The Columbia

SCIENCE AND TECHNOLOGY LAW REVIEW

www.stlr.org

"ROBUST NOTICE" AND "INFORMED CONSENT:" THE KEYS TO SUCCESSFUL SPYWARE LEGISLATION

Jordan M. Blanke[*]

As spyware, adware, and other computer programs that surreptitiously monitor user behavior become more prevalent, the United States Congress and a number of state governments have proposed legislation to target this problem. This article argues that any legislative solution must require robust, meaningful notice to users about the ramifications of the software they are installing, so that users can give their informed consent to install the software and accept its terms and conditions. The article discusses the background of the technological innovations that led to the present day computing environment. It then explores some of the common questions and answers that arise concerning spyware and discusses the strengths and weakness of various state and federal legislative approaches.

I. INTRODUCTION

Not long ago the computing world was shocked to learn that Prodigy software had the audacity to collect information from our personal computers and transmit it back to "headquarters."[1] Several years later, we learned that "cookies" enabled not only the reading, but also the writing, of information to and from our hard drives. A few short years later, we find ourselves losing control over the software and data that is routinely read, written, installed and run on our machines. In the name of technology, we have seemingly become too willing to accept practices that contradict years – sometimes even decades and centuries – of basic legal principles.

"Spyware" and "adware"[2] are everywhere. Basically, they are computer programs that are installed (or install themselves) on computers and perform activities that range from the

[*] Professor of Computer Information Systems and Law, Stetson School of Business and Economics, Mercer University, Atlanta, GA.

[1] *See* Michael W. Miller, *'Prodigy' Headquarters Offered Peeks into Users' Private Files*, Wall St. J., May 1, 1991, at B1. Prodigy was a joint venture of IBM and Sears. *Id.*

[2] *See infra* notes 8-10 and accompanying text for a discussion of the problems associated with defining "spyware" and "adware." Unless otherwise noted, I will use the term "spyware" to refer generically to both.

innocuous to the criminal, but almost always negatively affect the basic use and enjoyment of the machine. Stories abound of how it becomes virtually impossible to browse the Internet on a spyware-infected computer. A couple of states have already passed legislation specifically targeting this problem, while many others consider such legislation. Congress is also poised to make new law. Unfortunately, much of this effort will be useless unless the legislation addresses the core of the problem.

In this article, I will discuss the importance of "robust notice" and "informed consent." A robust notice would make a computer user aware of the fact that he or she is about to take an action that has ramifications, and would inform the user of the details of those ramifications. Requirements for a proper notice would address the form and placement of the notice, the content of the notice, and the duration of the notice. Only after such notice is provided could a user make an informed consent as to whether or not to install the software or accept the terms and conditions of an agreement to use the software or service. While proposed legislation attempts to address these issues in a variety of ways, the underlying legal concepts are certainly not new. Ultimately, the rationale behind any successful efforts to regulate spyware must trace their lineage to some basic legal principles – the right of the use and enjoyment of personal property, and the genuine assent to contract.

In Part II of this article I will discuss the background of the personal computer and some technological innovations that led to our present day computing environment. In Part III I will explore some of the questions that arise concerning spyware and in Part IV I will explore some of the possible answers. In Part V I will examine some of the legislative approaches taken at both the state and federal levels. In Part VI I will draw some conclusions.

II. BACKGROUND

A. *The Hard Drive*

It used to be that when someone purchased a computer, he or she also purchased software to use on the machine. Before the introduction of hard drives on personal computers, software literally was hand-loaded each time it was run. With the advent of the hard drive, one could permanently install the software that he or she used most often. Whenever one wanted to run a program, it was retrieved from the hard drive, loaded into memory, and executed. The hard drive made our lives much simpler.

B. *The Modem*

The introduction of the modem significantly changed our world. As soon as we plugged a telephone line into the back of a computer, we opened up a Pandora's Box. While our access to external information and services increased exponentially, it came at a great cost. We now have an environment in which that external world can also access us – and our data. No longer are we in complete control of our computers and the information that we store in them. How have we come to this point?

In 1991 there was much outrage over the audacity that Prodigy (and IBM and Sears) had when it retrieved data from a user's hard drive.[3] How could they think that we would sit idly by while they read information from our computers without our permission? Back then there was a simple solution – remove the Prodigy software from the computer.

C. *The Internet*

During the 1990s, the Internet and the World Wide Web dramatically changed our world. Notions of personal privacy were redefined and reshaped. People were more than willing to sacrifice some personal privacy for a low price. By 1999, for example, one could obtain a free computer merely by agreeing to be subjected to targeted advertising and to have one's Internet browsing activity observed.[4]

D. *Cookies*

When computer users became aware of the fact that "cookies" were storing personal information on their local hard drives, largely without their knowledge, many were upset.[5] However, they learned very quickly that, while cookies could be disabled, there was not much they could accomplish on the Web without them. It was a tedious task to respond to a browser's constant barrage of requests to permit cookies to be stored or retrieved. Most people decided it was much easier just to accept the cookies. They figured that as long as they did not disclose too much information, they were probably safe.

[3] *See* Miller, *supra* note 1. Fourteen years later, it is sadly ironic to read the (naively) indignant responses of Prodigy users who discovered private or confidential information from their hard drives contained inside some of the Prodigy system files: "What was getting out – if it got out – was harmless. But the fact that they could get in there really upset me," and "He [Prodigy subscriber] is still searching through his [Prodigy software], shouting expletives." *Id.* at B1, B6. At the time, Prodigy explained that information from one's hard drive could end up in some Prodigy system files "[b]ecause of an oddity in the inner design of PCs . . . . 'It's an unfortunate side effect of the way the operating system works,' says . . . a Prodigy technical staffer." *Id.* at B6.

[4] Khanh T.L. Tran, *EMachines to Buy Free-PC in Stock Deal*, Wall St. J., Nov. 30, 1999, at B6. "In February [1999], Free-PC jolted the computer industry when it said it would give away sub-$1,000 PCs made by Compaq Computer Corp. that came with free Internet service to people who agreed to share personal data and be exposed to targeted Internet advertising. Free-PC was bombarded with more than one million requests for machines." *Id.*

[5] *See* Alan Feigenbaum, *Shopping on the Web: It's Scary Out There*, N.Y. Times, Dec. 21, 1997, at 3; Joan E. Rigdon, *Internet Users Say They'd Rather Not Share Their 'Cookies'*, Wall St. J., Feb. 14, 1996, at B6. "Net surfers have complained on-line about the feature, saying it's an invasion of privacy and that it ties up the resources of their own computers." Rigdon, *supra*. at B6. "Netscape, the . . . maker of the No. 1 Internet browsing software, . . . responding to complaints from consumers, said it will change its Internet browser software so customers can prevent on-line merchants from tracking their footsteps in cyberspace." *Id.*

E. *Targeted Marketing*

Computer users next discovered the targeted or preferred marketing programs sold by companies like DoubleClick and Avenue A.[6] These programs collected information about users' browsing activities, and displayed advertising customized for each user based upon those activities. Generally users became desensitized to all of the information that was being collected about them. The size of the databases storing this collected information is now measured in terabytes.[7]

F. *Spyware*

Spyware is one of the latest of the many challenges that face computer users. It is often installed on a computer without the user's knowledge and (informed) consent. In many cases, the software is so insidious and invasive that it becomes virtually impossible to do anything on the computer. What makes it even worse is that the software is usually difficult or near impossible to remove. Not surprisingly, a cottage industry of anti-spyware software has emerged. Also, as is often the case when new problems arise in society, a variety of legislative measures have been proposed. Unfortunately, many of those proposals will prove to be impotent in battling spyware unless they very carefully craft their definitions.

III. SPYWARE: THE QUESTIONS

A. *What is Spyware?*

One of the biggest problems in trying to control spyware is defining it. In April 2004 the Federal Trade Commission sponsored a public workshop entitled *Monitoring Software on Your PC: Spyware, Adware, and Other Software*. In its report of that workshop (*Spyware Report*), the FTC discussed the challenges in defining "spyware:"

[6] *See* Julia Angwin, *DoubleClick Keeps Two Steps Ahead of Rivals*, Wall St. J., Apr. 26, 2001, at B6; Randall Rothenberg, *An Advertising Power, but Just What Does Doubleclick Do?*, N.Y. Times, Sept. 22, 1999, at G14. "Doubleclick's technology backbone, . . . DART, works by reading 22 criteria, many of them, like location, embedded in a user's Internet address, others, like time of day, based on external considerations. Spy programs called 'cookies,' usually dropped stealthily into a user's hard drive, can further refine the target by telling the server whether someone is a repeat visitor to a site or has seen a specific advertisement." Rothenberg, *supra*. at G14. "When a user calls up a Web page that employs the DART technology, a tag on the page signals Doubleclick's server to delve into its inventory of advertisements to find one -- and then another and another -- that matches the marketer's needs with the user's profile." *Id.*

[7] *See* Ken Spencer Brown, *China Open 'Windows' for Security System Makers*, Orange County Bus. J., Mar. 20, 2000, at 56. "DoubleClick, Inc., the controversial online advertising technology maker, has increased its use of networked storage . . . to more than 100 terabytes of space." *Id.* A terabyte is a measure of computer storage capacity and is equal to 2 to the 40th power, or approximately a trillion bytes, or a thousand billion bytes (a thousand gigabytes). *See* http://en.wikipedia.org/wiki/Terabytes.

> Panelists identified three main conceptual challenges in reaching a consensus definition of spyware. The first challenge concerns knowledge and consent. There appears to be general agreement that software should be considered "spyware" only if it is downloaded or installed on a computer without the user's knowledge and consent. However, unresolved issues remain concerning how, what, and when consumers need to be told about software installed on their computers for consent to be adequate . . . .
>
> Second, another question is whether the definition should limit "spyware" to software that monitors and collects data relating to computer use. Such a definition would be consistent with the fundamental concept that the software must "spy" on computer users. However, it presumably would not include software that does not collect data but adversely affects computer performance or otherwise interferes with the use of computers.
>
> A final challenge in reaching consensus on the definition of spyware is determining the nature and extent of harm that the software must cause. For instance, some would treat software that "trespasses" on a computer as spyware because they consider trespass to be per se harmful, even if the software is otherwise benign or beneficial. In contrast, there was general consensus throughout the workshop that software should cause some harm to users before being labeled spyware. There was disagreement, however, as to the type and magnitude of injury needed to meet this definition.[8]

Thus the primary challenges involved 1) the requisite knowledge and consent of the user, 2) the extent of "spying" done by the software, and 3) the nature of the harm done to the computer by the software.

