Loyola Consumer Law Review

Volume 17 | Issue 3 Article 3

2005

Spies among Us: Can New Legislation Stop Spyware from Bugging your Computer?

Michael D. Lane

Spies Among Us: Can New Legislation Stop Spyware from Bugging Your Computer?

By Michael D. Lane*

I. Introduction

Imagine that when you turn on your computer to access the Internet, invisible spies are watching your every move, even directing your browsing to sites you don't want to visit. Imagine your own computer working against you, using bandwidth and processing power to communicate information about you to remote locations. What you have imagined is known as spyware and probably exists in some form on your own computer.

Spyware—and how to combat it—has recently been a frequent topic of discussion in consumer and technology circles. The unfortunate reality is that many consumers are unaware that spyware exists, much less that it can cause serious problems. A recent survey by the National Cyber Security Alliance found that eighty percent of home personal computers are infected with spyware, but only ten percent of consumers had any idea what spyware programs do.[1] Microsoft has lost some of its share of the Internet browser market share to companies like Mozilla (maker of the Firefox browser), which has gained significant numbers of users by offering an Internet browser less susceptible to spyware attacks than Internet Explorer.[2] It is probable that these concerns over spyware and its ability to affect consumers prompted Microsoft's recent decision to jump into the

---

* J.D. candidate, May 2006, Loyola University Chicago School of Law; B.B.A. Finance, 2003, University of Notre Dame. The author would like to thank his family and friends for all their help and support throughout law school. Special thanks go to my father for his help and to Meg for always being supportive.

[1] Byron Acohido & Jon Swartz, *Market to Protect Consumer PCs Seems Poised for Takeoff; As Spyware, Viruses Spread, Threat to E-commerce Grows*, USA TODAY, Dec. 27, 2004, at B1.

[2] Gregg Keizer, *Microsoft Moves on Spyware to Stymie Firefox*, CMP TECHWEB, Dec. 17, 2004, 2004 WL 64589063, available at http://www.techweb.com/wire/security/55800866.

battle against spyware by offering free software, at least for now, to customers to combat malware.[3]

This article will examine spyware's legal status by first explaining what spyware is and how it affects consumers. Next, the problem of spyware will be examined under the legal mechanics currently employed by courts to explain why further legislative action may be necessary. Finally, new and proposed legislation that specifically targets spyware will be examined. By comparison to existing law its potential effectiveness in combating regulatory gaps that spyware can exploit will be determined.

II. Background on Spyware and the Law

A. The Growing Concern with Spyware

Spyware can do any number of things once it implants itself onto a computer's hard drive, including tracking the websites visited, logging the keystrokes made, or changing settings on the computer such as the "home page."[4] These types of attacks often render computers useless, forcing consumers to spend hundreds of dollars on software and professional assistance to remove the effects of spyware.[5] A recent newspaper column described the experience of Rachel Dodes, whose personal struggle against numerous insidious programs typifies a severe spyware infection.[6] Dodes, an Internet user, began by downloading a free program from the Internet, but unknowingly opened the door to a host of spyware programs.[7] She suffered a barrage of pop-up ads and lost control of her Internet browser.[8] Although she tried to use software designed to eliminate the threat, spyware's menacing nature escaped the ability of software to combat it, and some deleted files were even reinstalled when her

---

[3] David Bank & Robert A. Guth, *Microsoft Offers Free Software to Fight 'Spyware' and Viruses,* WALL ST. J., Jan. 7, 2005, at B3. (noting that malware includes several types of malicious software: spyware, worms, and viruses)

[4] Alex L. Goldfayn, *Spyware Tough to Stop, But Some Defenses Work*, CHI. TRIB., Jan. 1, 2005, at B4.

[5] Acohido & Swartz, *supra* note 1.

[6] Rachel Dodes, *Terminating Spyware with Extreme Prejudice,* N.Y. TIMES, Dec. 30, 2004, at G1.

[7] *Id.*

[8] *Id.*

computer rebooted.[9] In the end, she chose to spend hundreds of dollars backing up files and reinstalling her computer's software in order to avoid spending more money on an entirely new computer.[10]

Spyware attacks a computer in so many different ways that any legislation would have to address software that varies tremendously in terms of functionality and effects.[11] While some users agree to install spyware in clearly articulated license agreements, other spyware automatically installs itself through security flaws sometimes known as back doors, or through the fine print of complex end-user license agreements.[12] One of the problems in mounting a legal battle against spyware is the fact that it has so many forms and functions that make it hard to precisely define.[13] As described in a hearing before the House Subcommittee on Energy and Commerce, "'Spyware' programs can be installed on users' computers in a variety of ways, and they can have widely differing functionalities."[14]

Jeffrey Friedberg, Microsoft's Director of Windows Privacy, recently proposed to the House Subcommittee on Commerce, Trade, and Consumer Protection one way to help define spyware more precisely in legal terms.[15] In Mr. Friedberg's view, the emphasis of

---

[9] *Id.*

[10] *Id.*

[11] Brad Slutsky & Sheila Baran, *Just a Tad Intrusive?*, 14 BUS. L. TODAY 33 (2004) (noting that spyware can track internet behavior, collect personal information, send spam on behalf of third parties, change the user's home page, or generate ads).

[12] Ronald R. Urbach & Gary A. Kibel, *Adware/Spyware: An Update Regarding Pending Litigation and Legislation*, 16 NO. 7 J. PROPRIETARY RTS. 12, 12 (2004).

[13] *See Spyware: What You Don't Know Can Hurt You: Hearing on H.R. 2929 Before the Subcomm. On Commerce, Trade, and Consumer Protection, 109th Cong. (Apr. 29, 2004)* [hereinafter *Spyware Hearings*] (statement of Mr. Ari Schwartz, Associate Director, Center for Democracy and Technology), *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_house_hearings&docid=f:93308.pdf (Last visited May 10, 2005).

[14] *Spyware Hearings, supra* note 13 (statement of Mr. Ari Schwartz).

