Maurer School of Law: Indiana University
Digital Repository @ Maurer Law

Federal Communications Law Journal

Volume 59 | Issue 1 Article 6

12-2006

The Legal Status of Spyware

Daniel B. Garrie
Lexeprint

Alan F. Blakley
Thomas M. Cooley Law School

Mathew J. Armstrong
Rutgers University School of Law

Recommended Citation

Garrie, Daniel B.; Blakley, Alan F.; and Armstrong, Mathew J. (2006) "The Legal Status of Spyware," *Federal Communications Law Journal*: Vol. 59: Iss. 1, Article 6.
Available at: http://www.repository.law.indiana.edu/fclj/vol59/iss1/6

The Legal Status of Spyware

Daniel B. Garrie*

Professor Alan F. Blakley*

Matthew J. Armstrong*

* Daniel B. Garrie is the CEO of Lexeprint, Inc. Mr. Garrie received his J.D. from Rutgers University School of Law and has penned several law review articles on a variety of technology and legal issues. Mr. Garrie holds an M.A. and B.A. in computer science from Brandeis University. Mr. Garrie has worked around the world with various government agencies and corporations as a Senior Consultant. Mr. Garrie currently resides in New York City and can be reached at Daniel.Garrie@gmail.com.

* Professor Alan F. Blakley, Associate Professor of Law, Thomas M. Cooley Law School, Grand Rapids, Michigan, was managing partner of a law firm in Missoula, Montana for several years. While in practice, he provided risk management consulting in digital information for corporations, and he was class counsel for several consumer class action lawsuits. He has written three books on digital information and litigation, including *2006 Digital Litigation Handbook* published in Fall 2005 by American Lawyer Media. He is co-author of the Matthew-Bender book, MASTERING WRITTEN DISCOVERY. He has written extensively on civil procedure topics and privacy, including *To Squeal or not to Squeal: Ethical Obligations of Officers of the Court in Possession of Information of Public Interest*, 34 CUMB. L. REV. 65 (2004). He serves on the editorial board of *The Federal Lawyer* magazine and is Chair of the Steering Committee of The Sedona Conference Working Group on Privacy, Confidentiality, and Public Access.

* Matthew J. Armstrong is a J.D. candidate at Rutgers University School of Law, specializing in corporate and securities law. He received his B.A. in economics, *summa cum laude*, from Drew University in 2002. Armstrong has worked as a Summer Research Associate at the U.S. Securities & Exchange Commission and currently works as a law clerk for Kenney & Kearney, LLP, a law firm specializing in complex civil and criminal litigation.

I. OVERVIEW OF SPYWARE'S RELATIONSHIP WITH THE LAW

Identity theft is lucrative; stealing one's good name is lucrative. What liability deters the people who steal digital information, even if it might be considered worthless? The Federal Trade Commission logged up to 250,000 identity theft complaints in 2004—100,000 more than in 2002. By and large, the law has been silent; and companies, some legitimate and some not, continue to collect, store, and process consumer information. The law provides those whose private information is being misused little recourse and provides little protection for those legitimately mining information. Even though large-scale breaches grab the headlines, many victims of identity theft frequently cause the offending disclosure by unwittingly downloading software from the World Wide Web ("Web") or responding to email "phishing" and other online and offline scams. Although courts find a right to privacy in the United States Constitution, that right generally only protects citizens from invasions by the government, not by corporate America.

Today, federal law enables spyware, adware, and phishing businesses to mine consumer data with impunity. This Article demonstrates that although some laws are ineffective, others provide consumers with some minimal relief. In addition, the Article proposes an innovative solution. It also discusses the implications of the "evil-ution" of software developers in the context of the law, analyzing the evolution of the software developer, the impact of the rapidly increasing skill of the developers, and the disastrous outcomes that may occur if governments fail to act.

II. SPYWARE TECHNOLOGY: A TECHNICAL OVERVIEW

Understanding spyware requires the realization that any connection to a site on the Web is not passive, and the visitor does not wander around invisibly. Connecting to the Web is not like opening a book in the library and looking at its contents. While the person accessing the Web is gathering information from the site; the site knows the visitor is there, monitors the visitor's actions, and has varying levels of access—by the visitor's invitation—to that visitor's computer. One of the earliest forms of this active interaction was cookie technology.[1] Most users find cookies beneficial because they eliminate the need to repeatedly fill out order forms or re-register on Web sites.[2] For instance, with passwords being

[1] *See* Sarah Gordon, *Fighting Spyware and Adware in the Enterprise*, INFO. SYS. SEC. 14, 14 (July/Aug. 2005) (referring to spyware evolving from simple cookie technology).

[2] Inna Fayenson, *'Cookies' Challenge Meaning of Privacy*, NEW YORK L.J., Nov. 13, 2001, at S-10.

increasingly difficult to remember, some sites that require user names and passwords place cookies on the hard drive so the user has the option to log in automatically when visiting.[3]

The reality is, however, that many businesses seek more competitive advantages. Consequently, they have developed a variety of legitimate and illegitimate technologies to enhance their market advantage.[4] Data miners[5] that actively collect information, dialers that change the computer's dial-up networking,[6] worms that create self-replicating viruses,[7] and hijackers that hijack a user's home page are all examples of modifications of cookie technology.[8]

A. Spyware Defined

Spyware is generally defined as software that, once installed on a person's computer (usually without consent), collects and reports in-depth information about that end-user.[9] Spyware is the progeny of clickstream data or cookie-based data mining technology.[10] These technologies are viewed as instrumental to the operation of the global information society. To demonstrate this expansive reliance on cookie technologies, the reader need only view the cookies stored on any personal computer.[11] The intertwined nature of spyware to other data mining technologies makes

[3] *See* Rik Farrow, *Is Your Desktop Being Wiretapped?*, NETWORK MAG., Aug. 2003, at 52 (discussing keystroke logging so that "[a]n end user might use this record to create a macro so that a particular operation can be repeated.").

[4] *See, e.g.*, Fair Debt Collection Practices Act, 15 U.S.C. § 1692(e) (2000) (legislative response to combat illegitimate technologies).

[5] *See, e.g.*, Ronald Urbach & Gary Kibel, *Adware/Spyware: An Update Regarding Pending Litigation and Legislation*, 16 INTELL. PROP. & TECH. L.J. 12, 12–16 (2004).

[6] *See* Mark D. Collier, *Current Threats to and Technical Solutions for Voice Security*, Aerospace Conference Proceedings, 2002. 6 IEEE 6-2685, 6-2686 to 6-2690; Dennis Estacion, *Potential Security Problem looms for users of PC-based VoIP products*, IEEE CANADIAN REV. 19, 19-20 (Winter 2005).

[7] *See* Michael Pastore, *Inside Spyware: A Guide to Finding, Removing and Preventing Online Pests*, INTRANET JOURNAL (2006), http://www.intranetjournal.com/spyware (last visited Nov. 3, 2006).

[8] *See* Lavasoft, Spyware from A to Z, http://www.lavasoftusa.com/support/spywareeducationcenter/spyware_glossary.php (last visited Nov. 20, 2006).

[9] *See id.*

[10] *See generally* Michael Gowan, *How It Works: Cookies*, PCWORLD, Feb. 22, 2000, *available at* http://www.pcworld.com/article/id,15352/article.html#.

[11] Janine H. McNulty, *Who Is Watching Your Keystrokes?*, 2 J. HIGH TECH. L. 67, 79-81. An end-user can view all of the cookies stored on a local machine using Internet Explorer by following these steps: (1) open Internet Explorer; (2) select "Internet Options" under the "Tools" menu; (3) click on the "General" tab and click the "Settings" button; (4) click the "View Files" button; (5) sort files by type by clicking on "Type"; (6) find documents of the type labeled "Text Document." To see the information stored by the cookie in its raw and likely unintelligible format, double-click on one of these text files containing "cookie" in its file name.

regulation a very delicate and difficult process. Most Web Portals would be severely limited, if not rendered useless, in the absence of spyware-like technologies. Web sites that would not operate if such technology was prohibited are: www.yahoo.com; www.wamu.com; www.schwab.com; www.ibm.com.[12] Adjoining these Web sites are a slew of intranet and Web applications that utilize cookies and clickstream data for authentication.[13]

Spyware is capable of gathering a wide range of information, including Web-surfing habits, each and every keystroke, email messages, credit card information, and other personal information on users' computers.[14] In the world of technology, "spyware" is the umbrella term under which numerous technologies, both legal and malicious, fall. These include: adware,[15] trojans,[16] hijackers,[17] key loggers,[18] dialers, and malware.[19] While each of these technologies has its own unique behavior, for the most part they are all installed without a user's informed and explicit consent and tend to extract varying degrees of personal information, usually without that end-user's consent.[20] For instance, trojan spyware operates with a focus on stealing passwords by using a

[12] *See generally* Press Release, U.S. Dep't of Commerce, U.S. Census Bureau News, (Mar. 2, 2000), *available at* http://www.census.gov/Press-Release/www/releases/archives/retail_industries/000523.html.

[13] *See* Daniel B. Garrie, Matthew J. Armstrong & Donald P. Harris, *Voice Over Internet Protocol and the Wiretap Act: Is Your Conversation Protected?*, 29SEATTLE U. L. REV. 97, 108–09 (2005).

[14] Cade Metz, *Spy Stoppers*, PC MAG., Mar. 2, 2004, at 79, 80.

[15] Spyware differs from adware technology because the primary purpose of adware is to display advertisements on Web pages or in programs such that those advertisements generate income for the software owners. *See* Spyware from A to Z, *supra* note 8; *See also* James R. Hagerty & Dennis K. Berman, *New Battleground In Web Privacy War: Ads That Snoop*, WALL ST. J., Aug. 27, 2003, at A1.

[16] *See* Microsoft Help and Support, *Description of the Win32.DIDer Trojan Program,* http://support.microsoft.com/?scid=kb;EN-US;Q317013 (last visited Nov. 3, 2006) (stating that "Trojan programs are programs that pretend to do one thing while secretly doing something else.").

[17] *See How TopText Works*, SCUMWARE.COM, http://scumware.com/wm2.html (last visited Nov. 3, 2006) (equating Internet traffic hijacking with spyware) [hereinafter Scumware].

[18] *See* Kishore Subramanyam, Charles E. Frank & Donald H. Galli, *Keyloggers: The Overlooked Threat to Computer Security* at First Midstates Conference for Undergraduate Research in Computer Science and Mathematics, Oct. 2003, *available at* http://www.denison.edu/mathcs/mcurcsm2003/papers/keyloggers.pdf; Pete Cafarchio, *The Challenge of Non-Viral Malware*, PESTPATROL, http://www.pestpatrol.com/whitepapers/nonviralmalware0902.asp (last visited Nov. 3, 2006). *See generally* Dr. E. Eugene Schultz, *Pandora's Box: Spyware, Adware, Autoexecution, and NGSCB*, 22 COMPUTERS & SECURITY 366 (July 2003).

[19] *See* Cafarchio, *supra* note 18.

[20] *See generally* Janice C. Sipior et al., *The Ethical and Legal Concerns of Spyware,* 22 J. INFO. SYS. MGMT. 39 (Spring 2005) (discussing the controversy surrounding various forms of spyware).

"trojanized" piece of software to grab passwords. This occurs either directly from the keyboard or while in transit over the network. Trojan spyware has been implemented many times on a raft of different platforms and is installed without the user's consent.[21]

Spyware operates in relative secrecy, gathering end-user information without the end-user's consent or knowledge. When spyware successfully installs, it is difficult to remove because it embeds itself within the system and uses various techniques to detect and replace various files that are integral to the operation of the user's machine. Consequently, if a user rips out one or two parts, the undetected parts will come in and replace the files that were removed.[22] The outcome is that although the user is aware that spyware is installed, it is difficult for the user to remove, even when utilizing spyware removal technology.[23] Spyware blurs the existing fuzzy line between a malicious virus and an aggressive Internet marketing tool. Spyware, however, can monitor more than just the Web pages an Internet surfer visits;[24] it can also access the end-user's electronic file system,[25] email system, Web pages viewed, and any other unencrypted information the end-user accesses on the machine.[26]

While valid commercial uses for spyware exist, its primary purpose is to spy and to gather information by invading a user's protected digital space, unbeknownst to the end-user,[27] and to relay it to a third party. For instance, a malicious spyware application might "pop up" a dialog box that warns the user of a problem with his or her account only to redirect that person to a look-alike site, which then acquires personal financial resources of the user.[28] Generally, malicious spyware tends to be financially motivated, distinguishing itself from past viruses/malware.[29]

B. Spyware Has Two Primary Forms

Once installed on an end-user's machine, spyware can be catalogued

[21] *See* Cafarchio, *supra* note 18.

[22] *See* Schultz, *supra* note 18, at 366–67.

[23] *See* Schultz, *supra* note 18, at 366–67.

[24] *See* Urbach & Kibel, *supra* note 5, at 12-14.

[25] *See* Schultz, *supra* note 18, at 366–67.

[26] Christopher J. Volkmer, *Should Adware and Spyware Prompt Congressional Action?*, 7 J. OF INTERNET L. 1, 12-13 (May 2004).

[27] *See* Ed Foster, *The Spy Who Loves You: Some 'Free' Internet Services Come with the Kind of Surveillance You May Not Want*, INFOWORLD, May 17, 2002, http://www.infoworld.com/article/02/05/17/020520opgripe_1.html (referring to users downloading spyware agents unknowingly).

[28] *See* Jason Krause, *Prying Eyes: Self-Installing 'Spyware' Poses a Growing Threat to PCs*, 91 A.B.A. J. 60, 60 (May 2005).

[29] *See* Chris King, *The Business of Spyware*, ITDEFENSE, http://www.itdefensemag.com/5_06/articles2.php (last visted Nov. 3, 2006).

in one of two ways: (1) software-enabled installation of spyware via shareware applications; and (2) Web-enabled installation through a user's browser.[30] This distinction is drawn because spyware's delivery and installation mechanisms can be categorized as either software-enabled or Web-enabled spyware.[31]

1. Software-Enabled Installation of Spyware via Shareware

According to researchers from the University of Washington's Department of Computer Science and Engineering, software-enabled spyware installs itself by attaching to shareware software, such as Kazaa (http://www.kazaa.com/), which "has been the source of hundreds of millions of spyware installations."[32] Commonly, these software programs are embedded within a Dynamic Link Library ("DLL") that the intruder can manipulate at a later date. On average, infected computers have 93 spyware components,[33] making the process of removal—even for a knowledgeable technical person—an arduous and daunting, if not impossible, task. Software-enabled spyware that relies on this attachment mechanism for installation has been coined "piggy-backed spyware."[34]

The majority of software-enabled spyware programs fall within the "piggy-backed spyware" installation method.[35] After installation, the spyware remains hidden from the user, and because the user consented to its installation via the shareware application End-user License Agreement ("EULA"), it does not violate black-letter law when transmitting data to third parties. For instance, to ensnare a victim, commercial trojan spyware has been distributed in romantic, joke, and other e-cards.[36] All that is necessary to spy on unsuspecting parties is the email address of the target.[37]

[30] *See generally* Kevin Townsend, *Spyware, Adware, and Peer-to-Peer Networks: The Hidden Threat to Corporate Security* (PestPatrol, Inc., Technical White Paper, Apr. 2, 2003), *available at* http://www.pestpatrol.com/files/PDF/Whitepapers/SpywareAdware P2P.pdf.

[31] Alexander Moshchuk et al., *A Crawler-based Study of Spyware on the Web*, at 1 (U. of Wash. Dept. of Computer Science & Engineering), http://www.cs.washington.edu/ homes/gribble/papers/spycrawler.pdf (last visited Nov. 3, 2006).

[32] *Id.*

[33] *Id.*

[34] *See, e.g., id.*

[35] *Id.*

[36] Email PI has deployed this variation on the e-card approach that is "an unashamed example of commercial trojan spyware. . . [with] a selection of five different E-cards—romantic, joke and others, with which to ensnare your victim." Pete Simpson, *New Blends of Email Threats*, 24 CREDIT CONTROL 9, 12 (2003). *See also* Alan Blakley et al., *Coddling Spies: Why the Law Doesn't Adequately Address Computer Spyware*, 2005 DUKE L. & TECH. REV. No. 25, para. 29, http://www.law.duke.edu/journals/dltr/articles/PDF/2005DLT R0025.pdf.

[37] For example, users shared a program, Web Surfer Tool Bar, via email distribution,

Such spyware can remotely monitor every action taken on the end-user's machine, can be logged remotely, and has notable potential in industrial espionage as well as potential judicial repercussions.[38] This illustration demonstrates the potential of spyware to impact both commercial business and private citizens, irrespective of their locality. The reality is that spyware could be mining data[39] on the end-user's machine, monitoring instant messaging ("IM"), or monitoring voice conversations that utilize Voice over Internet Protocol telephony ("VoIP").[40]

2. Web-Enabled Installation of Spyware via Browser Vulnerability

The second type of spyware technology exploits vulnerabilities in Web browsers or Web-based applications to install themselves on end-users' machines.[41] Functionally, the capabilities of the spyware installed are analogous to those installed via shareware.

