View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Duke Law Scholarship Repository

CODDLING SPIES: WHY THE LAW DOESN'T ADEQUATELY ADDRESS COMPUTER SPYWARE

ALAN F. BLAKLEY[1]

DANIEL B. GARRIE[2]

MATTHEW J. ARMSTRONG[3]

ABSTRACT

Consumers and businesses have attempted to use the common law of torts as well as federal statutes like the Computer Fraud and Abuse Act, the Stored Wire and Electronic Communications and Transactional Records Act, and the Wiretap Act to address the expanding problem of spyware. Spyware, which consists of software applications inserted into another's computer to report a user's activity to an outsider, is as innocuous as tracking purchases or as sinister as stealing trade secrets or an individual's identity.

---

[1]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 was class counsel for several consumer class action lawsuits. He has written three books on digital information and litigation, including *2006 Digital Litigation Handbook* recently published by American Lawyer Media, available from www.lawcatalog.com. 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.

[2] Daniel B. Garrie is a J.D. candidate at Rutgers University School of Law, specializing in cyberlaw litigation. He received his M.A. and B.A. in computer science from Brandeis University in 2000 and 1999, respectively, with his coursework focused on artificial intelligence. Over the past eight years, Garrie has worked with the U.S. Department of Justice and other large corporations as an enterprise technical architect, focusing on Web-enabled enterprise systems.

[3] 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.

Existing law does not address spyware adequately because authorization language, buried in "click-through" boilerplate, renders much of current law useless. Congress must act to make spyware companies disclose their intentions with conspicuous and clearly-stated warnings.

INTRODUCTION

¶1 The law of the United States specifically addresses espionage, whether through the theft of government information[4] or, as the law also contemplates industrial espionage, through stealing trade secrets or patentable information.[5] But, what of the theft of other types of information from individuals' or business' computers? Most people are familiar with spyware's ability to infect computers and to record browsing habits, keystrokes, passwords, financial information, and other personal identification and to transmit it without the computer owner's knowledge.[6] Unfortunately for the person whose computer has been hijacked and whose information is being stolen, the law does not adequately address these types of spies, that is, spyware.

¶2 The law has not developed to address spyware because spyware is a relatively recent phenomenon, a phenomenon that is really an extension of cookie technology.[7] The problem is compounded by the fact that end-users connected to the World Wide Web ("Web") either intentionally or unintentionally invite others into their machines. This article describes spyware,[8] considers current efforts used to control spyware, and then proposes a solution that avoids crippling businesses that legitimately rely upon cookies while protecting businesses and consumers from illegitimate spyware.

I. THE EVIL GHOST IN THE MACHINE

¶3 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, is

---

[4] *See* 18 U.S.C. §§ 792-799 (2000).
[5] *See, e.g.*, Rambus, Inc. v. Infineon Tech. AG, 330 F. Supp. 2d 679, 692-93 (E.D. Va. 2004).
[6] *See generally* Merrill Warkentin, Xin Luo, & Gary F. Templeton, *A Framework for Spyware Assessment*, 48 COMM. OF THE ACM 8 (Aug. 2005).
[7] *See, e.g.,* Andrew Brandt, *How it Works: Cookies*, Feb. 22, 2000 (explaining how a cookie works), http://www.pcworld.com/hereshow/article/0,aid,15352,00.asp.
[8] For a complete description of spyware, see Warkentin, *supra* note 6.

monitoring 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.[9] Cookies are beneficial because they "[e]liminate[] the need to repeatedly fill out order forms or re-register on Web sites."[10] For instance, with passwords being increasingly difficult to remember, some sites that require user names and passwords place cookies on the hard drive so that the user has the option to log-in automatically when visiting.[11] Web-based businesses like cookies because they can use them to track "Web surfing behavior or patterns."[12] Businesses can target their advertising and show users products of interest based on past purchases.[13] Businesses, however, always seeking more competitive advantages, have developed a variety of legitimate and illegitimate technologies to enhance their market advantage.[14]

¶4 Adware, a cookie modification,[15] places either random or targeted advertisements on the screen of the user.[16] Generally, adware is not malicious.[17] Spyware, while similar to adware, is usually an application

---

[9] A website uses cookies to record "bits of identifying information on your hard drive, which the sites can use to track your activities and recognize you when you return." Brandt, *supra* note 7. "For some, [cookies] promise a more user-friendly Web; for others, they pose a privacy threat." *Id.*

[10] *See id.*

[11] For instance, the *New York Times* requires registration which is free, and its cookie logs the users into the site each time they visit. *Id.* Of course, users must beware to use this option only when confident that anyone with access to the hardware is authorized to visit the site.