Similarly, there is great difficulty in defining "adware," and in determining whether to classify it as spyware:

> Some types of adware monitor computer use (including websites visited), analyze that information to determine ads in which the users might be interested, and then display targeted ads to users based on this analysis. On the other hand, other types of adware do not monitor computer use and instead just serve advertising messages to users.
>
> Workshop panelists and commenters stated a range of views as to whether and when adware should be classified as spyware. Some panelists argued that adware is spyware if users have not received clear notice about what the software will do or have not provided adequate consent to its installation or operation.[9]

[8] Federal Trade Commission, *Monitoring Software on Your PC: Spyware, Adware, and Other Software*, at 3 (March 2005), http://www.ftc.gov/os/2005/03/050307spywarerpt.pdf (footnotes omitted) [hereinafter *Spyware Report*].

[9] *Id*. at 3-4.

A working definition for spyware proposed by the FTC and generally agreed to be a good starting point is "software that aids in gathering information about a person or organization without their knowledge and which may send such information to another entity without the consumer's consent, or asserts control over a computer without the consumer's knowledge."[10]

B. *How Do You Get Spyware?*

Spyware usually comes from the Web. It most often comes bundled with other software.[11] It may come as part of pre-installed software on a new computer or as part of software purchased from a retailer or downloaded from the Web. It may come via email - as an attachment, through a hyperlink, or as part of the message itself.[12] Sometimes it comes by way of "drive-by" download, where the software takes advantage of security vulnerabilities in one's Web browser.[13] Sometimes it is installed when a user clicks a button in a dialog box, often not understanding the purpose or effect of the action and many times being tricked to "consent" because of deceptive information presented on-screen.[14]

C. *What Does Spyware Do?*

Many spyware programs change a user's browser settings. For example, "browser hijacking" may cause one's home page to be diverted to some other site, new links to be inserted into one's "Bookmarks" or "Favorite Places," or search requests to be intercepted and forwarded to sites other than those requested.[15] Frequently spyware will cause a proliferation of "pop-up" windows. More insidious forms of spyware may track and transmit keystroke activity from

[10] *Id*. at 4.

[11] *Id*. at 7.

[12] *Id*. at 5.

[13] *Id*. at 6. Spyware often takes advantage of ActiveX technology that is built into Microsoft's Internet Explorer browser. Security warnings sometimes alert users that software is about to be installed. These warnings can be averted, however, if a user has lowered the default security level of the browser or by clever spyware code. *Id*.

[14] *Id*. at 6-7. The *Spyware Report* discusses "pop-under exploits" (where users are presented with Security Warning dialog boxes while visiting their favorite web sites and often give permission to install software under the mistaken belief that it is related to and at the request of that site), fake "operating system" messages (where users give permission to fix a purported operating system problem, but are really giving "permission" to the installation of spyware), and "imbedded image windows" (where users who attempt to deny permission by clicking "No" or "Cancel" or by "Xing" close the window are tricked into giving "permission" by virtue of clicking anywhere in the dialog box image). *Id*.

[15] *Id*. at 9.

one's computer (a "keystroke logger") or cause one's modem to dial costly long-distance telephone numbers for Internet access instead of the familiar local ones (a "dialer").[16]

Other spyware programs monitor browsing behavior and the Web sites that one visits. They may collect a variety of personal or sensitive information and transmit it to external locations.[17] Some of them collect and transmit information for purposes of generating targeted advertising or creating customer lists. Others can use the information for even more harmful purposes.[18]

However innocuous or invasive the spyware may be, one thing is undeniably true – it causes degradation in system performance, often significantly.[19] Spyware programs take up space on one's hard drive and usually reside in one's precious (and finite) computer memory. The programs can increase the number of computer operations required to be performed by the system by a factor of twenty.[20] Significantly slowed computer performance has become the number one spyware-related complaint heard by Dell computer customer support, accounting for more than 25% of such complaints.[21]

D. *Why Can't You Get Rid of Spyware?*

Unfortunately, one of the most annoying features of spyware is the difficulty in getting rid of it. Generally, the programs cannot be removed by normal means – the program usually does not appear in the Add/Remove Programs function of the operating system nor does it provide an uninstaller.[22] The programs often install as many as 4,000 files and make as many as 2,000 changes in the computer's operating system Registry.[23] The program files are often stored in folders or files whose names either constantly change or feign legitimacy by using the names of well-known programs.[24] Some of the more persistent spyware programs use "tricklers," whose purpose is to reinstall the program once it has been uninstalled.[25]

[16] *Id*. at 9-10.

[17] *Id*. at 10.

[18] The *Spyware Report* discusses the fact that information obtained from spyware poses a variety of privacy risks, including identity theft. *Id*. at 9-10. It also notes that as spyware becomes more sophisticated, businesses may face greater risks of exposure of confidential business information and trade secrets. *Id*. at 10.

[19] *Id*. at 9-10.

[20] *Id*. at 8.

[21] *Id*.

[22] *Id*. at 7.

[23] *Id*.

[24] *Id*.

[25] *Id*. at 8.

Assuming that one is computer-savvy enough to know that a spyware problem exists, he or she can obtain anti-spyware programs to combat the problem.[26] Often, however, one must use several programs in order to remove – and prevent the reinstallation of – the spyware programs. This pernicious nature of spyware should ultimately effect for new legislation. One of the sponsors of the *SPY ACT* bill described in committee hearings his alarm and irritation with the prevalence of spyware and "comment[ed] that he was forced to buy a new computer for his daughter after spyware clogged its operating system beyond repair."[27]

E. *Why Don't We Just Ban Spyware?*

There is definitely a movement afoot to ban spyware. California and Utah have already enacted anti-spyware statutes.[28] Bills are pending in 23 other states.[29] Several bills are being considered in both houses of Congress.[30] There are several problems, however, with this legislative effort. First, many of the bills focus on banning the activities themselves. Most of these activities, particularly the more egregious ones, like "keystroke logging," are already prohibited under other state or federal statutes.[31] While it is important to craft the legislation to

[26] A cottage industry of anti-spyware software is emerging, much like the anti-virus market. There are a number of well-known and reliable free programs for download on the Web: *Spybot – Search & Destroy* available at http://www.safer-networking.org/en/index.html, Lavasoft's *Ad-Aware Personal Edition* available at http://www.lavasoftusa.com, and Microsoft's *AntiSpyware* (Beta) available at http://www.microsoft.com/athome/security/spyware/software/default.mspx are some of the more popular. *See also Spyware Report*, *supra* note 8, at 31 n.134.

[27] Michael Grebb, *Congress Puts Spyware on Hitlist*, Wired News, ¶ 7 (Jan. 27, 2005), *at* http://www.wired.com/news/politics/0,1283,66407,00.html. (Representative Joe Barton of Texas, Chairman of the House Commerce Committee, discussing why the bill "is on the fast track"). *See infra* notes 84-102 and accompanying text for a discussion of the Securely Protect Yourself Against Cyber Trespass Act (SPY ACT), H.R. 29, 109th Cong. (2005).

[28] *See* Consumer Protection Against Computer Spyware Act, Cal. Bus. & Prof. Code §§ 22947-22947.6 (West 2005); Spyware Control Act, Utah Code Ann. §§ 13-40-101 to -401 (2005).

[29] These states include: Alaska (S.B. 140), Alabama (S.B. 122), Arizona (S.B. 2414), Arkansas (H.B. 2904), Florida (S.B. 2162), Georgia (S.B. 127), Illinois (H.B. 380), Indiana (H.B. 1714), Iowa (H.F. 614 and S.F. 465), Kansas (H.B. 2343), Maryland (H.B. 780, H.B. 945, S.B. 492 and S.B. 801), Massachusetts (S.B. 273 and S.B. 286), Michigan (S.B. 53, S.B. 54 and S.B. 151), Nebraska (L.B. 316), New Hampshire (H.B. 47), New York (A.B. 549, A.B. 2682 and S.B. 186), Oregon (H.B. 2302), Pennsylvania (H.B. 574), Rhode Island (H.B. 6211), Tennessee (H.B. 1742 and S.B. 2069), Texas (H.B. 1351, H.B. 1430, S.B. 327 and S.B. 958), Virginia (H.B. 1729 and H.B. 2215), and Washington (H.B. 1012). For detailed listings of all these bills, *see 2005 Legislation Relating to Internet Spyware or Advware* (Aug. 23, 2005), http://www.ncsl.org/programs/lis/spyware05.htm ; Benjamin Edelman, *State Spyware Legislation* (Aug. 31, 2005), http://www.benedelman.org/spyware/legislation/.

[30] *See* Securely Protect Yourself Against Cyber Trespass Act (SPY ACT), H.R. 29, 109th Cong. (2005); Internet Spyware (I-SPY) Prevention Act of 2005, H.R. 744, 109th Cong. (2005); Software Principles Yielding Better Levels of Consumer Knowledge Act (SPY BLOCK Act), S. 687, 109th Cong. (2005).

[31] "Sec.2. [of the proposed SPY ACT] is also puzzling because many, if not most, of the specified practices are already prohibited by existing law. For example, Sec.2(a)(5) prohibits 'Inducing the owner or authorized user to install or execute computer software by misrepresenting the identity or authority of the person or entity providing the computer software to the owner or user' -- which sounds like common law fraud, and is therefore already illegal.

include typical spyware activity sufficiently, it is more important to focus on the notice and consent requirements, because without them the legislative restrictions are typically benign.