One main difference between the two types of spyware is that several studies suggest that Web-enabled spyware is declining.[42] It is difficult to determine the exact cause of the decline of this form of spyware, but it is likely due to several factors: (1) public awareness; (2) adoption of anti-spyware tools; and (3) adoption of automated patch installation tools.[43] These three elements have essentially helped prevent this type of spyware from capitalizing on technology-based loopholes.

C. Adware Differs from Spyware

Spyware must be distinguished from adware. Adware is a modified derivative of cookie technology and places either random or targeted

which embedded in the HTML-formatted email a hidden link to a site that dropped an executable file into the C drive, and then exploited a known vulnerability in Internet Explorer to automatically execute a Java Script. Once installed, this application inserted multiple files on user systems and refreshed the system's registry keys, start-up page, and IE references every couple of seconds. The skill required by the end-user to remove this application extended beyond the average user's skill set. Furthermore, the application embedded many references to pornography and gambling sites, rendering the user's browser virtually nonfunctional. While Web Surfer Tool Bar was a form of adware, it could have just as easily been used to deliver a malicious spyware application that stole and/or mined a user's machine.

[38] Simpson, *supra* note 36, at 12–13.

[39] *Cybersecurity and Consumer Data: What's at Risk for the Consumer?: Hearing Before the H. Subcomm. On Commerce, Trade, and Consumer Prot. of the Comm. on Energy and Commerce*, 108th Cong. 58–59 (2003) (statement of Roger Thompson, Vice President of Product Development, PestPatrol), *available at* http://energycommerce.house.gov/108/action/108-52.pdf.

[40] *See* Garrie et al., *supra* note 13, at 122.

[41] Schultz, *supra* note 18, at 367.

[42] *See, e.g.*, Moshchuk, *supra* note 31, at 2.

[43] *See* Moshchuk, *supra* note 31, at 13.

advertisements on the screen of the user.[44] Adware is generally not malicious because it does not collect and use personal information for illegitimate purposes.[45] Spyware, while similar to adware, is usually an application installed on the user's computer and, by definition, is usually installed without the user's knowledge.[46] Not only can spyware monitor users' activities on the Web, but it can also monitor everything users do with their machines and transmit that information to an outside entity. Unfortunately, users mostly accept spyware unintentionally or without a full and informed understanding of its parameters when downloading something from the Web.

III. LEGAL TREATMENT OF SPYWARE

Spyware victims[47] pursuing civil remedies can currently pursue five theories of recovery: (1) trespass to chattels;[48] (2) the Stored Wire and Electronic Communications and Transactional Records Act ("Stored Communications Act");[49] (3) the Computer Fraud and Abuse Act ("CFAA");[50] (4) invasion of privacy;[51] and (5) the Wiretap Act.[52] Each of these theories of recovery has varying levels of success depending on the facts of the litigation, amount of damages, data mining methods, and the nature of consent inferred from the plaintiff's conduct. A complaint should allege any and all of these causes of action applicable, since the inner workings of the specific spyware program may not be known until after discovery.

First, spyware victims can assert a cause of action under the common law tort theory of trespass to chattels.[53] By inserting a code into another person's computer system, the spyware perpetrator enters an end-user's computer by intermeddling with it:

[44] Webopedia, The Difference Between Adware & Spyware, http://www.webopedia.com/DidYouKnow/internet/2004/spyware.asp (last visited Nov. 3, 2006).

[45] *See id.*

[46] Hagerty, *supra* note 15, at A1.

[47] Spyware affects not only individual users who wish to keep their personal information, such as credit card information, social security numbers, etc., private, but also businesses who wish not to have their secret processes, customer lists, financial information, etc., disclosed to competitors or others. All of these "persons" have a significant interest in the enforcement of controls on spyware perpetrators.

[48] *See* RESTATEMENT (SECOND) OF TORTS § 218 (1965); CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015 (S.D. Ohio 1997).

[49] *See* 18 U.S.C. § 2701 (2001); 18 U.S.C. § 2707 (Supp. III 2003). Other commentators have referred to this statute by other names.

[50] *See* 18 U.S.C. § 1030(g) (Supp. III 2003).

[51] *See* RESTATEMENT (SECOND) OF TORTS § 652B (1977).

[52] 18 U.S.C. § 2520 (Supp. III 2003).

[53] *See* RESTATEMENT (SECOND) OF TORTS § 218.

> One who commits a trespass to chattel is subject to liability to the possessor of the chattel if, but only if, . . . (b) the chattel is impaired as to its condition, quality, or value, or (c) the possessor is deprived of the use of the chattel for a substantial time . . . .[54]

Trespass to chattels claims arise under state common law, and therefore, their usefulness depends on whether a particular jurisdiction is willing to classify spyware violations as trespasses, as well as the requirements that individual jurisdictions may have for proving trespass to chattels. Trespass to chattels claims can also be hindered if a court finds that an end-user granted consent. As such, trespass to chattels claims present a strong cause of action against certain types of spyware in certain jurisdictions, and they should be asserted if applicable.

Second, spyware victims can assert claims under the CFAA if the aggregate damages over the course of a year exceed $5,000[55] or the spyware causes physical injury to any person.[56] The CFAA contains eight powerful civil and criminal causes of action designed to prevent unauthorized access to "protected computers" of U.S. government agencies, financial institutions, and private end-users.[57] As long as an end-user's computer is used in interstate commerce, it constitutes a "protected computer" and the end-user can bring an action for spyware violations under this Act.[58] Litigants alleging claims under the CFAA face two potential drawbacks: (1) end-users frequently authorize spyware data mining when they install the associated programs on their computers; and (2) spyware is unlikely to cause over $5,000 worth of damages unless a company has been victimized or multiple victims aggregate their damages.[59] Companies victimized by spyware will usually be able to meet the $5,000 damage requirement assuming they either have in-house staff or they hire a technology consultant to perform general system maintenance to eliminate the spyware and plug any holes it has created.[60] The CFAA

[54] *Id.*

[55] 18 U.S.C. § 1030(a)(4) (2000); 18 U.S.C. § 1030(a)(5)(B)(i) (Supp. III 2003).

[56] The CFAA makes it an offense to "knowingly cause[] the transmission of a program, information, code, or command" to intentionally cause damage to a protected computer. *See id.* at § 1030(a)(5)(A) (Supp. III 2003). *See also* United States v. Middleton, 35 F. Supp. 2d 1189, 1190–92 (N.D. Cal. 1999). The fact that the CFAA does not have a mens rea requirement for the damages element does not render the statute unconstitutional. *See* United States v. Sablan, 92 F.3d 865, 867–69 (9th Cir. 1996).

[57] *See* 18 U.S.C. § 1030(a)(1)–(2).

[58] The interstate commerce requirement can be met by demonstrating the end-user interacts via the Internet in some fashion with the respective spyware application.

[59] *See, e.g., In re* DoubleClick Inc. Privacy Litigation, 154 F. Supp. 2d 497, 520–23 (S.D. N.Y. 2001).

[60] *See, e.g.,* America Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 450–51 (E.D. Va. 1998) (holding that Internet site operator's use of Internet service provider membership in order to harvest email addresses of provider's customers and send bulk emails to those

provides the strongest cause of action available for businesses but does not afford the vast majority of end-users sufficient protection due to its high $5,000 jurisdictional requirement.[61]

Third, spyware victims may be able to assert causes of action under the Stored Communications Act which protects end-user digital privacy, be it email, IM, file transfer protocol, or other Internet-based communications when the information is stored on the end-user's machine.[62] A spyware victim alleging a violation of the Stored Communications Act must prove that the spyware program (1) intentionally, (2) in an unauthorized fashion, (3) gained access to a facility providing electronic communications, (4) obtained electronic or wire communications, and (5) the data acquired by the spyware program was in electronic storage.[63] Spyware programs mine data that resides electronically on end-users' machines.[64] Spyware violates the Stored Communications Act if it mines information in temporary storage intended to be an electronic communication without consent.[65] Two

customers—in violation of provider's terms of service—violated CFAA, which prohibits individuals from exceeding authorized access).

[61] *See* 18 U.S.C. § 1030(a)(4), (a)(5)(B)(i).

[62] Under 18 U.S.C. § 2711, the statutory definitions contained in 18 U.S.C. § 2510 of the Federal Wiretap Act also apply to the Stored Communications Act. *See* United States v. Maxwell, 42 M.J. 568, 575–76 (A.F. Ct. Crim. App. 1995), *review granted in part*, 44 M.J. 41 (C.A.A.F. 1996), *rev'd in part*, 45 M.J. 406 (C.A.A.F. 1996) (holding that the defendant had a reasonable expectation of privacy in email messages stored in an online service provider, America Online, and that this reasonable objective expectation of privacy, coupled with a subjective expectation of privacy, justified protection. The court distinguished between messages that were downloaded by another subscriber and messages retained in the system's computer when deciding whether the expectation for privacy was reasonable, and therefore, protected).

[63] *See, e.g.*, Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 114–15 (3d Cir. 2003) (holding the SCA applies to information in temporary or backup storage).

[64] Stefanos Gritzalis, *Enhancing Web privacy and anonymity in the digital era*, 12 INFO. MGMT. & COMPUTER SECURITY 255, 265 (2004).

[65] *See, e.g.*, United States v. Councilman, 373 F.3d 197, 201, 203 (1st Cir. 2004), *reh'g granted*, 385 F.3d 793 (holding that the defendants' copying of emails at the server level failed to constitute an interception and found the interception to be contemporaneous with transmission); United States v. Steiger, 318 F.3d 1039, 1048–49 (11th Cir. 2003), *cert. denied*, 538 U.S. 1051 (2003) (holding that "a contemporaneous interception—*i.e.*, an acquisition during 'flight'—is required to implicate the Wiretap Act with respect to electronic communications."); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878 (9th Cir. 2002) (holding that "for a website such as Konop's to be 'intercepted' in violation of the Wiretap Act, it must be acquired during transmission, not while it is in electronic storage."); Steve Jackson Games Inc. v. U.S. Secret Service, 36 F.3d 457, 458, 460 (5th Cir. 1994) (holding that seizure of stored but unread email messages was not an interception), *aff'g* 816 F. Supp. 432 (W.D. Tex. 1993) (requiring interception to be contemporaneous with transmission). *But see, Konop*, 302 F.3d at 886. (Reinhardt, J., concurring in part, dissenting in part) (dissenting "from Part B of Section I, which holds that the term 'intercept' in the Wiretap Act, as applied to electronic communications, refers solely to *contemporaneous* acquisition.").

drawbacks to the Stored Communications Act are that (1) personal data is not protected unless it is an electronic communication, and (2) spyware can mine any data on an end-user's machine as long as the end-user gives consent to mine data when the spyware is installed along with another freeware or shareware program. As a result, the Stored Communications Act gives spyware victims a rather limited cause of action when a stored electronic communication is mined without consent.

Fourth, spyware victims may have a cause of action under the tort of invasion of privacy, or as Restatement (Second) of Torts calls it, "intrusion upon seclusion."[66] The victim will claim that the spyware perpetrator, by inserting the spyware without the victim's permission, "intrudes . . . upon the solitude or seclusion of another *or his private affairs or concerns*," and there will be liability "if the intrusion would be highly offensive to a reasonable person."[67] The authors of the restatement specifically envision intrusions that are not physical. The restatement specifies that the intrusion "may be by some other form of investigation or examination into his private concerns, as by opening his private and personal mail, searching his safe or his wallet, examining his private bank account . . . ."[68] The only concern may be to show that "the intrusion has gone beyond the limits of decency"[69], leading to liability on the part of the perpetrator. Spyware victims, therefore, will be more likely to recover under an invasion of privacy theory if the spyware steals personally identifiable information, such as private bank accounts, credit card numbers, and social security numbers.[70]

Fifth, spyware victims may be able to assert a cause of action under the Federal Wiretap Act if the spyware intercepts an oral, wire, or electronic communication without consent.[71] Even though spyware's primary functional purpose is to make unauthorized interceptions of electronic communications, spyware developers have designed spyware programs capable of evading the Wiretap Act's reach.[72] Spyware makers

[66] RESTATEMENT (SECOND) OF TORTS § 652B.

[67] *Id.* (emphasis added).

[68] *Id.* at cmt. b.

[69] Hamberger v. Eastman, 206 A.2d 239, 242 (N.H. 1964) (citing RESTATEMENT (SECOND) OF TORTS § 867 cmt. j (1965) concerning the need to show that the limits of decency have been exceeded).

[70] *Id.*

[71] *See* 18 U.S.C. § 2510(1) (2000) (defining wire communication); 18 U.S.C. § 2510(2), (12) (2000) (defining oral communication and electronic communication).

[72] *See, e.g.*, U-Haul Int'l, Inc. v. WhenU.com, Inc., 279 F. Supp. 2d 723, 725 (E.D. Va. 2003). U-Haul sued WhenU.com, Inc. because its pop-up advertisements interfered with computer users' view of the company's Web sites. The court granted WhenU's motion for summary judgment, concluding "that WhenU's pop-up advertising does not constitute trademark or copyright infringement or unfair competition." WhenU has been sued by 1-800

have accomplished this evasion by engineering their software to record stored end-user files and end-user inputs *before* they are transmitted to another communicant.[73] In certain situations, however, spyware victims could successfully argue that while the spyware is merely tracking communications input by the end-user onto his or her own computer, the time between the end-user's input and the actual transmission of the bits of data to the other communicant is so short, on the order of milliseconds, that the communication begins contemporaneously with the end-user's input. The courts have not yet credited this argument. However, if they did, then a majority of spyware programs installed without actual consent could be found to violate the Wiretap Act, and consumers could have another cause of action against spyware proliferators.

In all five causes of action damages, can run the gamut from the minor annoyance of uninstalling or otherwise removing the spyware, to disposal of a computer that seems to have acquired a disease similar to syphilis—eating its brain away—to thousands of dollars of damage caused by the harvesting and exploitation of an end-user's personal information or identity. Since most consumers are unlikely to have damages in amounts sufficient to justify litigation, the class action device may be most useful, especially under the CFAA, which offers powerful civil causes of action as long as the victims can allege $5,000[74] in damages.[75] Since the spyware perpetrator's actions are the only actions relevant, and the cause of injuries arise from the single course of conduct under the control of the spyware perpetrator, courts may be more willing to certify these class actions.[76] Companies, however, will easily be able to meet the damages requirement given the loss in time, computing, people, and business resulting from malicious spyware operating on their systems.[77] However, *proving*

Contacts, Quicken Loans, U-Haul, and Wells Fargo, among others. WhenU prevailed on another motion for a preliminary injunction in *Wells Fargo & Co. v. WhenU.com, Inc.*, 293 F. Supp. 734 (E.D. Mich. 2003).

[73] *See* Pastore, *supra* note 7 (referring to spyware as recording URL sites visited and keystrokes).

[74] *See* 18 U.S.C. § 1030(a)(4); 18 U.S.C. § 1030 (a)(5)(B)(i) (Supp. III).

[75] The most creative plaintiff's attorney may attempt to use the civil remedy portion of the Racketeer Influenced Corrupt Organization Act ("RICO"). *See* 18 U.S.C. § 1964 (2000). While civil RICO actions are disfavored and would require a great deal of specialized proof, *see, e.g.*, Poulos v. Caesars World, Inc., 379 F.3d 654, 658 (9th Cir. 2004), the interested plaintiff's attorney may find a way to attack the spyware boon and acquire treble damages.

[76] *See, e.g.*, Watson v. Shell Oil Company, 979 F.2d 1014, 1022 (5th Cir. 1992) (certifying class for tort claims arising from oil refinery explosion).

[77] Corporate America, however, utilizes spyware technology to spy on their employees. *See* Andrew Schulman, *The Extent of Systematic Monitoring of Employee E-mail and Internet Use*, PRIVACY FOUND., July 9, 2001, http://www.sonic.net/~undoc/extent.h tm. Thus, companies using spyware in this context may be able to address malicious spyware in a most cost effective manner. *See* Annotation, *Recovery of Expected Profits Lost*

damages if someone has not hired an outsider to fix the system could cost more in expert testimony than the potential recovery.

A. Spyware Trespass to Chattels Actions

Spyware takes information from a computer without a person's permission and generally without a person's knowledge. Typically, when one thinks about trespass to chattels, the actual physical taking of a personal possession has occurred.[78] However, nothing in the definition of trespass to chattels[79] requires that the perpetrator actually possess the chattel. Merely interfering with it, impairing its condition,[80] or depriving the rightful owner of its use for a substantial time,[81] will suffice to create liability. When spyware infects a computer, by definition the computer's condition or value is impaired.[82] The user cannot use it for its intended purposes; its value as a repository of private information is clearly impaired. Furthermore, when the spyware hijacks the computer—redirecting any Internet search or homepage to a site the user does not desire and until the user can remove the spyware—the user is deprived of the desired use of the chattel for a period of time.[83]

Some litigation has already attempted to use trespass to chattels to impose liability on spyware or spyware-like applications. The results are inconsistent and particularly difficult due to the problems of quantifying and proving the damages. What monetary damage, for example, does an individual suffer when he or she must continually redirect a hijacked Web browser while surfing the Internet in pursuit of a hobby? How can the consumer quantify that damage? But, first, which courts have used trespass to chattels in this context at all?