[15] *Spyware Hearings, supra* note 13 (statement of Mr. Jeffrey Friedberg, Director of Windows Privacy, Microsoft) *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_house_hearings&docid=f:93308.pdf (Last visited May 10, 2005).

any law against spyware should be placed on lack of user notice and control, because some aspects of the technology itself have legitimate and beneficial uses.[16] Some characteristics of new technology can be beneficial to computer users by providing more customized and enhanced features, leading Friedberg to argue that Congress should use caution in designing new laws to combat spyware.[17] To avoid discouraging innovation, any such law should focus on deceptive behavior and its impact on the consumer rather than the functionality of the software or the act itself.[18] While recognizing that the Federal Trade Commission Act[19] ("FTC Act") and the Consumer Fraud and Abuse Act[20] ("CFAA") can be enforced more rigorously against spyware, Friedberg urged Congress to enact any new law to "supplement the existing legal framework only where gaps are identified."[21]

Currently, neither federal statutes such as the CFAA and the FTC Act, nor common law trespass to chattels, have been effectively used to combat the spyware problems that face consumers in cyberspace.[22] Under current enforcement of these legal doctrines, individual consumers are unprotected against makers of spyware in two main areas, one which Friedberg called "notice and consent," [23] and compensation.

In this article, notice and control refers to the fact that many people do not know about spyware, nor are able to control its functions once their computers are infected.[24] Because consumers

---

[16] *Spyware Hearings, supra* note 13 (statement of Mr. Jeffery Friedberg).

[17] *Id.*

[18] *Id.*

[19] Federal Trade Commission Act, 15 U.S.C. §§ 41-58 (2004).

[20] Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2004).

[21] *Spyware Hearings, supra* note 13 (statement of Mr. Jeffery Friedberg).

[22] *Spyware Hearings, supra* note 13 (statement of Mr. J. Howard Beales III, Director, Bureau of Consumer Protection, Federal Trade Commission) *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_house_hearings&docid=f:93308.pdf (Last visited May 10, 2005) (Mr. Beales noted that "[W]hat limits our ability to bring these cases is that . . . the bad guys ride off into the hills. But these are cyberhills and there are no footprints.").

[23] *Spyware Hearings, supra* note 13 (statement of Mr. Jeffery Friedberg).

[24] *See id.; See also* Goldfayn, *supra* note 4 (discussing users lack of spyware knowledge).

continue to be unaware of the problem of spyware, are often unaware of its installation, and are unaware of any way to remove it, such a regulatory gap exists in this area. Compensation, or deterrence, refers to the fact that where victims have been injured, some compensation from the offender could serve to make them whole.[25] Additionally, compensation or fines could serve a deterrent function, decreasing the amount of injurious spyware activity on the Internet.[26] If individual consumers are unable to seek compensation for the time and expense spent combating spyware, this could be viewed as such a regulatory gap in terms of compensation or deterrence. However, deterrence by means of consumer lawsuits is only one way to deal with the problem—the Federal Trade Commission could pursue makers of spyware who deceive the public.[27]

Deterrence by lawsuit may not even be extremely effective, as many persons who know they have a spyware infection are unable to find it on their computers, making it hard to identify.[28] The previous example of Ms. Dodes shows how consumers could click their way out of a private right of action—she accepted, without reviewing or understanding its significance, a license agreement provided by the software maker, which could prevent her from taking legal action because she gave her consent.[29] In addition, laws creating a private right of action would likely be viewed with suspicion by the software industry. All indications are that the current regulatory environment does not force spyware companies to provide explicit and adequate notice, or give consumers the ability to remove the program if its consequences are different than anticipated.[30]

Some may argue that rigorous enforcement of existing laws

---

[25] *See generally* Richard A. Posner, *An Economic Theory of the Criminal Law,* 85 COLUM. L. REV. 1193 (1985).

[26] *See id.*

[27] *Spyware Hearings, supra* note 13 (statement of Mr. J. Howard Beales III)

[28] *See* Andrew Briney, *Spywary,* INFO. SECURITY, Feb. 2005, at 72

[29] Courts have split on whether these so called "clickwrap" license agreements are valid in all cases; *Compare* Specht v. Netscape Communications Corp., 306 F.3d 17 (2d Cir. 2002) (court refused to enforce end user license agreement after consumer downloaded program) *with* Moore v. Microsoft Corp., 293 A.D.2d 587 (N.Y. App. Div. 2002) (clicking "I Agree" on end user license agreement creates valid contract).

[30] *Spyware Hearings, supra* note 13 (statement of Mr. J. Howard Beales III) (noting that it is possible to bring unfair practices actions for non-explicit end user license agreements, but the FTC has never done so in the software context).

may render it unnecessary to pass a new law to provide consumers the right to compensation through a private right of action, because spyware purveyor's conduct violates existing law.[31] In contrast to this view, some of the newly enacted or proposed anti-spyware laws contain provisions which would fill the regulatory gaps consumers currently face.[32] One major feature of the newly proposed anti-spyware laws is the inclusion of a right of action for consumers against the makers of spyware,[33] as well as heightened notice and removal requirements for any software that fits into a certain category, such as those that collect personally identifiable information.[34] The consumer's position can be protected under existing laws only if changes are made to the ways these laws are prosecuted and enforced. The desired deterrent effect could be achieved if rigorous application of the law creates a credible threat in the mind of spyware makers.[35] The remaining regulatory gap that deserves lawmakers' attention is the first problem identified—adequate notice to consumers and the ability to remove the problem.

B. Current Legal Framework

1. CFAA

The CFAA was originally enacted as a criminal statute to prosecute computer crimes of federal interest.[36] The CFAA was

---

[31] *Spyware Hearings, supra* note 13 (statement of Mr. J. Howard Beales III).

[32] *See, e.g.*, SPY ACT, H.R. 29, 109th Cong. (2005) (providing for notice to consumers prior to installation of spyware and potential for fines for violations).

[33] *See* Spyware Control Act, UTAH CODE ANN. §§ 13-40-101 to 13-40-401 (West 2004); SPY ACT, H.R. 29, 109th Cong. (2005), Internet Spyware Prevention Act of 2005, H.R. 744, 109th Cong. (2005).

[34] *See* Spyware Control Act, UTAH CODE ANN. §§ 13-40-101 to 13-40-401 (West 2004); SPY ACT, H.R. 29, 109th Cong. (2005), Internet Spyware Prevention Act of 2005, H.R. 744, 109th Cong. (2005).