Secondly, while the language of first-draft legislation often starts out very strong, there is a tendency for it to be greatly weakened by the time it is enacted. Unfortunately, much of the protection against spyware disappears in loopholes, exceptions and altered definitions before a bill is ever passed.[32]

Thirdly, because most of the legislation initially will be at the state level, we will inevitably see some variations in approach.[33] Some of these approaches will be more effective than others. Once federal legislation is passed, however, it will probably preempt most of the state legislation.[34] This will create a situation similar to that involving the federal anti-spam

Similarly, Sec.2.(a)(8)'s prohibition on removing security software echoes the existing Computer Fraud and Abuse Act, which prohibits 'exceed[ing] authorized access' to a computer." Benjamin Edelman, *What Hope for Federal Anti-Spyware Legislation?* (Jan. 19, 2005), http://www.benedelman.org/news/011905-1.html (citing the Computer Fraud and Abuse Act, 18 U.S.C.A. § 1030(a)(1) (2005)).

See Spyware Report, supra, at 4 ("Rather than adopting new laws to address spyware, some comments suggested that the government could challenge these particular acts and practices as unfair or deceptive in violation of Section 5 of the FTC Act.").

[32] Much of the impact that the California bill could have had was greatly reduced by drastically changing the language of the first draft. *See* infra notes 77-83 and accompanying text. Benjamin Edelman is a Ph.D. candidate at Harvard University and a graduate of its law school. He maintains the definitive Web site for material about spyware. *See* http://www.benedelman.org/news/092904-1.html. He describes some of the changes in California's bill:

> SB1436 had an opportunity to address these deceptive installation tactics by clarifying standards for notice and consent. Indeed, the first draft of SB1436 (dated February 19, 2004) addressed Claria's [installation] tactics directly: "'Spyware' means an executable program that automatically ... transmits to the provider ... data regarding computer usage, including ... which Internet sites are or have been visited by a user" -- exactly what Claria does. The February draft went on to set out various requirements and disclosure duties, even including a minimum font size for disclosure. That's not to say the February bill was perfect -- certainly there was more fine-tuning to be done. But it sought to establish disclosure duties for all companies transmitting information about users' online browsing -- not just a few outrageous outliers who send viruses.
>
> Unfortunately, SB1436's initial comprehensive approach somehow got lost between the February draft and the August revisions. A recent RedHerring article claims the bill was "gutted" by "the well-heeled and influential online advertising lobby." Claria's chief privacy officer recently stated that he had "met with the staffs of members who have proposed legislation" -- though not mentioning any special efforts to modify the bill. Whatever Claria's role, even a quick reading shows that the revised bill won't affect Claria's current practices.

Benjamin Edelman, *California's Toothless Spyware Law* (September 29, 2004), *at* http://www.benedelman.org/news/092904-1.html.

[33] As is often the case, the appropriate place for laws to evolve is in the "laboratory' of the states." *Cruzan v. Director, Missouri Dep't of Health*, 497 U.S. 261, 292 (1990) (O'Connor, J., concurring). *See also* Benjamin Edelman, *State Spyware Legislation* (Aug. 31, 2005), *at* http://www.benedelman.org/spyware/legislation/.

[34] The SPY ACT would preempt all state spyware laws except "trespass, contract, or tort law" or "other State laws to the extent that those laws relate to acts of fraud," H.R. 29, 109th Cong. § 6 (2005). The SPY BLOCK Act would preempt all state spyware law except "State criminal, trespass, contract, tort, or anti-fraud law," S. 687, 109th Cong. § 10 (2005).

law.[35] By the time the federal law was about to be passed, 44 state attorneys general and the attorney general for the District of Columbia opposed its passage.[36] They believed that the act would do more harm than good because stricter state laws would be preempted.[37] The federal anti-spam law has proven to be very ineffective in preventing spam.[38]

IV. SPYWARE: THE ANSWERS

Legislative efforts should focus on providing strict and enforceable requirements for robust notice and informed consent. Relying on basic property and contract principles, these new laws would permit computer users to retake control of their machines.

We have lost sight of a basic reality – the computer is our property. We purchased it and its resources, including the hard drive and the memory. We pay for the electricity that runs it. And we pay for the telephone or cable connection that permits us to connect to the Internet.

The absurdity of the present situation is illustrated by some basic analogies, however simplified they may be. What if someone snuck into our house and, without permission, placed a listening device in our living room and plugged it into an electrical socket? What if someone broke into our automobile, placed a speaker right next to us in the passenger seat, and plugged it into the cigarette lighter? And what if this speaker spewed out advertisements all day long? What would our reaction be? How is spyware any different?

A. *Trespass to Chattels*

Basic property law teaches us that we have the right to the use and enjoyment of our personal property.[39] Furthermore, we enjoy our greatest expectation of privacy in our homes.[40] We certainly can choose to install listening devices in our homes or speaker systems in our cars if we so desire. But that choice is ours. We have the right to use our property however we see fit. Why does this principle not extend to our computers, particularly personal computers in our own homes?

[35] CAN-SPAM Act of 2003, 15 U.S.C. §§ 7701-7713 (2005). *See* Jordan M. Blanke, *Canned Spam: New State and Federal Legislation Attempts to Put a Lid On It*, 7 Comp. L. Rev. & Tech. J. 305, 317-18 (2004).

[36] David McGuire, *States Object to Spam Legislation*, Wash. Post (April 30, 2003).

[37] *Id.*

[38] *See* Tom Zeller, Jr., *Law Barring Junk E-Mail Allows a Flood Instead*, N. Y. Times, Feb. 1, 2005, at A1; David McGuire, *A Year After Legislation, Spam Still Widespread; Technology Seen as Best Deterrent*, Wash. Post, Jan. 4, 2005, at E5; Daniel Nasaw, *Federal Law Fails to Lessen Flow of Junk E-Mail*, Wall St. J., Aug. 10, 2004, at D2.

[39] See Restatement (Second) of Torts §§ 217-18 (1965).

[40] See *Kyllo v. U.S.*, 533 U.S. 27, 31 (2001); *Silverman v. U.S.*, 365 U.S. 505, 512 (1961); Craig Hemmens & Chris Mathias, *United States v. Banks: The "Knock-and-Announce" Rule Returns to the Supreme Court*, 41 Idaho L. Rev. 1, 4 (2004) (discussing the common law origins of the maxim: a man's home is his castle).

The doctrine of trespass to chattel has recently been rescued from relative obscurity and thrust into the legal spotlight in the cyberlaw arena.[41] The doctrine has been successfully applied in a variety of computer-related situations.[42] While critics believe that the doctrine may be stretching too far to fit situations for which it certainly was not developed,[43] and that other, newer doctrines, like cyber-nuisance,[44] may be more suitable, the underlying rationale behind the

[41] "Trespass to chattel, a centuries-old tort theory that languished for years in the dusty archives of obscure legal doctrines learned and then promptly forgotten in the first year of law school, has unexpectedly found new life courtesy of the Internet." Tamara Loomis, *Internet Trespass: Companies Turn to an Old Tort for a New Reason*, N.Y. Law J., Jan. 10, 2002, at 5. "' An arcane 18th century legal doctrine is suddenly the darling of cyberspace.'" *Id.* (quoting attorney John D. Canoni). Traditional trespass to chattels doctrine requires that the interference with possession of the personal property is harmful to the "materially valuable interest in the physical condition, quality, or value of the chattel, or if the possessor is deprived of the use of the chattel for a substantial time." Restatement (Second) of Torts § 218 cmt. E (1965). See Laura Quilter, *Regulating Conduct on the Internet: The Continuing Expansion of Cyberspace Trespass to Chattels*, 17 Berkeley Tech. L.J. 421, 424-30 (2002); Ronnie Cohen & Janine S. Hiller, *Towards a Theory of Cyberplace: A Proposal for a New Legal Framework*, 10 Rich. J.L. & Tech. 2 (2003); David M. Fritch, *Click Here for Lawsuit – Trespass to Chattels in Cyberspace*, 9 Tech. J. & Pol'y 31 (2004).

[42] Courts have recognized trespass to chattel in cases involving spam, *see CompuServe, Inc. v. Cyber Promotions*, Inc, 962 F. Supp. 1015 (S.D. Ohio 1997); *America Online, Inc. v. IMS*, 24 F. Supp. 2d 548 (E.D.Va. 1998); *America Online, Inc. v. LCGM, Inc.*, 46 F. Supp. 2d 444 (E.D.Va. 1998), and automated software "robots" or "spiders" that continually access Web sites, *see eBay, Inc. v. Bidder's Edge, Inc.*, 100 F. Supp. 2d 1058 (N.D. Cal. 2000); *Register.com, Inc. v. Verio, Inc.*, 126 F. Supp. 2d 238 (S.D.N.Y. 2000); *Southwest Airlines Co. v. FareChase, Inc.*, 318 F. Supp. 2d 435 (N.D. Tex. 2004). In *Intel Corp. v. Hamidi*, 71 P.3d 296 (Cal. 2003), the Supreme Court of California rejected a claim of trespass to chattel, holding that a series of e-mails sent by a former, disgruntled employee did not sufficiently harm the plaintiff's personal property. The court, however, recognized the viability of the tort if there was factual support of actual harm. In discussing some of the cases cited earlier in this footnote, the court stated that "the defendant's use of the plaintiff's computer system was held sufficient to support an action for trespass when it actually did, or threatened to, interfere with the intended functioning of the system, as by significantly reducing its available memory and processing power." *Id.* at 306. In *Ticketmaster Corp. v. Tickets.com, Inc.*, 2003 U.S. Dist. LEXIS 6483 (C.D. Cal. 2003), the court found insufficient evidence of harm to support a trespass action, finding neither physical injury to the chattel nor sufficient evidence that the "spider" adversely affected the use or utility of the computer system. *See also* Quilter, *supra* note 41, at 430-35; Geoffrey D. Wilson, Notes & Comments, *Internet Pop-Up Ads: Your Days are Numbered!: The Supreme Court of California Announces a Workable Standard for Trespass to Chattels in Electronic Communications*, 24 Loy. L.A. Ent. L.J. 567 (2004).