The Second Circuit had occasion to analyze whether the use of a robot (an automated software program) to search another's database was a trespass to chattels.[84] Internet Corporation for Assigned Names and Numbers ("ICANN") authorized Register.com ("Register") to register domain names for those wishing to establish Web sites on the Internet.[85]

by Lessor's Breach of Lease Preventing or Delaying Operation of New Business, 92 A.L.R. 3d 1286, 1288–89 (1979).

[78] *See, e.g.*, Bogart v. Chapell, 396 F.3d 548, 557 n.7 (4th Cir. 2005).

[79] RESTATEMENT (SECOND) OF TORTS § 218.

[80] *Id.* at (b).

[81] *Id.* at (c).

[82] *Id.* at (b).

[83] *Id.* at (c).

[84] *See* Register.com, Inc. v. Verio, Inc. (*Register II*), 356 F.3d 393, 396–97 (2nd Cir. 2004) (describing the operation of Verio's software program).

[85] *Id.* at 395 (describing Register's appointment by ICANN to serve as registrar of domain names).

Another company, Verio, designed "WHOIS", a software program that it used as a robot to search contact information available over the Internet to find entities that had newly registered domain names.[86] Verio then contacted the people who had registered the new Web sites to solicit them to use Verio's Web site design development and operation services.[87] Verio's activities created confusion as to whether it was Register or Verio contacting the new registrants.[88] Register brought a lawsuit in the federal court for the Southern District of New York against Verio under a variety of theories, including trespass to chattels, seeking a preliminary injunction.[89]

To prevent Verio from confusing consumers by searching Register's database and soliciting Register's clients, the trial court issued an injunction barring Verio from using Register's trademarks, accessing Register's computers, or using data obtained from Register's database.[90] In the portion of the opinion relevant to trespass to chattels, the Second Circuit held this a viable cause of action under the circumstances,[91] in spite of Verio's two-prong argument for reversal of the trial court's opinion.[92] First, Verio argued that its robot's invasion of Register's servers caused no harm to Register.[93] Relying upon the trial court's findings of fact, the Second Circuit found that the trial court was not unreasonable in finding that:

> [w]hile Verio's robots alone would not incapacitate Register's systems . . . if Verio were permitted to continue to access Register's computers through such robots, it was 'highly probable' that other Internet service providers would devise similar programs to access Register's data, and that the system would be overtaxed and would crash.[94]

Furthermore, the Second Circuit adopted the lower court's finding that Verio's search robots, while performing their work, were consuming "a significant portion of the capacity of Register's computer systems."[95]

[86] *Id.* at 396.

[87] *Id.* (describing means of solicitation).

[88] *Id.* at 397 (describing Verio's sollicitations).

[89] Register claimed that Verio caused confusion among customers, accessed Register's computers without authorization, violated the Computer Fraud and Abuse Act and trespassed on Register's chattels. *Id.* at 397.

[90] *See Register II,* 356 F.3d at 395.

[91] *Id.* at 404–05.

[92] *Id.* at 404 (stating the injunction premised on Register's claim of trespass to chattels was within the range of the District Court's discretion).

[93] *Id.* at 404–05 (outlining Verio's contentions).

[94] *Id.* at 404.

[95] *Register II,* 356 F.3d at 404.

Verio next argued that Register *impliedly* gave Verio permission to access the WHOIS database through Register.[96] Somehow the court held that Register's filing a complaint in court gave sufficient notice to Verio that "its use of robots was not authorized and, according to Register's contentions, would cause harm to Register's systems."[97] Consequently, the court reasoned that Register revoked any potential implicit authorization it had given to Verio by filing the litigation. This portion of the Second Circuit's opinion is troubling because it seems to gloss over the question of consent. However, in the appended opinion of Judge Fred I. Parker, the reasoning concerning consent is more complete.[98] Judge Parker wished to affirm the trial court's preliminary injunction on the trespass to chattels claim to prohibit Verio from accessing Register's computer systems using the software robot for multiple automatic excessive searches, but he thought that the terms of the injunction were too broad.[99]

Judge Parker gave a more satisfying analysis of the trespass to chattels cause of action, finding it a reasonable use in this context and finding that the digital world has "breathed new life into the common law cause of action for trespass to chattels by finding it viable online. . . "[100] Judge Parker applied the four elements of the tort to the facts. First, Verio intended to use its robot to make successive inquiries.[101] Second, the robot used Register's computer system, consuming some of its capacity.[102] Third, the system had a finite capacity.[103] Finally, considering consent, Judge Parker stated that "since at least the initiation of this lawsuit, Verio was not authorized to use its search robot to access Register.com's computer systems. . . "[104] yet it continued to do so.

Register had argued that the terms of its agreement to allow access to its database *withheld* consent to searches using automated robots. However,

[96] *Id.* (contending robot access through Register was *not authorized*).

[97] *Id.* at 405.

[98] *See id.* at 438. Originally, Judge Parker was assigned to write the court's decision. During deliberations, he had agreed with the other two judges on the panel. In the process of drafting the court's opinion, however, he changed his mind. The other two members of the panel remained convinced that the trial court should be affirmed. Judge Parker died prior to the issuance of the final opinion. As a result, the other judges appended his draft to the court's opinion, which, in many ways, is a more complete account than that of the court. *Id.* at 395 n.1.

[99] *Id.* at 439 (directing the district court to modify the third paragraph of the injuction on remand).

[100] *Register II*, 356 F.3d at 436.

[101] *Id.* at 437.

[102] *Id.*

[103] *Id.*

[104] *Id.*

the trial court analyzed the language in Register's terms of use.[105] Register's terms of use limiting anyone's use of its Web site or database prohibited using the WHOIS data to "*enable* high volume, automated, electronic processes that apply to Register.com. . . "[106] The trial court held that the temporal aspect of the language did not withhold consent to automatically *collect* information from the WHOIS database, but only to use the data *after* collection through an automated system.[107] However, the trial court held, and the Second Circuit affirmed, that at least as of the date the lawsuit was filed, consent was withdrawn.[108] The trial court implies that there was a date prior to the filing of the litigation when Register explicitly withdrew any implied consent.[109]

Whether consumers rely upon the trial court's version or the Second Circuit's opinion, either through the two remaining judges or Judge Parker, trespass to chattels is of limited value not only for businesses whose databases have suffered invasion, but for consumers. First, the question of implied consent raises difficulty. If, as in *Register II*, the court will imply consent through some "click through" boilerplate and require the person to file litigation or take some other affirmative action to revoke consent the consumer did not know was given, the cause of action becomes almost useless.

Furthermore, as *Register II* holds, when someone interferes by unauthorized use or intermeddling with a chattel, for liability purposes, the owner of the chattel must show actual damages.[110] On one encouraging note, the court found that inserting a software robot would by definition interfere with and consequently damage Register's use of its system.[111] The trial court spent more time than the circuit court discussing the harm to the chattel itself.[112] The trial court held that "evidence of mere possessory interference is sufficient to demonstrate the quantum of harm necessary to establish a claim for trespass to chattels."[113] The court was not bothered by Register's inability to document the exact extent of interference; rather it

[105] *See* Register.com, Inc. v. Verio, Inc. (*Register I*), 126 F. Supp. 2d 238, 249 (S.D.N.Y. 2000) (addressing posted policies and terms of use).

[106] *Id.* (emphasis added).

[107] *See id.* (noting the importance of the term barring future automated processes).

[108] *Id.*; *see also Register II*, 356 F.3d at 404–05, 437 n.56.

[109] *See Register I*, 126 F. Supp. 2d at 249.

[110] *See Register II*, 356 F.3d at 437–38 (citing RESTATEMENT (SECOND) OF TORTS § 218); *Register I*, 126 F. Supp. 2d at 250.

[111] *See Register II*, 356 F.3d at 438 (describing the trespass to Register's systems).

[112] *Compare Register I*, 126 F. Supp. 2d at 249–50 (describing harm caused by unauthorized access to Register's computer system), *with Register II*, 356 F.3d at 393 (accepting the harm without question).

[113] *Register I*, 126 F. Supp. 2d at 250.

was satisfied that Verio did not dispute the robot used some of Register's system capacity.[114] For the consumer, there likewise should be no difficulty in showing that the insertion of spyware uses some of the computer's capacity and, in other ways, interferes with the use of the computer.[115] But will this be enough to make the spyware perpetrator liable?

The trial court in *Register I*,[116] as well as the Second Circuit in *Register II*,[117] imported reasoning from a case from the United States District Court for the Northern District of California.[118] In that case, eBay sought an injunction against Bidder's Edge ("BE") to prohibit BE from accessing the eBay Web site with automated search technology.[119] Unlike Register.com, eBay's terms of use included a prohibition on the use of "any robot, spider, other automatic device, or manual process to monitor or copy our web pages or the content contained herein without our prior expressed written permission."[120] eBay, in its complaint, alleged a variety of causes of action including trespass to chattels.[121]

Interestingly, this court began with the proposition that "electronic signals generated by the [defendants'] activities were sufficiently tangible to support a trespass cause of action."[122] Most courts are satisfied that invading invisibly with electronic signals is a sufficient invasion for trespass to chattels.[123] However, the court's reasoning may prove helpful to consumers in a place that requires a *physical* trespass.

The court in *eBay v. Bidder's Edge* commenced its analysis with two

[114] *See id.*

[115] *See supra* Part II.

[116] *Register I*, 126 F. Supp. 2d at 250.

[117] *Register II*, 356 F.3d at 436 n.54.

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

[119] *Id.* at 1063–64.

[120] *Id.* at 1060 (citation to eBay User Agreement omitted). The court recognized that it was unclear whether BE had agreed to eBay's terms of use when it began using its automated system. *Id.*

[121] *Id.* at 1063.

[122] *Id.* at 1069 (citing Thrifty-Tel v. Bezenek, 54 Cal. Rptr. 2d 468, 473 n.6 (Cal. Ct. App. 1996) (holding that electronic signals generated over a telephone line are sufficient for use in a trespass to chattels claim). In *Thrifty-Tel* a long-distance telephone company brought an action against parents based upon the children's use of computer access to make long-distance telephone calls without accruing charges. The court held that "[t]respass to chattel, although seldom employed as a tort theory in California (indeed, there is nary a mention of the tort in Witkin's Summary of California Law), lies where an intentional interference with the possession of personal property has proximately caused injury." *Thrifty-Tel*, 54 Cal. Rptr. 2d at 473 (citation omitted). The court then goes through the history of trespass to chattel. *Id.* at 473 n.6. The court also cites to Indiana and Washington state courts which criminalize the activity of computer trespass. *Id.* at 473 n.7 (citing State v. McGraw, 480 N.E.2d 552, 554 (Ind. 1985) and State v. Riley, 846 P.2d 1365, 1373 (Wash. 1993)).

[123] *See, e.g.*, *eBay*, 100 F. Supp. 2d at 1069; *Thrifty-Tel*, 54 Cal. Rptr. 2d at 473.

elements necessary "for trespass based on accessing a computer system."[124] First, the plaintiff must show that the defendant "intentionally and without authorization interfered with plaintiff's possessory interest in the computer system. . ."[125] Second, plaintiff must prove that "defendant's unauthorized use proximately resulted in damage to plaintiff."[126] The court seemed to authorize consent as an affirmative defense.[127] It intertwined that affirmative defense with the "without authorization" portion of the first element.[128] In applying the law to the facts of the case, the court held that even if eBay's Web site were publicly accessible, the fact that eBay "explicitly notifies automated visitors that their access is not permitted. . ."[129] and BE continued to use an automated system "even after eBay demanded BE terminate such activity. . ."[130] eBay demonstrated that BE's activities lacked authorization and exceeded the scope of any granted previously by eBay.[131] Unlike Register, eBay "repeatedly and explicitly notified BE" to cease using an automated system.[132] While this course of action may be preferable, in the case of an individual owner of a computer who is unaware of the placement of spyware on that computer, if a court requires repeated revocation of any purported consent, the consumer could never prevail in a trespass to chattels case. In *Register I & II* and *eBay v. Bidder's Edge*, the plaintiffs maintained Web presences, therefore inviting people to enter their Web sites. Individual owners of computers invite Web presences to visit their computers by accessing Web sites. Spyware perpetrators will argue analogously to the perpetrators in *eBay v. Bidder's Edge* and *Register I & II* that the consumers implicitly gave consent.

All three of these courts seem to gloss over the requirement of damage to the chattel itself. They seem to assume that the use of another's computer constitutes intermeddling that creates sufficient damage for liability.[133] The *eBay v. Bidder's Edge* court found that even though eBay does not claim BE's sending between 80,000 and 100,000 requests to

[124] *eBay*, 100 F. Supp. 2d at 1069.

[125] *Id.* at 1069–70.

[126] *Id.* at 1070.

[127] *See id.*

[128] *See id.*

[129] *Id.*

[130] *eBay*, 100 F. Supp. 2d at 1070.

[131] *Id.* The court cited City of Amsterdam v. Daniel Goldreyer, Ltd., 882 F. Supp. 1273, 1281 (E.D.N.Y 1995), for the proposition that exceeding the scope of consent can subject one to liability in trespass to chattels even though there is not a complete conversion of the chattel. The court also referred to Civic Western Corp. v. Zila Industries, Inc., 66 Cal. App. 3d 1, 17 (1977), in the context of trespass to real property, holding that when limited consent is given and the defendant exceeds that limited consent, a trespass has occurred.

[132] *eBay*, 100 F. Supp. 2d at 1070.

[133] *Id.* at 1071.

eBay's computer systems each day

> has led to any physical damage to eBay's computer system, nor does eBay provide any evidence to support the claim that it may have lost revenues or customers based on this use, eBay's claim is that BE's use is appropriating eBay's personal property by using valuable bandwidth and capacity and necessarily compromising eBay's ability to use that capacity for its own purposes.[134]

The court reasoned that even though BE's use of the system may only be a small portion of that system's capacity, "BE has nonetheless deprived eBay of the ability to use *that* portion of its personal property for its own purposes."[135] The court went on to find that eBay need not wait for a disaster before applying for relief.[136] The court seems to hold that using a portion of the computer system to the exclusion of the rightful owner is sufficient to qualify as trespass to chattels.

Another case from a federal court in California demonstrates the attempt to use trespass to chattel to reach through the spyware or robot creator to the beneficiary of that spyware's spying.[137] In *Oyster Software*, the plaintiff claimed that Forms Processing, Inc. ("FPI") had contracted with a company named Top-Ten Promotions ("Top Ten") to find metatags on Oyster Software's ("Oyster") site for FPI to use so that those searching the Web would find FPI's Web site rather than Oyster's.[138] FPI moved for partial summary judgment alleging that Oyster had failed to raise a genuine issue of material fact because it was Top-Ten's robots that went to Oyster's Web site and that Oyster had presented no evidence that the robots interfered with Oyster's computer systems.[139] First, the court denied the motion because it could not determine whether Top-Ten was vicariously liable as an employee of FPI or not liable due to an independent contractor relationship.[140] "[E]ven if FPI knew nothing about Top-Ten's initial act of sending robots to Oyster's web site and copying its metatags, it may still be liable for Top-Ten's trespass if Oyster can persuade a jury that Top-Ten was an employee rather than a consultant."[141] The court held that such determinations are generally a question of fact.[142] The plaintiff, in a similar case, will need to develop facts sufficient to show that the spyware

[134] *Id.* (citations omitted).

[135] *Id.* (emphasis added).

[136] *Id.* at 1072.

[137] Oyster Software, Inc. v. Forms Processing, Inc., No. C000724(JCS), 2001 WL 1736382 (N.D. Cal. Dec. 6, 2001).

[138] *Id.* at *2.

[139] *Id.* at *11.

[140] *Id.*

[141] *Id.*

[142] *Id.* (citing Bradbury v. Phillips Petroleum Company, 815 F.2d 1356, 1360 (10th Cir. 1987)).

perpetrator is in fact an employee and not an independent contractor.[143]

The court then considered the amount of interference necessary to sustain a trespass claim. Relying upon the analysis in *eBay v. Bidder's Edge*, the court found that under California law, minimal interference based merely on evidence of use may be sufficient to support trespass to chattels,[144] and the proper damages analysis considers lost profits.[145] For an individual whose computer is invaded by spyware, there will be no lost profits. Consequently, the *Oyster* case may not have any value for consumer protection.

The U.S. District Court for the Central District of California distinguished *Ticketmaster Corp. v. Tickets.com, Inc.* from *eBay v. Bidder's Edge*, and gave consumers a well-developed outline of the argument that unauthorized invasion of a computer can be trespass to chattels.[146] The court set forth an almost logical progression.

"The computer is a piece of tangible personal property."[147] Despite the fact that computers did not exist when trespass to chattels was first developed under the common law, and even though computers are "operated by mysterious electronic impulses . . . [,]the principles should not be too different."[148]

The court reasoned that since "the electronic impulses can do damage to the computer or to its function in a comparable way to taking a hammer to a piece of machinery, then it is no stretch to recognize the damage as trespass to chattels and provide a legal remedy for it."[149] What difference, the court asks, is there to bombarding a computer with electronic information in the form of data and any other type of trespass? The court does not follow through the same list of physical items leading to trespass as in *Thrifty-Tel*,[150] but it might have. In *Thrifty-Tel*, the court went from physical touching, to dust particles, to microscopic particles or smoke, to sound waves, to electronic signals showing that computer data could well be the basis for trespass.[151]

The *Ticketmaster* court distinguished its facts from *eBay v. Bidder's Edge* in holding that there was no obstruction to the basic function or harm

[143] The plaintiff must use state law concerning independent contractor status to meet this burden.