[12] *Id.*

[13] For instance, Amazon.com updates its page view depending upon who is looking and that person's purchase history. *Id.*

[14] For a list of the various applications, see Lavasoft, Spyware & Harmful Technologies, http://www.lavasoftusa.com/trackware_info/spyware_tech (last visited Sept. 19, 2005). Such tools as data miners that actively collect information, dialers that change the computers dial-up networking, worms that create self-replicating viruses, and hijackers that hijack a user's home page are all examples of modifications of cookie technology. *Id.*

[15] For the difference between adware and spyware, see Webopedia, Spyware, http://www.webopedia.com/DidYouKnow/internet/2004/spyware.asp (last visited Sept. 19, 2005).

[16] *Id.* Many times these advertisements appear on the web page being visited; however, sometimes they appear as "pop-ups" superimposing themselves on the page being visited or as "pop-unders" so they appear on the users screen after closing the particular web page or closing other applications. Pop-unders, while not as annoying at the time they appear, can be more problematic because they may contain animations that cause the entire system to run more slowly for no apparent reason.

[17] *Id.*

installed on the user's computer, and, by definition, installed without the user's knowledge. Spyware can monitor everything users do with their machines, not only their activities on the Web, and transmit that information to an outside entity.[18] Unfortunately, users mostly accept spyware unintentionally or without full and informed knowledge of its parameters when downloading something from the Web. The spyware company usually claims users consented to the installation of spyware by accepting a licensing agreement.[19] Typically, a user merely "clicks through" boilerplate without reading it.[20]

¶5 The most glaring problem for both businesses and the courts is to walk the fine line between two regulatory strategies: shutting down spyware that, collects and uses end users' information without first obtaining full, informed consent; or eliminating the ability of businesses to employ target advertising and simultaneously making it more difficult for consumers to conduct business with their computers. For instance, the government could outlaw any type of cookie technology on the Web. Although this would solve the problem of spyware, the end-result would cripple Internet businesses. Alternately, authorities could continue forcing consumers and businesses to apply the ineffective existing law. The balance of this iBrief describes the methods tried in the past, mostly without success, and posits a potential solution.

II. TRADITIONAL COMMON LAW THEORIES

¶6 Victims of spyware have attempted to use two different traditional common law theories to address spyware: trespass to chattels;[21] and intrusion upon seclusion.[22] While consumers have attained some success with each of these theories, courts are inconsistent in the rules applicable to

---

[18] *Id.* "Because spyware exists as independent executable programs, they have the capability to monitor your key strokes, scan files on the hard drive, snoop other applications, such as chat programs or word processors, install other spyware programs, read cookies, change the default home page on the Web browser, while consistently relaying this information back to the spyware author who will either use it for advertising and marketing purposes or sell the information to another party." *Id.*

[19] This is the fundamental problem with enforcement under the current legal theories, as discussed more fully below with respect to each of the potential existing solutions. *See infra* notes 57-62, 69-73 and accompanying text.

[20] *Id.* One of the authors is willing to admit that he "clicks through" without reading the terse and incomprehensible terms. He suspects the vast majority of readers do also.

[21] *See* RESTATEMENT (SECOND) OF TORTS § 218 (1965) (describing trespass to chattels).

[22] *See id.* at § 652B (describing intrusion upon seclusion).

their use.[23] Due to inconsistencies, practitioners must be very careful in attempting to use these or other theories of common law liability to attack spyware.

A. Trespass to Chattels

¶7 Using trespass to chattels usually requires a great deal of creativity by the attorney and the court. One such creative application arose in *Register.com, Inc. v. Verio, Inc.*, a case in the United States Court of Appeals for the Second Circuit.[24] The litigation in *Register.com* arose after the defendant, Verio, allegedly placed a computerized robot on Register.com's system.[25] The plaintiff claimed that the use of this robot constituted a trespass to chattels.[26] The Second Circuit affirmed the trial court's holding that liability for trespass to chattels could apply in this situation.[27] Verio argued that the robot caused no harm to Register.com's chattel because it did not shut the system down.[28] However, the court found that even though this robot might not incapacitate the system, this and other robots had the *potential* to incapacitate the system and such potential was sufficient for liability under the tort.[29] The Second Circuit also adopted the trial court's finding that the robot used significant amounts of Register.com's system.[30]