[35] *See* Posner, *supra* note 25.

[36] Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1127 (W.D. Wash. 2000) (*citing* S. Rep. No. 99-432, at 3 (1986) (outlining the CFAA legislative history and its expansion by Congress)); *See generally* Deborah F. Buckman, Annotation, *Validity, Construction, and Application of Computer Fraud and Abuse Act*, (18 U.S.C. § 1030), 174 A.L.R. Fed. 101 (2001) (discussing how the CFAA was first passed as a counterfeit access device and was created to prohibit unauthorized access to federal interest

amended in 1994 to provide for a private right of action where "any person who suffers damage or loss by reason of a violation of this section."[37] This private action is limited only to certain situations: (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.[38]

The most likely case for an individual consumer who wishes to bring a private action against a spyware maker under the CFAA is a situation where there has been damage or a loss of $5,000 in a year.[39] The statute defines damage as "any impairment to the integrity or availability of data, a program, a system, or information."[40] "Loss" can be "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service."[41] The $5,000 figure need not come from any one single action, but can result from multiple events over a year.[42]

In many cases, courts have defined "damage" to include an unauthorized slowdown of computer processing or an unauthorized use of finite computing power.[43] In *America Online, Inc. v. National*

---

computers).

[37] 18 U.S.C. § 1030(g) (2004).

[38] 18 U.S.C. § 1030.

[39] Only in extremely rare cases would a consumer have worry that a spyware attack could cause "an impairment or modification of any medical treatment, diagnosis, examination, or care"; "physical injury"; or "a threat to public health or safety." 18 U.S.C. § 1030(a)(5).

[40] 18 U.S.C. § 1030(e)(8).

[41] 18 U.S.C. § 1030(e)(11).

[42] Creative Computing v. Getloaded.com LLC, 386 F.3d 930, 934 (9th Cir. 2004).

[43] Am. Online, Inc. v. Nat'l Health Care Disc., Inc., 174 F. Supp. 2d 890, 899 (N.D. Iowa 2001). *See also* Four Seasons Hotels and Resorts B.V. v. Consorcio Barr, S.A., 267 F. Supp. 2d 1268, 1322-23 (S.D. Fla. 2003) (holding that damages result when there is intentional access without permission and when people cause

Health Care Discount, Inc., America Online ("AOL") sued a sender of bulk e-mail ("spam") for unauthorized access to its computer network, which used only a small fraction of the company's computing power.[44] Because this use affected the "integrity or availability" of AOL's servers and computers, causing damage over $5,000, it fell within the scope of the CFAA, entitling AOL to recover.[45]

There are significant differences in the treatment courts have given the damage requirement of the CFAA,[46] with some courts holding that that the $5,000 may properly come from only one computer,[47] and others finding that claims may be aggregated among multiple plaintiffs to reach the $5,000 damage or loss figure.[48] *In re DoubleClick, Inc. Privacy Litigation*[49] was a suit launched by a group of consumers with concerns about privacy stemming from DoubleClick's collection of information through Internet "cookies."[50] The plaintiffs made a claim under the CFAA that the cookies used by DoubleClick to access their personal computers and collect their personal information were unauthorized.[51] DoubleClick did not dispute this claim, but did contest the applicability of the CFAA on the basis that no single user complained that DoubleClick's cookie had caused $5,000 in damage.[52] In dismissing the CFAA claim, the court found that the amount of damages could only be aggregated "over victims and time for a single act," and that no complaint involving a single computer had been damaged over the $5,000

---

congestion).

[44] *Nat'l Health Care Disc.*, 174 F. Supp. 2d at 899.

[45] *Id.*

[46] *See* Luke J. Albrecht, *Online Marketing: The Use of Cookies and Remedies for Internet Users*, 36 SUFFOLK U. L. REV. 421, 431-33, 444-45 (2003).

[47] *In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 524 (S.D.N.Y. 2001).

[48] *In re* Am. Online, Inc. Version 5.0 Software Litig., 168 F. Supp. 2d 1359, 1374 (S.D. Fla. 2001) [hereinafter *Version 5.0*]; *In re* Toys R Us, Inc., Privacy Litig., No. 00-CV-2746, 2001 WL 34517252, at *10 (N.D. Cal. Oct. 9, 2001).

[49] *DoubleClick, Inc.*, 154 F. Supp. 2d at 500-04.

[50] *Id.* at 502-03 ("Cookies are computer programs commonly used by Web sites to store useful information such as usernames, passwords, and preferences, making it easier for users to access Web pages in an efficient manner.").

[51] *Id.* at 519-20.

[52] *Id.* at 520.

threshold in a single year.[53]

The opposite result was reached in *In re America Online, Inc. Version 5.0 Software Litigation,* where the court found that damages or losses could be added across a group of plaintiffs injured as a result of a violation of the CFAA.[54] *Version 5.0* was a class action by Internet users and other Internet service providers ("ISPs") against AOL for allegedly violating several federal and state laws by distributing Version 5.0 of its popular Internet access software, and allowing consumers to install the allegedly flawed program on their computers.[55] The court rejected the statutory analysis of *DoubleClick*, holding that the court in that case failed to properly find a "dangling participle" in the part of the statute relating to damage "to a protected computer."[56] The court instead determined that the language allowed for aggregation, and that Congress' continued expansion of the CFAA further supported aggregation of the damage amount.[57] In language reflective of the dilemma consumers face under *DoubleClick's* interpretation of the CFAA, the court recognized that requiring each home user to have over $5,000 in damages would not protect consumers "because $5,000 is far more than the average price of a home computer system."[58]

A similar argument made by plaintiffs in the class action suit *In re Toys R Us, Inc., Privacy Litigation* was accepted by the court.[59] This case once more dealt with the placement of cookies on plaintiffs' computers which, unbeknownst to plaintiffs, tracked their web browsing and purchasing activity.[60] The court recognized that when it "liberally construed" the statute, the placement of cookies on consumers' computers could constitute a single "act" under the CFAA, and that damages could be aggregated across the class.[61] In approving aggregation, the court noted the Senate committee report

---

[53] *Id.* at 524-26.