[144] *Oyster Software*, 2001 WL 1736382 at *13.

[145] *Id.* at *13 n.11.

[146] Ticketmaster Corp. v. Tickets.com, Inc., No. 99CV7654, 2000 WL 1887522, at *4 (C.D. Cal. Aug. 10, 2000).

[147] *Id.*

[148] *Id.*

[149] *Id.*

[150] *Thrifty-Tel*, 54 Cal. Rptr. 2d at 473 n.6.

[151] *Id.*

to the chattel in *Ticketmaster* as there had been in *eBay v. Bidder's Edge* because there was no interference with the regular use of Ticketmaster's equipment.[152] The court does, however, summarize *eBay v. Bidder's Edge* in a helpful manner: "the harm to the equipment foreseen was to its intended function, not the physical characteristics of the computer."[153] Consequently, in a trespass to chattels case, a consumer only needs to show that the insertion of spyware impaired the function of the equipment. Apparently, in California federal courts, trespass to chattels based upon the use of spyware seems alive, well, and available to consumers.

Unfortunately, the Supreme Court of California muddied the water with a decision in an email case.[154] The *Intel Corp* majority opinion distinguished *eBay v. Bidder's Edge* on the basis that some injury must be shown.[155] The court claimed that *Oyster* incorrectly applied California law in stating that actionable trespass to chattel exists simply based on use.[156] The California Supreme Court majority opinion clearly requires some impairment of the chattel or the chattel's function.[157] The court also refused to extend California's common law trespass to chattels to include "otherwise harmless electronic communication whose contents are objectionable."[158] In essence, this decision eviscerates any potential trespass to chattels cause of action for consumers in California state courts.

Two strong dissenting opinions followed the *Intel Corp* holding.[159] Both dissenters believed that trespass to chattels should be actionable due to the cost imposed upon the plaintiff by the interloper's use of the system.[160] What *Intel Corp* demonstrates is that the tort of trespass to chattels is a developing field and consumers using it must be careful to demonstrate the elements, especially lack of consent,[161] as well as damage to the chattel itself.[162] While trespass to chattels may be the strongest tort action available to consumers, it is not adequate to the task of imposing sufficient liability on spyware perpetrators to cause them to cease their activities.

[152] *Ticketmaster Corp.*, 2000 WL 1887522 at *4.

[155] *Id.*

[154] *See generally* Intel Corp. v. Hamidi, 71 P.3d 296, 300 (Cal. 2003) (holding "trespass to chattels . . . does not encompass, and should not be extended to encompass, an electronic communication that neither damages the recipient computer system nor impairs its functioning.").

[155] *Id.* at 306.

[156] *Id.* at 307 n.5.

[157] *Id.*

[158] *Id.* at 308.

[159] *See id.* at 313 (Brown, J., dissenting); *id.* at 325 (Mosk, J., dissenting).

[160] *See id.* at 323, 327.

[161] *See, e.g.*, *eBay*, 100 F. Supp. 2d at 1070.

[162] *See Intel Corp.*, 71 P.3d at 306.

B. Spyware Under the Computer Fraud and Abuse Act

The CFAA is a set of eight criminal and civil causes of action that prevent unauthorized access to "protected computers" of United States government agencies, financial institutions, and private party end-users.[163] A "protected computer" under the CFAA is one used either exclusively by the U.S. government or a financial institution,[164] or one "which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States."[165] End-users who are victims of spyware can only assert civil causes of action under the CFAA if the unauthorized invader has caused:

> (i) loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000.00 in value; (ii) the modification or impairment or potential modification or impairment of the medical examination, diagnosis, treatment, or care of 1 or more individuals; (iii) physical injury to any person; (iv) a threat to public safety or health; or (v) damage affecting a government computer system used by or for a governmental entity in furtherance of the administration of justice, national defense, or national security.[166]

1. Meeting the Damage Requirement for Civil Claims

Spyware victims can assert civil claims under the CFAA to recover damages against unauthorized computer users whenever the invader directly or indirectly causes some physical harm to befall *any person* through the unauthorized use.[167] Absent actual physical injuries, most civil litigants will be required to show $5,000 in aggregate damages over a one-year period.[168] This will be a high hurdle for most litigants, especially considering that the cost of a top-of-the-line end-user system is less than $4,000.[169] The complete destruction of a computer by malicious code may not be sufficiently damaging to permit an end-user to assert a cause of

[163] *See* 18 U.S.C. § 1030(a)(1)–(2) (2000).

[164] *See id.* § 1030(e)(2)(A).

[165] 18 U.S.C. § 1030(e)(2)(B) (Supp. III 2003).

[166] *See id.* § 1030(a)(5)(B)(i)–(v); Anne P. Mitchell, *Vendor Liability for Advertising in Unsolicited Commercial E-mail*, 22 J. MARSHALL J. COMPUTER & INFO. L. 137, 138–39 (2003) (arguing that assigning liability to vendors is a viable way to address the spyware problem).

[167] *See* 18 U.S.C. § 1030(g) (Supp. III 2003) (emphasis added).

[168] *See* 18 U.S.C. § 1030(a)(4) (2000); 18 U.S.C. § 1030(a)(5)(B)(i) (Supp. III 2003).

[169] *See* Dell, http://www.dell.com/content/products/features.aspx/cto_xpsnb_m1710?c=us&cs=19&l=en&s=dhs (last visited Nov. 8, 2006). Gaming systems are one of the higher-end computer products purchased by end-users because of their technologically advanced processors, video cards, and sound cards.

action under the CFAA.[170] End-users will likely have to either band together in a class action to aggregate their damages or claim that extensive data has been destroyed and must be restored by a forensic computer technician. While both of these damage calculation strategies will help spyware victims assert claims under the CFAA, the large $5,000 damage requirement, in conjunction with the cost of finding an expert to testify, will likely foreclose the majority of end-users from being able to file successful CFAA actions against spyware distributors.[171]

Banding together to form a class action may be possible when particularly offensive spyware or computer virus programs destroy numerous hard drives or steal personally identifiable information from multiple users in a short period of time.[172] Spyware victims will likely need to aggregate damages because claimants cannot bring a cause of action under the CFAA unless the defendant causes $5,000 of damage *to a single protected computer*.[173] If the class can assert damage to a single protected computer, then all injured class members may bring claims even if their individual damages are less than $5,000.[174] This may, however, be difficult given spyware's ability to impact end-users all around the world. It may be unlikely that multiple victimized end-users will be aware of others who are similarly situated, enabling them to aggregate their damages in a class action. Furthermore, the CFAA forces individual victims to act quickly since the statute of limitations from the discovery of damages is only two years.[175] The CFAA damage calculation mechanism also limits damage aggregation to meet the $5,000 requirement to a one-year period for all plaintiffs.[176] Plaintiffs will likely be unaware of both of these provisions. Therefore, if plaintiffs' damages are sufficient and if they can afford it,

[170] Deborah F. Buckman, Annotation, *Validity, Construction, and Application of Computer Fraud and Abuse Act (18 U.S.C.A. § 1030)*, 174 A.L.R. FED. 101, 132 (2005).

[171] This could be changed if inflationary forces overcome declining equipment costs and cause the value of the average computer system to exceed $5,000. However, inflation would have to cause the price of the average hard drive to exceed $5,000 since in nearly all cases, absent a fried motherboard or CPU, the aggrieved end-user could just swap in a new hard drive and his or her computer would run like new.

[172] *See* 18 U.S.C. § 1030(a)(4) (2000); 18 U.S.C. § 1030 (a)(5)(B)(i) (Supp. III 2003).

[173] *See* Thurmond v. Compaq Computer Corp., 171 F.Supp. 2d 667, 681 (E.D.Tex. 2001) The case held that:

> no one can bring a cause of action unless the defendant causes an aggregate of $5,000 "damage" to a protected computer. If defendant causes such damage, then any injured person may bring a claim even if, his or her own "damage," is less than $5,000. Accordingly, Plaintiffs must offer summary judgment evidence of a transmission to a computer that caused loss of at least $5,000.

Id.

[174] *Id.*

[175] *See* 18 U.S.C. § 1030(g) (Supp. III 2003).

[176] *See* 18 U.S.C. § 1030(a)(4) (2000); 18 U.S.C. § 1030(a)(5)(B)(i) (Supp. III 2003).

they will be more likely to take their own actions to court themselves rather than as a class. If spyware victims want to have the best possible chances of recovery, they must act quickly to find other similarly situated plaintiffs to assert a class action claim under the CFAA's numerous protective causes of action. Plaintiffs will likely only use the class option if there is a particularly widespread product that drives a class action lawyer to assert such a suit. Otherwise, plaintiffs are only likely to use this option if they know someone else personally who has been similarly victimized, an unlikely, but possible occurrence if the virus or spyware spreads by email contact lists.

End-users asserting CFAA claims on their own will be forced to argue that their lost data caused such a grave inconvenience that their total losses exceeded $5,000.[177] "Loss" is defined under the CFAA as "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."[178] The definition of "loss" appears to cover the costs of identifying the extent of damage to the end-user's compromised system and restoring the end-user's system to its previous condition.[179] Even if an end-user purchases a brand new computer, it is unlikely that the end-user's losses would even exceed $4,000. End-users could, however, exceed the $5,000 loss requirement by claiming that valuable data has been lost or compromised, destroying its value.[180] Further end-user losses may result if personally identifiable information is compromised, such as banking or credit card information, and subsequently used to make unauthorized purchases.[181] Finally, in some instances, end-users may be

[177] *See* 18 U.S.C. § 1030(a)(4) (2000); 18 U.S.C. § 1030(a)(5)(B)(i) (Supp. III 2003).

[178] 18 U.S.C. §1030(e)(11) (2000).

[179] *See* EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 585 (1st Cir. 2001) (holding that appellees suffered a detriment and a disadvantage constituting a loss under the CFAA by having to expend substantial sums to assess the extent, if any, of the physical damage to their Web site caused by appellants' intrusion). The court further held that the detriment, disadvantage, or physical damage caused by appellant's intrusion into appellee's system constitutes a loss under the CFAA. "That the physical components were not damaged is fortunate, but it does not lessen the loss represented by consultant fees. Congress's use of the disjunctive, 'damage or loss,' confirms that it anticipated recovery in cases involving other than purely physical damage." *Id. But see In re* Intuit Privacy Litig., 138 F. Supp. 2d 1272, 1281 (C.D. Cal. 2001) (explaining loss means "irreparable damage" and any other interpretation "would render the term 'damage' superfluous"); *Register I*, 126 F. Supp. 2d at 252 n.12 (noting lost business or goodwill could not constitute loss absent the impairment or unavailability of data or systems).

[180] Damage is defined under the CFAA as "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8) (2000).

[181] Stephanie Byers, Note, *The Internet: Privacy Lost, Identities Stolen*, 40 BRANDEIS

able to meet the $5,000 requirement by hiring a computer forensic technician to restore their data or to track down the compromised data—although what consumer would pay $5,000 with the hope of recovering it during litigation?[182] Moreover, if the consumer can replace the system for less than $5,000, the defendant may argue that the plaintiff failed to mitigate loss by hiring a technician rather than simply buying a new system. While the definition of "loss" includes these costs, economics (and common sense) counsels end-users to buy a new computer instead. The result could be that end-users are inadvertently denied from asserting a cause of action under the favorable CFAA statute.

Unlike individual end-users, large corporations and other businesses that are victimized by spyware will usually be able to satisfy the $5,000 damage requirement under the CFAA.[183] Given the size of corporate information technology systems, even a minimal spyware attack could create significant damages as numerous computer technicians purge spyware from the systems, restore data, and repair any security holes that the spyware may have created.[184] Computer technicians are compensated generously, and hiring a single technician for a week would likely exceed $5,000 in damages notwithstanding the compromised data's diminution in value and potential public relations damages or derivative liability if spyware steals personally identifiable customer information. Further, it makes sense to fix the system rather than, as in the case of the consumer, buy a new system. Due to the size and value of their IT networks, businesses and corporations are the best suited candidates for asserting causes of action under the CFAA. Whenever a business experiences an IT network violation by spyware, hackers, or computer viruses, the company's

L.J. 141, 150 (2001).

[182] *See EF Cultural Travel BV*, 274 F.3d at 585.

[183] *See* 18 U.S.C. § 1030(a)(4) (2000); 18 U.S.C. § (a)(5)(B)(i) (Supp. III 2003).

[184] *See* Dave Piscitello, *Keep Spyware Off Your Business Network*, SMALLBIZPPIPELINE, (Jan. 10, 2005) (on file with *Journal*) (providing an example of how rapidly spyware-induced productivity loss and helpdesk costs can accumulate). For instance:

> [a] user installs a free toolbar and web accelerator, and inadvertently installs spyware embedded in these freebies. The particular pests he has installed prove to be removal resistant: attempts to remove the pests damage critical operating system files, such as the Windows Registry, dynamic link libraries, and TCP/IP configuration files. The spyware render the PC inoperable.
>
> The user calls the help desk. Support staff invest an estimated 2–4 hours investigating, repairing or rebuilding the PC's primary partition, and restoring the user's local work environment, including applications and data files.
>
> The total time cost for this incident is about one half to one employee-day—that's assuming that the employee is unproductive during this repair time. An organization with 1,000 employees might get 10 such incidents per work day; some back-of-the-envelope calculations yield a spyware cost of $512,000 to $1.24 million.

Id.

legal group should consider filing a cause of action under the CFAA.

2. Civil Causes of Action Applicable to Spyware

The CFAA contains eight separate civil and criminal statutes generally protecting end-users from malicious Internet users who intentionally access computers without authorization or exceed their authorization and cause damages to the computer. One section of the CFAA, 18 U.S.C. § 1030(a)(5)(A)(i), is particularly tailored to protect end-users against spyware by enabling end-users to assert causes of action against a person who "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer."[185] A protected computer is one that is used in interstate or foreign commerce or communication.[186] Spyware distributors create and distribute spyware programs as addendums to other desirable freeware and shareware programs.[187] If spyware mines data without the end-user's authorization or exceeds the end-user's authorization, then the spyware entities have knowingly created and distributed a program that has caused damage without authorization, thereby violating §1030(a)(5)(A)(i) of the CFAA.

CFAA spyware suits hinge on two elements: the $5,000 aggregate damage requirement discussed in the previous section and the issue of *authorization*. Exceeding authorized access is defined under the CFAA as "access[ing] a computer with authorization and . . . us[ing] such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[188] It is foreseeable that a multitude of spyware programs could be accused of either operating without authorization or exceeding their authorized access since they are installed onto an end-user's machine without the end-user's knowledge.[189] Developers may be liable for spyware applications that secretly install programs for damages that those programs create under the CFAA, assuming that they cause more than $5,000 in damage to a class of plaintiffs within a one-year period.

[185] 18 U.S.C. § 1030(a)(5)(A)(i) (Supp. III 2003).

[186] 18 U.S.C. § 1030(e)(2)(B) (2000). *See also* Credentials Plus v. Calderone, 230 F. Supp. 2d 890, 906 (N.D. Ind. 2002) (holding that plaintiff's computer is a protected computer under the CFAA because it is used to send and receive email to customers throughout the United States).

[187] *See* Krause, *supra* note 28, at 60.

[188] 18 U.S.C. § 1030(e)(6) (2000). *See also EF Cultural Travel BV*, 274 F.3d at 582 (affirming that competitor exceeded authorized access when using program to glean prices from plaintiff's Web site).

[189] *See* Mathias Klang, *Spyware: Paying for Software with Our Privacy*, 17 INT'L REV. L. COMPUTERS & TECH. 313, 314–15 (2003).

Spyware programs that obtain an end-user's consent during the installation process are less likely to be liable under the CFAA.[190] While the CFAA does permit a cause of action against spyware that "exceeds authorized access," spyware companies are able to insulate themselves from this liability by openly disclosing in the EULA in broad terms, an intention to mine data or install other programs on an end-user's computer.[191] Spyware companies can bury these contractual provisions deep within legal boilerplate contracts that end-users are unlikely to read.[192] Therefore, while the spyware obtains contractual consent through a purchaser's duty to read,[193] the end-user arguably does not have sufficient notice of the spyware's intentions or even its existence. Even when end-users read EULA agreements, it is still unlikely that they will comprehend the spyware's intentions, or even its existence, if the data mining provisions are stated in extremely broad terms. In these situations, a determining court will examine specific contractual terms that the end-user has probably never actually read before. As long as the spyware's actions fall within the

[190] *Id.* at 314–16.

