

First Do No Harm: The Problem of Spyware

by
SUSAN P. CRAWFORD¹

Introduction

Online problems are popularly understood to be easily susceptible to offline legal categorizations and, thus, solutions.² "There is nothing new under the sun," we say to one another over and over again in the cyberlaw arena. But spyware³ 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

¹ Assistant Professor, Cardozo School of Law. Thanks to Lori 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.

² 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"); 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).

³ 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 (home page, 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, *Ghosts in Our Machines: Background and Policy Proposals on the "Spyware" Problem*, Nov. 2003, at <http://www.cdt.org/privacy/031100spyware.pdf> (last visited Aug. 19, 2005).

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/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 laws;⁴ 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-combatting products and services.

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

⁴ The Federal Trade Commission (“FTC”) has taken this route successfully. *See infra* Part I.D.iii.a. This Article is focused on the first and third of the three options I describe, and it does not go into the various unfair trade practice litigation routes that might be available to private litigants.

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.⁵ 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 spyware 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."

⁵ The content community draws specific links between 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 Senate Committee on the Judiciary*, 108th Cong. (2003) (statement of Sen. Orrin Hatch). At the conclusion of the hearing, "Sen. Orrin Hatch (R-UT), the Chairman of the Committee, . . . 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> (last visited Aug. 19, 2005). It is true that 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, at <http://www.benedelman.org/spyware/p2p/> (last visited Aug. 19, 2005).

Part I of this Article surveys the legislative landscape as of early 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 27 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 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 issues⁶ and are unlikely to be found to be constitutional.⁷ 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.⁸ Third, many legislators appear to view spyware as an assault on privacy interests, a view that does

⁶ In the language of *American Libraries Association v. Pataki*, these acts represent an unconstitutional projection of state law into conduct that occurs outside the relevant state, burden interstate commerce in ways that clearly exceed benefits to intrastate commerce, and interfere with Congressional determinations that the "Internet is one of those areas of commerce that must be marked off as a national preserve to protect users from inconsistent legislation that, taken to its most extreme, could paralyze development of the Internet altogether." 969 F. Supp. 160, 169 (S.D.N.Y. 1997). See *infra* Part I.C, note 40.

⁷ Given the state laws' focus on content of software, these laws may be unconstitutional under the First Amendment as well. See *ACLU v. Miller*, 977 F. Supp. 1228 (N.D. Ga. 1997) (invalidating state law criminalizing internet transmissions that falsely identify the sender) (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, likely sweep innocent, protected speech within their scope, and are often vague in their use of terms. See *infra* Part I.D.i.

⁸ See *infra* Part I.D.ii.

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. Finally, existing law directed toward remediating oppressive relationships, including both prima facie tort claims and federal statutory schemes, may adequately address spyware.

Part II provides concrete suggestions for addressing spyware. There is no one organization with sufficient knowledge to recognize "bad" spyware and know what to do. 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 III 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, it may be that individuals need to choose to cede some control over their machines to technical networks that will help in the constant fight against oppressive spyware 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.

I. 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 opportunity to refuse? Is spyware a type of software that allows the unauthorized use of trademarks in search terms (or visits to particular web sites) 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 Act⁹ 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.¹⁰ 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

⁹ UTAH CODE ANN. § 13-40-101 (2005) (the "Act").

¹⁰ For example, MP3 players, screensavers, file sharing applications, online games, and shopping tools.

triggered by the software are reported back to central SaveNow servers, search terms and web sites 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's site, sued WhenU, the company behind SaveNow.¹¹ When 1-800 Contacts gained an early victory against WhenU in that lawsuit,¹² 1-800-Contacts went the legislative route and urged the Utah legislature to pass a bill addressing SaveNow's tactics.¹³ Although a large coalition of substantial online companies lobbied against the bill,¹⁴ it was enacted into

¹¹ 1-800 Contacts sued WhenU in federal court in New York on the theory that WhenU's advertisements infringe 1-800 Contacts's trademark and copyrights. *1-800 Contacts, Inc. v. WhenU.com, Inc.*, 309 F.Supp.2d 467, 472 (S.D.N.Y. 2003) (preliminary injunction granted on trademark challenge; copyright challenge denied). The Second Circuit reversed this decision in June 2005, ruling that WhenU does not "use" 1-800's trademarks within the meaning of the Lanham Act, 153 U.S.C. § 1127, when it (1) includes 1-800'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 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).

¹² *Id.* The New York district court decision (now reversed) conflicted with two earlier decisions by federal district courts in Virginia and Michigan. *U-Haul Int'l, Inc. v. WhenU.com, Inc.*, 279 F. Supp.2d 723 (E.D. Va. 2003) (WhenU pop up advertisements not 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 Gator Corporation, now owned by Claria Corp., has also been sued several times for similar actions. *See, e.g.*, *In re Gator Corp.*, No. 03-MD-1517 (N.D. Ga. Aug. 20, 2003) (docket information for consolidated actions). *Washingtonpost.Newsweek Interactive Company, LLC v. Gator Corporation* resulted in an injunction in favor of the web site operators and eventually settled in 2003. No. CIV.A..02-909-A (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> (last visited Aug. 19, 2005).

¹³ *See Burns, Wyden Told to Focus Anti-Spyware Bill on Action, Not Technology*, Washington Internet Daily, 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").