A class-action suit was filed in the Circuit Court of Cook County, Illinois, alleging that DirectRevenue, LLC "deceptively downloaded harmful and offensive spyware to unsuspecting users' computers" and "unlawfully used and damaged plaintiffs' computers to make money for themselves while willfully disregarding plaintiffs' rights to use and enjoy their personal property." Karen D. Schwartz, *Spyware Lawsuit Alleges Computer Hijacking* (Apr. 5, 2005), http://www.eweek.com/article2/0,1759,1782649,00.asp.

[43] In *White Buffalo Ventures, LLC v. Univ. of Tex. at Austin*, 420 F.3d 366, 377 n.24 (5th Cir. 2005), the court criticized the broadened extension of the doctrine, stating that "in many of the 'digital trespass' cases, where a plaintiff bases a trespass to chattels theory on a defendant's unauthorized use of a network/computer system, the court will merely conclude, without evidence or explanation, that the allegedly unauthorized use burdened the system." *See* Dan L. Burk, *The Trouble with Trespass*, 4 J. Small & Emerging Bus. L. 27 (2000); Quilter, *supra* note 41, at 435-43; Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 Cal. L. Rev. 439, 483-88 (2003).

[44] *See* Steven Kam, Note, *Intel Corp. v. Hamidi: Trespass to Chattels and a Doctrine of Cyber-Nuisance*, 19 Berkeley Tech. L.J. 427 (2004).

trespass doctrine is still most appropriate: individuals are entitled to the use and enjoyment of their personal property.

B. *Genuine Assent*

Basic contract principles teach us that a contract cannot be enforced without genuine mutual assent.[45] This became a primary focus in many of the cases that decided the enforceability of "shrink-wrap," "click-wrap" and "browse-wrap" licenses.

Shrink-wrap licenses began appearing in the 1980s on the outsides of boxes of off-the-shelf software, contained within the package's shrink-wrap. They were intended to present the purchaser with a list of terms that would be accepted on a "take-it-or-leave-it" basis.[46] Today shrink-wrap licenses are more commonly found inside of boxes accompanying software or hardware. The purpose is the same – if you buy the product (and retain it without objection), you have agreed to and accepted the terms of the license. Early cases tended not to enforce shrink-wrap agreements because of concerns over the existence of assent.[47] Later cases tend to enforce shrink-wrap agreements as long as they are somewhat reasonable.[48]

Click-wrap licenses typically appear on the screen of a computer user before he or she is about to download or install a piece of software. Generally, the trend is towards enforcement of such agreements.[49]

[45] "Generally, mutual assent means that there has been a 'meeting of the minds' and that both parties understand what is meant by the terms of a given agreement." Jennifer Femminella, Note, *Online Terms and Conditions Agreements: Bound by the Web*, 17 St. John's J. Legal Comment. 87, 101 (2003) (citing E. Allen Farnsworth, Farnsworth on Contracts §3.6, 119 (2d. 1990)). "Contract law is at its strongest where there is an actual agreement between the parties. That is, after all, the basis of a contract." Mark A. Lemley, *Intellectual Property and Shrinkwrap Licenses*, 68 S. Cal. L. Rev. 1239, 1286 (1995).

[46] *See* Ryan J. Casamiquela, *Contractual Assent and Enforceability in Cyberspace*, 17 Berkeley Tech. L.J. 475, 477 (2002).

[47] *See Step-Saver Data Sys., Inc. v. Wyse Tech.*, 939 F.2d 91 (3d Cir. 1991) (refusing to enforce a shrink-wrap agreement absent assent of the purchaser); *Vault Corp. v. Quaid Software Ltd.*, 847 F.2d 255 (5th Cir. 1988) (affirming a district court finding that a shrink-wrap license was a contract of adhesion and therefore unenforceable).

[48] *See Hill v. Gateway 2000, Inc.*, 105 F.3d 1147 (7th Cir. 1997) (holding that a purchaser who had not objected within the 30 days specified in the license contained inside the box with the item purchased had accepted those terms contained in the license); *ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447 (7th Cir. 1996) (holding that the purchaser had assented to the terms of the shrink-wrap license when he accepted the seller's offer). *But see Klocek v. Gateway, Inc.*, 104 F. Supp. 2d 1332 (D. Kan. 2000) (refusing to enforce a shrink-wrap agreement contained in the box, finding that the terms of the agreement had not become part of the transaction).

[49] *See I.LAN Sys., Inc. v. Netscout Serv. Level Corp.*, 183 F. Supp. 2d 328 (D. Mass. 2002) (enforcing a click-wrap license agreement that required the user to click on a box stating "I agree"); *Caspi v. Microsoft Network, L.L.C.*, 323 N.J. Super. 118 (N.J. Super. Ct. App. Div. 1999) (enforcing a license agreement where users were required to review license terms in a scrollable window and click either "I Agree" or "I Don't Agree"); *Barnett v. Network Solutions, Inc.*, 38 S.W.3d 200 (Tex. App. 2001) (enforcing the terms of a contract that required users to scroll through terms before accepting or rejecting them). *But see Am. Online, Inc. v. Superior Court*, 108 Cal. Rptr. 2d 699 (Cal. Ct. App. 2001) (refusing to enforce the terms of a click-wrap agreement where enforcement would be contrary to public policy).

Browse-wrap licenses typically do not require any affirmative action by a user. There may be a reference on the screen to a license agreement or a request to read a license, but there is no requirement to click anything before proceeding with an installation or download. Because of this, courts have been reluctant to find assent. Accordingly, it is unlikely that we will see many more of these licenses in use.[50]

It is the distinction between the often-enforced click-wrap agreements and the rarely-enforced browse-wrap agreements that is most important. In determining whether such an agreement should be enforced, a court will often look at whether the person was aware that his or her actions in clicking a button or downloading a piece of software would create a contract.

Do we focus on the *subjective* intent – the awareness that one is entering into an agreement under which he or she will be bound – or on the *objective* intent – the knowledge that one is about to click a button in order to install or download a piece of software? Has "[i]ntent in contract law [become] a conscious will to do an act, rather than an intent to effect a contractual relationship?"[51]

> A key issue in the common law of contracts that is especially relevant to determining the enforceability of click-wrap agreements is whether assent should be determined on the basis of the parties' actual or apparent intentions. The subjective approach looks to the actual intentions of the parties and is reflected in the Second Restatement of Contracts. In order for a contract to be formed under the subjective approach, there must be a "meeting of the minds" between the parties. Assent is binding only to those terms to which the parties have agreed in fact. The objective approach, in contrast, looks to the external or objective appearance of the parties' intentions as manifested by their actions.[52]

In *Specht*, [53] the Second Circuit Court of Appeals affirmed the district court's determination that a contract had not been formed by the plaintiffs' acts of downloading a piece of defendant's software from the Internet. The plaintiffs had not been required to click on a button that acknowledged their agreement to the terms of defendant's license. Rather, there was merely an invitation, at the bottom of the screen, for a user to agree to the terms of the license before downloading the software. In finding for the plaintiffs, the district court stated that "the case law on software licensing has not eroded the importance of assent in contract formation. Mutual assent is the bedrock of any agreement to which the law will give force."[54]

The appellate court affirmed this holding and added:

[50] *See Specht v. Netscape Commc'ns Corp.*, 306 F.3d 17 (2d Cir. 2002) (refusing to enforce a license that the users may not have even seen) (*see infra* notes 53-55 and accompanying text); *Pollstar v. Gigmania, Ltd.*, 170 F. Supp. 2d 974 (E.D. Cal. 2000) (questioning whether the user was aware of and assented to the license agreement).

[51] Lawrence Kalevitch, *Contract, Will & Social Practice*, 3 J.L. & Pol'y 379, 390 (1995).

[52] Zachary M. Harrison, Note, *Just Click Here: Article 2B's Failure to Guarantee Adequate Manifestation of Assent in Click-Wrap Contracts*, 8 Fordham Intell. Prop. Media & Ent. L.J. 907, 917.

[53] *Specht v. Netscape Commc'ns Corp.*, 150 F. Supp 2d 585 (S.D.N.Y. 2001), *aff'd*, 306 F.3d 17 (2d Cir. 2002).

[54] *Id*. at 596.

> [M]utual manifestation of assent, whether by written or spoken word or by conduct, is the touchstone of contract. … *cf.* Restatement (Second) of Contracts § 19(2) (1981) ("The conduct of a party is not effective as a manifestation of his assent unless he intends to engage in the conduct and knows or has reason to know that the other party may infer from his conduct that he assents."). Although an onlooker observing the disputed transactions in this case would have seen each of the user plaintiffs click on the SmartDownload "Download" button, . . . a consumer's clicking on a download button does not communicate assent to contractual terms if the offer did not make clear to the consumer that clicking on the download button would signify assent to those terms, *see Windsor Mills*, 101 Cal. Rptr. at 351. ("When the offeree does not know that a proposal has been made to him this objective standard does not apply."). California's common law is clear that "an offeree, regardless of apparent manifestation of his consent, is not bound by inconspicuous contractual provisions of which he is unaware, contained in a document whose contractual nature is not obvious." *Id.*[55]

Benjamin Edelman documents a 56-screen long license agreement by Claria that is presented to users when attempting to install Kazaa (with which Claria's software is bundled).[56] In a survey by PC Pitstop, 74% of Claria users were unaware that the software was installed.[57] Similarly, Edelman documents a 45-screen long license presented by WhenU for its software that is bundled with BearShare.[58] According to the same PC Pitstop survey, 87% of WhenU users were unaware that the software was installed.[59] Claria and WhenU adamantly oppose the notion that their software is spyware or adware, claiming that their users have voluntarily given consent to installation.[60]

[55] *Specht*, 306 F.3d at 29-31 (applying California law regarding contract formation). This case was responsible for the demise of browse-wrap licenses. Virtually all transactions on the Web now use click-wrap licenses that attempt to elicit an affirmative response from a user (i.e., a click).