[191] *See id. See also* I.Lan Sys. v. Netscout Serv. Level Corp., 183 F. Supp. 2d 328, 338 (D. Mass. 2002) (enforcing terms of clickwrap agreement where the assent is explicit and holding that clickwrap license agreements are an appropriate way to form contracts). The court stated:

> To be sure, shrinkwrap and clickwrap license agreements share the defect of any standardized contract—they are susceptible to the inclusion of terms that border on the unconscionable—but that is not the issue in this case. The only issue before the Court is whether clickwrap license agreements are an appropriate way to form contracts, and the Court holds they are. In short, I.Lan explicitly accepted the clickwrap license agreement when it clicked on the box stating "I agree."

Id.; ProCD, Inc., v. Zeidenberg, 86 F.3d 1447, 1452 (7th Cir. 1996) (citing U.C.C. § 2-204 (1994) and stating that "[a] vendor, as master of the offer, may . . . propose limitations on the kind of conduct that constitutes acceptance"); M.A. Mortenson Co., Inc. v. Timberline Software Corp., 998 P.2d 305, 311–14 (Wash. 2000) (holding that where a vendor and purchaser utilized a license agreement in prior course of dealing, a shrinkwrap license agreement constituted contract formation under § 2-204, not contract alteration under § 2-207). *But see* Klocek v. Gateway, Inc., 104 F. Supp. 2d 1332, 1341 (D. Kan. 2000) (holding that because plaintiff is not a merchant, additional or different terms contained in the Standard Terms did not become part of the parties' agreement unless plaintiff expressly agreed to them); Step-Saver Data Sys., Inc. v. Wyse Tech., 939 F.2d 91, 98 (3d Cir. 1991) (holding that the parties' conduct in shipping, receiving and paying for product demonstrates existence of contract and that the box top license constitutes proposal for additional terms under § 2-207 which requires express agreement by purchaser); Ariz. Retail Sys., Inc. v. Software Link, Inc., 831 F. Supp. 759, 765 (D. Ariz. 1993) (holding when vendor entered into contract by agreeing to ship goods, or at least by shipping goods to buyer, license agreement constitutes proposal to modify agreement under U.C.C. § 2-209, which requires express assent by buyer); U.S. Surgical Corp. v. Orris, Inc., 5 F. Supp. 2d 1201, 1206 (D. Kan. 1998) (holding that single-use language on product's label was proposed modification under § 2-209, which requires express assent by purchaser).

[192] *See I.Lan Sys.*, 183 F. Supp. 2d at 338.

[193] *Id.*

disclosed terms, the spyware developers should not face any liability.[194] Thus, the CFAA's authorization requirement gives spyware developers a substantial ability to control their ultimate liability by disclosing their spyware's capabilities and data mining intentions. While this theoretically protects consumer interests by encouraging disclosure, spyware's ability to abuse the process by hiding disclosure clauses within boilerplate contracts gives spyware developers an unfair advantage under the law.

Although the authorization requirement will impede some spyware victims' CFAA actions, many actions will not be foreclosed because most spyware programs do not disclose their software's capabilities in an EULA. Since most spyware mines data on an end-user's computer without their knowledge or consent, most spyware applications never disclose their presence to end-users. These unauthorized spyware programs violate the CFAA, and victims will be able to recover civil damages if they can meet the $5,000 damage requirement. If enough successful actions are filed, more spyware developers will incorporate the EULA disclosure model into that of the bundled freeware or shareware program. Such an outcome will likely cause consumers more harm than good because of spyware's ability to meet its legal contractual disclosure requirements via the burying technique. A more effective solution would have to originate with the legislature. The legislature could solve this problem and protect both end-users and spyware developers at the same time by adopting a set of spyware EULA disclosure requirements to ensure that end-users actually have adequate notice when they install and consent to spyware installations.[195]

C. Spyware Under the Stored Communications Act

Spyware arguably violates the Stored Communications Act[196] because it mines personal information from an end-user's communication facility, be it a computer, cell phone, or PDA, without the end-user's consent. The Stored Communications Act provides a civil cause of action for parties victimized by unauthorized third-party access to their stored

[194] *Id.*

[195] *See Infra* Part IV.

[196] The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act ("USA PATRIOT Act") of 2001 was passed in the wake of the events of September 11 and amended the Stored Communications Act, thus relaxing the constraints of the Stored Communications Act. *See* Pub. L. No. 107-56, §§ 209–210, 212, 220, 223, 505, 815 (2001) (codified as amended in scattered sections throughout 18 U.S.C.). For example, sections 210 and 211—codified at 18 U.S.C. § 2703(c)(2)(A)–(F) and 47 U.S.C. § 551(c)(2)(D)—expanded the type of information that government entities can obtain from electronic communication service providers without a court order.

electronic communications.[197] The Stored Communications Act is intended to protect end-user digital privacy in email, IM, file transfer protocol, and other Internet based communications when the information is stored on the end-user's machine and is not accessible.[198]

To maintain a successful cause of action under the Stored Communications Act,[199] a spyware victim must show: (1) intentional; (2) unauthorized access; (3) to a facility providing an electronic communication service; (4) that obtains a wire or electronic communication; (5) in electronic storage.[200] The legislative history of the Stored Communications Act indicates that it was intended to include "storage in any other form including storage of magnetic tapes, disks or other media."[201] This provision, however, does not apply to conduct that is authorized "by the person or entity providing a wire or electronic communications service" or by the "user" of that service.[202] By design, spyware programs seek to mine the information without explicit "authorization" from the end-user.[203] Although some spyware programs do acquire "authorization" by disclosing their software's capabilities in an EULA, many do not. Spyware programs that access stored electronic communications on an end-user's system without previously disclosing the software's capabilities and intentions violate the Stored Communications Act.[204]

[197] 18 U.S.C. § 2707(a) (requiring a violation be made either knowingly or intentionally to justify relief).

[198] *See supra* note 62 and accompanying text.

[199] Offense.—Except as provided in subsection (c) of this section whoever—

> (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or
>
> (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

18 U.S.C. § 2701(a) (2000).

[200] The term "electronic storage" is defined to mean "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication. . . " 18 U.S.C. § 2510(17) (2000).

[201] S. Rep. No. 99-541, at 16 (1986). The legislative history indicates that a communication is considered to be "in storage" both when it is temporarily stored on the computer of the electronic communications service prior to receipt by the recipient of the communication and when it is stored on the computer after receipt.

[202] 18 U.S.C. § 2701(c) (2000).

[203] *See generally* Schultz, *supra* note 18.

[204] While multitudes of spyware violate the Stored Communications Act, the degree of guilt hinges upon the nature of the accessed communications. Spyware programmers cannot prove that the end-user intended to give the spyware programs access to the electronic communications. In most cases, spyware programmers must also overcome the presumption

1. First Element: Intent

The first element of the Stored Communications Act requires a spyware company to have acted with the intent of accessing the stored communications on the end-user's machine. In most cases this element is proved with ease because spyware programs are purposefully written with the intent to find and copy specific information on an end-user's machine,[205]and then to transmit it to the spyware system.[206] Spyware companies will argue in defense that their spyware programs mistakenly and, consequently, unintentionally send back extra data that they did not request. This argument, however, should be easily resolved by analyzing the application code to determine if the program intentionally sought to mine the purported extra data. While courts may permit spyware creators to use this defense for subsets of data that the spyware was not supposed to mine, it cannot be used for all mined data since spyware programs are designed to collect data. Thus, spyware victims will be able to satisfy the intent element in most unauthorized spyware data mining cases.

2. Second Element: Authorization

The second element of the Stored Communications Act requires a spyware program to mine data without an end-user's authorization. Spyware programs that do not disclose their presence or their intentions to mine an end-user's data violate the authorization prong because they operate without the end-user's consent, a necessary element of "authorization." Spyware can obtain "authorization" either through legal authorization in the form of a government issued search warrant or through an end-user's consent. While end-users may initially consent to the installation of freeware or shareware programs that later install spyware, the end-user certainly does not explicitly, or arguably even implicitly, consent to the piggybacking spyware program's mining of personal electronic communications stored on the end-user's machine. Some courts have found that although the interception of electronic communications does not require explicit consent, consent can only be implied if the end-user has notice and actually gives consent.[207] When spyware is installed on end-users' machines without the end-user's knowledge, they cannot give

that spyware by its very definition, implies that the actions were taken without the end-user's "authorization."

[205] In this context, "machine" could encompasses desktops, servers, laptops, cell phones, PDA, electronic devices, hand-held devices, and computers.

[206] The spyware program can elect to transmit the information to devices other than a server. The focus is not on the particular medium upon which the spyware's program communication is stored, but rather that it is being transmitted to a third-party device without "authorization" from the end-user.

[207] *See In re* Pharmatrak, Inc. Privacy Litig., 329 F.3d 9, 20 (1st Cir. 2003).

actual consent because they do not have notice. As a result, whenever a spyware program operates without at least giving the end-user notice of its installation and its intention to mine data, the Stored Communications Act's lack of authorization will be met. But, what is sufficient notice? Does a boilerplate "click through" contract on a Web site suffice?

In some instances, however, end-users will consent to the installation of a program that includes a spyware component, such as Kazaa.[208] However, while the end-user consents to the installation of the program itself, the end-user has no way of knowing what the spyware will record. Courts determining whether end-users have given actual consent will take either of the following inconsistent positions: (1) by consenting to the tied program's installation, the end-user impliedly consents to the spyware's data mining, or (2) the mere use of a spyware laden program is insufficient to impute actual consent for the spyware to ravage all of the information stored on an end-user's system. The current trend in the courts suggests that they will likely require spyware to give the end-user notice of specific electronic communications that it will mine in order to acquire actual consent.[209] But, if this notice need only be buried in boilerplate contract, will it have any value to the consumer?

Even if a court finds that a spyware program received actual end-user consent to mine data, spyware developers can still violate the Stored Communications Act by exceeding an end-user's authorization. End-users can grant spyware partial consent to mine different subsets of information stored on their facilities based on the express terms of the use agreement. If spyware receives only partial consent, data not expressly included in the agreement will be off-limits to mining.[210] The ability to grant limited consent is supported by cases interpreting the Wiretap Act, which have

[208] *See* Scumware, *supra* note 17.

[209] The issue of whether end-users have authorized spyware to mine stored personal information and electronic communications will be the focus of legal disputes until Congress or the States mandate specific required disclosures. Due to the Internet's global reach, a mandatory disclosure law passed by Congress would enable spyware companies to create and issue one version of their software to be distributed over the Internet regardless of the end-user's location. The disclosures would be included in the EULA or in the download's read-me file in bold letters at the top of the page. Mandatory disclosures would assist both end-users and spyware creators because the end-users would be able to make informed decisions, and the spyware creators would be absolved from liability under the Stored Communications Act as long as the program only mines data stipulated in the disclosure paragraph. Without a statutorily mandated rule for spyware disclosures, end-users will remain unaware of the extent to which their information is being mined, and spyware creators will continue operating under the constant threat of class action lawsuits. This is not a preferable operating environment for either of the parties involved.

[210] Furthermore, if the spyware program is transmitting a social security number and related information, the spyware program must be encrypted and comply with any regulations pertaining to the transmission of personal information.

held that a third-party data interceptor does not obtain end-user consent where the user consents to the mining of nonpersonally identifiable information, but refuses to permit the mining of personally identifiable information.[211] Courts have also held that consent cannot be inferred from the mere use of a product or the purchase of a service.[212] The requirement of actual consent, while never explicitly held necessary under the Stored Communications Act, should be applied because both the Stored Communications Act and the Wiretap Act are part of the ECPA and share the same definitions.[213] Therefore, both the courts and the legislature require spyware companies to either disclose specific subsets of files they will be mining or to obtain broad consent without any limitations to all files contained on an end-user's machine. If this consent is not obtained, then spyware companies run the risk of exceeding their authorization on the end-user's system and violating the second prong of the Stored Communications Act.

Unfortunately, spyware companies can circumvent the authorization element by drafting EULAs that include language granting the spyware blanket access to mine all data on an end-user's machine.[214] Spyware programs use numerous deceptive techniques to elicit such "explicit" end-user consent, such as including a voluminous EULA that only describes the program's capabilities or by stating in extremely broad language that the program can search for and use end-user data. A particularly insidious trick is to bury the spyware consent clause within the tied freeware or shareware program's EULA. Most end-users faced with a contract consisting of more than a few pages are unlikely to read every single page or understand all of the legalese they have read. Most read none of the EULA, but simply click the "I agree" button to begin using the application.

3. Third Element: Facility Providing an Electronic Communication Service

The Stored Communications Act's third element requires plaintiffs to prove that when their data was mined, their system was operating as a facility providing electronic communication services to the spyware program. A court must find that the end-user's machine is being used as a facility through which "electronic communication service[s]" are being "provided" when the spyware program accesses and transmits files stored

[211] *Pharmatrak*, 329 F.3d at 20.

[212] *Id.*

[213] 18 U.S.C. § 2510(17) (2000) (defining "electronic storage"); 18 U.S.C. § 2711(1) (Supp. III 2000) (incorporating into § 2711 of the Wiretap Act all the definitions found in § 2510, including the definition of "electronic storage").

[214] *See supra* note 191 and accompanying text.

on an end-user's computer.[215] The Stored Communications Act defines an "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications."[216] Under this definition, spyware programs operating on end-users' computers utilize an "electronic communication service" because, without the "facility" provided by the end-user's machine, no communication could transpire between the spyware program and the entity to which it transmits the end-user's data.[217] Since spyware uses end-users' machines as facilities through which electronic communication services are provided, courts will likely hold that spyware programs that successfully mine and transmit data from an end-user's machine satisfy the Stored Communications Act's third prong.[218]

4. Fourth Element: Access to a Wire or Electronic Communication

The Stored Communications Act's fourth element is satisfied if a spyware program "obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage . . . ."[219] Most spyware programs will meet this element because they operate by accessing, recording, and transmitting end-users' "electronic communications," including Internet browsing habits, instant messaging conversations, and email. The Stored Communications Act defines "electronic communications" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce . . . ."[220] Spyware

[215] 18 U.S.C. § 2701(a)(1) (2000).

[216] *See* 18 U.S.C. § 2510(15) (2000); 18 U.S.C. § 2711(1) (Supp III 2003) (incorporating into § 2511 of the Wiretap Act the definition of "electronics communications service" found in section § 2510(15)).

[217] *See In re* Intuit Privacy Litig., 138 F. Supp. 2d 1272, 1276 (C.D. Cal. 2001) (stating that 18 U.S.C. § 2701 "does not require that there be a 'communication' at all." Since the primary act required for violation of § 2701 is the act of accessing electronically stored data, the existence or absence of communication is irrelevant).

[218] Spyware applications mine end-user transmissions without consent, which permits the court to find that the end-user's machine in such instances are acting as a facility for electronic communication services. On the other hand, if the end-user is utilizing technology that is not spyware driven, then the argument that the end-user's machine is a facility for providing electronic communication is not as strong. In this context the focus is not on unauthorized data mining of end-user personal information, but rather on the transmission of communications; and the end-user's machine is serving as a conduit for these communications.

[219] 18 U.S.C. § 2701(a)(2).

[220] *See* 18 U.S.C. § 2510(12) (defining "electronic communication"); 18 U.S.C. § 2711(1) (incorporating into § 2511 of the Wiretap Act the definition of "electronic communication" found in § 2510(12)).

programs intercept files either before or after an electronic communication has transpired while the files are stored in a Web browser cache on the host machine. End-users' computers are electromagnetic systems that transfer signals from program to program or from end-user to end-user. As long as an end-user's computer is on the Internet, it is a system that affects interstate or foreign commerce. Therefore, whenever spyware mines end-user information that has been or will be transmitted to another user, the spyware accesses "electronic communications" for the purposes of the Stored Communications Act.

Some spyware programs could conceivably operate without mining "electronic communications" by merely searching installed program files or other files containing documents not intended to be electronic communications. Most spyware programs, however, focus on mining temporarily stored electronic communications to find personally identifiable end-user information that can be sold for advertising purposes or exploited by the spyware company itself. Invariably, spyware programs operating on end-user machines will gain access to some form of electronic communications and transmit them without authorization. Due to the difficulty of determining which files a spyware program has actually accessed, spyware developers should have the burden of proving that the spyware operated without accessing temporarily[221] or permanently[222] stored electronic communication files. Therefore, in the vast majority of scenarios courts will likely find that spyware accesses a wire or electronic communication as long as the alleging party can prove that the spyware program was installed and running on its machine.

5. Fifth Element: In Electronic Storage

The Stored Communications Act's fifth and final element is satisfied if the spyware program accesses information stored in electronic format. To satisfy this element, a plaintiff will only need to prove that a spyware program accessed information stored on an end-user's machine. The Stored Communications Act defines "electronic storage" as, "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication . . . ."[223] All spyware programs operate on end-users' machines and access information that is either stored

[221] Temporarily stored electronic communications include all keystrokes, pointer movements, and mouse clicks input by an end-user.

[222] Permanently stored electronic communications include all emails or instant messaging conversations that are stored on the end-user's facility.