¹⁴ 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

law in March 2004.¹⁵ The Act barred any person from installing "spyware" on another person's computer or causing such installation.¹⁶ 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."¹⁷ 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 illegal.¹⁸ The bill provided for a private cause of action, and set damages at \$10,000 for each separate violation.¹⁹

Following a challenge by WhenU, a Utah state court on June 22, 2004 enjoined the Act from coming into force on dormant commerce clause grounds.²⁰ The court found that plaintiff had shown that compliance with the statute would be difficult and expensive, that the statute was vague, and

opposing the bill. *Utah Governor Mulls Spyware Bill, Industry Opposes; Constitutional Issues Raised*, ECOMMERCE LAW DAILY, Mar. 12, 2004, at <http://subscript.bna.com/SAMPLES/ecd.nsf/0/4574a5cb36c6555985256e5500022a0b?OpenDocument> (last visited Aug. 19, 2005).

¹⁵ Spyware Control Act, H.B. 323, Reg. Sess., codified as UTAH CODE ANN. § 13-40-101 (2005). The Spyware Control Act was passed by the Utah Legislature on March 3, 2004 after a 26 to zero vote in its favor. H.B. 323 Fourth Substitute, Utah State Legislature, at <http://www.le.state.ut.us/%7E2004/htmldoc/hbillhtm/HB0323S04.htm> (last visited Aug. 19, 2005). The bill was signed into law by Governor Olene S. Walker on March 23, 2004. *Id.*

¹⁶ "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. § 13-40-201(I)(a) and (b) (subsection indicators omitted).

¹⁷ *Id.* at § 13-40-102(1).

¹⁸ *Id.* at § 13-40-201.

¹⁹ *Id.* at § 13-40-301(1), (2).

²⁰ *WhenU.com, Inc., v. State*, Civ. Act. No. 040907578 (3d Dist. Utah, June 22, 2004), available at <http://www.benedelman.org/spyware/whenu-utah/pi-ruling-transcript.pdf> (last visited Aug. 19, 2005).

that it created a risk of different penalties and mandates being applied to online companies from state to state.²¹

In early 2005, Utah introduced revisions to the Act that are driven by pop-up ad generation concerns.²² 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.²³ 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.²⁴ 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.²⁵

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."²⁶ It provides a safe harbor for advertisers who "request[] information about a user's state of residence before sending the spyware or the pop-up advertisement to the user" when the user says he/she does not live in Utah.²⁷

B. Other State Bills

i. Bad Acts

²¹ *Id.*

²² H.B. 104, Spyware Control Act Revisions, 2005 Leg., 56th Sess. (Utah 2005).

²³ *Id.* at § 13-40-102(7).

²⁴ *Id.* at § 13-40-201.

²⁵ *Id.* at § 13-40-301, 302.

²⁶ 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* ALA v. Pataki, at 169-70 *supra* note 40.

²⁷ *Id.* at § 13-40-202.

Alabama, Arkansas, Arizona, California, Illinois, Michigan, Nebraska, New York, Rhode Island, Virginia, and Washington are considering or have enacted "bad acts laundry list" bills.²⁸ 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 email 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 antispyware 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."²⁹

ii. Trademark concerns

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

²⁸ S.B. 122, 2005 Leg. (Ala. 2005); S.B. 2904, 2005 Leg. (Ark. 2005); H.B. 2414, 47th Leg., 1st Reg. Sess. (Ariz. 2005); CAL. BUS. & PROF. CODE § 22947 (Deering 2005) (imposes a \$1000 penalty per violation); H.B. 380, 94th Gen. Ass. (Ill. 2005); H.B. 945, 2005 leg., Reg. Sess. (Ma. 2005); S.B. 151 (Mich. 2005); L.B. 316 (Neb. 2005); A.B. 549 (N.Y. 2005); H. 6211, Gen. Ass., Jan. Sess. (R.I. 2005); H.B. 2214, Gen. Ass. (Va. 2005); H.B. 1012, 59th Leg., 2005 Reg. Sess. (Wash. 2005). For updated status of state spyware bills, see <http://www.ncsl.org/programs/lis/spyware05.htm> (last visited Aug. 19, 2005).

²⁹ *Id.*

advertisements.³⁰ 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."³¹

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.³² Trademark owners and web site 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.³³

iii. Notice Concerns

Michigan, Pennsylvania, Oregon, Tennessee, and Texas have enacted or are considering notice bills, under which "spyware," broadly defined,³⁴ is

³⁰ S.B. 140, 24th Leg. (Alaska 2005); H.B. 1714, 2005 Reg. Sess. (Ind. 2005) (Art. 4.8, § 2: "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).

³¹ *Id.*, Art. 4.8, § 5(b)(2).

³² *Id.*, Art. 2, § 2(1).

³³ *Id.*, Chap. 3 § 3.

³⁴ *E.g.*, S.B. 151 (Mich. 2005) § 5(b)(5): "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

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."³⁵

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.³⁶ Although these state

response to the use of a computer program, computer, computer system, or computer network." *See also* H.B. 574 (Penn. 2005) (introduced Feb. 16, 2005) (defining "spyware" as "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. 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 email, all of which should, presumably, have been preempted by CAN-SPAM. The Tennessee bill contains both "notice" and "trademark" elements. H.B. 1742, 104th Gen. Ass. (Tenn. 2005); S.B. 327, 79th Leg. (Tex. 2005).

³⁵ H.B. 2302, 73rd Leg. Ass., 2005 Reg. Sess. (Ore. 2005) § 2(3).