[54] *Version 5.0*, 168 F. Supp. 2d at 1374.

[55] *Id.* at 1363-66.

[56] *Id.* at 1373.

[57] *Id.* at 1373-74.

[58] *Id.*

[59] *In re* Toys R Us, Inc., Privacy Litig., No. 00-CV-2746, 2001 WL 34517252, at *10-11 (N.D. Cal. Oct. 9, 2001).

[60] *Id.* at *1-2.

[61] *Id.* at *9-11.

for the CFAA stated that losses from a single act could be aggregated in order to reach the damage threshold.[62] Representing a positive argument for to consumers in spyware cases, the court also recognized that the expenses the victim incurs in remedying the defendant's actions are included in the damages for which Congress intended to compensate.[63]

Another case provides an example of a class action that was allowed to proceed under the CFAA where individuals suffered damage, but none of them individually suffered $5,000 in damage.[64] In *Miles v. America Online, Inc.*, individual consumers complained that AOL deceived them by advertising a flat monthly fee for unlimited Internet access, but failing to disclose that long-distance charges may apply.[65] The CFAA claim arose because of the software's "configuration" of the plaintiffs' computers, which caused the computers to dial telephone numbers that incurred various long distance charges.[66] The court allowed the initial class certification where the claims appeared to be meritorious.[67] The court made this decision based on the procedural distinction between a dismissal based on failure to state a claim upon which relief can be granted and dismissal based on lack of subject matter jurisdiction.[68] The court refused to dismiss the properly pled federal question for lack of subject matter jurisdiction because it was neither "immaterial and made solely for the purpose of obtaining jurisdiction," nor "wholly insubstantial and frivolous."[69]

A further monetary disincentive to consumer private action under the CFAA is the fact that courts have disallowed expenses incurred in tracking down the perpetrator to be included as a loss.[70] As *Tyco International (US), Inc. v. John Does, 1-3* demonstrates,

---

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

[63] *Id.* at *10.

[64] Miles v. Am. Online, Inc., 202 F.R.D. 297, 299-300 (M.D. Fla. 2001).

[65] *Id.* at 299.

[66] *Id.* at 300-01.

[67] *Id.* at 300 (noting that the possibility remained that no subject matter jurisdiction existed on the basis that the individual's claims should not be aggregated).

[68] *Id.*

[69] *Id.*

[70] Tyco Int'l (US), Inc. v. John Does, 1-3, No. 01 Civ. 3856, 2003 WL 21638205, at *1-3 (S.D.N.Y. July 11, 2003).

cyber attacks are often done in a sophisticated manner, making it more difficult for the average person to discover who was behind the cyber attack.[71] Tyco, the victim of a cyber attack, expended over $136,000 to track down the individuals who remotely carried out a series of attacks on their computer systems.[72] Logic dictates that an individual consumer would likely never take on such a cost if he could not be compensated by his attacker. The CFAA is designed not to provide this type of compensation, as it limits damages to only those listed in the statute, which includes economic damages—but not punitive damages.[73]

The CFAA in its current form retains potential for those wishing to pursue damaging spyware. However, given courts reluctance to aggregate claims to reach the $5000 threshold,[74] consumers may be unable to bring claims under the statute.

2. The FTC Act[75]

The Federal Trade Commission ("FTC") has the power to prohibit practices that are unlawful under the FTC Act, including those which are "unfair or deceptive."[76] The FTC Act prohibits "unfair methods of competition in or affecting commerce" and grants the U.S. Attorney General power to bring a civil action against violators,[77] which could result in imposition of fines of $10,000 for each violation and injunctive relief.[78] While these provisions are located in Section 45 of the U.S. Code, case law more commonly refers to its powers under the Act, or Section 5.[79]

Section 13(b) of the statute, or Section 53(b) of the code, grants the FTC power to bring an action to obtain relief for false or deceptive advertising.[80] Recently, the FTC has been using this power

---

[71] *Id.* at *1.

[72] *Id.* at *2.

[73] 18 U.S.C. § 1030 (g).

[74] *DoubleClick, Inc.*, 154 F. Supp. 2d at 524-26.

[75] Federal Trade Commission Act, 15 U.S.C. §§ 41-58 (2004).

[76] 15 U.S.C. § 45.

[77] 15 U.S.C. § 45(m).

[78] *Id.*

[79] *See, e.g.*, California Dental Ass'n v. F.T.C., 526 U.S. 756 (1999).

[80] *Id.* at § 53(b).

to protect the privacy of individuals by limiting how information is collected and used by Internet companies.[81] Some examples include cases against, or settlements with, Geocities, Liberty Financial, Eli Lilly, and Microsoft, among others, who were all utilizing Internet technology to aggregate consumer data and information.[82] The success of these cases bodes well for the FTC's use of Section 5 of the FTC Act to prosecute spyware cases, because it indicates the FTC's willingness to wade into cyberspace to enforce rules currently enforced in more familiar settings.

In *Federal Trade Commission v. Seismic Entertainment Productions, Inc.*, the FTC successfully sought a temporary restraining order against several companies that were in the business of exploiting certain vulnerabilities of Microsoft's Internet Explorer.[83] The defendants were a group of companies controlled by a man who had been sued many times for his involvement in sending spam e-mail.[84] The defendants installed a software code, "without the consumers' knowledge or authorization, that g[ave] the defendants access to those computers for purposes of advertising."[85] In granting a temporary restraining order, the court recognized the impact on consumers of many of the typical problems associated with spyware:

> . . .unauthorized changes of their home pages, difficulty using their computers, and infusions of pop-up ads, including pornographic ads and ads for anti-spyware software. The affected users were not notified of the defendants' activities and did not know what had caused the problems with their computers, making the defendants' activities both deceptive and unfair.[86]

The court found no countervailing benefits to consumers, and

---

[81] Kevin P. Cronin & Ronald N. Weikers, *Data Security and Privacy Law: Combating Cyberthreats,* DATA SEC. & PRIVACY LAW § 7:10 (2004).

[82] *Id.* (showing that often this collection of data is done through the use of "cookies").

[83] FTC v. Seismic Entm't Prods., Inc., No. Civ. 04-377-JD, 2004 WL 2403124, at *1 (D.N.H. 2004).