[223] *See* 18 U.S.C. § 2510(17)(A) (2000).

in files on a hard drive, stored in a Web browser's cache, or temporarily stored in the operating system's cache. As soon as an end-user inputs a signal into a computer, that signal is transformed into a digital bit of data, which is transmitted by the operating system to the program being utilized by the end-user. If necessary, this information is then graphically represented on the end-user's computer, for instance, as an image on the monitor. Only after an input is converted into the form of a bit can a spyware program track the end-user's activity on the computer. Therefore, all information mined by spyware is in "temporary, intermediate storage . . . incidental to the electronic transmission thereof."[224] All information, including both saved files and end-user inputs, constitute electronic files in "electronic storage" for purposes of the Stored Communications Act's fifth element.[225]

6. Spyware Does Not Fall Within a Recognized Defined Exception

Spyware developers sued under the Stored Communications Act can defend themselves by showing that their conduct falls within a recognized exception as defined in subsection (c) of § 2701. These exceptions include: (1) conduct authorized "by the person or entity providing a wire or electronic communications service;"[226] (2) conduct authorized "by a user of that service with respect to a communication of or intended for that user;"[227] or (3) conduct authorized in § 2703, 2704, or 2518 of title 18,[228] which essentially amounts to honoring a governmental subpoena to acquire stored electronic communications in electronic storage.[229] For spyware operating on an end-user's computer to satisfy any of these exceptions, it

[224] *Id.*

[225] *See* Sherman & Co. v. Salton Maxim Housewares, Inc., 94 F. Supp. 2d 817 (E.D. Mich. 2000). In *Sherman* the court found that the appliance manufacturer failed to state a claim against its former sales representative who allegedly obtained the manufacturer's sales data from the retailer's computer network and gave information to a competitor under Section 2701 et seq. of the Electronic Communications Privacy Act ("ECPA") prohibiting intentional accessing of electronic data without authorization, absent allegation that the representative's prior authorization to use retailer's computer network had been revoked or limited. *See also In re* Pharmatrak, Inc. Privacy Litig., 329 F.3d 9. *See Steiger*, 318 F.3d 1039, *cert. denied*, 538 U.S. 1051 (2003) (holding computer hacker's acquisition of information implicating defendant in sexual exploitation of children and possession of child pornography through use of virus that enabled him to access and download information stored on defendant's personal computer did not violate the Wiretap Act, since there was nothing to suggest that any information was obtained by hacker through contemporaneous acquisition of electronic communications while in flight).

[226] 18 U.S.C. § 2701(c)(1) (2000).

[227] *Id.* at (c)(2).

[228] *Id.* at (c)(3).

[229] 18 U.S.C. § 2703(a) (Supp. III 2003) (requiring disclosure of customer communications or records to governmental entity with valid warrant); 18 U.S.C. § 2704(a).

would have to receive end-user consent to mine data or be served with a valid governmental subpoena requiring it to do so. Since these exceptions fall right back into the Stored Communications Act's second prong, these exceptions do not lend any real assistance to spyware developers except that authorization need only be received from someone who uses an end-user's system, not the actual end-user.

7. The Stored Communications Act's Ability to Prevent Spyware

Most spyware actions brought under the Stored Communications Act will hinge upon (1) authorization, and (2) whether the mined data was a stored "electronic communication." Spyware developers can avoid liability under the Stored Communications Act by "disclosing" their program's intentions to mine data somewhere in a EULA and having the end-user agree to grant the program authorization to do so.[230] Currently, spyware developers have a significant advantage over end-users because they can bury broad, complex provisions deep within boilerplate legalese that end-users are unlikely to read. Most end-users never read EULAs anyway, and if they do so, are unlikely to understand exactly what they will be authorizing a spyware program to do if they accept the agreement. Contract law, moreover, imputes a duty to read on all parties to a contract and will only offer an end-user respite if a term in the contract is ambiguous or unconscionable. If ambiguous, it will be interpreted against the drafter. By acquiring legal counsel to draft unambiguous, yet deceptively vague EULAs, spyware developers can protect themselves from liability under the Stored Communications Act. Unconscionability will, likewise, be of little use. No consumer can show coercion to enter a contract or uneven bargaining position, especially if the spyware is part of freeware.

Where a spyware developer fails to include an EULA, or a crucial term in an EULA is determined to be ambiguous, the spyware developer could be found liable under the Stored Communications Act as long as the program accessed stored "electronic communications." However, the "electronic communications" requirement enables spyware operating on an end-user's machine to mine program files and other end-user documents that were not transmitted to another user and that were never intended to be transmitted as electronic communications. While this gives spyware companies the ability to mine certain end-user data absent authorization without violating the Stored Communications Act, most spyware programs do not limit themselves to this noncommunicated information. In fact, the most valuable information to a spyware program is information that end-users intend to be electronic communications, such as user inputs into Web

[230] *See I.Lan Sys.*, 183 F. Supp. 2d at 338.

browsers. While the "electronic communication" requirement will give spyware developers a defense to certain types of data mining, most will not be completely protected based on their current operational tendencies. As a result, as long as an end-user can show that a spyware program mined data on its computer without authorization, which is not an easy task in this world of complex EULAs; the end-user will likely be able to state a cause of action under the Stored Communications Act.

D. *Spyware Invasions of Privacy and Intrusions Upon Seclusion*

A person is liable for invasion of privacy "if the intrusion would be highly offensive to a reasonable person"[231] and when that person "intentionally intrudes, physically *or otherwise*, upon the solitude or seclusion of another *or his private affairs or concerns* . . . ."[232] Based upon the definition in the Restatement (Second) of Torts, the intrusion into a computer by a software application intrudes upon the private affairs or concerns of the owner of the computer. Even the comments of the Restatement make it clear that using electronic means is a method that fits within the definition.[233]

The standard case of violation of an individual's rights of privacy leading to tort liability involves some sort of eavesdropping by one individual on another individual or groups of individuals.[234] From a digital standpoint, the closest analogies to spyware are electronic surveillance and eavesdropping cases.

The New Hampshire Supreme Court had occasion to examine the tort of intrusion upon seclusion in connection with a landlord who installed and concealed a listening and recording device in the bedroom of a tenant husband and wife.[235] The New Hampshire Supreme Court began the analysis by determining whether a tort for intrusion upon physical and mental solitude could lie in New Hampshire.[236] The court detailed the history of the tort of violation of privacy.[237] Even though this case does not concern the use of application software to invade a user's computer, it does concern electronic impulses—that is electronic recording of private conversations including telephone calls—and states "intrusion upon the

[231] RESTATEMENT (SECOND) OF TORTS § 652(B) (1977).

[232] *Id.* (emphasis added).

[233] *Id.* at cmt. b. (mentioning "with or without mechanical aids," "tapping his telephone wires," and "examining his private bank account.").

[234] *See, e.g., Hamberger*, 206 A.2d 239.

[235] *Id.* at 241–42.

[236] *Id.*

[237] *Id.* at 241 (discussing tort violation of privacy cases in New York, Georgia, and Rhode Island).

plaintiff's solitude or seclusion is not limited to a physical invasion of his home or his room or his quarters."[238] Based upon its analysis of cases elsewhere, the New Hampshire Court held that a tort action would lie for invasion of privacy by planting microphones or taping telephone conversations.[239]

The court did not seem to be concerned with the question of whether or not placing recording devices in a bedroom is offensive to a person of ordinary sensibilities.[240] Interestingly, the defendant argued that the tort should not be actionable in this case, because there was no evidence that anyone actually *listened* to the activities in the bedroom.[241] The court did not credit this argument but stated that whether or not anyone listened, the tort would be actionable.[242] The court anticipated future technological advances by observing that "[t]he use of parabolic microphones and sonic wave devices designed to pick up conversations in a room without entering it and at a considerable distance away makes the problem far from fanciful."[243] A spyware perpetrator is similar to the user of the parabolic microphone. However, this perpetrator operates from a greater distance, does not need to wait for the subject being spied upon to speak or enter a room, and can operate without ever entering the room him or herself. Instead, the perpetrator can spy from a considerable distance and can still eavesdrop upon what could be the most intimate details of the subject's life simply by rummaging about in that subject's computer.

A New Jersey court considered the tort of invasion of privacy with respect to computer records in a family law case.[244] In that case, the husband unwittingly saved emails from his girlfriend.[245] He believed that his emails could only be found by using a password..[246] The computer was left in the marital residence where any family member could access it.[247] Even though the court held that the wife's rummaging through the email files was no "different than rummaging through files in an unlocked file cabinet,"[248] the case is instructive concerning the tort of intrusion upon seclusion with respect to electronic records.

[238] *Hamberger*, 206 A.2d at 241.

[239] *Id.*

[240] *Id.* at 241–42.

[241] *Id.* at 242.

[242] *Id.* (citing Carr v. Watkins, 177 A.2d 841 (Md. 1962); Bennett v. Norba, 151 A.2d 476 (Pa. 1959); Norris v. Moskin Stores, Inc., 132 So. 2d 321 (Ala. 1961)).

[243] *Id.* (citation omitted).

[244] White v. White, 781 A.2d 85 (N.J. Super. Ct. Ch. Div. 2001).

[245] *Id.* at 88.

[246] *Id.* at 87.

[247] *Id.* at 92.

[248] *Id.*

The court began with the Restatement (Second) of Torts definition[249] and had no difficulty finding that accessing computer records fit within one of the comments; that is that the intrusion need not be physical.[250] However, the court has problems with whether the intrusion would be highly offensive "when the actor intrudes into an area in which the victim has either limited or no expectation of privacy."[251] Because the husband left the computer in a room to which his wife had access, the court held that he had *no* expectation of privacy as to the contents of the computer.[252] This case is troubling from the standpoint of the consumer who is attempting to acquire a remedy against the spyware perpetrator. The court states, "a person's expectation of privacy to a room used for storage and to which others have keys and access is not reasonable. Defendant's subjective belief that the room was private is 'irrelevant.'"[253] The user of a computer may or may not know that being connected to the World Wide Web by telephone line or otherwise gives another person access to certain information in the computer. Analogizing from this case, spyware perpetrators can argue that computer owners' beliefs that their information is private are irrelevant because the standard knowledge in the industry is that online computers communicate with other computers.

A more helpful case comes from the Supreme Court of New Hampshire.[254] The United States District Court for the District of New Hampshire certified certain questions of law to the New Hampshire Supreme Court. Essentially, the federal court wanted to know whether a private investigator who acquired private information (such as social security numbers), and gave that information to another (the person hiring the private investigator) would be liable under the tort of intrusion upon seclusion.[255] Liam Youens contacted an Internet-based investigation and information service, known as Docusearch, to acquire information about Amy Lynn Boyer.[256] Youens purchased Boyer's social security number and employment information from Docusearch, and "on October 15, 1999, Youens drove to Boyer's workplace and fatally shot her as she left

[249] RESTATEMENT (SECOND) OF TORTS § 652(B) (1977).

[250] *Id.* at cmt. b.

[251] *White*, 781 A.2d at 92.

[252] *Id.*

[253] *Id.* (citing State v. Brown, 660 A.2d 1221 (N.J. Super. Ct. App. Div. 1995). This is particularly troubling in light of the Supreme Court of Washington's holding in *State v. Townsend*, 57 P.3d 255 (Wash. 2002). That court held that a person using email may be assumed to know that it is being recorded somewhere even if the person lacks actual knowledge of digital processes. *Id.* at 260. Therefore, people using email are deemed to have consented to recording of messages. *Id.*

[254] Remsburg v. Docusearch, Inc., 816 A.2d 1001 (N.H. 2003).

[255] *Id.* at 1004–05.

[256] *Id.* at 1005.

work."[257] The court's analysis begins with a blanket statement that "[a]ll persons have a duty to exercise reasonable care not to subject others to an unreasonable risk of harm."[258] The court went on to hold that "a party who realizes or should realize that his conduct has created a condition which involves an unreasonable risk of harm to another, has a duty to exercise reasonable care to prevent the risk from occurring."[259]

With respect to the spyware perpetrator, this case seems to indicate that not only the perpetrator but also the beneficiary of the spyware insertion, namely the merchant receiving the information or receiving the redirected Web browser, may be liable. Under the reasoning in *Remsburg*, the spyware perpetrator and the merchant receiving the benefit of the invasion of a person's computer not only *realize* that the conduct creates a condition involving an unreasonable risk to a person's privacy, but actually *intend* to create that unreasonable risk. The court in *Remsburg* identified two risks that were reasonably anticipated, and in the case of spyware perpetrators, should lead them to anticipate a form of stalking and identity theft.[260] The court concluded that "an investigator has a duty to exercise reasonable care in disclosing a third person's personal information to a client."[261] The investigator is to exercise reasonable care to ensure that nothing harmful comes from the release of information. However, all spyware does not intend harm to the individual computer owner.

The court held that whether an intrusion "would be offensive to persons of ordinary sensibilities is ordinarily a question for the fact-finder and only becomes a question of law if reasonable persons can draw only one conclusion from the evidence."[262] The court refused to hold that, as a matter of law, a person has a reasonable expectation of privacy in a social security number.[263] The second part of the tort of intrusion on seclusion seems to be a question, like negligence, that normally must be determined by a jury. Considering the volume of personal information in a computer, courts may hold as a matter of law that the intrusion and interception of computer-stored personal information is offensive to persons of ordinary sensibilities; and no reasonable juror could hold otherwise. At least that is the argument plaintiff's counsel will make in consumer civil liability. The court cited to a Minnesota federal court opinion that lists the following factors: the degree of intrusion, the context, the conduct, the circumstances

[257] *Id.* at 1005–06.

[258] *Remsburg*, 816 A.2d at 1006 (citation omitted).

[259] *Id.* at 1007 (citation omitted).

[260] *Id.*

[261] *Id.* at 1008.

[262] *Id.* (citation omitted).

[263] *Id.*

surrounding the intrusion, the intruder's motives and objectives, and the expectation of privacy of the person invaded.[264] Consumers will argue that based upon the context, the degree of intrusion, and the intruder's profit motives, courts should hold as a matter of law that invasion of a computer by spyware is objectively unreasonable and offensive.

The problem with tort liability for either this tort or the tort of trespass to chattels is damages. From a practical standpoint, who will bring these claims? First, consumers' actual damages will be minimal. Spyware may annoy consumers and even require them to spend hours trying to remove the offending applications, but few individuals will have sufficient damages to lead them to pursue a remedy. Moreover, with limited damages attorneys will not institute litigation because the client will not pay an hourly rate, and the attorney will starve on contingency arrangements unless the firm can identify enough victims for a class action.

E. The Wiretap Act, Spyware, Grokster, Napster, and Developers

Today, courts face a new situation where technology creators continually side-step laws meant to prevent their actions by breaking up software actions into multiple separate steps.[265] A prime example of the effects of technological "evil"ution is the Wiretap Act, which has been rendered significantly less effective by the legislature and the courts, which have both limited its provisions to protect only interceptions of communications in transit.[266] While this Wiretap Act construction

[264] *Remsburg*, 816 A.2d at 1009 (citing Bauer v. Ford Motor Credit Co., 149 F. Supp. 2d 1106, 1109 (D. Minn. 2001)).

[265] *See, e.g.*, Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd. 545 U.S. 913, 125 S. Ct. 2764, 2765 (2005) (holding that "[i]t is undisputed that StreamCast beamed onto the computer screens of users of Napster-compatible programs ads urging the adoption of its OpenNap program, which was designed, as its name implied, to invite the custom of patrons of Napster, then under attack in the courts for facilitating massive infringement.").

[266] Intertwined with the intent and consent elements in interpreting the Wiretap Act is the storage-transit dichotomy. Circuits that narrowly read the Wiretap Act require the interception to be contemporaneous with transmission. *See In re Pharmatrak, Inc. Privacy Litig.*, 329 F.3d at 21. Under this standard it is possible for a defendant to argue that there are two separate communications: one between the end-user and the intended Web Portal, and the second between the end-user and the spyware technology. *See* Chance v. Avenue A, Inc., 165 F. Supp. 2d 1153, 1155–57 (W.D. Wash. 2001); *In re DoubleClick Inc. Privacy Litigation*, 154 F. Supp. 2d at 503–04; *In re Pharmatrak, Inc. Privacy Litig.*, 329 F.3d at 12; *In re Intuit Privacy Litig.*, 138 F. Supp. 2d at 1275–76. Under this argument, a spyware program becomes a party to the conversation authorizing its interception of the data under the Wiretap Act. *See In re Pharmatrak, Inc. Privacy Litig.*, 329 F.3d at 19–22. Since the Wiretap Act allows either party to consent to the recording of data communications, the spyware program is not violating the Wiretap Act. This is permissible because the Wiretap Act presupposes that both parties to the conversation had knowledge that a conversation was in fact taking place. 18 U.S.C. § 2511(2)(d) (2000) (stating "[i]t shall not be unlawful for . . . a person not acting under color of state law to intercept . . . communication where such

adequately protects point-to-point telephone calls placed over the Public Switched Telephone Network ("PSTN"), it does not adequately protect electronic communications sent over the Internet, such as VoIP, which may be instantaneously stored on a server before, after, or during their transmission.[267] These temporary stops along the way enable programmers to take advantage of the Wiretap Act by developing programs that copy or intercept the communications while they are in the temporarily stored state and are not in transmission.[268] A notable number of spyware applications intercept data prior to transmission, thereby avoiding potential liability under the Wiretap Act.[269]

Spyware programs intercepting electronic communications while in transmission violate the Wiretap Act unless one of the parties to the communication consents to the interception.[270] While a few spyware programs still intercept electronic communications in transmission, most spyware programs avoid Wiretap Act liability by mining end-user data and electronic communications while they reside on the end-user's system prior to actual transmission. By copying the communications in an instant prior to transmission, most spyware programs intercept end-user electronic communications without being in direct violation of the current judicial construction of the Wiretap Act.[271]

1. The Wiretap Act Falls Short in Preventing Spyware from Operating

Whether deliberate or not, spyware companies have created a set of products capable of bypassing the Wiretap Act to accomplish exactly what it forbids—the interception of third-party communications without

person is party to the communication or when one of the parties has given prior consent"). Here, the end-user can assert that they lacked such knowledge and did not consent to the communication, but unfortunately, the law has precluded the end-user from asserting that the transmission occurred without their consent. *Id.*

[267] *See* Garrie et al., *supra* note 13, at 101, 120–22.