³⁶ *American Libraries Ass'n v. Pataki*, 969 F. Supp. 160, 171 (S.D.N.Y. 1997) (striking down NY statute that prohibited online dissemination of "harmful to minors" 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); *see also* *People v. Foley*, 692 N.Y.S.2d 248, 256 (App. Div. 1999) (holding that 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); *see also* *People v. Lipsitz*, 663 N.Y.S.2d 468, 475 (Sup. Ct. 1997) (holding that the application of New York consumer protection laws to New York business pursuant to Internet solicitations

bills/acts focus on spyware that has been installed on the computers of users inside the state, that installation requires a transmission that will 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.³⁷ Web publishers and software developers cannot effectively prevent the flow of information to any given state.³⁸ State regulations may burden interstate commerce “when a statute .

was proper under the dormant Commerce Clause). The constitutionality of state regulatory schemes that permit in-state wineries to ship alcohol to consumers but restricts the ability of out-of-state wineries to do so, which involve the interaction between the 21st Amendment and the dormant Commerce Clause, is under consideration by the Supreme Court. *Granholm v. Heald*, No. 03-1116, 2005 U.S. LEXIS 4174; *Mich. Beer & Wine Wholesalers Ass'n v. Heald*, No. 03-1120, 2005 U.S. LEXIS 4174; and *Swedenburg v. Kelly*, No. 03-1274, 2005 U.S. LEXIS 4174.

³⁷ See *Am. Booksellers Found. for Free Expression v. Dean*, 342 F.3d 96, 104 (2d Cir. 2003) (state statute concerning dissemination of harmful to minors material unconstitutional under 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 Communications, 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 (Ct. App. 2000) (state statute criminalizing pedophile activity constitutional; transmission of harmful sexual material to known minors in order to seduce them would not burden any legitimate commerce; statute distinguishable from *Pataki* case because intent requirement included).

³⁸ It is a matter of scholarly dispute whether technology now exists that could enable web sites 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

. . . has the practical effect of requiring out-of-state commerce to be conducted at the regulating state's direction,³⁹ and these state statutes have 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.⁴⁰

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 either House 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 include the Spy Act, the I-SPY Act, and the SPY-BLOCK Act.

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.

³⁹ *Brown & Williamson Tobacco Corp. v. Pataki*, 320 F.3d 200, 208–09 (2d Cir. 2003) (citations omitted).

⁴⁰ *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 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, Incorporated*, requires that "Where the statute regulates evenhandedly 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), and some commentators have argued that the Pataki approach to dormant Commerce Clause issues is overreaching and insufficiently nuanced. *See generally* 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); 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, 1216 (1998) (same concept).

i. Spy Act

The House bill in the lead as of May 2005, H.R.29 ("The Securely Protect Yourself Against Cyber Trespass Act" or "The Spy Act"), which preempts state legislation on these issues, is both a "laundry list of bad acts" bill and a notice bill.⁴¹ The Spy Act, which passed 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, Nebraska, 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.

The Spy Act "notice" provisions are far more complicated than those found in most of the state level bills.⁴² The Act begins by creating a defined term: "Information Collection Program" (or 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."⁴³ Next, the Act goes on to include in the ICP definition computer software that collects information about web

⁴¹ 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*, Washington Internet Daily, Mar. 10, 2005. Its sponsor, Rep. Mary Bono (R-CA), reintroduced the SPY ACT in January 2005, saying that she expected it to "sail through Congress this year." *Id.* Bono Statement accompanying H.R. 29, Jan. 5, 2005. *Id.* 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. *Id.* Chairman Barton (R-TX) has vowed to get H.R. 29 to the President's desk during 2005. *Id.*

⁴² Florida has introduced S.B. 2162 (Fla. 2005), and Georgia has introduced S.B. 127 (Ga. 2005), both of which appear to be very closely modeled on the SPY ACT.

⁴³ The Spy Act § 10 (name, physical address, email address, phone number, SSN, tax ID number, passport number, driver's license number, credit card number, access code, password, date of birth).

pages accessed by a computer⁴⁴ (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.⁴⁵

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 ICPs on a computer unless the ICP (1) provides notice (including 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, e.g., "This program will collect and transmit information about you. Do you accept?" or "This program will collect information about Web pages you access and will use that information to display advertising on your computer. Do you accept?"⁴⁶ The notice also must provide an opportunity for the user to see a description of the types of information to

⁴⁴ The Spy Act potentially covers all devices that compute all around the world. See *infra* note 51.

⁴⁵ The Spy Act § 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 web site accessed or (ii) a party authorized to facilitate the display or functionality of web pages 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 "web sites" or "pages".

⁴⁶ The required notices may not communicate effectively to the 10% of Americans who do not speak English. Census 2000 Brief, *Language Use and English-Speaking Ability: 2000* (Oct. 2003); <http://www.census.gov/prod/2003pubs/c2kbr-29.pdf> (last visited Aug. 19, 2005). Moreover, because the Act potentially affects devices around the globe, it may be that notices in Chinese would be more appropriate. See *infra* note 51.

be collected and sent by the ICP and an explanation of the purpose for these actions, 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.⁴⁷ The FTC is not, however, provided with additional funding for this drafting work.⁴⁸

⁴⁷ 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> (last visited Aug. 19, 2005). The Commerce Committee has jurisdiction over the FTC, and thus is interested in making spyware a deception issue subject to FTC rulemaking. Rep. Barton (R-TX), 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; revenge could be taken on them in the new telecommunications regulatory structure. 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, at http://itc.mit.edu/itel/docs/2002/defigueiredo_0502.pdf (last visited Aug. 19, 2005) (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).

