TEACHING A MAN TO FISH: WHY NATIONAL LEGISLATION ANCHORED IN NOTICE AND CONSENT PROVISIONS IS THE MOST EFFECTIVE SOLUTION TO THE SPYWARE PROBLEM

*M. Angela Buenaventura**

I. INTRODUCTION

[1] The term “spyware” encompasses a wide range of software designed to intercept or take partial control of a computer. Spyware slows down computers and forces computer users to expend resources on repair and installation of protective software.[1] Consumers also face the danger that personal information gathered through spyware will be misused. Thus, most people agree that spyware is an annoying and costly problem.[2] However, there is no consensus on the best way to solve the spyware problem. This article examines the methods currently being used to battle spyware, as well as proposed national spyware legislation. The article outlines the various weaknesses in these methods of combating the problem, and suggests how these weaknesses can be remedied.

[2] Part II of this paper will argue that state spyware legislation is inadequate to solve the spyware problem because of Dormant Commerce Clause issues and regulations that vary from state to state which lead to significant business planning and litigation costs. Part III will explore other methods used by plaintiffs to battle spyware: the Wiretap Act, the

* Associate Bryan Cave LLP; JD., Northwestern University School of Law, 2006. The author would like to express her gratitude to Steven Wernikoff, Andrea Matwyshyn, and Peter Neumer for their valuable insights and guidance.

[1] Federal Trade Commission Notices, Public Workshop: Monitoring Software On Your PC: Spyware, Adware, and Other Software, 69 Fed. Reg. 8538 (Feb. 24, 2004).
[2] Jane K. Winn, *Contracting Spyware by Contract,* 20 BERKLEY TECH. L.J. 1345, 1348 (2005).

Stored Communications Act, the Computer Fraud and Abuse Act, and the common law claim of trespass to chattels. It will argue that, because courts so liberally construe "consent" in the e-commerce realm, the Wiretap Act and the Stored Communications Act are weak weapons against spyware. In addition, this manuscript argues that the Computer Fraud and Abuse Act and the common law claim of trespass to chattels cannot adequately address the problem because these laws are merely after-the-fact solutions which do not prevent damage to computers in the first place. Part IV argues that national spyware legislation with detailed notice and consent requirements is necessary to address the spyware problem. Part V explores currently pending spyware legislation: the SPY ACT,[3] I-SPY,[4] and SPY BLOCK.[5] This section will focus on the notice and consent provisions included in the legislation. The final part will address the weaknesses in the notice and consent provisions of the proposed acts and suggest how these acts can be tweaked to remedy their shortcomings.

II. WHY NATIONAL LEGISLATION IS NECESSARY

A. STATE BILLS

[3] Currently, the only legislation that specifically addresses spyware exists at the state level. As of May 8, 2005 at least twenty-seven states were considering or had passed spyware legislation.[6] These state bills can be grouped into three loose categories: "bad acts bills," "notice bills," and "trademark bills."[7]

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

[4] Internet Spyware Prevention Act of 2005, H.R. 744, 109th Cong. (2005) [hereinafter I-SPY].

[5] Software Principles Yielding Better Levels of Consumer Knowledge Act, S. 2145, 109th Cong. (2005) [hereinafter SPY BLOCK].

[6] Susan P. Crawford, *First Do No Harm: The Problem of Spyware*, 20 BERKELEY TECH. L.J. 1433, 1436 (Summer 2005).

[7] *Id.* at 1437.

1. Bad Acts Bills

[4] Alabama, Arkansas, Arizona, California, Illinois, Maryland, Michigan, Nebraska, New York, Rhode Island, Virginia, and Washington have passed or are considering "bad acts bills."[8] Bad acts bills prohibit a laundry list of software that performs certain unsavory functions such as changing homepages, bookmarks, or modem, or other Internet access settings.[9] Such bills also prohibit software that transmits unauthorized e-mail messages, using the computer as part of a distributed denial of service attack, or "opening multiple, sequential, stand alone advertisements"[10] in a browser that cannot be closed without closing the browser or turning off the computer.[11] In addition, software which collects personally identifiable information through deceptive means is illegal.[12]

[5] Moreover, bad acts bills protect anti-spyware software such as Spybot by prohibiting deceptive prevention of a user's efforts to block software installations, misrepresentations that software will be uninstalled or disabled by what the user does next, and deceptive actions to disable anti-spyware software.[13]

2. Notice Bills

[6] Michigan, Pennsylvania, Oregon, Tennessee, and Texas have passed or are considering "notice bills."[14] Notice bills prohibit "spyware," defined

[8] *Id*. at 1441 n. 26 (citing S.B. 122, 2005 Leg. (Ala. 2005); S.B. 2904, 2005 Leg., Reg. Sess. (Ark. 2005); H.B. 2414, 47th Leg., 1st Reg. Sess. (Ariz. 2005); Cal. Bus. & Prof. Code § 22947 (West Supp. 2006); H.B. 380, 94th Gen. Ass. (Ill. 2005); H.B. 945, 2005 Leg., Reg. Sess. (Md. 2005); S.B. 151, 2005 Leg. (Mich. 2005); L.B. 316, 99th Leg., 1st Sess. (Neb. 2005); A.B. 549, 2005-2006 Reg. Sess. (N.Y. 2005); H. 6211, Gen. Ass., Jan. Sess. (R.I. 2005); H.B. 2215, 2005 Leg., Gen. Ass. (Va. 2005); H.B. 1012, 59th Leg., 2005 Reg. Sess. (Wash. 2005)). *See generally* National Conference of State Legislatures, 2005 State Legislation Relating to Internet Spyware or Adware, http://www.ncsl.org/programs/lis/spyware05.htm (last visited Dec. 10, 2005).

[9] *Id*. at 1441.