[268] *See* Garrie et al., *supra* note 13, at 121.

[269] *See, e.g.*, U.S. v. Ropp, 347 F. Supp. 2d 831 (C.D. Cal. 2004) (finding that because the captured keystrokes were not transmitted by a system that affects interstate commerce, spying with the device did not violate the federal act because it did not intercept the communication while it was being transmitted).

[270] *See* O'Brien v. O'Brien, 899 So. 2d 1133, 1136–37 (Fla. Dist. Ct. App. 2005) (distinguishing between a spyware program that breaks into a computer and retrieves information already stored on the hard drive, and a spyware program that copies the communication as it is transmitted and routes the copy to a storage file in the computer).

[271] *See, e.g.*, *EF Cultural Travel BV*, 274 F.3d at 581–82, n.10 (explaining, with respect to alleged unauthorized use of a Web site, Congress' failure to define "without authorization" in the CFAA, and discussing some possible, practicable definitions of the term).

consent.[272] Spyware achieves this feat through a two-step process whereby it first records end-user keystrokes,[273] pointer movements, and mouse clicks while an end-user views data on a computer; and in a second step, it transfers the data to an authorized server.[274] Spyware transactions are thus analyzed under the Wiretap Act as two distinct transactions: (1) data recording and (2) data transmission. In the recording phase, spyware tracks an end-user's keystrokes, pointer movements, and mouse clicks on a Web page viewed on the end-user's machine; or it records other transactions made on the local machine, such as altering a word or document or composing an email. In the transmission phase, spyware transmits the information it has recorded to the spyware's server.[275]

The act of combining these two actions enables spyware companies to intercept end-users' communications with Web Portals, friends, businesses, and other parties of interest.[276] In the present day, these "interceptions" fail to trigger civil or criminal liability under the Wiretap Act because neither step of the process contains an *unauthorized* third-party interception of an electronic, oral, or wire communication. The Wiretap Act specifically permits the intentional interception of wire, oral, or electronic communications[277] without a court order[278] as long as one of the parties to the communication consents to the interception.[279] By dividing the data-recording and transmission phases into two distinct acts, spyware does not violate the Wiretap Act because during the recording phase, the spyware "intercepts" the data before a transmission has taken place. Furthermore, during the transmission phase, both the spyware program itself and the spyware server "consent" to the data transmission, enabling the entire transaction to fall within the Wiretap Act's consent exception.

a. Recording Phase

During the recording phase, spyware does not *intercept* a real-time

[272] *See supra* Part II.

[273] *See, e.g.*, *Ropp*, 347 F. Supp. 2d at 831 (finding that because the captured keystrokes were not transmitted by a system that affects interstate commerce, spying with the device did not violate the federal act).

[274] Spyware is capable of transmitting much more than the Web shopping patterns of the end-user. This technology has the ability to transmit data stored on a machine.

[275] *See* Deborah Radcliff, *Spyware*, NETWORK WORLD, Jan. 26, 2004, at 51.

[276] "I agree with the Court that the distributor of a dual-use technology may be liable for the infringing activities of third parties where he or she actively seeks to advance the infringement." *Grokster*, 125 S. Ct. at 2787 (2005) (Breyer, J., concurring).

[277] 18 U.S.C. § 2511 (2000).

[278] *See* 18 U.S.C. § 2518 (2000) (limiting court-ordered surveillance to law enforcement bugs or wiretaps and establishing strict requirements for court-authorized interceptions of wire communications).

[279] 18 U.S.C. § 2511(2)(c)-(d) (2000) (containing consent exceptions).

third-party electronic communication sent over a wire in interstate commerce because the data resides entirely on the end-user's machine.[280] However, spyware does violate the Wiretap Act if it intercepts "electronic communications" in transient electronic storage that is intrinsic to the communication process.[281] Most spyware programs record data after it is input by the end-user but before the data is actually transmitted over the Internet.[282] The temporal difference between recording stored communications as opposed to transmitting electronic communications could be miniscule. Nonetheless, as long as the spyware records the data while it resides on the end-user's machine before it is transmitted, the spyware application has not violated the Wiretap Act. For example, when an end-user requests a Web page, a Web Portal transmits the Web page to the end-user's machine.[283] The Web page is then displayed on the end-user's own machine where the end-user can edit fields prior to the retransmission of data to the Web Portal that occurs once the end-user clicks a hypertext link.[284] A "communication" transpires for purposes of the Wiretap Act only when the end-user transmits data to the Web Portal.[285] As long as the spyware merely records the end-user's field inputs prior to resubmission of the information, no "interception" of an electronic communication sent over interstate lines has taken place, and the spyware publisher faces no liability under the Wiretap Act.

Although spyware creators can tap dance their way around the Wiretap Act's provisions by recording end-user data before transmission, they can still be found liable under the Wiretap Act for recording real-time

[280] *See* David M. Martin, Jr. et al., *The Privacy Practices of Web Browser Extensions*, 44 COMMC'N OF THE ACM 45, 48 (2001).

[281] *See* United States v. Councilman, 418 F.3d 67, 85 (1st Cir. 2005).

[282] *See* Conrad Burns, *Communications Policy for the Next Four Years*, 57 FED. COMM. L.J. 167, 169 (2005); Paula J. Bruening & Michael Steffen, *"Spyware": Technologies, Issues, and Policy Proposals*, 7 J. INTERNET L. 3, 6 (2004).

[283] *See* Martin et al., *supra* note 280.

[284] The World Wide Web enables an end-user to access a Web page, or other "resource," on the World Wide Web, by "typing the URL of the page" into their browser, or "by following a hypertext link to that page or resource." *See* Wikipedia, World Wide Web, How the Web Works, http://wikipedia.org/wiki/Worldwide_Web#How_the_web_works (last visited Nov. 12, 2006). "The first step, behind the scenes, is for the server-name part of the URL to be resolved into an IP address by the global, distributed Internet database known as the Domain name system or DNS." *Id.* Second, the end-user's HTTP request is sent to the Web server working at that IP address for the page required. *Id.* "The web browser's job is then to render the page as described by the HTML, CSS and other files received, incorporating the images, links and other resources as necessary" so that it "produces the on-screen 'page'" that is displayed to the end-user. *Id.*

[285] *See Councilman*, 418 F.3d at 85 (holding that the term "electronic communication" includes transient electronic storage that is intrinsic to the communication process, and hence, that interception of an email message in such storage is an offense under the Wiretap Act).

end-user communications. Under *United States v. Councilman*, spyware creators will be liable for making unauthorized interceptions of electronic communications in transient electronic storage that is intrinsic to the communication process.[286] For example, a spyware program monitoring fields input by an end-user on a real-time Java Applet could violate the Wiretap Act if the end-user's inputs are simultaneously being transmitted to another end-user.[287] Similarly, a spyware program running with system privileges could record inputs by an end-user onto a word document stored on a communal server where multiple end-users are involved in editing the document at the same time. In both of these situations, the spyware is intercepting end-user electronic communications in violation of the Wiretap Act because the end-user's inputs are being intercepted while being transmitted to other users.[288]

Spyware providers in the previously mentioned scenarios can still plead a consent defense arguing that the end-user offered either explicit or implicit consent to the third-party monitoring.[289] Spyware is most commonly loaded on an end-user's machine as a component of other "free" programs.[290] While end-users explicitly consent to the EULA terms of the entire software package, they do not explicitly consent to the capabilities and nefarious uses of the spyware[291] portions unless the capabilities of the spyware program are included in the EULA and the consumer reads it in its entirety. If so, spyware providers will have a strong defense for purposes of the Wiretap Act, since courts require consent to be actual, although it can be implied or explicit.[292] End-users may be able to overcome the consent defense if the EULA terms regarding the spyware are ambiguous or nonexistent. However, as long as the spyware discloses in the EULA that it will record information, end-users will have no cause of action under the Wiretap Act. Unfortunately, most end-users fail to read the EULA closely because they either cannot understand the terms of the contract, have no desire to read the contract, or have no conception of the risk that the contract could pose to their personal information.[293] Spyware distributors

[286] *Id.*

[287] *See, e.g.*, Eric Doyle, *Not All Spyware is as Harmless as Cookies: Block It or Your Business Could Pay Dearly*, COMPUTER WEEKLY, Nov. 25, 2003, at 32 (examining the various technologies that can be used to invade a user's machine and how they operate.)

[288] *See* Farrow, *supra* note 3, at 53.

[289] *See* Garrie et al., *supra* note 13, at 100, 118–19, 127.

[290] *See e.g.*, Scumware, *supra* note 17.

[291] *See generally Cybersecurity and Consumer Data: What's at Risk for the Consumer?: Hearing Before the H. Subcomm. On Commerce, Trade, and Consumer Prot. of the Comm. on Energy and Commerce*, 108th Cong. 61–63 (2003) (statement of Roger Thompson, Vice President of Product Development, PestPatrol).

[292] *See In re Pharmatrak, Inc. Privacy Litig.*, 329 F.3d at 19.

[293] A proposed solution would be for a law requiring all software containing spyware

exploit the general cultural apathy towards reading legalese, thereby acquiring end-user consent for virtually limitless electronic privacy transgressions. Nowadays, spyware is an enormous problem; in fact, some experts estimate that up to 80 percent of the machines have some form of spyware loaded unbeknownst to the user.[294] Unfortunately, due to the lax consent requirement and the restrictive interstate transmission requirement, the Wiretap Act is unable to protect most end-users from spyware's invasive tendencies.

b. Transmission Phase

The Wiretap Act's lax requirement of unilateral consent grants spyware developers nearly absolute protection from liability under the Wiretap Act when the spyware transmits data to the main server. The Wiretap Act only prohibits the intentional interception of wire, oral, or electronic communications[295] without a court order[296] if neither party to the communication consents to the interception.[297] Generally, courts can find that it is tautological that the spyware server receiving the data transmission from the end-user's computer consents to the receipt of the transmission. Therefore, it is irrelevant whether the party unknowingly "sending" the data actually consents to the transmission since the Wiretap Act only requires one of the two parties to consent. Because courts never reach the question of whether the transmitting party consents to the recording, courts need not consider whether the identity of the transmitting "person" is the spyware software, the end-user, or the end-user's computer. This ambiguity need not be resolved in a Wiretap Act analysis, although it could become a serious issue under individual state wiretapping acts, some of which require all parties to consent.

2. Conclusion: Spyware Faces Limited Liability Under the Wiretap Act

Spyware is usually designed to copy and transmit information input

to list at the top of the EULA in bold, capital letters, all of the capabilities of the spyware and the data that it will track. This law would also state that consumers cannot impliedly or explicitly consent to spyware interceptions unless the provisions of this law are followed. This would help push spyware under the Wiretap Act (although still unlikely because no "interception of a communication" takes place) as well as empower consumers to bring trespass to chattels claims against spyware distributors.

[294] *See* Metz, *supra* note 14, at 79-80.

[295] 18 U.S.C. § 2511 (2000).

[296] 18 U.S.C. § 2518 (2000) (limiting court-ordered surveillance to law enforcement bugs or wiretaps and establishing strict requirements for court-authorized interceptions of wire communications).

[297] 18 U.S.C. § 2511(2)(c)-(d) (2000) (containing consent exceptions).

into or stored on an end-user's computer, not to intercept electronic communications. The well-planned separation of data mining into the two separate steps of recording and transmission protects the majority of spyware data mining transactions from liability under the Wiretap Act. The required transmission over a wire in interstate commerce protects the majority of interceptions from liability in the recording phase while the lax unilateral consent requirement protects nearly all spyware transmissions from liability in the transmission phase. Spyware could, however, still face some potential liability under the Wiretap Act in the recording phase for transactions involving recording real-time end-user inputs that are simultaneously transmitted to other end-users.

In summation, spyware that either records end-users' keystrokes, pointer movements, and mouse clicks,[298] or transmits data stored on the end-user machine before the end-user communications are transmitted to a Web Portal faces no liability under the Wiretap Act.[299] While there is some potential liability under specific and more stringent state wiretapping statutes, there are many obstacles to bringing a successful claim. Whether by accident or by careful design, spyware developers have created software that does an end-run around the Wiretap Act. Courts making strict, literal, and statutory interpretations have all but eliminated the Wiretap Act's viability as a cause of action against spyware or any other electronic communication mining tools that copy only temporarily stored information without actually intercepting communications in transit. It remains to be seen whether this constructionist trend will continue unabated or shift toward a focus on statutory intent, following the Supreme Court's *Grokster* decision.

IV. SOLUTION TO CLOSE LOOPHOLE THAT ENABLES SPYWARE TO BYPASS THE LEGAL SYSTEM

Spyware victims have several legal vehicles as discussed above; however, no single cause of action provides the "silver bullet." Spyware is an epidemic generating innumerable privacy rights violations, causing identity theft with actual economic loss to individuals, resulting in loss of proprietary business information, as well as causing significant damage to infected personal computers or corporate computer systems. Presently, spyware victims must patch together a web of complex federal statutes and

[298] Monitoring mouse clicks may lead to liability under the Wiretap Act because as soon as the mouse is clicked on a link, a communication has been initialized, and the spyware is then "intercepting" that communication, albeit very close to the source on the end-user's computer. In addition, the transmission of other information that is of a private nature might constitute a cause of action under the concept of digital theft.

[299] Companies that produce spyware that does more than log keystrokes, cursor movements, or mouse clicks would be potentially liable under the Wiretap Act.

state common law theories instead of having a straightforward cause of action. While all of the potential remedies described above may provide assistance for some consumers and businesses in certain countries under the right circumstances, most spyware has been able to bypass any criminal or civil liability.

A. Anti-spyware Legislation: Multi-Click Consent Agreements Analogous to Initialing Each Pertinent Point Respective to Data Mining Performed by the Software Provider

Requiring by statute both general acceptance of EULA terms as well as specific acceptance at all relevant points where access is granted to the user's personal information would minimize unknowing consent by the end-user and consequently eliminate most spyware. Such a multi-click consent agreement itself should use language that can be understood by the least sophisticated consumer.[300]

This multi-click consent solution has two components. First, the consumer is required to consent through a series of "clicks." Second, the spyware vendor must retain the multi-click consent agreement. However, prior to the user's even addressing the details of the consent agreement, it is imperative that the vendor provide the user with a warning that clicking on the agreement has the same legal effect as physically signing a piece of paper. The end-user must comprehend that clicking "accept" is identical to "signing on the dotted line."

Only after the end-user understands the ramifications of "clicking" may the vendor present a multi-click consent EULA. This EULA should provide an overview of each portion of the agreement in plain English[301] and require the user to click "ok" for each clause relevant to the transmission of personal information to a third-party vendor, thereby signifying that the end-user read and consented to that use of personal information.[302] Essentially, each clause pertaining to data transmission of

[300] This standard appears in many existing federal consumer statutes. For instance, the Fair Debt Collection Act does not require the consumer to prove he or she was *actually* misled, but uses an "unsophisticated consumer" standard to determine whether a communication is misleading. *See, e.g.*, Peters v. General Service Bureau, Inc. 277 F.3d 1051, 1056 (8th Cir. 2002).

[301] The language of the EULA must be written with the understanding that the end-user is not a lawyer or a programmer. Therefore, any legal or technical language must be carefully defined in simple terms.

[302] The EULA should also provide the users with examples of the explicit information that the spyware agreement enables the program to mine from their machines. While the EULA currently may state that information is mined, under current practice it is unlikely that even the users who have read the EULA before clicking through can understand what data is being appropriated or the ramifications of its being mined. An example might read, "By installing this spyware application, you are consenting to the transmission of personal

personal data should require a check box to be clicked.