[84] *FTC Files First Spyware Case*, 22 NO. 10 ANDREWS COMPUTER & INTERNET LITIG. REP. 16, Oct. 19, 2004.

[85] *Seismic Entm't Prods., Inc.,* No. Civ. 04-377-JD, 2004 WL 2403124, at *1.

[86] *Id.* at *3.

noted that the defendants' activities "cause[d] substantial injury to consumers by negatively affecting the performance of their computers and requiring significant time and expense to remedy the problems."[87]

Cases like *Seismic Entertainment* show that the FTC is willing to extend its protection of consumers into cyberspace. As noted by FTC officials, Section 5 of the Act could potentially be used against spyware companies.[88] However, cases would have to be brought individually, and given budgetary constraints placed on the FTC, new legislation could provide additional means of consumer protection from spyware.[89]

3. Trespass to Chattels

Trespass to chattels occurs when one person intentionally either dispossess another of a chattel or uses or intermeddles with another's use of a chattel.[90] "Intermeddling" means intentionally bringing about a physical contact with the chattel.[91] One of the first cases to apply a trespass to chattels theory to a cyber-tort was *CompuServe Incorporated v. Cyber Promotions, Inc.*[92] In this case, the court followed recent rulings[93] and held that electronic signals used and read by a computer create sufficient contacts to support a trespass to chattels claim.[94] The victim of a trespass to chattels claim must suffer some actual damage and cannot sue for nominal damages.[95] However, as demands on "the disk space and drain [on] the processing power" made this part of the property unavailable to the victim, sufficient damages existed for a court to hear the trespass

---

[87] *Id.* at *4.

[88] *Spyware Hearings, supra* note 13 (statement of Mr. J. Howard Beales III).

[89] *Id.*

[90] Register.Com, Inc. v. Verio, Inc., 356 F.3d 393, 404 (2d Cir. 2004) (citing Restatement (Second) of Torts. § 217(b) (1965)).

[91] Restatement (Second) of Torts. § 217 cmt. e (West 2005).

[92] CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1015 (S.D. Ohio 1997).

[93] *See, e.g.*, Thrifty-Tel, Inc. v. Bezenek, 54 Cal. Rptr. 2d 468, 468 (Ct. App. 1996) (noting where the parents of a young hacker were sued for accessing a computer server in an attempt to locate a long-distance access code).

[94] *Cyber Promotions,* 962 F. Supp. at 1021.

[95] *Id.* at 1023.

claim.[96] Making note that self-help should be tried first, the court allowed the claim because the defendant acted to skirt any security measures CompuServe imposed.[97]

The theory of trespass to chattels has continued to expand in cyberspace beyond its first initial cases.[98] One of the most cited cases employing the theory in recent years is *eBay, Inc. v. Bidder's Edge, Inc.*[99] A well known Internet auction site, eBay, sued a competitor who used "robots," computer programs designed to continuously query the eBay site for auction information, along with other auction sites.[100] This information was subsequently consolidated and posted *en masse* in one location.[101] The court granted a preliminary injunction on the trespass claim because it found a likelihood of potential harm to eBay, a likelihood of success on the merits, and the balance of hardship in favor of eBay.[102] eBay was likely to succeed in showing that Bidder's Edge intentionally, and without authorization, interfered with eBay's use of its computer system, and that this interference proximately caused damage.[103] Although eBay advanced several theories as to why the value of its computer systems had been damaged, the court accepted the theory that the denial of an injunction would encourage other companies to mimic Bidder's Edge, thereby overloading eBay's systems.[104] Not every trespass is actionable, however, as the ruling has been limited only to those areas where there is a sufficient actual or threatened harm to a computer or a system.[105]

---

[96] *Cyber Promotions,* 962 F. Supp. at 1022.

[97] *Id.* at 1021-23.

[98] *See generally* Laura Quilter, *The Continuing Expansion of Cyberspace Trespass to Chattels,* 17 BERKELEY TECH. L.J. 421, 430-442 (2002) (discussing past cases and the assumptions underlying cyberspace trespass to chattels).

[99] eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058 (N.D. Cal. 2000).

[100] *Id.* at 1060-63.

[101] *Id.* at 1060-63.

[102] *Id.* at 1064-73.

[103] *Id.* at 1069-72.

[104] *eBay,* 100 F. Supp .2d at 1071-72.

[105] *See* Intel Corp. v. Hamidi, 71 P.3d 296, 300, 308-12 (Cal. 2003) (holding that a former employer cannot obtain an injunction against a former employee who sent several e-mails to all employees where only negligible computing power was used, and no threatened harm or imitation would create danger of sufficient damage).

Another interesting development in the area of trespass to chattels is the award of punitive damages for willful and wanton disregard of the property rights of others. One such case authorizing an award of punitive damages as a result of spam e-mail was *America Online Inc. v. National Health Care Discount, Inc.*[106] Here, the court found the defendant liable not only for trespass to chattels,[107] but also for a violation of the CFAA and Virginia's Computer Crimes Statute section 18.2-152.12.[108] The court found that because these theories were all based on the same act, no duplicative damages would be awarded.[109] The court calculated damages based on each e-mail sent, plus some amount for profit.[110] The court also awarded punitive damages,[111] ostensibly on the trespass claim, because the CFAA specifically limits recovery to economic damages[112] and the Virginia Statute does not provide for punitive damages.[113]

The ruling closely resembled a recent New York case, *Tyco International (US), Inc. v. John Does, 1-3,* in which the court awarded punitive damages based on a trespass to chattels claim where actual damages were neither calculated, nor sought.[114] The U.S. Supreme Court ruled that "'in actions of trespass and all action on the case for torts,'" a jury may inflict what are called exemplary, punitive, or vindictive damages upon a defendant.[115] The *Tyco* Court determined that punitive damages of $10,000 would be appropriate in this case, where the defendant's intent was to crash the plaintiff's

---

[106] Am. Online, Inc. v. Nat'l Health Care Disc., Inc., 174 F. Supp. 2d 890, 902 (N.D. Iowa. 2001).

[107] *Id.* at 900.