[10] CAL. BUS. & PROF. CODE § 22947 (West Supp. 2006).

[11] Crawford, supra note 6, at 1441.

[12] *Id*.

[13] *Id*.

[14] *Id*. at 1442-1443.

broadly within the bills,[15] unless a consumer is given the name and contact information of the person installing the software, notice of intent to install the software, a full license agreement, and a means by which to refuse the installation and avoid further contact.[16]

3. TRADEMARK BILLS

[7] Alaska, Indiana, Massachusetts, New Hampshire, Tennessee, and Utah have passed or are considering "trademark bills," which address software that triggers unauthorized advertisements.[17] For example, 1-800 Contacts, a Utah-based company, urged the state legislature to pass a spyware bill after it discovered that a company called SaveNow was installing software on consumers' computers which caused a directory of search terms and URLs to be saved on the users' desktop, then generated pop-up ads and coupons based on the saved data.[18] 1-800 Contacts was angry that a competitor's ads were being triggered by the software to appear in windows over the 1-800 Contacts site.[19] In order to be legal under trademark bills, software triggering ads must clearly identify the entity responsible for the ad and cannot be prompted by an unauthorized trademark use.[20] The consent requirement of these bills also calls for a "full, detailed, plain language license agreement."[21]

[15] *Id*. For example, Pennsylvania spyware legislation, H.B. 574, § 2 (Penn. 2005) (introduced Feb. 16, 2005), defines spyware as follows:

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

[16] Crawford, *supr*a note 6, at 1443.

[17] *Id*. at 1441-42,1442 n.28 (citing S.B. 140, 24th Leg. (Alaska 2005); H.B. 1714, 2005 Reg. Sess. (Ind. 2005); S.B. 273, 184th Gen. Ct. (Mass. 2005); H.B. 47 (N.H. 2005); H.B. 1742, 104th Gen. Ass. (Tenn. 2005)).

[18] *Id*. at 1438, citing *1-800 Contacts, Inc. v. WhenU.com, Inc.*, 309 F. Supp. 2d 467 (S.D.N.Y. 2003).

[19] *1-800 Contacts, Inc*., 309 F. Supp. at 472.

[20] Crawford, *supr*a note 6, at 1442 n. 28.

[21] *Id* at 1442.

B. Problems with State Bills

[8] Because regulating the Internet at the state level conflicts with the cross-boundary nature of the Internet, national legislation is necessary. The main problem with state bills is that although these bills target spyware loaded onto computers in the home state, the transmissions involved in installation comes from out of the state, and, in order to avoid liability, out-of-state businesses must conform to standards set by the most restrictive states.[22] Thus, these bills have the unfortunate consequence of allowing one state to dictate spyware policy for the whole country.

[9] Along with being a policy concern, the fact that a single state can regulate spyware nationwide also triggers Dormant Commerce Clause issues, meaning that these bills will most likely be found unconstitutional.[23] In addition, regulations that vary from state to state lead to significant business planning costs as well as needless litigation of uncertain causes of action.[24] Therefore, spyware must be combated at the national level.

III. Why Other Laws are Insufficient to Cope with the Spyware Problem

[10] State spyware legislation is not the only tool currently being used to combat spyware: spyware can also be challenged under the Wiretap Act, the Stored Communications Act, the Computer Fraud and Abuse Act, and the common law claim of trespass to chattels.

A. The Wiretap Act and the Stored Communications Act

[11] Section 2511(1)(a) of the Wiretap Act prohibits any person from "intentionally intercepting . . . any wire, oral, or electronic communication."[25] The term "intercept" is defined as "the aural or other

[22] Peter S. Menell, *Regulating "Spyware": The Limitations of State "Laboratories" and the Case for Federal Preemption of State Unfair Competition Laws*, 20 BERKELEY TECH. L.J. 1363, 1375-76 (Summer 2005).
[23] Crawford, *supra* note 6, at 1443-44.
[24] Menell, *supra* note 22, at 1412.
[25] 18 U.S.C. § 2511(1)(a) (2000).

acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."[26] One can argue that URLs convey the meaning of a communication. By virtue of the way certain web forms operate, some search terms and other information that a user wishes to remain private can be incorporated into a URL.[27] For example, a search of an online drug store for "Prozac" could generate a page of search results identified by a URL that contains the search term "Prozac." Hence, claims could be brought under the Wiretap Act when a keystroke monitor or software for contextual advertising acquires URLs and search terms.

[12] Another electronic surveillance law that has been used to combat spyware is the Stored Communications Act (SCA).[28] The SCA prohibits gaining unauthorized access to a "facility through which an electronic communication service is provided," and thereby "obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system . . . ."[29] The SCA has been used by plaintiffs to challenge a third party's use of cookies.[30] In *In re DoubleClick*, although the court ultimately disposed of the claim on another issue, the plaintiffs challenged the third-party advertiser's use of cookies under the premise that the "facilities" which the third party accessed were the plaintiffs' computers.[31]

[13] However, because the Wiretap Act and the SCA contain consent exceptions, which can be very liberally construed by courts, these acts cannot be relied upon to prevent spyware installation. Section 2511(2)(d) of the Wiretap Act provides:

> It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the

[26] *Id*. at § 2510(4).

[27] Patricia L. Bellia, *Spyware and the Limits of Surveillance Law*, 20 BERKELEY TECH. L.J. 1283, 1311 (Summer 2005).

[28] 18 U.S.C. §2701(a) (2000).

[29] *Id.* at §2701(a)(2).

[30] *In re* Doubleclick, Inc., 154 F. Supp. 2d 497 (S.D.N.Y. 2001).

[31] *Id*. at 509.

> communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.[32]

Similarly, under the SCA, a defendant's access to a protected facility is not prohibited unless "access without authorization" or exceeding authorized access is shown.[33] The SCA contains an exception for conduct undertaken with the consent of a "user [of an electronic communication service] with respect to a communication of or intended for that user."[34]

1. CONSENT AND "I AGREE" BUTTONS

[14] Spyware bundled with a program that a computer user willingly downloads almost always obtains "consent" via an "I agree" button somewhere during the installation procedure, and usually in some hidden manner. For example, Kazaa, a free peer-to-peer file-sharing application commonly used to exchange MP3 music files, is bundled with adware that generates revenue for the company.[35] An unsuspecting user who has not carefully read the terms of Kazaa's licensing agreement or who does not understand the terms of the agreement can unwittingly agree to interceptions under the Wiretap Act by clicking an "I Agree" button. Thus, the first major issue that arises when addressing the consent exceptions in the Wiretap Act and the SCA in the spyware context is whether clicking an "I Agree" button, displayed in connection with a license agreement detailing the capabilities of software, would constitute consent to the installation of spyware under the acts.

[15] In the e-commerce realm, courts are willing to construe the clicking of an "I Agree" button as consent whether or not meaningful consent was actually present, and whether or not the user even saw the terms to begin with. In *I.Lan Systems, Inc. v. NetScout Service Level Corp.*, the court

[32] 18 U.S.C. §2511(2)(d) (2000).

[33] 18 U.S.C. §2701(a) (2000).

[34] 18 U.S.C. §2701(c) (2000).

[35] John Borland, *Spike in "Spyware" Accelerates Arms Race*, CNET NEWS.COM, Feb. 24, 2003, http://news.com.com/2009-1023-985524.html?tag=cd_mh (describing the expansion of spyware and efforts to combat it).

enforced a license where the terms of the license appeared on screen prior to software installation and the defendant checked an "I Agree" box.[36] Similarly, in *Forrest v. Verizon Commications, Inc*., the court enforced a forum selection clause where terms were displayed in a scroll box and the plaintiff subscriber clicked the "Accept" button.[37] In *Caspi v. Microsoft Network, L.L.C.*, the court enforced a forum selection clause contained in an agreement with an ISP, even though the prospective subscriber could only access the service by clicking "I Agree."[38]

[16] Thus, because courts have been willing to interpret the mere click of an "I accept" button as consent, even if meaningful consent was in fact absent, it is likely that courts would consider users who click an "I agree" button to have consented to the hidden terms included in bundled software license agreements. Therefore, the SCA and the Wiretap Act cannot effectively battle the spyware problem.

2. THIRD PARTY CONSENT

[17] The second major issue that arises when addressing the consent exceptions in the Wiretap Act and the SCA is whether defendants can argue that a third-party advertiser consented to the interception at issue. For example, *In re Pharmatrak Inc. Privacy Litigation* involved a service provided to pharmaceutical companies by Pharmatrak. [39] Pharmatrak collected website traffic and aggregate usage information for these pharmaceutical companies' websites, but promised the companies that it would not expose them to liability by collecting personal data from customers.[40] However, Pharmatrak inadvertently collected personal information from customers, apparently as a result of two of the subscribing companies changing the method they used to retrieve the information from Pharmatrak.[41] When a group of plaintiffs alleged that Pharmatrak had violated the Wiretap Act, Pharmatrak asserted that, because the customers provided their information to Pharmatrak's client pharmacies, the pharmacies were parties to the communications and

[36] *I.Lan Sys., Inc. v. NetScout Serv. Level Corp.*, 183 F. Supp. 2d 328 (D. Mass. 2002).
[37] *Forrest v. Verizon Commc'ns, Inc.*, 805 A.2d 1007 (D.C. 2002).
[38] *Caspi v. Microsoft Network, L.L.C.*, 732 A.2d 528 (N.J. Super. Ct. App. Div. 1999).
[39] *In re Pharmatrak Inc.*, 329 F.3d 9 (1st Cir. 2003).
[40] *Id*. at 17.
[41] *Id*. at 15-16.

consented to the use of Pharmatrak's system.[42] However, the First Circuit rejected the consent argument because, although the pharmaceutical companies had in general terms consented to the use of Pharmatrak's proposed system for gathering data on customers, the companies never agreed to the gathering of personally identifiable information.[43] Nevertheless, under a different set of factual circumstances – perhaps a case in which a website's privacy statement contained buried text explaining that personally identifiable information would be collected – a defendant could easily argue that the third-party advertiser consented to the interception.

[18] In summary, because courts appear willing to apply the consent exceptions to careless clicks of "I agree" buttons and third-party consent, surveillance laws are weak weapons against spyware.[44]

B. The Computer Fraud and Abuse Act and Trespass to Chattels

[19] The Computer Fraud and Abuse Act (CFAA) and the common law claim of trespass to chattels are two other methods of potentially

[42] *Id.* at 19.

[43] *Id.* at 20.

[44] Along with notice and consent issues, there are some other problems with using the Wiretap Act and the SCA to combat spyware. The Wiretap Act requires that a communication be "intercepted." Some types of spyware, such as keystroke monitors, capture data only within a single computer system, e.g. between the keyboard and the CPU. Two courts considering the issue of whether acquiring data within a single system can constitute an interception of an electronic communication, and more specifically addressing the issue of keystroke monitors under the Wiretap Act, have held that if a device or program captures a communication at a point where the communication is still internal to the user's system, then no interception occurs. United States v. Scarfo, 180 F. Supp. 2d 572 (D.N.J. 2001); United States v. Ropp, 347 F. Supp. 2d 831 (C.D. Cal. 2004). *See also* Bellia , *supra* note 27, at 1311. In addition, data collected by spyware may not be considered the "contents" of a communication. Under the Wiretap Act, "contents" include the "substance, purport, or meaning" of a communication." 18 U.S.C. § 2510(8) (2000). Thus, a defendant could argue that when keystroke monitors or adware collects URLs and search terms, the communications do not constitute "contents" of a communication. With respect to the SCA, as one commentator has noted, even if a court were to accept the proposition that a user's hard drive can be considered a facility, the hard drive does not provide and "electronic communications service." Even if a court treats "internet access" as the relevant electronic communications service, then the user's hard drive is not a "facility" through which internet access is provided. *Id*. at 1334.