[56] *See* Benjamin Edelman, *Claria License Agreement Is Fifty Six Pages Long*, http://www.benedelman.org/spyware/claria-license/ (last visited Nov. 14, 2005).

[57] *Id.*

[58] *See* Benjamin Edelman, *WhenU License Agreement Is Forty Five Pages Long*, http://www.benedelman.org/spyware/whenu-license/ (last visited Nov. 14, 2005).

[59] *Id.*

[60] *See* Benjamin Edelman, *Claria's Practices Don't Meet Its Lawyers' Claims* (Jan. 4, 2005), http://www.benedelman.org/news/010405-1.html. In fact, it was WhenU that successfully brought suit against the State of Utah to temporarily enjoin enforcement of the Spyware Control Act. Utah Code Ann. §§13-40-101-401 (2005). WhenU alleged that the Act violated the Commerce Clause of the United States Constitution and prohibited commercial speech protected by the First Amendment. The court granted the preliminary injunction, finding that there was a substantial likelihood of success on some of the Commerce Clause challenges. *WhenU.com, Inc. v. Utah, Civ. Act.* No. 040907578 (3d Dist. Ct. Utah June 22, 2004). Interestingly, in its complaint, WhenU made the following allegations:

> 16. As set forth in greater detail below, WhenU's software follows the user's activity in his Internet browser and uses that activity to determine the category of goods or services in which the

The importance of a genuine assent is clear. All too often, spyware purveyors hide behind the line of click-wrap cases that look only to objective intent. Just because someone clicks a button, it does not necessarily follow that there is even an objective intent to enter into a contractual relationship. Unless there is some robust notice regarding the significance of the action, there should be no genuine assent. Courts should not find genuine assent merely because (objectively) a button was clicked.[61]

> user is interested. In order to protect user privacy, the software's decisions regarding which ads to retrieve and display are all processed on the user's own personal hard drive.
>
> 37. The use of SaveNow [WhenU's proprietary software program] is entirely consensual. Consumers obtain the SaveNow software because they choose to do so. Typically, they decide to download SaveNow software and to accept the ads it delivers in return for obtaining a popular software application for free.
>
> 39. During the SaveNow installation process, the consumer always receives a notice stating that SaveNow is part of the download, and explaining how SaveNow functions.
>
> 40. To proceed with the installation, the consumer must affirmatively accept a license agreement for SaveNow (the License Agreement).
>
> 41. WhenU's License Agreement is a short, two-page agreement written to be as intelligible as possible to the average computer user. It clearly explains that the software generates contextually relevant advertisements and coupons, utilizing "pop-up" and various other formats.
>
> 42. The software cannot be installed unless the consumer affirmatively accepts the terms of the License Agreement.

WhenU.com, Inc. v. Utah, Civ. Act. No. 040907578 (3d Dist. Ct. Utah, filed Apr. 12, 2004).

[61] One of the main reasons for the drafting of a proposed Article 2B of the Uniform Commercial Code was to validate shrink-wrap licenses. Margaret Jane Radin, *Humans, Computers, and Binding Commitment*, 75 Ind. L.J. 1125, 1140 (2000). "The reasons the Article 2B draft was so controversial make UCITA [Uniform Computer Information Transactions Act] equally controversial. One reason is its shrink-wrap validation and other expansions of licensors' rights at the expense of licensees." *Id.*

> The provisions of UCITA that have the effect of validating most shrink-wrap licenses and the analogous Web contracts involve creation of a new category called "mass-market" transactions . . . The notion of consent is embodied in-metamorphosed into-a concept of "manifesting assent." Manifestation of assent can include breaking the shrink-wrap, clicking on a link, or commencing to use information.
>
> It certainly seems that UCITA's definition of manifestation of assent stretches the ordinary concept of consent (contested as it was). That stretching starts with the substitution of the word "assent" for the word "consent." In my dictionary, "consent" is one of the meanings of "assent." Nevertheless, "assent" has connotations of acquiescence, of mere failure to remove oneself from a process; "consent," on the other hand, seems surrounded with more connotations of voluntary involvement of oneself in a process . . . By substituting "assent," UCITA seems to be validating the take-it-or-leave-it nature of the terms that come with these mass-market transactions.

Id. at 1141-42 (citations omitted).

"Contract law struggles to find ways to accommodate such 'contracts of adhesion' without wholly discarding the requirement of a 'meeting of the minds.' Significant portions of the current U.C.C. are devoted to the problem." Lemley, *supra* note 45, at 1287.

C. *Robust Notice and Informed Consent*

In order for legislation to be effective, great attention must be paid to the notice and consent requirements. Notice and consent are the first two, and arguably the most important, of the "five core principles of privacy protection" that are termed "fair information practices" and outlined by the Federal Trade Commission in its 1998 report to Congress concerning the collection and use of personal information on the Internet.[62]

The "five core principles" are: "(1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress."[63] Concerning the principle of notice, the *Privacy Report* states: "The most fundamental principle is notice. Consumers should be given notice of an entity's information practices before any personal information is collected from them. Without notice, a consumer cannot make an informed decision as to whether and to what extent to disclose personal information."[64]

The term "robust notice" was introduced legislatively in the Online Personal Privacy Act, a bill proposed in the Senate in 2002.[65] The bill required opt-in consent for "sensitive personally identifiable information"[66] and opt-out consent for "non-sensitive personally identifiable

[62] *See* Federal Trade Commission, Privacy Online: A Report to Congress (June 1998), http://www.ftc.gov/reports/privacy3/priv-23a.pdf.

[63] *Id.* at 7. "The second widely-accepted core principle of fair information practice is consumer choice or consent." *Id.* at 8. *See also* Jordan M. Blanke, *"Safe Harbor" and the European Union's Directive on Data Protection*, 11 Alb. L.J. Sci. & Tech. 57, 58-71 (2000) (discussing the origin of the fair information practices in principles set forth by the Organization for Economic Cooperation and Development (OECD) in its 1980 report, *Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*).

[64] Federal Trade Commission, *supra* note 62, at 7.

[65] Online Personal Privacy Act, S. 2201, 107th Cong. § 102(c) (2002). The term "robust notice" had actually been used by the Federal Trade Commission (FTC) in some of its reports prior to 2002. For example, in its *Online Profiling: A Report to Congress (Part 2): Recommendations* (July 2000), *available at* http://www.ftc.gov/os/2000/07/onlineprofiling.htm, the FTC applauded efforts by the Network Advertising Initiative (made up of Internet advertisers like DoubleClick and Avenue A) at self-regulation of the industry. *Id.* at 5. The NAI principles, as reported by the FTC, included this statement: "Where personally identifiable information is collected for profiling, a heightened level of notice, 'robust' notice will be required at the time and place such information is collected and before the personal data is entered." *Id.* at 9. *But see* Courtenay Youngblood, Case Notes and Comments, *A New Millennium Dilemma: Cookie Technology, Consumers, and the Future of the New Internet*, 11 DePaul-LCA J. Art & Ent. L. & Pol'y 45, 76-79 (2001) (finding the NAI principles a good first step, but expressing fear over the "poodle, home alone, watching over the valuables").

[66] Online Personal Privacy Act, S. 2201, 107th Cong. (2002). "Sensitive financial information" was defined in § 401(14) and "sensitive personally identifiable information" was defined as:

> personally identifiable information about an individual's--
> (A) individually identifiable health information . . .;
> (B) race or ethnicity;
> (C) political party affiliation;
> (D) religious beliefs;
> (E) sexual orientation;
> (F) a Social Security number; or
> (G) sensitive financial information.

information."[67] For both kinds of information, Internet service providers and operators of commercial web sites had to provide "clear and conspicuous" notice of:

> (1) the specific types of information that will be collected;
> (2) the methods of collecting and using the information collected; and
> (3) all disclosure practices of that provider or operator for personally identifiable information so collected, including whether it will be disclosed to third parties.[68]

For "sensitive personally identifiable information," Internet service providers and operators of commercial web sites could not:

> (1) collect sensitive personally identifiable information online, or
> (2) disclose or otherwise use such information collected online, from a user of that service or website,
> unless the provider or operator obtains that user's consent to the collection and disclosure or use of that information before, or at the time, the information is collected and the user's consent is manifested by an affirmative act, in a written or electronic communication.[69]

For "non-sensitive personally identifiable information," Internet service providers and operators of commercial web sites could not:

> (1) collect personally identifiable information not described in subsection (b) ["sensitive personally identifiable information"] online, or
> (2) disclose or otherwise use such information collected online, from a user of that service or website,

Id. at § 401(15).

[67] *Id.* at § 102(c)(1). "Personally identifiable information" was defined as "individually identifiable information about an individual collected online, including--

> (i) a first and last name, whether given at birth or adoption, assumed, or legally changed;
> (ii) a home or other physical address including street name and name of a city or town;
> (iii) an e-mail address;
> (iv) a telephone number;
> (v) a birth certificate number;
> (vi) any other identifier for which the [FTC] finds there is a substantial likelihood that the identifier would permit the physical or online contacting of a specific individual; or
> (vii) information that an Internet service provider, online service provider, or operator of a commercial website collects and combines with an identifier described in clauses (i) through (vi) of this subparagraph."

Id. at § 401(11)(a). "Non-sensitive personally identifiable information" (as used in § 102(c)(1)) included any "personally identifiable information" that was not deemed to be "sensitive personally identifiable information." *Id.* at § 102(c)(1).

[68] *Id.* at § 102(a).

[69] *Id.* at § 102(b).

> unless the provider or operator provides *robust notice* to the user, in addition to clear and conspicuous notice, and has given the user an opportunity to decline consent for such collection and use by the provider or operator before, or at the time, the information is collected.[70]

"Robust notice" was defined as "actual notice at the point of collection of the personally identifiable information describing briefly and succinctly the intent of the Internet service provider, online service provider, or operator of a commercial website to use or disclose that information for marketing or other purposes."[71] The purpose of robust notice is to inform users that they have a choice in deciding whether to continue with the next action, for example, disclosing personally identifiable information, or installing a piece of software that will collect such information or monitor their Internet browsing.