[108] VA. CODE ANN. § 18.2-152 (1999) (the computer crimes statute provides for protection against, among other causes of action, computer fraud, unsolicited bulk electronic mail, computer trespass, invasion of privacy, theft of computer services, and harassment).

[109] *Nat'l Health Care Disc., Inc.*, 174 F. Supp. 2d at 900.

[110] *Id.* at 900-01.

[111] *Id.* at 902.

[112] 18 U.S.C. § 1030(g) (2005).

[113] VA. CODE ANN. § 18.2-152.12.

[114] Tyco Int'l (US), Inc. v. John Does, 1-3, No. 01 Civ. 3856, 2003 WL 21638205, at *4 (S.D.N.Y. 2003).

[115] Molzof v. United States, 502 U.S. 301, 306 (1992), *cited in* Tyco Int'l (US), Inc. v. John Does, 1-3, No. 01 Civ. 3856, 2003 WL 21638205 at *4 (S.D.N.Y. 2003).

servers in order to deter other such actions.[116]

III.Consumer Impact: Why the Current Regime Leaves a Regulatory Gap

A. Notice / Control

Despite the attention to spyware of many in the software industry, the average consumer is still ignorant of its methods, and is unable to remove it from his computers.[117] The current legal mechanisms are retrospective in nature: a consumer (or a group of consumers) must file an action under the CFAA or common law trespass to chattels arguing that its specific action was a violation under one particular set of facts; the FTC must then determine that a spyware purveyors software action is deceptive, and then find and pursue the company, something that is often easier said than done.[118] How could the current laws be providing adequate notice and control where the evidence is clear that the average consumer does not know spyware is on his computer, does not know who put the spyware on his computer, and cannot remove the spyware from his computer?[119]

The CFAA does not proscribe specific standards for companies to follow, leaving consumers in no better position to learn about or control spyware.[120] Although the action of much spyware violates many of the terms of the statute, the requirement that any access to computers be authorized[121] is muddled by two factors. First, the question is obscured in cases where spyware notice is buried deep within end user license agreements, forcing courts to first deal with whether this constitutes consent.[122] Second, unless the

---

[116] *Tyco Int'l*, 2003 WL 23374767 at *4.

[117] *See* Slutsky & Baran, *supra* note 11.

[118] *Spyware Hearings, supra* note 13 (statement of Mr. J. Howard Beales III) (noting the difficulty of pursuing cyber-criminals).

[119] Acohido & Swartz, *supra* note 1, at B1.

[120] *See* 18 U.S.C. § 1030.

[121] *Id.*

[122] *Compare* Specht v. Netscape Communications Corp., 306 F.3d 17 (2d Cir. 2002) (court refused to enforce end user license agreement after consumer downloaded program) *with* Moore v. Microsoft Corp., 293 A.D.2d 587 (N.Y. App. Div. 2002) (clicking "I Agree" on end user license agreement creates valid contract).

statute clearly allows for aggregation among consumers, it is highly unlikely that the average consumer will suffer the requisite $5,000 damage threshold in one year.

Similarly, trespass to chattels, as a common law doctrine, does not require software to provide notice in any specific manner, nor does it require companies to make their spyware easy to control or remove. In cases where the defendant argues that the consumer consented to the installation of the spyware, the court has to determine whether the action of the spyware exceeded the plaintiff's consent.[123] In any case, the best the consumer can currently hope for is a ruling that a particular set of spyware, distributed by a particular software company, amounted to trespass or intermeddling with the consumer's chattels.

The FTC Act currently provides the best hope for consumers in setting a standard for notice and control. This is due to the simple fact that the FTC is a single actor that could target specific practices, setting precedent and potentially influencing other spyware companies to reform their behavior.[124] However, even the FTC faces the problem of taking action retrospectively. The FTC can only bring a civil action after determining that a particular practice is deceptive.[125]

Because either consumers or the FTC would have to bring a civil action against a spyware company on a case-by-case basis, no specific standard is set to require standardized notice of the actions of the spyware. No specific removal requirements are articulated to allow consumers to easily remove unwanted spyware from their computers.

B. Compensation / Deterrence

The current legal environment is ineffective in terms of providing consumers with compensation for their damages or in imposing monetary damages that could serve as a deterrent to future offenders. Most consumers would be unable to meet the damage requirement of the CFAA acting alone,[126] the damages for trespass to

---

[123] *See* CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1027 (S.D. Ohio. 1997) (this assumes that the court in question would accept a clickwrap license agreement as any kind of consent at all).

[124] *See* Posner, *supra* note 25.

[125] 15 U.S.C. § 45.

[126] 18 U.S.C. § 1030 (a).

chattels are difficult to measure,[127] and budgetary constraints place logical limits to the amount of cases the FTC can bring against spyware companies.[128]

Under the CFAA, although the spyware programs may harm the host computer, the consumer is unable to take action except in the most severe cases of spyware infection, such as cases of identity theft.[129] While many companies are able to meet the damage threshold on their own, individuals generally cannot unless the courts are willing to allow their claims to be aggregated across a group of consumers.[130] The few lawsuits that have been brought by corporations under the CFAA may serve some deterrent function, but the impact of these cases has done little to stem the rising tide of spyware infecting consumer's computers.

While individual consumers may be able to receive compensation in some cases, most spyware does not cause the type of damage necessary to support an injunction or claims for damages. As in *eBay*, the courts have difficulty determining the exact amount of damage caused by use of consumer's processing power,[131] and consumers do not face the same threats from similar behavior as a major online company.[132] Only an extension of recent punitive damage awards would threaten spyware companies, but most courts have been unwilling to impose such damages in cyberspace.[133]

While there is potential for current laws to provide compensation or deterrence functions, a regulatory gap remains in this area. Consumers all too often give up their own private right of action by failing to read licensing agreements. Added to the courts' unwillingness to extend class actions or aggregation to CFAA claims and the lack of punitive damages available under trespass to chattels claims, consumers face an uphill battle when seeking compensation

---

[127] *eBay*, 100 F. Supp. 2d at 1071-72 (where the court struggled with the concept of loss of value under this theory, but nevertheless found a likelihood of success on the merits bases on encouraging similar behavior).