combating spyware. The CFAA was originally enacted to prosecute computer crimes of federal interest,[45] but was amended in 1994 to provide for a private right of action.[46] A private right of action is available (1) where there is loss to one or more persons aggregating $ 5,000 in any one year period; (2) where there has been - or there is a potential for - an impairment or modification of any medical treatment, diagnosis, examination, or care; (3) where there has been physical injury; (4) where there is a threat to public health or safety; or (5) where there is damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security.[47]

[20] Consumers can also combat spyware under the common law claim of trespass to chattels. According to the Restatement of Torts, "[a] trespass to a chattel may be committed by intentionally . . . using or intermeddling with a chattel in the possession of another,"[48] where "the chattel is impaired as to its condition, quality, or value . . . ."[49] One of the most commonly cited cases involving trespass to chattels in cyberspace is *eBay, Inc. v. Bidder's Edge, Inc.*[50] In this case, eBay sued a competitor who inundated its site with "robots," or computer programs designed to constantly query the eBay site for auction information. Bidder’s Edge used robots to collect information from eBay and other auction sites, and then consolidated the information on its own site.[51] The court granted a preliminary injunction on the trespass claim because it found that the denial of an injunction would encourage other companies to mimic Bidder's Edge, thereby overloading eBay's systems.[52]

1. After-the-Fact Solutions

[21] Unfortunately, the CFAA and the common law claim of trespass to chattels also prove to be incomplete solutions to the spyware problem.

[45] S. REP. NO. 99-432, at 4 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 2479, 2482.
[46] 18 U.S.C. § 1030(g) (2000).
[47] *Id.* at §1030(a)(5)(B)(i)-(v).
[48] RESTATEMENT (SECOND) OF TORTS § 217(b) (1965).
[49] *Id.* § 218(b).
[50] *eBay, Inc. v. Bidder's Edge, Inc.*, 100 F. Supp. 2d 1058 (N.D. Cal. 2000).
[51] *Id.* at 1060-63.
[52] *Id.* at 1072.

The main problem with these solutions is that they are merely after-the-fact solutions. They do not require software purveyors to provide any specific kind of notice to begin with, or require companies to make their spyware easy to control or remove. Thus, like the Wiretap Act and the SCA, these solutions cannot effectively combat spyware because they do not allow consumers to have a meaningful say in what software can be legally installed on their computers and, hence, cannot prevent the damage caused by spyware.

2. DAMAGE THRESHOLDS

[22] Furthermore, the damage thresholds of the CFAA and the trespass to chattels claims also render these solutions ineffective to combat spyware. These damage requirements allow courts to decide how undesirable or harmful a given piece of software is, rather than letting consumers decide for themselves what software can legally be installed on their computers.

[23] As mentioned previously, if an individual wanted to bring an action against a spyware company under the CFAA, they would most likely have to prove a loss of $5,000 in a year.[53] Courts differ widely in their interpretation of the $5,000 damage requirement. Some courts have held that claims may be aggregated among multiple plaintiffs to fulfill the $5,000 loss in one year requirement,[54] while others require that the $5,000 loss must be inflicted on a single computer.[55] For example, in *In re DoubleClick*, the court held that because DoubleClick's collection of data through cookies had not caused $5,000 in damage to a single computer, the CFAA did not apply.[56] The court found that the damages could only be aggregated "over victims and time for a single act."[57] By contrast, in *In re Toys R Us, Inc.*, the court found that the placement of cookies on consumers' computers could constitute a single act and that damages could be aggregated across the class.[58]

[53] 18 U.S.C. § 1030(a)(5)(b)(i) (2000).

[54] *See, e.g., In re* DoubleClick Inc., 154 Supp. 2d at 524.

[55] *See, e.g., In re* Am. Online, Inc. Version 5.0 Software Litig., 168 F. Supp. 2d 1359, 1374 (S.D. Fla. 2001); *In re* Toys R Us, Inc. Privacy Litig., No. 00-CV-2746, 2001 WL 34517252 (N.D. Cal. 2001).

[56] 154 F. Supp. 2d at 524.

[57] *Id.*

[58] *Toys R Us*, 2001 WL 34517252, at *11.

[24] There is a similar damage threshold implied in the common law claim of trespass to chattels. If a court finds that damage caused by trespass is not serious enough, a consumer attempting to use this common law claim to punish a violation is out of luck. *Ticketmaster Corp. v. Tickets.com, Inc.* provides one example of a trespass to chattels claim in the e-commerce realm failing because a court did not find that enough damage had been caused.[59] In *Ticketmaster*, Tickets.com, a direct competitor to Ticketmaster, provided event information to the public via its website.[60] Tickets.com used spiders to search and copy information from Ticketmaster's site, and then provided unauthorized deep links to Ticketmaster's site, allowing visitors to access information on its site and bypass its main page and associated advertising.[61] Ticketmaster brought suit alleging, among other things, trespass to chattels from Tickets.com.[62] In evaluating the trespass claim, the Ticketmaster court denied the injunction because of insufficient proof of trespass and irreparable injury.[63] The court stated:

> A basic element of trespass to chattels must be physical harm to the chattel (not present here) or some obstruction of its basic function (in the court's opinion not sufficiently shown here). TM has presented statistics showing an estimate of the number of hits by T.Com spiders in its own computers and has presented rough comparisons with the total use of the computers by all users of the computers. The comparative use by T.Com appears very small and there is no showing that the use interferes to any extent with the regular business of TM.[64]

[59] *Ticketmaster Corp. v. Tickets.com, Inc.*, No. 99CV7654, 2000 WL 1887522 (C.D. Cal. 2000).
[60] *Id.* at *1.
[61] *Id.* at *2.
[62] *Id.* at *3.
[63] *Id.* at *4.
[64] *Id.*

IV. Key Elements of National Spyware Legislation: Notice, Consent, Removal Requirements

A. The Inadequacies of Current Legislation

[25] As detailed above, if one surveys current legislation, it becomes apparent that the major weakness in the existing body of law is that software purveyors are not required to give consumers meaningful notice and consent before installing potentially damaging software. Current laws make it too easy for a consumer to "consent" to spyware without ever realizing that spyware is being loaded onto the consumer's computer.