⁴⁸ The Spy Act's anointing of the FTC as the drafter of spyware rules may remind some among you 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, Sept. 12, 2000, at http://news.zdnet.com/2100-9595_22-523848.html?legacy=zdn; *see also* 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, <http://www.sfgate.com/cgi-bin/Article.cgi?file=/chronicle/archive/2000/04/21/BU102542.DTL&type=business> (last visited Aug. 19, 2005); *see also* Electronic Privacy Information Center, *The Children's Online Privacy Protection Act*, <http://www.epic.org/privacy/kids/> (last visited Aug. 19, 2005) (noting criticism: "Critics have claimed that the methods outlined by the FTC for verification—sending/faxing signed printed forms,

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 this 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.

ii. I-SPY Act of 2005

The House Judiciary Committee introduced its own bill, the "Internet Spyware (I-SPY) Prevention Act of 2005," H.R. 744, which passed 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.⁴⁹ 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

supplement of credit card numbers, calling toll-free numbers, or forwarding digital signatures through email—are too costly, cumbersome, and inadequate in protecting personal information. Even though new technologies are being developed, the current verification methods are too slow and impractical. The process of verification of mails, emails, and credit card numbers may take over a day. Further, disclosure of credit card information will expose the parents to the same privacy risks that they are trying to protect their children from and deter them from using such online services in general. As a consequence, children may manipulate information to access these websites, and in the long run, online businesses may either eliminate children-focused sites.").

⁴⁹ 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) (2005).

intentionally break into a computer and uses that software in furtherance of another federal crime.

iii. SPY BLOCK Act

The Senate is considering the "Software Principles Yielding Better Levels of Consumer Knowledge Act" (Spy Block Act, S. 2145) co-sponsored by Sens. Burns (R-MT) and Wyden (D-OR). 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 software⁵⁰ on a computer⁵¹ 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."⁵² 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;

⁵⁰ Under the Spy Block Act, "the term 'software' means any program designed to cause a computer to perform a desired function or functions." S. 2145, 108th Cong. § 12(9) (2004) ("Spy Block Act").

⁵¹ As in the other federal pieces of legislation, "computer" is defined very broadly to include all computers around the world. *Id.*

⁵² Spy Block Act § 4(a).

. . . 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 –
(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 . . .
[and notice that "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 information may be used and distributed" has not been provided]⁵³

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."⁵⁴ 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.⁵⁵

It is likely that the Senate will pass the Burns-Wyden bill (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. It is hard to lobby against a bill labeled as fixing "spyware."

D. Implications of Pending Legislation

i. Implication One: Design Mandates

⁵³ *Id.* at § 3.

⁵⁴ *Id.* at § 7(b).

⁵⁵ *Id.* at § 10.

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 Burns-Wyden bill), 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.

For example, under the proposed SPY ACT, all "information collection programs" must provide "notice" and include required functions in order to be considered lawful.⁵⁶ 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."⁵⁷ 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 Senate Burns-Wyden bill (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

⁵⁶ H.R. 2929.EH, 108th Cong. (2004) § 3(b).

⁵⁷ *Id.*

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, 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 web sites.⁵⁸ 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?

Similarly, Google is now offering an updated version of the popular Google Toolbar that allows users to highlight text on any web page and be sent directly to another site—even though the author of the web page did not insert a link in the underlying text.⁵⁹ In effect, Google is adding its own links to pages, starting initially with US addresses as the highlighted text

⁵⁸ See Yahoo Search Help: Y!Q Search, at <http://help.yahoo.com/help/us/ysearch/yq/index.html>.

⁵⁹ Anita Hamilton, *Google Tricks*, TIME MAGAZINE, Mar. 7, 2005, <http://www.time.com/time/archive/preview/0,10987,1032364,00.html> (last visited Aug. 19, 2005).

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.⁶⁰ 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?⁶¹

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 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

⁶⁰ Google's 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.*, is still pending as of March 2005. No. C03-5340 (N.D. Ca. Nov. 26, 2003). Judge Brinkema of the Eastern District of Virginia recently indicated that she would be issuing a decision concerning Google's use of keywords to trigger advertisements, and would find that Google's practices were not infringing others' trademarks. *Geico v. Google, Inc.*, 330 F. Supp. 2d 700, (E.D. Va. 2004); *see also* Stefanie Olsen, *Google Wins in Trademark Suit With Geico*, NEWS.COM, Dec. 15, 2004, at http://news.com.com/Google+wins+in+trademark+suit+with+Geico/2100-1024_3-5491704.html

⁶¹ 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: Toolbar With Account Guard, at <http://pages.ebay.com/help/announcement/4.html>.

trip are available from different companies.⁶² 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.⁶³

Cookies, text files that are sent by a web server 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 web sites 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?⁶⁴

⁶² See Sidestep: The Traveler's Search Engine: About Sidestep, at http://www.sidestep.com/html/about_sidestep/main.html (last visited Aug. 19, 2005).

⁶³ See 2005 Spyware Study, sponsored by Unisys Corp., presented by the Ponemon Institute (May 12, 2005), http://www.networkadvertising.org/spyware-forum/2005_Consumer_Spyware_Survey_NAI_051205.pdf (last visited Aug. 19, 2005) (reporting national survey of 2000 internet users) (most people download free software and do not want new anti-spyware laws to prevent them from being able to download such software).

⁶⁴ Updating virus control requires 'spyware,' and parental controls (settings that a user can use 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.

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 trojan horses, or changing a PC's settings) should be legal. I am saying, however, that we do not know what new software applications will be developed that have both "spying" and "serving" elements. Right now, we know that enhanced search toolbars and third-party cookies both spy and serve. We do not know 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.⁶⁵

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, from circumvention),⁶⁶ and *prevent* code by law from being exported (if it uses an encryption algorithm that exceeds certain limits),⁶⁷ but only when the government is acting as a customer (or funder) can it *mandate* that code

⁶⁵ It is true that the use of voluntary privacy notices has had good effects on data practices in the US, 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. 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* I.D.i.

⁶⁶ Dennis S. Karjala, *Distinguishing Patent and Copyright Subject Matter*, 35 CONN. L. REV. 439 (2003); Digital Millennium Copyright Act, 17 U.S.C.A. § 1201 (West 2005).