[128] *Spyware Hearings, supra* note 13 (statement of Mr. J. Howard Beales III).

[129] Pest Patrol, Inc., *PestPatrol Product Development VP Roger Thompson to Testify Before Congress on Dangers of Spyware*, BUS. WIRE, Nov. 18, 2003 (noting that the average identity theft results in $9,800 in profit for the thief).

[130] *Version 5.0*, 168 F. Supp. 2d at 1374.

[131] *eBay*, 100 F. Supp. 2d at 1071.

[132] *Id.* at 1071-72.

[133] Michael L. Rustad, *Punitive Damages in Cyberspace: Where in the World is the Consumer?*, 7 CHAP. L. REV. 39, *passim* (2004).

or deterrence under the current legal framework.

Punitive damages imposed on spyware makers could serve as a deterrent against the continued use of such devices to invade the computers of consumers.[134] Additionally, the financial rewards that punitive damages bring could help consumers pay for the time and expense of cleaning their systems of spyware or in purchasing a new system, depending on the severity of the infection. Recently, Michael L. Rustad, a Suffolk University Law School professor, conducted a comprehensive analysis of all Internet-related cases where punitive damages were awarded.[135] Interestingly, Rustad found that no consumer was able to receive punitive damages based on any online sale or service, or in any cases where personal information had been harvested.[136]

Additionally problematic in both the CFAA and trespass to chattels cases is the fact that consumers themselves have to face the defense of consent to end-user license agreements prior to the installation of any software.[137] The use of trespass to chattels in spyware cases is an interesting and novel application of a common-law theory, but its effectiveness is limited by the following considerations: Especially because many purveyors of spyware use legal means, such as licensing agreements, to protect themselves, consumers may be unable to assert claims against spyware companies unless they violate their own agreements.[138] Trespass to chattels has the potential to be a stopgap measure[139] against the worst spyware offenders, but would likely not even be as effective as FTC action.

While the FTC cannot provide compensation to every consumer that has been injured by spyware,[140] rigorous pursuit of spyware under the FTC Act would serve a powerful deterrent

---

[134] *See* Rustad, *supra* note 133.

[135] *Id.*

[136] *Id.* at 50-52.

[137] *Software Varieties Pose Legal Challenges*, 3 NO. 24 CYBERLAW CRIME REPORT 10 (Dec. 1, 2003).

[138] *Id.*

[139] *See generally,* Michael L. Rustad and Thomas H. Koenig, *Cybertorts and Legal Lag: An Empirical Analysis*, 13 S. CAL. INTERDISC. L.J. 77 (2003) (arguing that legal mechanisms are behind in their deal with changes in the way technology affects torts, and courts sometimes apply old theories in novel manners to compensate for this lag).

[140] *See* Federal Trade Commission Act, 15 U.S.C. §§ 41-58 (2004) (showing that the FTC Act does not provide for private recovery).

function. It could protect consumers from the worst spyware offenders, such as those that perpetrate identity theft, as well as discourage similar behavior from other offenders. The complaint filed by the FTC in *Seismic Entertainment Products* cited the specific harms of spyware: "Defendants' practices cause or have caused consumers' computers to malfunction, slow down, crash, or cease working properly, and cause or have caused consumers to lose data stored on their computers."[141] Some might hope that continued vigilance by the FTC in protecting the rights of consumers from the unfair practices of some spyware makers seem to make a new law unnecessary. Companies could easily be deterred by injunctions or actions for disgorgement of improperly gained profits.

A rigorous crackdown on "unfair practices" by the FTC may also not be sufficient to provide adequate notice to consumers. While strong action by the FTC could potentially eliminate some of the problems caused by spyware that refuses to be removed from computers, this would have to be done on a case-by-case basis, which would not be as effective as a standard practice. The current action taken by the FTC, while a positive step towards a resolution of the spyware problem, will likely not completely solve the problem that consumers face in gaining compensation from spyware makers, or in deterring their behavior altogether.[142]

IV.Recent Laws and Proposals—Help for Consumers?

In 2004, Utah became the first state to pass legislation specifically addressing the issue of spyware.[143] "Spyware" is defined under the statute to be any software that monitors a computer's usage, reports on that usage, or triggers advertisements, and does not provide the adequate notice (as defined by the statute) of its actions.[144] The statute does provide exceptions for cookies and other potentially harmless software.[145] A suit can be brought by the

---

[141] Plaintiff's Complaint at ¶ 13, 2004 WL 2309585, FTC v. Seismic Entm't Prods., Inc., 2004 WL 2403124 (D.N.H. 2004).

[142] *See* Jessi Hempel, *The Hand that Bytes You,* BUSINESSWEEK, Mar. 21, 2005, at 11 (noting that companies are driven by profit to pursue spyware, even making contradictory investments by selling software that removes spyware).

[143] Spyware Control Act, UTAH CODE ANN. §§ 13-40-101 to 13-40-401 (West 2004).

[144] Utah Code Ann. § 13-40-102(4).

[145] Utah Code Ann. § 13-40-102(5).

consumer, or by any advertiser or website that has had its content obscured by pop-up advertising.[146] The relief under the statute includes an injunction against the action, plus the greater of actual damages or $10,000, which can be increased for a knowing violation.[147] No class actions may be filed under Utah's law and ISPs are immune from violation of the advertisement portion of the statute.[148]

However, the law is not without controversy. It has been challenged by WhenU, an ad-ware company and frequent litigant, which took issue with the "context-based triggering mechanism" language of the law.[149] The company was granted a preliminary injunction against enforcement of the law by a Utah court on grounds that it potentially violates the commerce clause of the United States Constitution.[150]

If the law survives a constitutional challenge and is not later pre-empted, it will serve as a meaningful deterrent to the spyware problem by allowing a minimum damage recovery of $10,000.[151] Additionally, future programs would be required to provide adequate notice of their consequences, as well allow for simple removal from affected computers.[152] The law's exceptions for certain cookies, and disallowance where sufficient notice has been provided, allows for consumer protection without stifling innovation.[153]

Congress has addressed the spyware issue and is poised to take action against spyware. One law, introduced in the House is called I-SPY[154] and was passed by the House of Representatives 415-

---

[146] Utah Code Ann. § 13-40-301.