¶8 Unfortunately, the opinion provides a mixed blessing for the spyware victim. The court held that the terms of use on Register.com's

---

[23] For instance, a federal court in California has held that simply invading someone's computer and using it can constitute trespass to chattels. *See* Oyster Software, Inc. v. Forms Processing, Inc., No. C-00-0724 JCS, 2001 WL 1736382, at *40 (N.D. Cal. Dec. 6, 2001). On the other hand, the California Supreme Court has held that the court in *Oyster Software* incorrectly applied California law and that California requires that the chattel actually be impaired in its function for trespass to chattel to occur. Intel Corp. v. Hamidi, 71 P.3d 296, 307 n. 5 (Cal. 2003).

[24] 356 F.3d 393 (2d Cir. 2004). The *Restatement (Second) of Torts* defines trespass to chattels in terms of someone without permission interfering with the chattel so that it "is impaired as to its condition, quality, or value, or . . . [the owner] is deprived of the use of the chattel for a substantial time . . . ." RESTATEMENT (SECOND) OF TORTS § 218.

[25] *Register.com*, 356 F.3d at 397. In this case, it was an automated software program that searched Register.com's database for contact information allegedly to steal Register.com's clients. *Id.* at 395. A robot is a software application that automatically searches for information.

[26] *Id.* at 396-97.

[27] *Id.* at 404-05.

[28] *Id.* at 404.

[29] *Id.*

[30] *Id.*

website did not prohibit Verio from using a data mining system like a robot to collect information automatically.[31] The problem, of course, in implying consent is that with consumers and others "clicking through" a boilerplate agreement by "clicking" on a button that says "I agree with the terms," they may be unwittingly and without full information consenting to the installation of spyware on their machines.

¶9 The greatest problem, however, with trespass to chattels is that the plaintiff must show actual damage to the chattel.[32] This problem haunted the California Supreme Court, causing it to refuse to apply California's common law trespass to chattels to fashion a remedy for a spyware installation.[33] The court, not willing to accept the theory propounded by the Second Circuit that potential damage to a system suffices, held electronic impulses do not injure the chattel and, therefore, a claim under trespass to chattels failed for lack of demonstrable damages.[34]

B. Intrusion Upon Seclusion

¶10 The tort of intrusion upon seclusion, or violation of the right of privacy,[35] gives spyware victims little additional help. Like trespass to chattels and other tort theories, plaintiffs must prove the existence of damages. Unless counsel can identify sufficient damages, the theory, while interesting from an intellectual standpoint, provides little assistance to the victim. Furthermore, courts frequently find other excuses for not imposing liability under a privacy tort.

---

[31] *Id.* at 437 n.56, 404–05. The trial court held that language in Register.com's database authorization allowed individuals to collect information automatically but not to use automated systems with the data after it was collected. Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 249 (S.D.N.Y. 2000). The Second Circuit affirmed this holding; however, both courts found that as of the date the lawsuit was filed, the consent was withdrawn. *See id*. at 249; *Register.com*, 356 F.3d at 437.

[32] *See* RESTATEMENT (SECOND) OF TORTS § 218 (1965); *see Register.com*, 356 F.3d at 437-38.

[33] Intel Corp. v. Hamidi, 71 P.3d 296, 308-09 (Cal. 2003).

[34] The California Supreme Court contended that Oyster Software, Inc. v. Forms Processing, Inc., No. C-00-0724 JCS, 2001 WL 1736382 (N.D. Cal. Dec. 6, 2001), misapplied California law. *Intel Corp*., 71 P.3d at 1357 n.5. The federal courts in California seem more likely to allow trespass to chattels. *See, e.g.,* Ticketmaster Corp. v. Tickets.com, Inc., No. 99CV7654, 2000 WL 1887522 (C.D. Cal. Aug. 10, 2000) (holding that computers are tangible personal property and that invading them with electronic impulses constitutes to trespass to chattels).