B. The Nature of Spyware

[26] The nature of spyware bolsters the proposition that meaningful notice and consent requirements are the key to effective legislation.

1. "Spyware" Is Hard to Define

[27] "Spyware" means different things to different people. What one person views as harmful software another person may view as helpful. Although many extreme types of spyware may be universally viewed as "bad software" in the eyes of the computer user (i.e. software that secretly installs itself onto a computer to steal personal information to be used for identity theft), other types of software may be viewed as desirable by some individuals and not desirable by others. For example, SideStep is a program that informs a user who has purchased a plane ticket whether better deals on the same trip are available with other airlines. However, potentially useful programs such as SideStep track what users see and what users' preferences are. These programs also have extensive information about users' offline activities.[65] While some users might view this as intrusive software and wish to prevent it from installing itself onto their computers, others would welcome its installation. Thus, spyware legislation that is anchored in notice and consent requirements will allow users to define for themselves what constitutes unwelcome spyware.

[65] *See* Megan Johnston, *Struggling Upstream*, FORBES, November 14, 2005, at 100.

2. CHANGING TECHNOLOGY

[28] Spyware technology is constantly advancing, causing legislation that is too specific (e.g. "bad acts" legislation) to become quickly outdated. Therefore, more flexible legislation is necessary. As one commentator has noted, "The fact is that laws for controlling inappropriate and unethical uses of technology are always framed after the problem has mutated into wildly different forms and the issues are rarely understood by the lawmakers who sign them off anyway."[66] Decisions about what kinds of software should be installed on consumers' computers should not be left in the hands of legislators. Notice and consent requirements would force software purveyors to explain which functions each new piece of software performs and allow users to make case-by-case decisions on which types of novel software to allow onto their computers as technology progresses. In addition, flexible legislation rooted in consumer consent would also avoid stifling innovation.

V. DOES PENDING SPYWARE LEGISLATION FIT THE BILL?

[29] The best way to combat spyware is to anchor spyware legislation in meaningful user notice and consent. This section explores currently pending spyware legislation and, more specifically, the notice and consent provisions included in the legislation.

A. I-SPY AND SPY ACT

[30] The Securely Protect Yourself Against Cyber Trespass Act ("SPY ACT"), which was introduced by Representative Mary Bono during the 109th Congress and passed in the House on May 23, 2005, is a complex and comprehensive proposal to fight spyware. The SPY ACT outlaws many of the functions currently performed by spyware, for example "delivering advertisements that a user of the computer cannot close . . . "[67] and "modifying . . . security or other settings of the computer that protect information about the owner or authorized user for the purposes of causing

[66] Mark Gibbs , *Banning the Licking of Toads*, NETWORK WORLD, Oct. 11, 2004, at 62.
[67] Securely Protect Yourself Against Cyber Trespass (SPY) Act, H.R. 29, 109th Cong. at 2(a)(1)(E) (2005).

damage or harm to the computer or owner or user."[68] In this regard, it is similar to the state "bad acts" bills.

[31] The Internet Spyware Prevention Act of 2005 (I-SPY) is the criminal component of the SPY ACT/I-SPY package. In contrast to the regulatory framework of the SPY ACT, I-SPY combats spyware by imposing penalties for actual harm to computers.[69] I-SPY focuses on protecting personal information and safeguarding consumers from spyware that attacks security protection that is already in place on computers.[70] Under I-SPY, anyone who uses spyware to intentionally break into a computer and either alter the computer's security settings, obtain personal information with the intent to defraud or injure a person, or with the intent to damage a computer, faces up to a two-year prison sentence. Those who use software to intentionally break into a computer and then uses that software in furtherance of another federal crime face the same penalty.[71]

[32] Although I-SPY focuses on penalties after the fact and does not contain notice and consent provisions, the SPY ACT includes a notice requirement for software downloads containing spyware that collects information.[72] The notice provisions in the SPY ACT require "clear and

[68] *Id.* § 2(a)(2)(D).

[69] Crawford, *supra* note 6, at 1448.

[70] Internet Spyware Prevention (I-SPY) Act, H.R. 744, 109th Cong. at 2 (2005).

[71] *Id.* § 1030A

[72] SPY ACT, H.R. 29, at 3:
SEC. 3. PROHIBITION OF COLLECTION OF CERTAIN INFORMATION WITHOUT NOTICE AND CONSENT.