For instance, "piggyback spyware" applications such as Kazaa would no longer be able to embed a provision in their EULA granting consent to the installation of spyware applications that are invisible to the user. Instead, the multi-click EULA would bring a specific consent component to the user's attention that would only grant the spyware permission to install and operate on the user's machine *after* the user is informed in plain and unambiguous language of the personal data that the spyware may record and, potentially, transmit. Therefore, Kazaa and other such "piggyback spyware" that operates with a current EULA loophole would be greatly limited. They would likely be unable to obtain the average end-user's consent to the software installation once the ramifications are explained in a lengthy and easy to understand EULA in plain English that the end-user can only accept in small portions. This first component will better protect users against "piggyback spyware" applications because multi-click consent in plain English ensures that users are no longer unknowingly consenting to the installation and operation of spyware applications through a cumbersome, incomprehensible, and generally unread EULA.[303]

The second statutory component requires vendors to store the user's multi-click consent on their servers for as long as they use, sell, or collect the user's data. By compelling storage of the multi-click consent, the valid commercial user can show consent to rebut claims by users that the companies' spyware operated in a manner "invisible" to the user. For instance, a company could rebut a user's claim that the company obtained personal information without the user's consent with documentary evidence of the user's explicit multi-tiered consent to the installation and operation of the software. Commercial users consequently have a viable affirmative defense, and the judiciary gains a mechanism permitting judges to differentiate between nefarious and permissible spyware.

The multi-click consent solution enables the law to differentiate between data mining by companies that monitor pages visitors view on their own Web sites (a practice with clear commercial advantages that does not violate the end-user's personal privacy) from data mining done by spyware programs actually installed on the end-user's personal computer to monitor keystrokes, passwords, and other personal information without the user's consent.[304] Documenting this distinction will facilitate civil and criminal prosecution of unlawful spyware because such unlawful vendors

information. This information includes the following . . . . . Examples of such data are as follows. 1. Mary J. Jenkins; 07/05/1969 DOB, etc."

[303] *See I.Lan Sys.*, 183 F. Supp. 2d at 338.

[304] It is beyond the scope of this Article to provide the technical details of how such technology would operate, but further information is available from Daniel Garrie.

would lack the users' consent, whereas lawful vendors would have the users' consent.[305] Thus, the multi-tiered consent solution directly addresses unlawful spyware while directly addressing the highly problematic "piggyback spyware" issue. Most importantly, even the average user will be protected from the misleading and cumbersome consent agreements through which "piggyback spyware" currently operates.

Ideally, anti-spyware legislation gives the best overall solution to users in the United States. This solution could be achieved by amending the Stored Communications Act to heighten the requirements for "authorization" and "consent." Increasing the disclosure and consent requirements for obtaining "authorization" and "consent" enables both general and specific programs to operate and ensures the end-users know to what datasets they are granting the programs access.[306] Consequently, this solution allows the market's invisible hand to re-allocate resources in a manner consistent with society's desires, and it does not eliminate legitimate data mining and harvesting businesses because users control the data on their machines. Moreover, it grants these vendors legitimate and effective affirmative defenses which hinge on the fact that they can demonstrate both "authorization" and "consent" occurred between their product and the end-use.[307]

Finally, a multi-click EULA incorporation into the anti-spyware legislation will ensure that any litigation pertaining to spyware has specific elements and components that the defendant failed to meet. Such legislation could mirror current federal consumer legislation such as the Fair Debt Collection Practices Act ("FDCPA")[308] that authorizes statutory remedies and attorney's fees for the prevailing consumer, envisions class actions, and sets a "least sophisticated consumer" standard. In 1977 Congress amended the Consumer Credit Protection Act to create the FDCPA.[309] It specifically found that "[e]xisting laws and procedures for redressing the[ ] injuries are inadequate to protect consumers."[310] Similarly, Congress should find that existing laws, both statutory and based

[305] The EULA should also detail the fact that the spyware will be transmitting data over the Internet, perhaps incurring Internet data transmission fees to the end-user as well as subjecting it to further interception by others.

[306] One possibility is to require these programs to disclose the specific data they are accessing and/or mining in bold letters at the top of the EULA.

[307] The adoption of this solution could also create a market for different types of spyware that mine different types of data. In this way, consumers could select freeware and shareware programs based on the capabilities of the bundled spyware and the consumers' valuation of the data that would be mined.

[308] *See* 15 U.S.C. § 1692 (2000).

[309] *See* Pub. L. 95-109, §§ 802 et seq., 91 Stat. 874 (codified at 15 U.S.C. §§ 1692 et seq.) (1977).

[310] 15 U.S.C. § 1692(b) (2000).

on common law torts, are inadequate to address similar abusive and deceptive[311] practices of spyware on behalf of consumers. Just as with debt collection, spyware "practices are carried on to a substantial extent in interstate commerce and through means and instrumentalities of such commerce,"[312] justifying congressional action.

Because few debt collection practices gave rise to sufficient damage to encourage private enforcement, but were collectively significant in leading to, among other things, "invasions of individual privacy,"[313] Congress fashioned an appropriate remedy in the spyware context for the same reasons. First, Congress authorized private rights of action[314] for individual actions of actual damages and created statutory damages of no more than $1,000.[315] Furthermore, the FDCPA authorized attorneys' fees and costs to the prevailing plaintiff.[316]

Perhaps most importantly, Congress gave explicit authorization of class actions with actual damages for each individual, as well as statutory damages not to exceed the lesser of $500,000 or one percent of the defendant's net worth.[317] The attorneys' fees provision[318] also applies to class actions. To protect the debt collector operating in good faith who makes a simple error, Congress inserted the opportunity for that defendant to show "by a preponderance of evidence that the violation was not intentional and resulted from a bona fide error notwithstanding the maintenance of procedures reasonably adapted to avoid any such error."[319] Finally, Congress created concurrent jurisdiction between state and federal courts.[320] While abusive practices of debt collectors still occur, by and large the statute has successfully curtailed such practices while ensuring that those who collect debts using non-abusive means "are not competitively disadvantaged . . . ."[321]

If lawmakers did pass such anti-spyware legislation including a multi-click EULA component, programs that auto-update on behalf of the end-user and any other action the end-user approves would automatically be exempted because the end-user would already have given informed consent. Consequently, such legitimate businesses would find protection in

[311] *See id.* § 1692(a).
[312] *Id.* § 1692(d).
[313] *Id.* § 1692(a).
[314] *Id.* § 1692k(a).
[315] 15 U.S.C. §§ 1692k(a)(1), (a)(2)(A).
[316] *Id.* § 1692k(a)(3).
[317] *Id.* § 1692k(a)(2)(B).
[318] *Id.* § 1692k(a)(3).
[319] *Id.* § 1692k(c).
[320] 15 U.S.C. § 1692k(d).
[321] *Id.* § 1692(e).

the legislation. The proposed legislation, however, should ensure that anything that is added or installed without the end-user's consent as reflected in the multi-click EULA requirements or installed on a computer on behalf of someone other than the actual owner of the machine is a violation of the anti-spyware legislation.

1. Global Spyware and the Data Mining Industry

While amending the United States' law would notably improve the situation with respect to spyware, it would not end the spyware epidemic. Spyware is a borderless pandemic—spyware vendors could still operate effectively outside the reach of the United States jurisdiction. Therefore, in order to effectively implement a multi-click consent EULA, a uniform law should be developed standardizing the enforcement of spyware control worldwide. Until the vast majority of governments address spyware through multi-click consent, spyware vendors will continue to capitalize on different countries' laws.

While the data mining and spyware industries may be likely to resist any such multi-click consent requirement, spyware is analogous to cigarettes in that consumers should, at the very least, be informed of the potential harm that they may incur. Even though cigarette manufacturers resisted warnings, many countries require them for the physical health of their citizens. Similarly, countries should require multi-click consent requirements for the "privacy health" of their citizens. Like cigarette smokers, end-users would still be able to allow spyware to operate on their systems if they chose to do so. The significant difference would be that the end-users would be able to make an informed choice—just as those who smoke presumably know of the harms that prolonged exposure to noxious cigarette fumes can cause to their bodies. Utilizing this multi-click consent approach and incorporating explicit and understandable consent language would greatly alleviate unwanted privacy intrusions by data mining programs.[322] A civil enforcement giving significant civil damages to aggrieved individuals irrespective of their actual losses can help ensure that perpetrators who mine personal data without informed consent are brought to justice.[323]

2. Potential Non-Statutory Solutions

While the international community is increasingly regulating activities on the Internet with promising positive law,[324] another viable tool

[322] *See* Blakley et al., *supra* note 36, at para. 32.

[323] *See* Daniel B. Garrie, *Warning: Software May be Hazardous to Your Privacy!*, 2 J.L. & POL'Y FOR THE INFO. SOC'Y (2006).

[324] *See generally* Mary Rundle, *Beyond Internet Governance: The Emerging*

for preventing spyware privacy infringements is to give courts greater, prompt access to information about emerging technologies and their potential to violate individuals' rights. It is imperative that courts around the world be informed so they can be empowered to apply existing privacy laws in their respective countries to new cases involving data processing disputes. This is especially true because many countries have adopted legislation, such as the European Directive of 1995[325] that could be applied to spyware. Unfortunately, the technological underpinnings are increasingly complicated, and judges need to have access to all available information to fully understand the technologies and how they are being used, or could be used, to violate the law. For instance, the Reference Scientific Manual[326] is used by United States federal judges to cover various complex technological and scientific issues with which they may be unfamiliar. To date, it does not have any pertinent information on spyware or other complex Web-enabled software. This void in technological reference material and education should be corrected by providing an educational curriculum accessible to judges.

Such a curriculum might include a combination of online, in-person, and paper materials; and it could utilize a variety of educational tools so as to maximize accessibility to all judges across national borders. By standardizing not only data mining law, but also the technical education and methods of applying such laws to specific cases, those who use spyware technologies for unethical ends will be at a tremendous disadvantage. Judicial education would help to establish a complete and potentially consistent body of case law in the international community because judges would have full understanding of how much privacy infringement data mining technologies are capable of having. Ideally, an internationally standardized technology curriculum for judges could be an extremely useful aid to justices presiding over privacy disputes involving new technologies.

B. Legislative Intent Is Accepted by Courts

Instead of waiting for the legislature to act, the courts could act now to slow the spyware dilemma. Today courts are faced with a new situation

International Framework for Governing the Networked World (The Berkman Center for Internet & Soc'y at Harvard Law School, Research Publication No. 2005-16, Fall 2005) *available at* http://cyber.law.harvard.edu/home/uploads/514/2005_Rundle_BeyondInternet Governance.pdf. (detailing ways in which countries can regulate the Internet).

[325] Council Directive 95/46, 1995 O.J. (L 281) 31 (EC) [hereinafter Directive 95/46/EC].

[326] REFERENCE MANUAL ON SCIENTIFIC EVIDENCE (Federal Judicial Ctr. ed., 1994) [hereinafter REFERENCE MANUAL].

where creators of software[327] continually side step laws meant to prevent their actions.[328] A prime example of where a firm grasp of software played a notable role is in *Grokster,*[329] where the Supreme Court held that a software distributor of multiple use technology might be liable for the infringing on activities of third parties where the parties actively seek to advance the infringement.[330] The Court further held that the lower courts must be mindful of technology developers who, with devious intent, successfully code around the law.[331] *Grokster* compels lower courts to examine whether the design of a software application is sought to side step the law.[332] Although *Grokster* is applicable only in the copyright realm, the Supreme Court's focus on the inner-workings of filesharing technology demonstrates the growing need for judges to hear such matters to possess a framework for understanding software and to examine the intent of the legislature that passed the original statute. Perhaps the Supreme Court points the way for lower courts to find new ways to address the spyware problem. In *Grokster,* the Court is arguably reversing a long-standing legal trend by moving away from a literal application of common law authority and statutes, especially those dealing with technological matters, when the "full transaction" clearly violates a legal principle or the drafters' intent.

[327] Computer "software" is generally defined as that material, separable from the "hardware," or physical equipment which comprises the computer programs and instructions. *See generally* William A. Fenwick & Gordon K. Davidson, *Admissibility of Computerized Business Records*, 14 AM. JUR. PROOF OF FACTS 2D 173. Software has also been more widely defined as all those aspects of the computer which are not hardware, and thus includes such known programming elements as educational material, manuals, training of personnel, and perhaps even maintenance of the hardware. *See* John G. Martin, Note, *The Revolt Against the Property Tax on Software: An Unnecessary Conflict Growing out of Unbundling*, 9 SUFFOLK U. L. REV. 118 (1975). For the purposes of this annotation, the category of computer software includes (among other items) computer programs, the media on which they were recorded, and the services which may be rendered to the computer purchaser by the manufacturer after purchase of the machine; only the computer machinery itself is considered hardware.

[328] *See Grokster*, 125 S. Ct. at 2780 (holding that "[i]t is undisputed that StreamCast beamed onto the computer screens of users of Napster-compatible programs ads urging the adoption of its OpenNap program, which was designed, as its name implied, to invite the custom of patrons of Napster, then under attack in the courts for facilitating massive infringement.")

[329] In *Grokster*, the Supreme Court found that although the black letter of the law had been followed in the context of determining liability, the intent behind the specific actions directed the outcome against Grokster. 125 S. Ct. at 2767.

[330] *Id.* at 2787 (Breyer, J., concurring).

[331] *See generally id.* at 2791–92 (Breyer, J., concurring); Cable/Home Communication Corp. v. Network Productions, Inc., 902 F.2d 829, 842, 847 (11th Cir. 1990); Vault Corp. v. Quaid Software, Ltd., 847 F.2d 255, 262 (5th Cir. 1988); Doe v. GTE Corp., 347 F. 3d 655, 661 (7th Cir. 2003) ("A person may be liable as a contributory infringer if the product or service it sells has no (or only slight) legal use . . . .").

[332] *See Grokster*, 125 S. Ct. 2764.

While the *Grokster* decision narrowly applies only to copyright violations, the Supreme Court's method of focusing on the distributor's intent and the product's advertised use may influence lower courts to broadly construe other common law holdings and statutes dealing with technology to prevent programmers from taking advantage of rigid legal constructs. In the context of spyware programs, a compelling argument can be raised that while spyware does not violate the letter of the Wiretap Act when viewed on microscopic or micro-temporal levels, it violates the spirit of the law and should be considered to violate the Act when spyware programs are constructed deliberately to intercept electronic communications, even if those communications are stored instantaneously on a server. By doing so, the courts would both deter devious technological development occurring at the edge of legality and would prevent the common law and statutes from having their power and effectiveness constantly whittled away by individuals looking for legal avenues to perform lucrative business acts that require them to "break the law."

When dealing with nefarious technological innovation, courts should not require the legislature to be exceptionally vigilant because doing so would force the legislature to constantly redraft and repass legislation every few years as technologists find ways around existing laws. Instead, courts should begin interpreting technological statutes broadly to enforce the statutory intent when technologists continuously attempt to contravene the statutes' purposes through technological "evil"ution. While the Supreme Court's *Grokster* decision is a significant step in the right direction, it is unlikely that lower courts will move noticeably away from the literal interpretation framework they have used in the past. Therefore, the most pragmatic solution is for state legislatures or Congress to draft provisions that prevent technologists from creating products designed to avoid statutory liability but that violate the spirit of the law.

V. CONCLUSION

The existing tort theories of liability and statutes do not provide consumers an adequate remedy for spyware perpetrators. Perhaps some of the theories may help large corporations that have extensive damage. Perhaps some attorneys may bring claims as class actions. However, generally, the availability of defenses such as authorization based on implied consent in a lengthy, legalistic EULA, eviscerates such relief. Furthermore, the limited damages available to the consumer reduce the likelihood of finding meaningful representation.

Courts' interpretations of the statutes are inconsistent, and courts' applications of tort liability depend upon each of the states' tort laws. Even within a state, the federal court and the state court may interpret tort law differently.[333] Moreover, even if courts allow tort liability, damages are unlikely to be sufficient to deter spyware perpetrators.

Congress should act to remedy the situation and to create uniform national law. Congress could address the significant spyware problem by carefully crafting requirements for those engaged in data mining from consumers. First, spyware perpetrators must have the responsibility to show that the consumer explicitly and knowingly authorized the data mining. Spyware can be defined in such a way that legitimate cookie technology can continue to serve legitimate business needs and consumer desires. After defining spyware activities, Congress can state that no one engaged in those activities may claim that a consumer implicitly authorizes data mining. Congress can create a presumption that the existence of language within an EULA alone is not sufficient to authorize such activity. As in another consumer protection law, the Truth in Lending Act, Congress can require any explicit agreement to be clear and conspicuous.[334] Congress can require the disclosure to include explicit and simple language concerning the effects of agreeing. And, in addition, it can mandate that the spyware user bears the burden of proving that the agreement is clear and conspicuous and that the end-user explicitly agreed. Such requirements cannot possibly hurt the legitimate business if coupled with a provision such as the FDCPA's bona fide error provision.[335]

Finally, statutory penalties significant enough to deter bad actors and to encourage private attorneys to bring enforcement actions, coupled with Congressional approval of class action relief, can help eliminate spyware used for bad purposes. Consumers need protection, but the protection should not hamper legitimate business. Rather than hoping that courts will fashion remedies to protect both legitimate business and consumers, Congress needs to act. Spyware is not only annoying, it is dangerous to businesses and to consumers; private attorneys and the courts do not have the resources to address the problem.

[333] *Compare eBay*, 100 F. Supp. 2d at 1070 (finding trespass to chattels with no "real" damage) *with Intel Corp.*, 71 P.3d at 300 (eviscerating the tort in terms of spyware).

[334] *See* Truth in Lending Act, 15 U.S.C. § 1635(a) (2000).

[335] 15 U.S.C. § 1692k(c) (2000).