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

¶11 For instance, in *White v. White*,[36] a New Jersey family court held that the tort of intrusion upon seclusion could apply to the access of computer records.[37] However, because the computer in question was located in a common area, the court held that anyone with access to that common area would not be subject to liability for intrusion upon seclusion.[38] This case sends another mixed message; the tort might work, but only if the computer is not accessible. The court specifically held that "[a] 'reasonable person' cannot conclude that an intrusion is 'highly offensive' when the actor intrudes into an area in which the victim has either a limited or no expectation of privacy."[39] The court further held that the fact that others had access to the computer made expectations of privacy unreasonable.[40]

¶12 The spyware perpetrator might use such language from *White* to justify intrusion into a computer over the Web. In *White*, the husband did not know that his wife could access the contents of his computer but had left it in a physical place where she could, in fact, access it.[41] Similarly, individuals connecting to the Internet may not realize that the owners of sites they access can also access their information. However, those sites can in fact access the information, and users, like Mr. White, are leaving their computers in an accessible place, even if it is only accessible in cyberspace. Therefore, a spyware perpetrator could rely on this case for the proposition that connecting a computer to the Web gives others access, and in fact, invites others in, thereby making an expectation of privacy unreasonable.

¶13 At the other end of the spectrum, the New Hampshire Supreme Court, in *Remsburg v. Dousearch, Inc.*, considered the tort of intrusion upon seclusion from the opposite point of view, holding that alleged invading individuals must "exercise reasonable care not to subject others to an unreasonable risk of harm."[42] This seemed to indicate the court was beginning from the opposite direction from the court in *White*. In *White*, the question was whether or not the person being invaded had a reasonable expectation of privacy. In *Remsburg*, the New Hampshire court asked whether the person doing the looking was subjecting the other to an

---

[36] 781 A.2d 85 (N.J. Super. Ct. Ch. Div. 2001).
[37] *Id.* at 91. In that case, the husband and estranged wife were living in the same house. *Id.* at 87. The wife gained access to the husband's computer and found e-mails between the husband and his other woman. *Id.* The husband mistakenly believed that his e-mail account could only be accessed by using his password. *Id.*
[38] *Id.* at 92.
[39] *Id.*
[40] *Id.*
[41] *Id.* at 87.
[42] 816 A.2d 1001, 1006 (N.H. 2003).

unreasonable risk of harm. The *Remsburg* court held that someone who should realize that the conduct may create "an unreasonable risk of harm to another has a duty to exercise reasonable care to prevent the risk from occurring."[43]

¶14 Irrespective of a court's point of view in imposing or denying liability, the current common law fails to meet the needs of the consumer or of businesses in addressing spyware. First, the tort of trespass to chattels is marginally helpful because of the difficulty in establishing damage to the chattel and the argument of implied consent.[44] Second, the tort of intrusion upon seclusion suffers from the same difficulty in establishing damages, focuses on consent, and depends upon whether the court's initial position is that the victim's expectation of privacy is reasonable or the proposition that the spyware perpetrator has a duty to prevent harm to the victim.

III. POTENTIONAL STATUTORY REMEDIES

¶15 Three separate federal laws are applicable in the spyware context: the Computer Fraud and Abuse Act ("CFAA");[45] the Stored Wire and Electronic Communications and Transactional Records Act ("Stored Communications Act");[46] and the Wiretap Act.[47] Unfortunately, none of these acts were designed to address the issues presented by spyware, and each has significant drawbacks.

A. Computer Fraud and Abuse Act ("CFAA")

¶16 Under the CFAA, spyware victims can assert a civil cause of action provided they can show aggregate damages during a one-year period of at least $5,000 in value,[48] some modification or impairment of medical information,[49] a physical injury,[50] a threat to the public health or safety,[51] or some damage to a government computer system.[52] For the individual computer user, the only potentially applicable claim, and also the most

---

[43] *Id.* at 1007. Perhaps the difference in the two cases can be understood from looking further at the facts of these cases. In *White*, the case concerned viewing e-mails showing an extramarital affair, whereas *Remsburg* concerned the stalking and murder of a woman.

[44] See *infra* notes 57-62, 69-73 and accompanying text, for the treatment of implied consent.

[45] 18 U.S.C. § 1030 (2000 & Supp. 2004).

[46] *Id.* §§ 2701, 2707 (2000 & Supp. 2004).

[47] *Id.* § 2511 (2000 & Supp. 2004).

[48] *Id.* § 1030(a)(5)(B)(i) (Supp. 2004).

[49] *Id.* § 1030(a)(5)(B)(ii) (Supp. 2004).

[50] *Id.* § 1030(a)(5)(B))iii) (Supp. 2004).