> (a) Opt-in Requirement. Except as provided in subsection (e), it is unlawful for any person—
>
> > (1) to transmit to a protected computer, which is not owned by such person and for which such person is not an authorized user, any information collection program, unless--
> >
> > > (A) such information collection program provides notice in accordance with subsection (c) before execution of any of the information collection functions of the program; and
> > >
> > > (B) such information collection program includes the functions required under subsection (d); or
> >
> > (2) to execute any information collection program installed on such a protected computer unless--
> >
> > (A) before execution of any of the information collection functions of the program, the owner or an authorized user of the protected computer

conspicuous notice in plain language," that notice be clearly distinguished from any other information presented at the same time on the computer, and that notice contain particular required texts in English, with three possibilities depending on the type of software:

> (1) [T]his program will collect and transmit information about you. Do you accept?
>
> (2) [T]his program will collect information about Web pages you access and will use that information to display advertising on your computer. Do you accept?
>
> (3) [T]his program will collect and transmit information about you and will collect information about Web pages you access and use that to display advertising on your computer. Do you accept? [73]

In addition, before accepting the consumer must be able to see exactly what type of information is being collected and the purpose for which such information is to be collected and sent.[74]

[33] Information collecting programs must also be fitted with a disabling function that "is easily identifiable to a user of the computer" and "can be performed without undue effort or knowledge by the user of the protected computer."[75] With regard to the removal requirements, the SPY ACT provides that programs must be easily removable by the consumer, and a clear delineation between which "pop-up" advertising is caused by which spyware program so that consumers can easily remove unwanted pop-up generating software.[76]

> has consented to such execution pursuant to notice in accordance with subsection (c) . . . .

[73] *Id.* § 3(c)(1)(B)(i)-(iii).
[74] *Id.* § 3(c)(1)(D).
[75] *Id.* § 43(a)(1)(A)-(B).
[76] *Id.* § 3(d)(1).

B. SPY BLOCK

[34] The Senate is considering the Software Principles Yielding Better Levels of Consumer Knowledge Act ("SPY BLOCK" Act).[77] The SPY BLOCK Act is in part a "bad acts" bill, but also contains many notice and consent provisions. Under SPY BLOCK, it is unlawful for "any person who is not the user of a protected computer to install computer software on that computer, or to authorize, permit, or cause the installation of computer software on that computer," unless notice is provided. Notice must:

> (1) include a clear notification, displayed on the screen until the user either grants or denies consent to installation, of the name and general nature of the computer software that will be installed if the user grants consent; and
>
> (2) include a separate disclosure, with respect to each information collection, advertising, distributed computing, and settings modification feature contained in the computer software, that
>
> > (A) remains displayed on the screen until the user either grants or denies consent to that feature.[78]

[35] Furthermore, depending on the software's functions, different types of notice must be provided before installation. If the software contains an information collection feature, then notice must describe: (1) the type of personal or network information to be collected and transmitted by the computer software; and (2) the purpose for which the personal or network information is to be collected, transmitted, and used.[79] If the software contains pop-up ad features, then notice must provide:

> (i) a representative example of the type of advertisement that may be delivered by the computer software;

[77] *Supra* note 5.
[78] *Id.* § 3(a).
[79] *Id.* § 3(a)(2)(B).

> (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 service.[80]

If the software contains a distributed computing feature,[81] then notice must describe:

> (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

[80] *Id.* § 3(a)(2)(C).

[81] The term "distributed computing feature" means a function of computer software that, when installed on a computer, 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).

> messages the computer software will cause the computer to transmit.[82]

[36] If the software contains a settings modification feature, then notice must provide "a clear description of the nature of the modification, its function, and any collateral effects the modification may produce."[83] In addition, like the SPY ACT, under SPY BLOCK software must offer an uninstall function, and software purveyors must provide "a clear description of procedures the user may follow to turn off such feature or uninstall the computer software."[84]

VI. SUGGESTED IMPROVEMENTS

[37] The SPY ACT/I-SPY and SPY BLOCK Acts could prove to be very effective in the fight against spyware. Many provisions address the major shortfalls of current state laws being used to battle spyware. Most notably, the acts focus on the importance of providing computer users with notice and requiring that software purveyors obtain meaningful consent. Unlike the Wiretap Act and the SCA, the proposed legislation requires clear and conspicuous notice provisions, which ensure that computer users cannot accidentally click away their rights when notice of a piece of spyware's capabilities are buried within the terms of the license agreement. In addition, unlike the Wiretap Act and the SCA, potential defendants cannot hide behind a third party's alleged consent in order to escape liability for installing potentially harmful software. Because the proposed acts focus on clear and conspicuous notice and consent provisions they can also prevent damage before it happens, unlike the after-the-fact solutions provided by the CFAA and trespass to chattels claims. Furthermore, consent can, in effect, be revoked under these proposed acts because they require that software be fitted with removal capabilities.

[38] There are, however, a few major weaknesses in the notice and consent provisions of the proposed acts. The next section suggests how these acts can be tweaked to remedy their shortcomings.

[82] *Id*. § 3(a)(2)(D).

[83] SPY BLOCK, *supra* note 5 at § 3(a)(2)(E).

[84] *Id*. § 3(a)(2)(F).

A. RIGID DEFINITIONS

[39] The notice provisions in both the SPY ACT and SPY BLOCK are written to apply to very specific types of technology. Very specific wording does make what is required of software purveyors clear, but (1) these provisions may allow certain types of software that a consumer may find undesirable to slip through the cracks; and (2), these provisions can become quickly outdated as technology progresses.

[40] The main problem with the notice and consent provisions found in the SPY ACT is that these provisions only apply to software programs falling under the Act's definition of "information collection program."[85] Thus, other software that consumers may find undesirable can still be installed without any notice or consent. For example, some political data-mining companies collect and share aggregated, non-personally identifiable information with campaigns.[86] Many of these companies build their political databases by providing free e-mail services and requiring subscribers to fill out questionnaires.[87] Initial questionnaires collect the demographics of database members, such as age, gender, income,

[85] *Id.* § 3(b)(1):

> (b) Information Collection Program.
>
> > (1) In general. For purposes of this section, the term "information collection program" means computer software that performs either of the following functions:
> >
> > > (A) Collection of personally identifiable information. The computer software--
> > >
> > > > (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) Collection of information regarding web pages visited to deliver advertising. The computer software--
> > >
> > > > (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.