⁶⁷ 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. Parts 730-774.

have particular attributes.⁶⁸ 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."⁶⁹ 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 view [doing so] as a content-based regulation of speech."⁷⁰ Although it is true that commercial speech receives less protection than non-commercial speech,⁷¹ and that disclosures can be required to keep commercial speech from being deceptive,⁷² it is not at all clear that software is commercial speech.

The Supreme Court has identified three factors which identify commercial speech when existing in combination: (1) advertisement; (2) mentioning a specific product by name; and (3) economically motivated speech.⁷³ 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.⁷⁴ 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

⁶⁸ 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 Child Online Protection Act, imposing fines and prison terms for the knowing posting for "commercial purposes" of web content that is harmful to minors likely unconstitutional because not least restrictive means available).

⁶⁹ *Wooley v. Maynard*, 430 U.S. 705, 714 (1977).

⁷⁰ 487 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).

⁷¹ *Ohralik v. Ohio State Bar Ass'n*, 436 U.S. 447, 456 (1978).

⁷² *Zauderer v. Office of Disciplinary Counsel of Sup. Ct. of Ohio*, 471 U.S. 626, 651 (1985).

⁷³ *Bolger v. Youngs Drug Prods. Corp.*, 463 U.S. 60, 66-67 (1983) (striking down ban on mailings of contraceptive ads).

⁷⁴ *Junger v. Daley*, 209 F.3d 481, 485 (6th Cir. 2000).

the intermediate scrutiny applied to commercial speech or the strict scrutiny applied to pure speech.⁷⁵ And even if software is commercial speech, it 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*.⁷⁶ 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."⁷⁷

Third, users⁷⁸ 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.⁷⁹ HTML, after all, is itself a making-invisible of the functionality 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 web pages accessed by the computer, or that is executed or installed without the user's knowledge,

⁷⁵ *Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n*, 447 U.S. 557, 564 (1980) (under intermediate scrutiny, regulation must not be more extensive than necessary to serve that interest); *Boos v. Barry*, 485 U.S. 312, 321 (1988) (giving strict scrutiny standard; government must show a compelling interest in restricting the speech and that the restriction is necessary and narrowly tailored to achieve that end).

⁷⁶ 447 U.S. at 564.

⁷⁷ *Zauderer*, 471 U.S. at 644.

⁷⁸ Although all the policy talk surrounding the spyware bills concerns "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.

⁷⁹ See generally M. Mitchell Waldrop, *THE DREAM MACHINE: J.C.R. LICKLIDER AND THE REVOLUTION THAT MADE COMPUTING PERSONAL* (Penguin Books 2001).

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?⁸⁰ Probably not. Users who set their browsers to "do 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 web site.

Fourth, insisting on "notice and consent" for broadly-defined "spyware" will lead to a hopelessly impoverished and meaningless regime. No one will understand what his "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 information 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.⁸¹ In effect, the government will be requiring users to click helplessly

⁸⁰ 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 web site, (b) does not send information to someone other than the web site operator, and (c) does not prompt advertising other than ads on the web pages within that particular web site, it will not be considered an ICP. Email from David Cavicke, General Counsel and Chief Counsel for Commerce Trade and Consumer Protection, House Committee on Energy and Commerce (Mar. 11, 2005) (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.*

⁸¹ See *ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447 (7th Cir. 1996) (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); see also *M/S Bremen v. Zapata Off-Shore Co.*, 407 U.S. 1 (1972); *Carnival Cruise Lines, Inc. v. Shute*, 499 U.S. 595 (1991).

along, assenting to something they do not understand over and over again.⁸² 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 "where" the ad came from?

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"—there are few lobbyists for spyware, malware, and adware—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 generally⁸³ 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.⁸⁴ Staff to Senators will freely say 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.⁸⁵ 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).⁸⁶ And the

⁸² 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, or at least not publicly.

⁸³ 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* (Cardozo Law School Legal Studies Research Paper Series, Cardozo Legal Studies Research Paper No. 102, 2005).

⁸⁴ *Metro-Goldwyn-Mayer Studios, Inc., v. Grokster, Ltd.*, 1245 S. Ct. 2764 (2005).

⁸⁵ Tom Sydnor, Senate Judiciary staff member for Sen. Orrin Hatch, Public Statement at The Modest Proposals 2.0 Conference at Cardozo Law School (Feb. 25, 2005).

⁸⁶ *In the Matter of Communications Assistance for Law Enforcement Act and*

telecommunications industry would like to see broad application of "consumer privacy" mandates to IP-enabled services,⁸⁷ 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 to you. "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.⁸⁸ 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."⁸⁹ But

Broadband Access and Services, ET Docket No. 04-295, RM-10865, Notice of Proposed Rulemaking and Declaratory Ruling, Aug. 9, 2004 (the CALEA NPRM).

⁸⁷ *In the Matter of IP-Enabled Services*, WC Docket No. 04-36 (Rel. Mar. 10, 2004).

⁸⁸ 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) (uses of encryption technology to protect communications and provide data security).

⁸⁹ The Restatement (Third) of Torts: Products Liability breaks down the definition into three distinct areas: "Manufacturing Defects—when the product departs from its intended design, even if all possible care was exercised. 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

because direct physical injury is not caused by software, it should not be 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.⁹⁰ Software is much more like speech than it is a product.⁹¹ It is not clear that rendering code subject to "failure to warn" standards would improve the quality of software.⁹² And it would undoubtedly constrain what new code is allowed to do, limit user experiences, and lead to a flurry of inexplicable notices and labels⁹³ that might drive people away from the online world.

alternative design renders the product not reasonably safe. 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 RESTATEMENT (THIRD) OF TORTS: PRODUCTS LIABILITY § 2 (1998). 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 Litigation*, 334 F.3d 643 (7th Cir. 2003).