Directly flowing from this notion of robust notice is informed consent. As Professor Paul Schwartz explained:

> It would be difficult for adware and spyware companies to make an argument for free choice to trade personal data in the absence of sufficient notice of data collection and processing practices. Informed consent to adware and spyware would require notice of such practices; without it, there is no free choice to trade data.[72]

The only way a person can give truly informed consent is if he or she has received robust notice. This notice must include information sufficient to inform the person of the consequences of his or her action. Strict provisions for robust notice must be implemented in order to guarantee that an informed consent creates a genuine assent. Any successful spyware legislation will have to carefully detail the requirements of this robust notice.

V. Legislative Approaches

A. *Utah*

Amid much opposition, Utah became the first state to enact anti-spyware legislation, the Spyware Control Act, on March 23, 2004.[73] The conduct prohibited by the Act was relatively straightforward. A person could not:

[70] *Id.* at § 102(c) (emphasis added).

[71] *Id.* at § 401(13).

[72] Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 Harv. L. Rev. 2055, 2074 (2004). Schwartz suggests that "[t]he area of informed consent to medical decisionmaking provides possible analogies" for spyware consent regulation. *Id.* at 2074 n.101.

[73] Utah Code Ann. §§ 13-39-101 to -401 (2004). On June 22, 2004, the enforcement of the Act was enjoined by a state court. *See supra* note 60.

> 1. install spyware on another person's computer;
> 2. cause spyware to be installed on another person's computer; or
> 3. use 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.[74]

However, the Act contained an extremely complicated definition of "spyware:"

> "Spyware" means software residing on a computer that:
>
> (a) monitors the computer's usage;
>
> (b) (i) sends information about the computer's usage to a remote computer or server; *or*
>
> (ii) displays or causes to be displayed an advertisement in response to the computer's usage if the advertisement:
>
> (A) does not clearly identify the full legal name of the entity responsible for delivering the advertisement;
>
> (B) uses a federally registered trademark as a trigger for the display of the advertisement by a person other than:
>
> (I) the trademark owner;
>
> (II) an authorized agent or licensee of the trademark owner; *or*
>
> (III) a recognized Internet search engine;
>
> (C) uses a triggering mechanism to display the advertisement according to the Internet websites accessed by a user; *or*
>
> (D) uses a context based triggering mechanism to display the 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; *and*
>
> (c) does not:
>
> (i) obtain the consent of the user, at the time of, or after installation of the software but before the software does any of the actions described in Subsection (4)(b):
>
> (A) to a license agreement:
>
> (I) presented in full; *and*
>
> (II)written in plain language;
>
> (B) to a notice of the collection of each specific type of information to be transmitted as a result of the software installation;
>
> (C) to a clear and representative full-size example of each type of advertisement that may be delivered;
>
> (D) to a truthful statement of the frequency with which each type of advertisement may be delivered; *and*

[74] *Id*. at § 13-39-201.

> (E) for each type of advertisement delivered by the software, a clear description of a method by which a user may distinguish the advertisement by its appearance from an advertisement generated by other software services; *and*
>
> (ii) provide a method:
>
> (A) by which a user may quickly and easily disable and remove the software from the user's computer;
>
> (B) that does not have other effects on the non-affiliated parts of the user's computer; *and*
>
> (C) that uses obvious, standard, usual, and ordinary methods for removal of computer software.[75]

The definition provided extensive notice requirements in subsection (c)(1), but was too convoluted to be useful.

In 2005, Utah amended the Spyware Control Act to include a much simpler definition of spyware:

> "Spyware" means software on the computer of a user who resides in this state that:
>
> (i) collects information about an Internet website at the time the Internet website is being viewed in this state, unless the Internet website is the Internet website of the person who provides the software; and
>
> (ii) uses the information described in Subsection (8)(a)(i) contemporaneously to display pop-up advertising on the computer.[76]

[75] *Id*. at § 13-39-102(4). "Spyware" specifically did not include:

> (a) software designed and installed solely to diagnose or resolve technical difficulties;
>
> (b) software or data that solely report to an Internet website information previously stored by the Internet website on the user's computer, including:
>
> (i) cookies;
>
> (ii) HTML code; or
>
> (iii) Java Scripts; or
>
> (c) an operating system.

Id. at § 13-39-102(5).

[76] Utah Code Ann. § 13-39-102(8)(a) (2005).

"Spyware" specifically does not include:

> (i) an Internet website;
>
> (ii) a service operated by an Internet or online service provider accessed by a user;
>
> (iii) software designed and installed primarily to:
>
> (A) prevent, diagnose, or resolve technical difficulties;
>
> (B) detect or prevent fraudulent activities; or
>
> (C) protect the security of the user's computer from unauthorized access or alteration;
>
> (iv) software or data that reports information to an Internet website previously stored by the Internet website on the user's computer, including cookies;
>
> (v) software that provides the user with the capability to search the Internet; or
>
> (vi) software installed with the consent of a user whose primary purpose is to prevent access to certain Internet content.

Id. at § 13-39-102(8)(a).

While this definition is certainly much less cumbersome than the first one, it essentially guts the Act of its original aggressive approach to spyware. Virtually all of the notice language was removed.

B. *California*

As initially drafted and introduced in the California Senate, S.B. 1436 provided a short and straight-forward notice requirement:

> (a) A person or entity that provides computer software containing spyware to a computer in California shall disclose the following information to the recipient of the software:
>
> (1) That the software contains spyware.
>
> (2) What the spyware does.
>
> (b) The statement required by subdivision (a) shall be in at least 18-point type and shall be included in the first appearing of the following:
>
> (1) The software's opening download.
>
> (2) The Web site of the provider or of the software.
>
> (3) The initial installation screen for the software.[77]

Coupled with a short and well-crafted definition of "spyware,"[78] the legislation initially appeared to have a good chance of accomplishing its goal.[79] Unfortunately, the bill was

[77] S. 1436, § 22947.2, 2003-04 Leg. Sess. (Cal., introduced February 19, 2004), *available at* http://www.leginfo.ca.gov/pub/03-04//bill/sen/sb_1401-1450/sb_1436_bill_20040219_introduced.pdf.

[78] *Id.*

> For purposes of this chapter, "spyware" means an executable 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:
>
> (a) Personal information or data of a user.
>
> (b) Data regarding computer usage, including, but not limited to, which Internet sites are or have been visited by a user.

Id. at § 22947.1.

[79] *Id.*

> This bill would require a person or entity providing computer software containing spyware, as defined, to a computer in California to disclose to the recipient that the software contains spyware and what the spyware does. The bill would authorize the recipient of computer spyware transmitted in violation of the prohibitions, the Internet service provider, or the Attorney General to bring an action to recover actual damages. The bill would authorize these parties to recover liquidated damages of $1,000 per transmission, subject to reduction by a court for specified reasons. The bill would provide for an award of reasonable attorney's fees and costs to a prevailing plaintiff.

Legislative Counsel's Digest, S. 1436 *supra*.

amended nine times before it was passed, and most of its important language was removed.[80] The law enacted by California no longer provides for specific notice requirements, no longer defines "spyware," and no longer provides for a right of private action.[81] Instead, it now requires that proscribed acts be committed with intentional misrepresentation or by "intentionally deceptive" means.[82] Ultimately, the law will be incapable of accomplishing anything productive.[83]

C. *Federal – SPY ACT*

The proposed SPY ACT,[84] before the House of Representatives, has two main sections. Section 2 prohibits a variety of spyware activities, but only if they are the result of "deceptive acts or practices."[85] While it would be nice to prevent browsers from being diverted, home pages

[80] *See* Susan Kuchinskas, *California Spyware Bill: 'Worse Than Nothing'* (Sept. 16, 2004), http://www.internetnews.com/security/article.php/3409281.

[81] *See* Consumer Protection Against Computer Spyware Act, Cal. Bus. & Prof. Code § 22947 (2005). However, there is a bill pending before the California Senate that would provide for a private action for violations of the spyware law. *See* S. 92, 2005-06 Leg. Sess. (Cal., introduced Jan. 14, 2005), *available at* http://www.leginfo.ca.gov/pub/bill/sen/sb_0051-0100/sb_92_bill_20050114_introduced.pdf.

[82] "Intentionally deceptive" means any of the following:

> (1) By means of an intentionally and materially false or fraudulent statement.
> (2) By means of a statement or description that intentionally omits or misrepresents material information in order to deceive the consumer.
> (3) By means of an intentional and material failure to provide any notice to an authorized user regarding the download or installation of software in order to deceive the consumer.

Cal. Bus. & Prof. Code §§ 22947.1(h) (2005).

[83] Two privacy advocacy rights groups, World Privacy Forum and Privacy Rights Clearinghouse, wrote a letter to California Governor Schwarzenegger, urging him to veto the bill. *Privacy Groups Urge Gov. Schwarzenegger to Veto Spyware Bill*, Sept. 12, 2004, http://www.privacyrights.org/ar/SB1436Letter.htm. They stated that implementing the bill "might well prove to be worse than enacting no spyware law at all" because of the high standards of proof regarding "actual knowledge," "conscious avoidance of knowledge," "willfulness," "intent to deceive," and "intentionally deceptive." *Id.* The groups also stressed the importance of "basing spyware legislation on the OECD 'fair information principles' of notice, consent, and purpose specification" and criticized the legislation for lacking this. *Id.*

[84] Securely Protect Yourself Against Cyber Trespass Act (SPY ACT), H.R. 29, 109th Cong. (2005).

[85] SEC. 2. PROHIBITION OF DECEPTIVE ACTS OR PRACTICES RELATING TO SPYWARE.