[51] *Id.* § 1030(a)(5)(B)(iv) (Supp. 2004).

[52] *Id.* § 1030(a)(5)(B)(v) (Supp. 2004).

difficult to establish, is the aggregate of $5,000 in damage. Even the most expensive personal computer costs much less than this.[53] An alternative possibility would be for the individual to claim the loss of personal data exceeding the $5,000 limit.[54] The question this raises for the individual consumer is whether litigation and the necessity of experts to show the extent of loss are worth the chance of recovery.[55] For the individual consumer, without a class action, the potential value of CFAA disappears. Furthermore, even if a class action arises, at least one of the members of the class must have $5,000 worth of damages to allow the other class members' claims to survive.[56] The damage threshold eliminates CFAA as an avenue of redress for most consumers.

¶17 Businesses and corporations with large networks and expensive machines are the best candidates to succeed under the CFAA. Such entities are most likely to have losses exceeding the $5,000 minimum. However, businesses have a different but equally daunting problem under the CFAA: authorization.[57] The CFAA specifically states that only if unauthorized access is used "to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter"[58] will liability exist. Spyware programs almost always obtain the end-user's "consent," somewhere during the installation procedure and usually in some hidden manner, thus making the CFAA a marginally useful tool to combat spyware even when the victim has sufficient damage.

¶18 Further complicating this issue is the inconsistency among courts. For example, the court in *Specht v. Netscape Communications Corp.* held that parties are not bound by inconspicuous contractual provisions of which they are unaware of or contained in documents whose contractual nature is not obvious.[59] In *Netscape*, the Second Circuit, applying California law,

---

[53] See, for example, the Dell Inspiron XPS, a gaming notebook computer priced at $2,828 at www.dell.com (last visited Sept. 20, 2005). Gaming computers, because of their advanced graphics and other attributes, are among the most expensive.

[54] See, for example, Stephanie Byers, *Internet: Privacy Lost, Identities Stolen*, 40 BRANDEIS L.J. 141 (Fall 2001), for a description of losses due to identity theft and the potential liability of those stealing the information.

[55] This assumes the spyware perpetrator can be found and has not disappeared into cyberspace.

[56] *See* Thurmond v. Compaq Computer Corp., 171 F. Supp. 2d 667, 681 (E.D. Tex. 2001) (holding that at least one protected computer must have an aggregate of over $5,000 in damage for a class to be certified). Once the class can find one protected computer, all injured class members may bring their claims, even if their individual damages are less than $5,000. *Id.*

[57] *See* 18 U.S.C. § 1030(e)(6).

[58] *Id.*

[59] 306 F.3d 17, 29-30 (2d Cir. 2002) (applying California law).

held that "a consumer's clicking on a download button does not communicate assent to contractual terms if the offer did not make clear to the consumer that clicking on the download button would signify assent to those terms."[60]

¶19 In a diametrically opposed case, *i.Lan Systems, Inc. v. Netscout Service Level Corp.*, the federal district court in Massachusetts held that simply clicking on the "I Agree" box *was* an appropriate way to form a contract.[61] Therefore, when a spyware company buries its contractual provisions inside a boilerplate that an end-user is unlikely to read, the CFAA may become useless because of the consent exemption. On the other hand, since spyware programs frequently do not disclose their software's capabilities with sufficient detail, victims can argue that the spyware activities exceed the authorization. However, as the law stands currently, victims must hope their court follows the *Netscape* reasoning.

B. Stored Wire and Electronic Communications and Transactional Records Act ("Stored Communications Act")

¶20 Since it could be argued that spyware collects personal information from an individual through a communication without that individual's