⁹⁰ Section 402A of the Restatement provides the framework for products liability law. *See* *Winter v. G.P. Putnam's Sons*, 938 F.2d 1033, 1034 (9th Cir. 1991), "[t]he purposes served by products liability law . . . are focused on the tangible world. . . ."

⁹¹ The Magnuson Moss Warranty-Federal Trade Commission Improvements Act, 15 U.S.C.A. § 2301-2312 (West 2005), which establishes minimum standards for consumer product warranties, may apply to software sold to consumers. I attended a 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.

⁹² *See* Jeffrey Neuberger and 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").

⁹³ Compare the experience of consumers with required financial privacy notices under Title V of the Gramm-Leach-Bliley Act, 15 U.S.C.A. §§ 6801-6809 (West 2005). The 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*

Because legislation is primarily a one-way ratchet,⁹⁴ 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 strangers and converse with them. Do you REALLY WANT TO DO THIS?"

ii. 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 US 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" (or "CAN-SPAM Act") 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

Financial Privacy Notices, Privacy Rights Clearinghouse, July 2001, at <http://www.privacyrights.org/ar/GLB-Reading.htm> (last visited Aug. 19, 2005).

⁹⁴ As just one example, in the Uniting and Strengthening America by Providing Appropriate Tools required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (the "Patriot Act"), Congress made substantial changes to the 1978 Foreign Intelligence Surveillance Act, Pub. L. No. 95-511, 92 Stat. 1783 ("FISA"). Although there is a sunset for these FISA changes in the Patriot Act scheduled for Dec. 31, 2005 (§ 224), it is very unlikely that we will return to pre-9/11 standards for foreign intelligence surveillance.

⁹⁵ See Pub. L. No. 108-187, 117 Stat. 2699 ("CAN-SPAM Act"); see also Fact Sheet: President Bush Signs Anti-Spam Law, Dec. 16, 2003, at <http://www.whitehouse.gov/news/releases/2003/12/20031216-4.html> (last visited Aug. 19, 2005); see also Tom Zeller, *Law Barring Junk E-Mail Allows a Flood Instead*, NEW YORK TIMES, Feb. 1, 2005, at A2.

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

Unsolicited email on the internet has actually increased since the passage of CAN-SPAM, and now amounts to 80 percent or more of all email 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 that statute creates. Spammers, meanwhile, have changed their tactics since CAN-SPAM was enacted, and are now

⁹⁶ See CAN-SPAM Act, 15 U.S.C.A. § 7708(b) (West 2005).

⁹⁷ *Id.* § 5(a)(3).

⁹⁸ *Id.* § 5(a)(5)(A).

⁹⁹ *Id.* § 7(a).

¹⁰⁰ See, e.g., Associated Press, *Spam senders convicted in first felony case*, Nov. 3, 2004, <http://www.msnbc.msn.com/id/6401091/> (last visited Aug. 19, 2005) (spammers assessed nine years in prison plus fines).

¹⁰¹ *Id.* § 7(f).

¹⁰² *Id.* § 7(g).

¹⁰³ Tom Zeller, *Law Barring Junk E-Mail Allows a Flood Instead*, NEW YORK TIMES, Feb. 1, 2005, at A2; 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> (last visited Aug. 19, 2005) (reporting Postini claim that legitimate nonspam email down to twelve percent in Dec. 2004; MX Logic claim that 25% of all email was legitimate as of Nov. 2004).

using "zombie 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 US.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.

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.

iii. Implication Three: A Complicated Relationship With Existing Laws

¹⁰⁴ *Id.*

¹⁰⁵ Dan Ilet, *US Leads the Dirty Dozen Spammers*, NEWS.COM, Dec. 24, 2004.

¹⁰⁶ Chris Hoofnagle of the Electronic Privacy Information Center made this point at a Feb. 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*, Mar. 4, 2005, <http://www.epic.org/reports/decadedisappoint.html> (last visited Aug. 19, 2005).

In response to the spyware epidemic, some legislators 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 practices¹⁰⁸ (including notice, consent, access, and security) would be required of all US online participants.¹⁰⁹

¹⁰⁷ Editorial, *The Spies in Your Computer*, THE NEW YORK 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 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. For background, see U.S. Dep't. of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens* viii (1973) (stating five principles: no data record-keeping systems to be secret; access by subject; information obtained for one purpose not to be used for another purpose without consent; correction by subject; reliability and security of data required); see also Organization 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); see also 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) (grants 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., Testimony of Ari Schwartz, Associate Director Center for Democracy and Technology, before the House Committee on Energy and Commerce on "Combating Spyware: H.R. 29, the SPY ACT" (January 26, 2005), available at <http://www.cdt.org/testimony/20050126schwartz.pdf> (last visited Aug. 19, 2005); Prepared Statement of Jerry Berman, President, Center for Democracy and Technology, before the Senate Committee on Commerce, Science, and Transportation, Subcommittee on Communications, on "the SPY BLOCK Act" (March 23, 2004) ("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").

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"

¹¹⁰ See Louis Brandeis & Samuel Warren, *The Right of Privacy*, 4 Harv. L. Rev. 193 (1890) (law should create right to privacy protecting private facts)[hereinafter Brandeis & Warren]; *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") (case held that 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) [hereinafter *Olmstead*]; *Katz v. United States*, 389 U.S. 347, 351-52 (1967) (overruling *Olmstead*) ("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") [hereinafter *Katz*]; *Kyllo v. United States*, 533 U.S. 27, 40 (2001) (when "the Government uses a device not in the general public use, to explore the 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") [hereinafter *Kyllo*]; see also *Village of Belle Terre v. Boraas*, 416 U.S. 1, 13 (1974) (Marshall, J., dissenting) (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).

¹¹¹ "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 comprise every form of possession—intangible as well as tangible." Brandeis and Warren, *supra* note 110, at 193.