> (a) Prohibition- It is unlawful for any person, who is not the owner or authorized user of a protected computer, to engage in deceptive acts or practices that involve any of the following conduct with respect to the protected computer:
>
> > (1) Taking control of the computer by--
> >
> > > (A) utilizing such computer to send unsolicited information or material from the protected computer to others;
> > > (B) diverting the Internet browser of the computer, or similar program of the computer used to access and navigate the Internet--
> > >
> > > > (i) without authorization of the owner or authorized user of the computer; and

and bookmarks from being modified, software from being installed despite efforts to prevent it,

> (ii) away from the site the user intended to view, to one or more other Web pages, such that the user is prevented from viewing the content at the intended Web page, unless such diverting is otherwise authorized;
>
> (C) accessing or using the modem, or Internet connection or service, for the computer and thereby causing damage to the computer or causing the owner or authorized user to incur unauthorized financial charges;
>
> (D) using the computer as part of an activity performed by a group of computers that causes damage to another computer; or
>
> (E) delivering advertisements that a user of the computer cannot close without turning off the computer or closing all sessions of the Internet browser for the computer.
>
> (2) Modifying settings related to use of the computer or to the computer's access to or use of the Internet by altering--
>
> (A) the Web page that appears when the owner or authorized user launches an Internet browser or similar program used to access and navigate the Internet;
>
> (B) the default provider used to access or search the Internet, or other existing Internet connections settings;
>
> (C) a list of bookmarks used by the computer to access Web pages; or
>
> (D) security or other settings of the computer that protect information about the owner or authorized user for the purposes of causing damage or harm to the computer or owner or user.
>
> (3) Collecting personally identifiable information through the use of a keystroke logging function.
>
> (4) Inducing the owner or authorized user to install a computer software component onto the computer, or preventing reasonable efforts to block the installation or execution of, or to disable, a computer software component by--
>
> (A) presenting the owner or authorized user with an option to decline installation of a software component such that, when the option is selected by the owner or authorized user, the installation nevertheless proceeds; or
>
> (B) causing a computer software component that the owner or authorized user has properly removed or disabled to automatically reinstall or reactivate on the computer.
>
> (5) Misrepresenting that installing a separate software component or providing log-in and password information is necessary for security or privacy reasons, or that installing a separate software component is necessary to open, view, or play a particular type of content.
>
> (6) Inducing the owner or authorized user to install or execute computer software by misrepresenting the identity or authority of the person or entity providing the computer software to the owner or user.
>
> (7) Inducing the owner or authorized user to provide personally identifiable, password, or account information to another person--
>
> (A) by misrepresenting the identity of the person seeking the information; or
>
> (B) without the authority of the intended recipient of the information.
>
> (8) Removing, disabling, or rendering inoperative a security, anti-spyware, or anti-virus technology installed on the computer.
>
> (9) Installing or executing on the computer one or more additional computer software components with the intent of causing a person to use such components in a way that violates any other provision of this section.

Id. at § 2.

and anti-spyware and anti-virus software from being removed or disabled, the section leaves too much to the interpretation of "deceptive."[86] Prospective violators will certainly claim that their practices were not deceptive and that, in fact, the user had actually consented to the act or practice.[87]

Section 3 is much more promising. First, it requires opt-in consent before "any information collection program" can be transmitted to or executed on a computer.[88] Notice must be provided in a specified manner and any information collection program must contain certain specified functions.[89]

> An "information collection program" is defined as computer software that
> (A) (i) collects personally identifiable information; and
> (ii) (I) sends such information to a person other than the owner or authorized user of the computer, or
> (II) uses such information to deliver advertising to, or display advertising on, the computer.
> (B) (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.[90]

Subsection 3(c) is devoted entirely to notice and consent requirements. The notice must be "clear and conspicuous" and "in plain language."[91] It must be distinguished "from any other

[86] Benjamin Edelman, *What Hope for Federal Anti-Spyware Legislation?*, http://www.benedelman.org/news/011905-1.html (last visited Jan. 31, 2005).

[87] *Id.*

[88] H.R. 29 § 3(a)(1).

[89] *Id.* § 11(13)(A). "Personally identifiable information" is defined as the "following information, to the extent only that such information allows a living individual to be identified from that information:

> (i) First and last name of an individual.
> (ii) A home or other physical address of an individual, including street name, name of a city or town, and zip code.
> (iii) An electronic mail address.
> (iv) A telephone number.
> (v) A social security number, tax identification number, passport number, driver's license number, or any other government-issued identification number.
> (vi) A credit card number.
> (vii) Any access code, password, or account number, other than an access code or password transmitted by an owner or authorized user of a protected computer to the intended recipient to register for, or log onto, a Web page or other Internet service or a network connection or service of a subscriber that is protected by an access code or password.
> (viii) Date of birth, birth certificate number, or place of birth of an individual, except in the case of a date of birth transmitted or collected for the purpose of compliance with the law.

[90] *Id.* § 3(b)(1).

[91] *Id.* § 3(c)(1).

information visually presented contemporaneously on the computer."[92] Furthermore, the notice must contain one of the following statements (or one that is substantially similar):

> "This program will collect and transmit information about you. Do you accept?"
> "This program will collect information about Web pages you access and will use that information to display advertising on your computer. Do you accept?"
> "This program will collect and transmit information about you and will collect information about Web pages you access and use that information to display advertising on your computer. Do you accept?"[93]

This is the best part of the legislation. The message could not be any clearer. It is this kind of robust notice that will permit a computer user to make an informed consent.[94]

Subsection 3(c) also requires that the notice provides the user with the ability to grant or deny the opt-in consent, or to abandon the transmission or execution of the information collection program.[95] Additionally, the notice must provide an option for the user to display on the computer, before granting or denying consent, a clear description of:

> (i) the types of information to be collected and sent (if any) by the information collection program;
> (ii) the purpose for which such information is to be collected and sent; and
> (iii)in the case of an information collection program that first executes any of the information collection functions of the program together with the first execution of other computer software, the identity of any such software that is an information collection program.[96]

The Subsection also provides that the notice required for subsections 3(c)(1)(B), 3(c)(1)(C) and 3(c)(1)(D) must remain on the screen until the user grants or denies consent, abandons the transmission or execution of the information collection program, or selects the option to see specifics about the information to be collected.[97]

Two provisions of Subsection 3(c) do leave some room for improvement. First, a "single notice" rule permits multiple information collection programs to give just one "clear and conspicuous notice in plain language."[98] While there are certainly situations for which this

[92] *Id.* § 3(c)(1)(A).

[93] *Id.* § 3(c)(1)(B).

[94] *See* Benjamin Edelman, *Methods and Effects of Spyware: Response to FTC Call for Comments* (Mar. 19, 2004), http://www.benedelman.org/spyware/ftc-031904.pdf#page=7 (illustrating a good example of Google's plain language, honest approach to acquiring user consent before installation of the Google Toolbar).

[95] H.R. 29 § 3(c)(1)(C).

[96] *Id.* § 3(c)(1)(D).

[97] *Id.* § 3(c)(1)(E).

[98] *Id.* § 3(c)(2).

might make sense, it may also provide a loophole for the unscrupulous to piggyback the installation of several programs with one notice. The legislation seems to be aware of this possibility as it retains the requirement of subsection 3(c)(1)(D) that there be a separate option for each information collection program for the user to see further specifics about the information to be collected.[99]

Secondly, there is a requirement to provide additional notice and obtain additional consent if there are changes in the information collection program.[100] However, this subsequent notice and consent is required only if the information to be collected or sent is of a type or for a purpose that is "materially different from" the original type or purpose.[101] Again, while in certain situations this might make sense, there are many opportunities for abuse.

The other important provision of Section 3 is the requirement that certain functions be contained in any information collection program. Specifically, there must be:

> (1) DISABLING FUNCTION- With respect to any information collection program, a function of the program that allows a user of the program to remove the program or disable operation of the program with respect to such protected computer by a function that--
> (A) is easily identifiable to a user of the computer; and
> (B) can be performed without undue effort or knowledge by the user of the protected computer.
>
> (2) IDENTITY FUNCTION-
> (A) In General—With respect only to an information collection program that uses information collected in the manner described in subparagraph (A)(ii)(II) or (B)(ii) of subsection (b)(1) and subject to subparagraph (B) of this paragraph, a function of the program that provides that each display of an advertisement directed or displayed using such information when the owner or authorized user is accessing a Web page or online location other than of the provider of the computer software, is accompanied by the name of the information collection program, a logogram or trademark used for the exclusive purpose of identifying the program, or a statement or other information sufficient to clearly identify the program.[102]

These requirements are certainly consistent with the notion of informed consent. If a user does consent, but later changes his or her mind, there should be a way for that consent to be withdrawn. Because many spyware programs are difficult to disable or remove, these required functions are important.

In summary, the SPY ACT, particularly Section 3, does a good job of addressing robust notice and informed consent. It requires that notice be clear and conspicuous and in plain

[99] *Id.* § 3(c)(1)(D).

[100] *Id.* § 3(c)(3).

[101] *Id.* § 3(c)(3)(B).

[102] *Id.* § 3(d).

language. It requires that the user be informed in detail of the types of information collected and the uses therefore. Additionally, it requires that the notice remain on the screen until the user decides whether or not to consent.

D. *Federal – SPY BLOCK Act (109th Session)*

The proposed SPY BLOCK Act,[103] before the Senate, looks quite different from the SPY ACT, but takes a somewhat similar approach, with less promising results. It has several sections that deal with spyware activities, but that are hampered by definitional problems. It has one section that addresses notice and consent requirements, but is not as stringent as the requirements of the SPY ACT.

a. Section 2

Section 2 addresses "prohibited practices related to software installation."[104] It prohibits the "surreptitious installation" of software that "conceals from the user of the computer the fact that the software is being installed," or "prevents the user of the computer from having an opportunity to knowingly grant or withhold consent to the installation."[105] Without further definition, "conceals" and "knowingly grant or withhold" provide too much room for interpretation.

Furthermore, there is an exception that begs for abuse: "the subsection does not apply to . . . the installation of software that ceases to operate when the user of the computer exits the software or service through which the user accesses the Internet, if the software so installed does not begin to operate again when the user accesses the Internet via that computer in the future."[106] This would seem to exempt any software that only operates while someone is accessing the internet – like most spyware, for example.