---

[60] *Id.*

[61] 183 F. Supp. 2d 328, 338 (D. Mass. 2002). *See also* ProCD, Inc., v. Zeidenberg, 86 F.3d 1447, 1452 (7th Cir. 1996) (explaining that under U.C.C. § 2-204, vendor, as master of offer, may propose limitations on kind of conduct that constitutes acceptance; § 2-207 does not apply in case with only one form); M.A. Mortenson Co., Inc. v. Timberline Software Corp., 998 P.2d 305, 311-14 (Wash. 2000) (holding that where vendor and purchaser utilized license agreement in prior course of dealing, shrink-wrap license agreement constituted issue of 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) (explaining that parties' conduct in shipping, receiving and paying for product demonstrates existence of contract; box top license constitutes proposal for additional terms under § 2-207 which requires express agreement by purchaser); Arizona Retail Sys., Inc. v. Software Link, Inc., 831 F. Supp. 759, 765 (D. Ariz. 1993) (explaining that vendor entered into contract by agreeing to ship goods, or at latest by shipping goods to buyer; license agreement constitutes proposal to modify agreement under § 2-209 which requires express assent by buyer); and U.S. Surgical Corp. v. Orris, Inc., 5 F. Supp. 2d 1201, 1206 (D. Kan. 1998) (finding that sales contract concluded when vendor received consumer orders; single-use language on product's label was proposed modification under § 2-209 which requires express assent by purchaser).

consent, spyware arguably violates the Stored Communications Act.[62] The Act specifies a private cause of action to protect individuals in their privacy.[63]

¶21 The Stored Communications Act requires proof of five elements. The access must: (1) be to "a facility through which an electronic communication service is provided;" (2) be intentional; (3) exceed authorization; (4) "obtain[], alter[], or prevent[]" a wire or electronic communication; and (5) involve a communication maintained in electronic storage in that system.[64]

¶22 First, the court needs to determine whether the information resides in "a facility through which an electronic communication service is provided."[65] This element is generally not a problem under the definition of facility.[66] Spyware, by its very definition, uses an individual's or a business' machine as a facility through which it can access electronic information. Consequently, this element of the Stored Communications Act does not raise problems.

¶23 The second element, intent, should also be easy to satisfy.[67] Even if a spyware manufacturer claims that some of the information mined from the user's computer and returned to the spyware company was mistakenly collected, the spyware company certainly cannot claim that it did not intentionally access information on the individual's computer.

¶24 Once again, authorization may limit the utility of this statutory remedy.[68] Will a court hold that "clicking through" the "I agree" included in a lengthy boilerplate agreement demonstrates consent to the spyware's mining of data, or will it hold that actual informed and knowing consent is

---

[62] *See* 18 U.S.C. §§ 2701-11 (2000 & West Supp. 2005).

[63] *Id.* § 2707. The civil cause of action allows equitable or declaratory relief, *id.* § 2707(b)(1), as well as attorneys' fees, *id.* § 2707(b)(3), and compensatory damages of no less than $1,000, *id.* § 2707(c). In the event the violation was "willful or intentional, the court may assess punitive damages." *Id.*

[64] *Id.* § 2701(a).

[65] *Id.* § 2701(a)(1).

[66] The Stored Communications Act adopts the definitions included in the Wiretap Act. *Id.* § 2711(1) (Supp. 2004). Under the Wiretap Act, an "electronic communication service" is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." *Id.* § 2510(15). Under such a definition, an individual's home computer qualifies as an electronic communication service because it has the ability to send or receive electronic communications.

[67] *See id.* § 2701(a)(1).

[68] 18 U.S.C. § 2701(a)(1) includes "without authorization" while 18 U.S.C. § 2701 includes "exceeds an authorization" both of which can be used by the spyware company as a defense.

required?[69] If courts require explicit authorization, spyware companies can effectively nullify the requirement so long as courts allow them to bury the notice in a lengthy document that no one will read [and probably designed so no one ever could read it]. While many courts have held that mere use of a product or purchase of a service is not sufficient to infer consent,[70] other cases such as *i.Lan Systems*[71] allow spyware companies to circumvent this element by burying boilerplate authorization in a "click through" agreement.[72]

¶25 The next element of the Stored Communications Act requires that the spyware company access an "electronic communication."[73] While it is possible that spyware programs might operate solely on installed program files on a host computer, it is extremely unlikely that the spyware could avoid all end-user information that fits the definition of an electronic communication.[74] So, litigants should have no trouble with this element.

¶26 The final element is equally easy to satisfy. This element requires that information be "in electronic storage"[75] at the time it is accessed. Since all spyware programs operate on host machines that have transformed input into digital electronic information, spyware by definition must access information in electronic storage at the time.

¶27 While there are some exceptions to the Stored Communications Act concerning governmental subpoenas[76] and other types of authorization,[77]

---

[69] Some courts have found that although the interception of electronic communications does not require explicit consent, consent can only be inferred if the end-user has notice and actually gives informed consent. *In re* Pharmatrak, Inc. Privacy Litig., 329 F.3d 9, 20 (1st Cir. 2003).