¹¹² *Id.*, *Olmstead* dissent, *supra* note 110; *Kyllo*, *supra* note 110.

¹¹³ Although the preceding discussion should make clear that not all of the pending spyware bills are the same, or even similar, many of them go far beyond requiring restraints on the use or collection of personally identifiable information to constraining the use or collection of use data generally. *E.g.*, Spy Act § 3(B)(1)(b)

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 with them through, for example, hijacking their browsers, or using their PC for an attack on others, or flashing unwanted popup ads at them. 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 concern about spyware, we can discover that existing federal and state laws and court-created doctrines directed toward addressing oppressive relationships may adequately address users' legal issues.

(covering "computer software . . . that (i) collects information regarding the Web pages accessed using the computer; and (ii) uses such information to deliver advertising to, or display advertising on, the computer").

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

a. Federal Law

There are several federal laws addressing computer privacy. The federal Computer Fraud and Abuse Act already makes unauthorized 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 makes it a crime and a statutory tort to intercept electronic communications, to disclose intercepted communication, or to use intercepted communications.¹¹⁹ ECPA also makes criminal (and tortious) the unauthorized access to "stored

¹¹⁵ 18 U.S.C.A § 1030 (2005) ("CFAA"). The central offense under the CFAA is the abuse of a computer to obtain information. *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121, 1128-29 (W.D. Wash. 2000) (employer sued former employees and competitor who hired them under the CFAA for taking information).

¹¹⁶ Civil causes of action under the CFAA are available against the violator for compensatory damages and injunctive relief. *See* 18 U.S.C.A § 1030(g) (2005). *See Pac. Aerospace & Elecs., Inc. v. Taylor*, 295 F. Supp. 2d 1188, 1196 (E.D. Wash. 2003) (employers "are increasingly taking advantage of the CFAA's civil remedies to sue former employees and their new companies who seeks a competitive edge through wrongful use of information from the former employer's computer system").

¹¹⁷ 18 U.S.C.A § 1030(g) (2005).

¹¹⁸ *See, e.g., Four Seasons Hotels and Resorts B.V. v. Consorcio Barr, S.A.*, 267 F. Supp. 2d 1268 (S.D. Fla. 2003) (hotel licensee violated CFAA by attempting within a one-year period to intentionally access without authorization the licensor's protected computers, spoofing of 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). Law enforcement actions against people installing spyware on public terminals (in Kinko's) under the CFAA have been successful; *cf In re Doubleclick, Inc. Privacy Litigation*, 154 F. Supp.2d 497(S.D.N.Y. 2001) (dismissing CFAA claim based on placement of Doubleclick cookies because any damages caused by Doubleclick's activities did not meet the threshold required by CFAA).

¹¹⁹ 18 U.S.C. § 2510 (1994) ("ECPA").

electronic communications."¹²⁰ To the extent 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.¹²¹ In October 2004, FTC sought and obtained a federal court injunction against Seismic Entertainment Productions, Inc., Smartbot.net, Inc., and Sanford Wallace, after alleging that these actors had installed software code onto users' computers without the users' authorization that changed users' home pages, downloaded and installed various other programs,¹²² caused an incessant stream of pop-up messages to be displayed, and then triggered ads for defendants' "anti-spyware" programs.¹²³ 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 and the court agreed with this assessment and granted an injunction—adding that it thought defendants' actions were "deceptive" as

¹²⁰ *Id.* at §§ 2701-10.

¹²¹ 15 U.S.C.A § 45(a) (West 2005) prohibits unfair or deceptive acts or practices in or affecting commerce.

¹²² FTC's memorandum in support of its TRO application states, "These programs bombard computers with even more pop-up ads, monitor where users travel on the Internet, hijack Internet searches, insert tool bars on web pages, collect information entered into online forms, and create security holes that are used to install even more software." FTC's Memorandum in Support of Plaintiff's Motion for a Temporary Restraining Order With Expedited Discovery, Preservation of Documents and Order to Show Cause Why a Preliminary Injunction Should Not Issue Against Defendants, at 9, *FTC v. Seismic Entm't Prods., Inc.*, No. 04-377-JD (D. N.H. Oct. 21, 2004); *available at* <http://www.cdt.org/privacy/spyware/spywiper/20041021seismicruling.pdf> (last visited Aug. 19, 2005).

¹²³ *Seismic Entm't Prods.*, *supra* note 122.

¹²⁴ *Id.*

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.A. § 45(n) (West 2005).

well as "unfair."¹²⁶ Thus, the FTC has had no trouble proceeding against classic "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 famously imposes civil liability for "any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising,"¹²⁸ and provides for citizen standing to bring claims as private attorneys general where there is no showing of harm to themselves—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.

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

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." FTC Memorandum, *supra* note 121, at 8. In March 2005, the FTC brought a similar action in the U.S. district court in Spokane, Wa. against a deceptive anti-spyware vendor, Spyware Assassin, "which it says used pop-ups and banner ads to trick computer users into thinking their computers were infected by spyware, then claiming its \$29.95 software would remove spyware and prevent future breaches." WASHINGTON INTERNET DAILY, Mar. 11, 2005. *FTC v. Maxtheater*, No. 05 -CV-0069-LRS (E.D. Wash. 2005) (issuing a temporary restraining order).

¹²⁷ E.g., Colorado, Delaware, Georgia, Hawaii, Illinois, Maine, Minnesota, Nebraska, New Mexico, Ohio, Oklahoma, Oregon.

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

¹²⁹ *See Barquis v. Merchants Collection Ass'n of Oakland, Inc.*, 7 Cal. 3d 94, 110 (1972); CAL. BUS. & PROF. CODE § 17204 (Deering 2005).