Section 2 prohibits any misleading inducement to give consent to the installation of software by means of a "materially false or misleading representation" concerning the identity of the operator of a website, or the identity of the author, publisher or distributor of the software, or of the "nature or function of the software," or of the "consequences of not installing the software."[107] Once again, however, this prohibition applies only if one can prove there was a "materially false or misleading misrepresentation" made. This may prove to be a difficult burden.

[103] Software Principles Yielding Better Levels of Consumer Knowledge Act (SPY BLOCK Act), S. 687, 109th Cong. (2005).

[104] *Id.* § 2.

[105] *Id.* § 2(a)(1).

[106] *Id.* § 2(a)(2)(D).

[107] *Id.* § 2(b).

Section 2 also prohibits "the installation of software on the computer if the software cannot subsequently be uninstalled or disabled by an authorized user through a program removal function that is usual and customary with the user's operating system, or otherwise as clearly and conspicuously disclosed to the user."[108] The effect of this provision, however, will be drastically limited because the

> subsection shall not be construed to require individual features or functions of a software program, upgrades to a previously installed software program, or software programs that were installed *on a bundled basis with other software* or with hardware to be capable of being uninstalled or disabled separately from such software or hardware.[109]

Because much spyware is installed as part of bundled software, this limitation will eviscerate the rule.

b. Section 3

Section 3 of the SPY BLOCK Act is similar to Section 3 of the SPY ACT, but has inferior notice and consent requirements. It prohibits the installation or use of software that includes a "surreptitious information collection feature."[110] A "surreptitious information collection feature" is defined as software that

> (1) collects information about a user of a protected computer or the use of a protected computer by that user, and transmits such information to any other person or computer–
>
> > (A) on an automatic basis or at the direction of person other than an authorized user of the computer, such that no authorized user knowingly triggers or controls the collection and transmission;
> > (B) in a manner that is not transparent to an authorized user at or near the time of the collection and transmission, such that no authorized user is likely to be aware of it when information collection and transmission are occurring; and
> > . . . .
>
> (2) begins to collect and transmit such information without prior notification that–
>
> > (A) clearly and conspicuously discloses to an authorized user of the computer the type of information the software will collect and the types of ways the information may be used and distributed; and

[108] *Id.* § 2(c)(1).

[109] *Id.* § 2(c)(2)(B) (emphasis added).

[110] *Id.* § 3(a)(1).

> (B) is provided at a time and in a manner such that an authorized user of the computer has an opportunity, after reviewing the information contained in the notice, to prevent either–
>
> (i) the installation of the software; or
>
> (ii) the beginning of the operation of the information collection and transmission capability described in paragraph (1).[111]

While this section does require notice and consent, it is not as specific in its requirements as those in the SPY ACT. It requires clear and conspicuous disclosure, but does not address any specifics about form, content, or duration of the notice.

c. Section 4

Section 4 attempts to prohibit adware but is so full of potential loopholes that it would likely be completely ineffective. It prohibits the installation "of software that causes advertisements to be displayed to the user without a label or other reasonable means of identifying to the user . . . which software caused the advertisement's delivery."[112] First, if a spyware program identifies the software responsible for displaying the advertisement, it is in compliance with the provision. Second, an exception permits such advertisement without identification as long as it is done on a website operated by the publisher of the software or if the operator of a website has provided express consent for such ads.[113]

d. Section 5

Section 5 is similar to Section 2 of the SPY ACT. It prohibits a variety of spyware activities, but only if they are the result of "an unfair or deceptive act or practice."[114] Once again, the effectiveness of this section would likely depend upon the interpretation of this phrase by the courts.

[111] *Id.* § 3(c).

[112] *Id.* § 4(a).

[113] *Id.* § 4(b).

[114] *Id.* § 5. Among the practices prohibited are using a computer to send unsolicited information to other computers, diverting an Internet browser to another website, displaying advertisements in browser windows that are not easily terminated, removing or disabling privacy or security protections installed on the computer, or modifying computer settings, such as default home pages, bookmarks, or security settings. *Id.*

E. *Federal – SPY BLOCK Act (108th Session)*

It is disheartening to compare the SPY BLOCK Act proposed in the 109th session of Congress with the one proposed in the previous session.[115] The earlier bill was constructed upon a foundation of robust notice and informed consent which, unfortunately, is lacking in the later version.

a. Section 2

Section 2 addressed the "unauthorized installation of computer software."[116] It prohibited the installation of software unless

1. the user of the computer has received notice that satisfies the requirements of section 3;
2. the user of the computer has granted consent that satisfies the requirements of section 3; and
3. the computer software's uninstall procedures satisfy the requirements of section 3.[117]

b. Section 3

Section 3 addressed the "notice, consent, and uninstall requirements."[118] The notice required by Section 3 had to be clear and remain displayed on the screen until the user either granted or denied consent to install the software.[119] In addition, there had to be a separate disclosure for each of four enumerated features that may be contained in the software, and such disclosure also had to remain on the screen until the user either granted or denied consent to that feature:

For an *information collection feature*, the disclosure had to provide a "clear description" of

(i) the type of personal or network information to be collected and transmitted by the computer software; and
(ii) the purpose for which the personal or network information was to be collected, transmitted, and used.[120]

[115] *See* Software Principles Yielding Better Levels of Consumer Knowledge Act (SPY BLOCK Act), S. 2145, 108th Cong. (2004).

[116] *Id.* § 2.

[117] *Id.* § 2(a).

[118] *Id.* § 3.

[119] *Id.* § 3(a)(1).

[120] *Id.* § 3(a)(2)(B). An "information collection feature" was defined as a function of software that, when installed, "collects personal or network information about the user of the computer and transmits such information to any other party on an automatic basis or at the direction of a party other than the user of the computer." *Id.* § 8(9).

For an *advertising feature*, the disclosure had to provide

> (i) a representative example of the type of advertisement that may be delivered by the computer software;
> (ii) a clear description of–
>
> > (I) the estimated frequency with which each type of advertisement may be delivered; or
> > (II) the factors on which the frequency will depend; and
>
> (iii) a clear description of how the user can distinguish each type of advertisement that the computer software delivers from advertisements generated by other software, Internet website operators, or services.[121]

For a *distributed computing feature*, the disclosure had to provide a "clear description" of

> (i) the types of information or messages the computer software will cause the computer to transmit;
> (ii)(I) the estimated frequency with which the computer software will cause the computer to transmit such messages or information; or
> (II) the factors on which the frequency will depend;
> (iii) the estimated volume of such information or messages, and the likely impact, if any, on the processing or communications capacity of the user's computer; and
> (iv) the nature, volume, and likely impact on the computer's processing capacity of any computational or processing tasks the computer software will cause the computer to perform in order to generate the information or messages the computer software will cause the computer to transmit.[122]

For a *settings modification feature*, the disclosure had to provide "a clear description of the nature of the modification, its function, and any collateral effects the modification may produce."[123]

[121] *Id.* § 3(a)(2)(C). An "advertising feature" was defined as a function of software that, when installed, "delivers advertisements to the user of that computer." *Id.* § 8(2).

[122] *Id.* § 3(a)(2)(D). A "distributed computing feature" was defined as a function of software that, when installed, "transmits information or messages, other than personal or network information about the user of the computer, to any other computer without the knowledge or direction of the user and for purposes unrelated to the tasks or functions the user intentionally performs using the computer." *Id.* § 8(7).

[123] *Id.* § 3(a)(2)(E). A "settings modification feature" was defined as a function of software that, when installed,

> (A) modifies an existing user setting, without direction from the user of the computer, with respect to another computer software application previously installed on that computer; or
> (B) enables a user setting with respect to another computer software application previously installed on that computer to be modified in the future without advance notification to and consent from the user of the computer.

Id. § 8(15).

In addition, there had to be a "clear description" of the procedures that a user may follow in order to turn off a feature or uninstall the software.[124] A "clear description" was defined as a "description that is clear, conspicuous, concise, and in a font size that is at least as large as the largest default font displayed to the user by the software."[125]

Section 3 required not only consent by the user to the installation of the software, but also an "affirmative consent" to each of the four features that may be contained therein.[126] "Affirmative consent" was defined as "consent expressed through action by the user of a computer other than default action specified by the installation sequence and independent from any other consent solicited from the user during the installation process."[127]

The "uninstall procedures" provision of Section 3 required that computer software

> (1) appear in the "Add/Remove Programs" menu [of the computer's] operating system . . . ;
> (2) be capable of being removed completely using normal procedures . . . ; and
> (3) [for software containing] an advertising feature, include an easily identifiable link clearly associated with each advertisement that the software causes to be displayed, such that selection of the link by the user of the computer generates an on-screen window that informs the user about how to turn off the advertising feature or uninstall the computer software.[128]

In short, the previously proposed SPY BLOCK Act was far superior to the present one. It was structured upon a foundation of robust notice and informed consent, and provided specific details for implementation of those requirements. It is unfortunate that the newer bill abandoned that foundation.

VI. Conclusion

Spyware has become a bigger problem than spam. It not only is annoying, but also often prevents a computer from operating effectively and efficiently. We have reached the point where we need a legislative solution. It would be preferable to have one federal law to regulate everything, rather than a variety of different state laws. However, as we have learned from the CAN-SPAM Act,[129] if the federal law is weak and preempts the state law, we probably would be better off without it.

[124] *Id.* § 3(a)(2)(F).

[125] *Id.* § 8(4).

[126] *Id.* § 3(b).

[127] *Id.* § 8(3).

[128] *Id.* § 3(c).

[129] Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699.

One of the challenges facing legislative bodies will be to draft language that will thwart not only those programs that surreptitiously install themselves, but also those programs whose distributors claim were installed with the consent of the user. In order to accomplish this, the legislation must focus on robust notice and consent requirements. Ideally, all provisions should hinge upon whether a user has given a truly informed consent. The law should not permit spyware to deprive computer users of their rights to use and enjoy their personal property by hiding behind the façade of a contractual relationship lacking genuine assent.