[70] *In re Pharmatrak*, 329 F.3d at 20.

[71] iLan Sys., Inc. v. Netscout Serv. Level Corp., 183 F. Supp. 2d 328 (D. Mass. 2002).

[72] As a District of Massachusetts court held, "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.* at 338.

[73] 18 U.S.C. § 2701(a) (2000).

[74] Once again, the Stored Communications Act refers to the Wiretap Act for its definition of electronic communication. In the Wiretap Act, electronic communication includes any data transmitted "in whole or in part . . . affect[ing] interstate or foreign commerce." *Id.* § 2510(12). By its very definition, spyware seeks to acquire such data and transmit electronically to the spyware company for the benefit of a commercial enterprise.

[75] *Id.* § 2701(a).

[76] *See id.* §§ 2703(a), 2704(a) (2000 & Supp. 2004).

the only impact of these exceptions would be with respect to the authorization element described above. Consequently, as with the other potential remedies, if "authorization" can be redefined, a remedy may exist. This must be resolved legislatively since most of the litigation will rely upon individual state contract laws. Only if a uniform law is enacted or if Congress intervenes to make the law uniform for interstate communications will some consistency occur.

C. The Wiretap Act

¶28 The Wiretap Act[78] would seem to be the best avenue to address spyware. However, unlike the Stored Communications Act, courts have limited its provisions to apply only to interception of electronic information in transit.[79] The Wiretap Act was designed not to protect digital communication but to protect telephone calls over traditional networks.[80] Spyware companies have taken advantage of the storage-transit dichotomy to develop programs that intercept communications while they are in a

---

[77] *See id.* § 2701(c)(1)-(2).

[78] *Id.* § 2510 et seq. (2000 & Supp. 2004).

[79] One of the main problems of the Wiretap Act is the storage—transit dichotomy. Circuits that narrowly read the Wiretap Act require any interception to be contemporaneous with transmission. *See In re* Pharmatrak, Inc. Privacy Litig., 329 F.3d 9, 21 (1st Cir 2003). 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 generally*, Chance v. Avenue A, Inc., 165 F. Supp. 2d 1153, 1155-57 (W.D. Wash. 2001); *In re* DoubleClick Privacy Litig., 154 F. Supp. 2d 497, 503-04 (S.D.N.Y. 2001); *In re Pharmatrak, Inc.*, 329 F.3d at 12; *In re* Toys R Us, Inc. Privacy Litig., No. M-00-1381 MMC, 2001 U.S. Dist. Lexis 16947, at *3 (N.D. Cal. 2001); *In re* Intuit Privacy Litig., 138 F. Supp. 2d 1272, 1274 (C.D. Cal. 2001). 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*, 329 F.3d at 19-22. Since the Wiretap Act allows either party to consent to the recording a 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.A. § 2511(2)(d) (2000) (stating that a party may consent to the interception of only part of a communication or to the interception of only a subset of its communication). Here, the end-user can assert that he or she 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*.

[80] *See generally* Daniel B. Garrie, Mathew J. Armstrong & Alan F. Blakley *Voice Over Internet Protocol: Reality v. Legal Fiction*, FED. LAW. Aug. 2005, at 7, 34.

temporarily stored state, therefore not being transmitted.[81] Spyware has achieved the ability of bypassing the Wiretap Act in a two-step process. First, it has been designed to record individual user's keystrokes or other data input actions.[82] Then in the next step, the spyware transmits the information to the spyware's creator.[83] As the Central District of California said in *United States v. Ropp*, spyware companies that have taken advantage of the confusion generated by the storage-transit dichotomy have gotten away with accessing data in spite of the Wiretap Act.[84] The Wiretap Act can still be used in limited situations where information is recorded during real time communication. Furthermore, as discussed below, the government may prosecute manufacturing, advertising, and selling a tool for use to intercept live real time communications.[85]

¶29 The government recently tried to approach spyware from a slightly different perspective that may provide some relief under the Wiretap Act for the most egregious perpetrators.[86] In *Perez-Melara*, the defendant allegedly created and marketed a program called Loverspy[87] to monitor the on-line behavior of suspected unfaithful spouses.[88] The defendant sold the progam to individuals to "monitor, record and report all electronic mails, passwords, chat sessions, instant messages and websites visited by any user of the victim computer."[89] The manufacturer and seller allowed the purchaser of the software to send a Loverspy greeting card through e-mail

---

[81] *Id.* For a more in-depth analysis, see Daniel B. Garrie, Mathew J. Armstrong, & Donald P. Harris, *Voice Over Internet Protocol and the Wiretap Act: Is Your Conversation Protected?*, 29 SEATTLE U.L. REV. 95 (Fall 2005).

