us technically will we survive the coming malware difficulties. Laws and litigation will not shield us, because the rate of change is too great and the varieties of attack too diverse. What the body does with overwhelming flows of sensory data is to "chunk" it, creating metainformation that can be dealt with. Similarly, these new networks will have a real role in collecting data about information flows, chunking it, and using the patterns that are revealed to protect their subscribers. The network will know when it is under attack and will pay attention. We, as individuals acting alone, are no longer capable of protecting ourselves from electronic attack. (Of course, individuals who have access to peer-created shields will be protected. I am talking about individuals trying to decide on the acceptability of every electronic message.)

The boundaries between these immunity networks will need to be real as well. Where these boundaries are unclear, dangerous electronic conditions may exist. Voluntary separation, with well-policed gateways that open deliberately, may be the best alternative to violence. I am troubled by this suggestion, because I am loath to create gatekeepers that have power over my or anyone else's communications. But even the co-inventor of the TCP/IP protocol, Vint Cerf, said recently that he wished that end-to-end authentication had been part of the protocol's original design.[153] Gateways between networks could check for communications that were adequately credentialed, and could perhaps do so in a lightweight fashion. To the extent we are at the beginning of a cataclysmic series of malware invasions, we may need to support good fences in order to keep communications flowing at all.[154]

The legal status of immunity networks raises fascinating questions that range far beyond the scope of this initial, exploratory study of the relatively narrow subject of spyware legislation. It may be that we have come into an era in which we need governments and hierarchies for atom-based

153. Vint Cerf, General Comments at The Freedom To Connect Conference, Silver Spring, Maryland (March 30, 2005).

154. *See* David R. Johnson, Susan P. Crawford & John G. Palfrey, Jr., *The Accountable Internet: Peer Production of Internet Governance*, 9 VA. J.L. & TECH. 9 (2004).

issues—when to put someone in prison, when to settle a property dispute—but that networks of various kinds, chosen by us, can best deal with the problems of digital bits. We may need to tell terrestrial governments that they are in charge of atoms—food and chemicals—but not in charge of minds or culture. This may happen as a matter of course, without explicit statements on anyone's part, as governments and prosecutors come to recognize the need to defer to networks that are solving problems for citizens. Until this recognition dawns, the only appropriate governmental initiative should be to do no harm.