[86] *See* Philip N. Howard, *Deep Democracy, Thin Citizenship: The Impact of Digital Media in Political Campaign Strategy*, 597 ANNALS 153, 164-165 (2005).

[87] *Id.* § 165.

expected major purchases, hobbies, interests, family size, and education.[88] Because these companies may only collect and share aggregated information, as opposed to personally identifiable information, their software would be immune from the notice and consent provisions of the SPY ACT. Consumers who may not want this software on their computer, because it could slow down their computer or because they do not want their data to be collected even not personally identifiable, would not have proper notice of the software's functions. In addition, because the definition of "information collection program" is so specific, software developers could create spyware that falls outside the definition in order to avoid these notice and consent requirements.

[41] Similarly, SPY BLOCK's notice provisions, which call for specific types of notice depending on whether software has information collection features, pop-up ad features, distributed computing features, or settings modification features, can quickly become outdated as technology outside these four functionality categories is developed.

B. UNDEFINED CONSENT

[42] Furthermore, neither the SPY ACT nor SPY BLOCK contains a clear description of what constitutes consent. The SPY ACT does not define what qualifies as consent, and SPY BLOCK merely states:

> (b) Consent. For purposes of section 2(a)(2), consent requires—
>
> > (1) consent by the user of the computer to the installation of the computer software; and
> >
> > (2) separate affirmative consent by the user of the computer to each information collection feature, advertising feature, distributed computing feature, and settings modification feature contained in the computer software.[89]

[88] *Id.*

[89] SPY BLOCK, *supra* note 5, at §3(b).

"Consent" is therefore left open to interpretation. Has a person who clicked an "I agree" button after reading notice which was conspicuous but written in a confusing or misleading manner consented? Under the acts, the answer could possibly be 'yes.'

C. PROPOSED SOLUTIONS

[43] Unlike the SPY ACT, ideal spyware legislation would contain notice and consent provisions which apply to all software that will potentially be installed onto a computer,[90] not just software that falls under a specific

[90] *See* SPY ACT, *supra* note 3, at 3(b)(2) (exceptions outlined in the SPY ACT and SPY BLOCK should still be honored in order to avoid overwhelming the computer user with unnecessary warnings:

> (2) Exception for software collecting information regarding web pages visited within a particular Web site. Computer software that otherwise would be considered an information collection program by reason of paragraph (1)(B) shall not be considered such a program if--
>
> (A) the only information collected by the software regarding Web pages that are accessed using the computer is information regarding Web pages within a particular Web site;
>
> (B) such information collected is not sent to a person other than--
>
> (i) the provider of the Web site accessed; or
>
> (ii) a party authorized to facilitate the display or functionality of Web pages within the Web site accessed; and
>
> (C) the only advertising delivered to or displayed on the computer using such information is advertising on Web pages within that particular Web site.

See also SPY ACT, *supra* note 3, at 5(b):

> (b) Exception Relating to Security. Nothing in this Act shall apply to--
>
> (1) any monitoring of, or interaction with, a subscriber's Internet or other network connection or service, or a protected computer, by a telecommunications carrier, cable operator, computer hardware or software provider, or provider of information service or interactive computer service, to the extent that such monitoring or interaction is for network or computer security purposes, diagnostics, technical support, or repair, or for the detection or prevention of fraudulent activities; or
>
> (2) a discrete interaction with a protected computer by a provider of computer software solely to determine whether the user of the computer is authorized to use such software . . . .

See also SPY BLOCK, *supra* note 5, at 5:

> SEC. 5. EXCEPTIONS.
>
> (a) Preinstalled Software…

definition which may become outdated. In addition, rather than providing specific notice requirements for discrete categories of spyware as SPY BLOCK does, ideal national spyware legislation would provide detailed yet flexible notice requirements applicable to all types of software, even as technology progresses.

[44] For example, in order to ensure notice is adequately conveyed to a consumer, legislation could include a list of factors that must be met in order for notice to be considered "clear and conspicuous." The FTC has defined "clear and conspicuous" in its business guide for online advertising, "Dot Com Disclosures: Information About Online Advertising."[91] The factors detailed in this guide could be borrowed and integrated into the spyware legislation. This would cause spyware purveyors to pay particular attention to: (1) the placement of the required disclosure and its proximity to the "I agree" button or other consent method; (2) the prominence of the required disclosure; (3) the presence of distracting features; (4) the need for the repetition of the required disclosure due to the length of the notice; (5) the adequacy of volume, cadence and duration of any audio disclosure; and (6) the understandability of the language of the disclosure.[92] These factors could rein in courts which, as detailed above in Part III, appear to vary widely in their understanding of "clear and conspicuous" in the e-commerce realm.

> (b) Other Exceptions. Sections 3(a)(2), 3(b)(2), and 4 do not apply to any feature of computer software that is reasonably needed to –
>
> > (1) provide capability for general purpose online browsing, electronic mail, or instant messaging, or for any optional function that is directly related to such capability and that the user knowingly chooses to use;
> > (2) determine whether or not the user of the computer is licensed or authorized to use the computer software; and
> > (3) provide technical support for the use of the computer software by the user of the computer.
>
> (c) Passive Transmission, Hosting, or Link . . .
> (d) Software Resident in Temporary Memory . . .
> (e) Features Activated by User Options…

[91] BUREAU OF CONSUMER PROTECTION, FED. TRADE COMM'N, DOT.COM DISCLOSURES: INFORMATION ABOUT ONLINE ADVERTISING, *available at* http://www.ftc.gov/bcp/conline/pubs/buspubs/dotcom/index.html.

[92] *See id.* at 5-6.