[82] Such interception has been held not to violate the act because the information was intercepted prior to its transmission. Unites States v. Ropp, 347 F. Supp. 2d 831, 837 (C.D. Cal. 2004). The court there held that "although defendant engaged in a gross invasion of privacy by his installation of the KeyKatcher on Ms. Beck's computer, his conduct did not violate the Wiretap Act. While this may be unfortunate, only Congress can cover bases untouched." *Id.* at 838.

[83] For the differences between adware and spyware, see *supra* note 16.

[84] 347 F. Supp. 2d at 838.

[85] The Wiretap Act, like the Stored Communications Act, authorizes recovery of civil damages for persons whose communications are intercepted in violation of the act. *See* 18 U.S.C. § 2520 (2000) (concerning damages, including punitive damages, and attorneys' fees).

[86] *See* United States v. Perez-Melara, No. 05 CR 1264LAB, 2005 WL 2173087 (S.D. Cal. July 21, 2005); Jason Schossler, *"Spyware Creator Facing Up to 175 Years in Prison,"* ANDREWS COMPUTER AND INTERNET LITIG. REP., Sept. 20, 2005, at 10.

[87] *Perez-Melara*, 2005 WL 2173087 at Count 1.

[88] *Id.* at ¶ 2.

[89] *Id.*

to the victim.[90] When the victim opened the seemingly innocuous greeting card sent from a spouse or friend, it installed a spyware application in the victim's computer to report use information back to the "electronic mail address of the purchaser."[91]

¶30 The government charged the creator of this spyware with manufacturing, advertising, and promoting interception devices in violation of the Wiretap Act.[92] Perhaps this use of the Wiretap Act, targeting the manufacturer of spyware, will lead to an effective use of that law in at least some situations.

IV. PROPOSED SOLUTION

¶31 While all of the potential liability described above may provide assistance for some consumers and businesses in the right court and under the right circumstances, most spyware has been able to bypass any criminal and civil liability. The best solution to the problem, that would not have the side-effect of prohibiting the legitimate business of Internet companies, would be nationwide legislation through an act of the United States Congress requiring any entity doing business in the United States to acquire express authorization and informed consent to the specific access being granted anytime someone places an application on another's computer.[93]

¶32 As a start, the legislation could require that any site that will install an application onto the other user's computer must have clear and explicit warnings in plain English enabling the user to understand exactly what the application will do, including the information it will gather, who will receive the information, how it will be used and any potential modifications of the user's system the application will cause. "Click-Through" and End-User License Agreements or authorizations are not acceptable. First, the agreement must begin with a conspicuous statement that by accepting the terms, the user is authorizing outside access to the user's information. Perhaps examples of the information to be collected and mined would be included. Then the authorization, or End-User's License Agreement, would have a series of simple statements and the recipient would need to agree with each one. In any event, each and every result of the installation of the application must be specifically disclosed and accepted by the end-user.

---

[90] *Id.* at ¶ 5.
[91] *Id.* at ¶ 6.
[92] 18 U.S.C. § 2512(1) (2000 & Supp. 2004).
[93] This could be accomplished by an amendment to the Stored Communications Act because unlike the Computer Fraud and Abuse Act, it does not have a minimum damage requirement. Furthermore, by requiring such authorization and consent for any person or entity doing business in the United States, the problem of monitoring international compliance is limited.

Finally, the legislation must have statutory penalties so the consumer need not prove specific damages.

CONCLUSION

¶33 The existing theories of liability do not provide adequate remedies either for consumers or for businesses. The major problem is the inconsistent definition of "authorization." Simply defining "authorization" by statute is not enough. Congress must be careful to define spyware in such a way that legitimate Internet businesses using cookie technology can continue to operate while at the same time eliminating implicit acceptance and authorization and requiring, as with all other consumer protection laws, that such authorization be explicit, fully informed and in simple, CONSPICUOUS language. Congress can act to eliminate this dangerous and growing threat to individual privacy and to legitimate business. Due to inconsistent state law and judicial interpretations, the remedy must be statutory, and it must be national.