[147] *Id.*

[148] Utah Code Ann. § 13-40-302.

[149] *Utah Judge Halts Spyware* Law, 6 No. 2 ANDREWS E-BUS. L. BULL. 14, 14 (2004).

[150] *Id.*

[151] Utah Code Ann. § 13-40-102 (providing for a minimum of $10,000 judgment against spyware makers).

[152] § 13-40-102(4)(c).

[153] *See* Utah Code Ann. § 13-40-102(5) (the law's safe haven for companies who provide notice protects legitimate business concerns).

[154] Internet Spyware Prevention Act of 2004, H.R. 4661, 108th Cong. (2004) [hereinafter I-SPY].

0 during the 108th Congress,[155] although no such vote has yet been taken during the 109th. I-SPY amends the CFAA to include protection of personal information and to safeguard security protection already existing on computers.[156] It states that "no person may bring a civil action under the law of any State if such action is premised in whole or in part upon defendant's violating this section."[157] In other words, enforcement of the statue is left to the Attorney General, which is given a $10 million yearly budget to combat spyware.[158]

I-SPY's focus is on the protection of personally identifiable information and the customer's existing security protection,[159] which are only two aspects of the problem with spyware. The list of personally identifiable information is limited to name, address, e-mail address, telephone number, social security number, and credit or bank account information.[160] Under I-SPY, consumers would have much greater protection against spyware activity that is most likely to cause serious financial harm—i.e. identity theft—but are not given added protections against other forms of threats posed by spyware.[161] However, the punishable offense is merely the collection of that information with intent to injure, not necessarily its use.[162] Additionally, consumers would be protected from spyware that attacks security protection already in place in the computer.[163] Without understating the potential value that this legislation would have in combating the growing threat of identity theft, it leaves something to be desired in the fight against spyware. While many programs would be illegal under this regime, many spyware programs exceed the capacity of security programs to detect and eliminate the threat.[164]

---

[155] 150 CONG. REC. D1031-01, D1032 (2004).

[156] I-SPY, *supra* note 154, at § 2.

[157] *Id.*

[158] *Id.* at § 3.

[159] *Id.* at § 2.

[160] *Id.*

[161] I-SPY, *supra* note 154, at § 2.

[162] *Id.*

[163] *Id.*

[164] *See* Slutsky & Baran, *supra* note 11 (spyware programs can be buried deep inside hard drives making them difficult to detect).

A more comprehensive proposal to fight spyware is the Securely Protect Yourself Against Cyber Trespass Act ("SPY ACT"), introduced by Representative Mary Bono during the current 109th Congress.[165] The legislation is fairly complex, but outlaws many of the practices currently used by manufacturers of spyware[166] and creates rigorous notice and removal requirements for spyware that collects information about the consumer.[167] The statute calls for the involvement of the FTC in regulating spyware[168] and, in most cases, federalizes legislation aimed at the spyware problem.[169]

The SPY ACT's notice section calls for a comprehensive notice requirement for software downloads containing spyware that collects information,[170] one of the chief problems with the current legal regime. The notice must be clearly displayed for the consumer to accept or decline, with three possibilities depending on the type of software:

> 1) This program will collect and transmit information about you. Do you accept?
>
> 2) This program will collect information about Web pages you access and will use that information to display advertising on your computer. Do you accept?
>
> 3) This program will collect and transmit information about you and your computer use and will collect information about Web pages you access and use that information to display advertising on your computer. Do you accept?[171]

The consumer would be able to see what type of information is to be collected in more detail, and for what purpose the information is to be collected, without having to accept.[172] Another important

---

[165] SPY ACT, H.R. 29, 109th Cong. (2005) [hereinafter SPY ACT].

[166] *Id.* at § 2.

[167] *Id.* at § 3.

[168] *Id.* at §§ 3-4.

[169] *Id.* at § 6.

[170] SPY ACT, *supra* note 165, at § 3.

[171] *Id. at* § 3(c)(1)(B).

[172] *Id.* at § 3(c)(1)(D).

consumer feature of the SPY ACT is its proposed removal provisions, which require the program to be easily removable by the consumer, and its provisions for clear markings delineating which "pop-up" advertising is caused by which spyware program.[173] The FTC would be authorized to issue regulations to further the goal of both removal and notice under this section.[174]

The enforcement of the law would be left to the FTC under its powers of the FTC Act, with certain modifications: the statute allows a $33,000 or $11,000 penalty for each computer affected by a violation of Sections 2 or 3, respectively; and fines of $3 million and $1 million for each violation of Sections 2 or 3 that affect multiple computers, respectively.[175] The SPY ACT would preempt similar state laws, except state trespass, contract, tort law, or fraud.[176] Interestingly, the statute provides an exception for cookies, and its effective date runs only through the end of 2009.[177]

This type of act would protect against some of the worst purveyors of spyware, and would fill at least part of the legal gap currently in existence. The consumer would be given more explicit notice requirements, allowing consumers to make the choice of what programs to install with full knowledge of their potential harms.[178] Additionally, they would be able to remove unwanted software from their computers. This would solve part of the problem with current schemes to limit spyware—namely the question of consent. When users merely skip over a license agreement, they may be waiving their right to hold spyware distributors liable for any damage that may be caused by the program.

IV. Conclusion

Rigorous enforcement of current laws is necessary to battle the growing threat of spyware to consumers. Such spyware programs could undermine the continued growth of the Internet as a forum for commerce and interaction. Currently, however, only a few cases can be brought by individual consumers against spyware companies and

---

[173] SPY ACT, *supra* note 165, at § 3(d)(1).

[174] *Id.* at § 3(d)(3).

[175] *Id.* at § 4(a)-(b).

[176] *Id.* at § 6(a)(3).

[177] *Id.* at §§ 8, 11(c).

[178] SPY ACT, *supra* note 165, at § 3.

the FTC can likely target only the most egregious offenders. Proposed laws should not encourage litigation to the point where innovation on the Internet is stifled, as consumers may be willing to permit advertisements in order to use a free program in some cases. Consumers, however, should have the choice to install any spyware-containing programs, and should always have the ability to completely remove any program they find offensive or of no use.

***