[45] In order to define the flexible parameters for notice, spyware legislators could also borrow from other fields. In the realm of legal ethics, Model Rule 1.0(e) defines "informed consent" as "the agreement by a person to a proposed course of conduct after the lawyer has communicated adequate information and explanation about the material risks of and reasonably available alternatives to the proposed course of conduct."[93] The Restatement (Second) of Agency 376 defines consent as "[t]he existence and extent of the duties of the agent to the principal are determined by the terms of the agreement between the parties, interpreted in light of the circumstances under which it is made, except to the extent that fraud, duress, illegality, or the incapacity of one or both of the parties to the agreement modifies it or deprives it of legal effect."[94] In the torts realm, for medical negligence to constitute malpractice a successful suit will depend on the plaintiff's ability to demonstrate five key elements: (1) the physician's duty owed to the patient to provide information; (2) breach of the physician's duty; (3) harm suffered by the patient; (4) the relation of the harm to the development of an undisclosed risk; and (5) evidence that had the patient been informed of the risk, he or she would not have consented to the procedure.[95]

[46] Borrowing from these elements, national legislation could require notice to include: (1) adequate information about what functions the software performs; and (2) material risks of the software, e.g., will it share personal information or change or disable the functionality of a user's machine as set by the user. Deceit should violate consent. In addition, in examining informed consent courts could consider the harm suffered by the user, and the relation of that harm to the development of an undisclosed risk.

[47] Further, if there is a question as to whether it is reasonable to expect a consumer has read and understood the terms of an agreement, survey evidence could be utilized. With respect to advertising, the FTC’s Policy Statement on Deception states that an advertisement is deceptive where there is “a misrepresentation, omission or other practice that misleads the

[93] Model Rules of Conduct 1.0(e).

[94] Restatement of (Second) Agency 376.

[95] RUTH R. FADEN & TOM L. BEAUCHAMP, A HISTORY AND THEORY OF INFORMED CONSENT 23-49 (1986).

consumer acting reasonably in the circumstances, to the consumer's detriment."[96] In order to determine what a "consumer acting reasonably in the circumstances" would do, the FTC has increasingly used consumer surveys and such objective evidence as proof of the likeliness to mislead in advertising.[97] In addition, courts frequently adopt surveys to determine consumers' perceptions in trademark infringement cases brought under the Lanham act.[98] In order to ensure software purveyors obtain meaningful user consent before installing software onto a computer, legislation could require that if there is a question as to whether a reasonable consumer would be able to read and understand notice provisions, both plaintiff and defendant may present survey evidence.

VII. CONCLUSION

[48] National spyware legislation is necessary because the only current legislation specifically addressing the problem exists on a state level. State spyware legislation, which varies from state to state, leads to significant business planning and litigation costs.[99] In addition, the ability of one state to set policy for the whole country via state spyware legislation triggers Dormant Commerce Clause issues.[100] Because of these factors, spyware must be combated at the national level.

[49] While spyware can be challenged under laws which were not specifically enacted to address the spyware problem, namely the Wiretap Act, the Stored Communications Act, the Computer Fraud and Abuse Act, and the common law claim of trespass to chattels, these laws are inadequate to combat the problem because they do not allow consumers to have a meaningful say in what software can be legally installed on their

[96] FTC POLICY STATEMENT ON DECEPTION, *available at* http://www3.ftc.gov/bcp/policystmt/ad-decept.htm (1983).

[97] *See, e.g.*, Kraft, Inc. v. F.T.C., 970 F.2d 311 (7th Cir. 1992), *cert. denied*, 507 U.S. 909 (1993); In re Thompson Medical Co., Inc., 104 F.T.C. 648 (1984); *Stouffer Foods Corp.*, 5 Trade Reg. Rep. (CCH) ¶ 23,686 (1994).

[98] Peter H. Huang, *Moody Investing and the Supreme Court: Rethinking the Materiality of Information and the Reasonableness of Investors*, 13 S. CT. ECON. REV. 99, 114 (2005).

[99] Menell, *supra* note 21, at 1412.

[100] Crawford, *supr*a note 6, at 1443.

computers. The Wiretap Act and the Stored Communications Act have "consent exceptions" which can be so liberally construed by courts that consumers can unwittingly "consent" to the installation of spyware. The Computer Fraud and Abuse Act, and the common law claim of trespass to chattels, are problematic because they are after-the-fact solutions that cannot prevent problems to begin with.

[50] National spyware legislation currently being proposed, i.e. the SPY ACT, I-SPY and SPY BLOCK, could be very effective in battling the spyware problem. These bills contain detailed notice and consent provisions, and thus can avoid the problems posed in vague and loosely enforced consent provisions of the Wiretap Act and the SCA, and the nonexistent notice and consent provisions in the CFAA and the common law claim of trespass to chattels. This legislation, grounded in notice and consent requirements, would provide for the flexibility needed to battle ever-changing spyware technology.

[51] Although the proposed legislation is very promising, there are still a few areas that could be improved. First, the notice and consent provisions of the SPY ACT and SPY BLOCK are written to apply to very specific types of technology, and thus some software that certain users may consider harmful would not be subject to these provisions. Second, the limited application would prevent legislation from battling new forms of potentially harmful spyware. Third, neither SPY ACT nor SPY BLOCK contain a clear description of what constitutes consent. Because "consent" is left open to interpretation, even if computer users are given notice that is written in a confusing or misleading manner, courts may interpret consent to this type of notice to be "informed."

[52] In order to improve the currently proposed legislation, legislators could look to the FTC's "clear and conspicuous" guidelines for internet advertising to shape spyware legislation's notice requirements. Legislators could borrow elements of informed consent from other fields, and require that notice include adequate information about (1) what functions the software performs, and (2) material risks of the software. In examining informed consent, courts could look at the harms suffered by the user and the relation of the harm to the development of an undisclosed risk. Lastly, if there is a question about whether it is reasonable to expect

that a consumer has read and understood the terms of an agreement, survey evidence could be utilized.