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

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

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 New Mexico, Missouri, and New York. *See* Schmitz v. Smentowski, 109 N.M. 386, 399 (1990); *Beavers v. Johnson Controls World Servs., Inc.*, 120 N.M. 343 (N.M. Ct. App. 1995); *Curiano v. Suozzi*, 63 N.Y.2d 113, 117-18 (1984); *Board of Education v. Farmingdale Classroom Teachers Ass'n*, 38 N.Y.2d 397, 380 (1975); *Bandag of Springfield, Inc. v. Bandag, Inc.*, 662 S.W.2d 546, 553 (Mo. Ct. App. 1983).

¹³¹ *ATI, Inc. v. Ruder & Finn, Inc.*, 42 N.Y.2d, 457 (1977).

¹³² *See* RESTATEMENT, (SECOND) OF TORTS, *supra* note 130, at cmt. a: "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."

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; his thesis was that "[T]he intentional infliction of temporal damage, or the doing of an act manifestly likely to inflict such damage and inflicting it, is actionable if done without just cause" (quoting Oliver Wendell Holmes, Jr., *Privilege, Malice and Intent*, 8 Harv.L.Rev. 1, 3 (1894) (footnote omitted)).

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 US, 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.

II. 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)

¹³⁴ Testimony of Ari Schwartz, Associate Director, Center for Democracy and Technology before the Senate Committee on Commerce, Science, and Transportation (May 11, 2005) *available at* <http://www.cdt.org/testimony/20050511schwartzspyware.pdf> (last visited Aug. 19, 2005) (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").

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 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 Spyware, like antigens comes in a multitude of forms. No centralized command-and-control "inoculation" system could ever deal with spyware, because the learning/feedback loops would simply be too slow and too

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

¹³⁶ Stephanie Forrest and Steven Hofmeyr, *John Holland's Invisible Hand: An Artificial Immune System*, Presentation at the Festschrift held in honor of John Holland (May, 1999), at <http://www.cs.unm.edu/~steveah> (last visited Aug. 19, 2005).

¹³⁷ Id.

¹³⁸ Computer scientists know this well, and have been working comfortably with this metaphor for some time. See Forrest and Hofmeyr, *supra* note 134. 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.

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.

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 meta-information that will help other users. And it would 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 in immunity ideas.¹⁴² Sana's software can "learn and take care of itself."¹⁴³ It "installs on

¹³⁹ A 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, MONITORING SOFTWARE ON YOUR PC: SPYWARE, ADWARE, AND OTHER SOFTWARE, 14 (Spyware Workshop, Staff Report, the Federal Trade Commission, March 2005), <http://www.ftc.gov/os/2005/03/050307spywarerpt.pdf> (last visited Aug. 19, 2005).

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.*

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, Home Page, at <http://www.sanasecurity.com> (last visited Aug. 19, 2005). Computer scientists have been talking about software in

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 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 we will soon have "immunity networks" available to us (either on our own desktops or within our own networks) that will learn our hard drives and

biological terms for some time. *See, e.g.*, Stephanie Forrest, Justin Balthrop, Matthew Glickman, David Ackley, *Computation in the Wild*, in THE INTERNET AS A LARGE-SCALE COMPLEX SYSTEM (K. Park and W. Willinger, eds. forthcoming); <http://crypto.stanford.edu/portia/pubs/articles/FBGA1917099772.html> (last visited Aug. 19, 2005) (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 TECHNOLOGY REVIEW, Oct. 2003, <http://www.techreview.com/Articles/03/10/tr100computing1003.asp> (last visited Aug. 19, 2005); Dan Neel, *Sana Gives Desktop PCs Autoimmunity*, SECURITYPIPELINE.COM, Oct. 25, 2004, at <http://www.securitypipeline.com/news/51200074> (last visited Aug. 19, 2005).

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. *Know Your Enemy: Tracking Botnets: Using Honeynets to Learn More About Bots* (The Honeynet Project and Research Alliance, Research Paper of Use of Honeynets to Learn More About Botnets, Mar. 13, 2005) at <http://www.honeynet.org/papers/bots/> (last visited Aug. 19, 2005). 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.* Note the legal risks of monitoring networks, from book chapter dedicated to this subject: "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." *Id.*

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 want to 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 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% of their customer service resources responding to spyware-related inquiries.¹⁴⁹

¹⁴⁶ Cisco is already doing this. See *Core Elements of the Cisco Self-Defending Network Strategy* (Cisco Self-Defending Network, White Paper 2005), at http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns413/networking_solution_s_white_paper0900aecd80247914.shtml (last visited Aug. 19, 2005). 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), at <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.

¹⁴⁸ EarthLink offers a free software suite to its users that blocks spyware, spam, and viruses. Earthlink TotalAccess, at <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> (last visited Aug. 19, 2005).

¹⁴⁹ Jim Thompson, *Malware Returns*, ISP-PLANET, May 27, 2005, at <http://www.isp-planet.com/business/2005/spyware.html> (last visited Aug. 19, 2005).

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 are only dealing with a virus," and "help the body develop its own defenses." Congress, like an HMO, should approve (or defer to)

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&leftidx=9&lselect=0> (last visited Aug. 19, 2005) (reporting that 80% 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 provision may provide a useful path towards solvency.

¹⁵¹ See Microsoft Networking Research Group, *Self-Organizing Neighborhood Wireless Mesh Networks*, at <http://www.research.microsoft.com/mesh/> (last visited Aug. 19, 2005) (describing 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.

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.

III. 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 singlehandedly 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

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, *at* <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.

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 recognize 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 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 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.

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, and John G. Palfrey, Jr., *The Accountable Internet: Peer Production of Internet Governance*, 9 VA. J.L. & TECH. 9 (2004).