4-2006

Rethinking Spyware: Questioning the Propriety of Contractual Consent to Online Surveillance

Wayne R. Barnes
Texas A&M University School of Law, wbarnes@law.tamu.edu

Rethinking Spyware: Questioning the Propriety of Contractual Consent to Online Surveillance

Wayne R. Barnes[*]

The spyware epidemic has reached new heights on the Internet. Computer users are increasingly burdened with programs they did not knowingly or consciously install, which place strain their computers' performance, and which also trigger annoying "pop-up" advertisements of products or services which have been determined to match the users' preferences. The users' purported preferences are determined, in turn, by the software continuously monitoring every move the consumer makes as she "surfs the Internet." The public overwhelmingly disapproves of spyware which is surreptitiously placed on computers in this manner, and yet most legal commentators and industry participants have assumed it is appropriate so long as some modicum of perceived consent is granted, as in a click-through on a lengthy End-User License Agreement momentarily displayed on the computer screen. This Article seeks to illuminate the true nature of the spyware bargain, and questions the propriety of sanctioning such "surveillance bargains" under principles of contract law. Such bargains may often be unenforceable because a term allowing continual surveillance may be beyond the range of reasonable expectations of most consumers. Even if not, however, the privacy implications are such that we as a society may wish to condemn such "bargains to be spied upon," and conclude that such contracts should simply be unenforceable as a matter of public policy, and therefore banned.

[*] Associate Professor, Texas Wesleyan University School of Law. I would like to thank Ben Edelman and Frank Snyder for their invaluable comments in discussing this topic with me and for helping me formulate the ideas presented in this Article. Further thanks to Frank for reviewing an earlier draft.

TABLE OF CONTENTS

INTRODUCTION

Spyware has emerged as one of the most serious scourges of the Internet. Millions of people likely have spyware on their computers, but almost no one knows they have it.[1] It may have been secretly loaded onto their computers without their knowledge. Or, they may have "agreed" to its installation by clicking their assent to a license agreement that came with another program that they downloaded. Regardless, the spyware application may be performing a wide range of undesirable activity on their computers, from outright theft of credit card numbers and other financially valuable data, to surveillance of every movement these consumers make on the Internet.[2] In the cases where the software is simply foisted onto an unsuspecting consumer's computer without any pretense of obtaining consent, there is fairly uniform sentiment in government and industry that such behavior is either already illegal or soon will be, once any of several current spyware legislation proposals are passed into law.

However, the proposition that a consumer may contractually consent to the installation of such software is accepted almost without any serious debate. Freedom of contract is, of course, a revered concept in our capitalistic society, but the privacy implications of spyware are profound. The spyware bargain contemplates a consumer obtaining a modestly valued software application, often a game, a utility of some kind, or one of the popular peer-to-peer file sharing applications such as KaZaa. In return, instead of paying money, the primary consideration flowing from the consumer is her agreement to allow the software application to install the spyware on her computer. The consumer typically "agrees" to the spyware by clicking "I accept" on a screen containing reference to a lengthy End User License Agreement ("EULA"), which virtually no one reads. The spyware's sole purpose is to conduct constant surveillance of the consumer's online activities, secretly collecting information on such activities and transmitting it back to the distributor of the spyware. The spyware distributor typically does this in the name of developing the consumer's "marketing profile," so it can then deliver "contextually relevant" advertisements, usually in the form of the dreaded "pop-up ads" on the consumer's screen. For this reason, this type of spyware is usually referred to as "adware."

However benign the concept of ad-supported free software may be in theory, the utilization of open-ended, constant surveillance of the

---

[1] *See infra* notes 66-67 and accompanying text.

[2] *See infra* notes 22-28 and accompanying text.

consumer wherever she goes on the Internet is troubling from a fundamental privacy perspective. If the consumer goes to a medical website to research cancer, ads for cancer treatment may follow. If the consumer goes to a pornographic site, or any other site which she may not desire others to know about, ads in that area may follow. Regardless of whether the spyware program displays ads, it still systematically collects information. Unlike cookies or other commonly accepted means of collecting consumer website usage, spyware conducts this surveillance and collection supposedly pursuant to the consumer's contractual consent. However, once the consumer initially clicks "I accept," she may never again be aware of the program's surveillance and transmission of her private web browsing data. Many in the software industry have championed these arrangements, and resistance against them is sometimes weak because the law perceives the consumer to have granted contractual consent.

The purpose of this Article is to question the propriety of that contractual consent, given the privacy implications of spyware. Part I of this Article discusses the history of spyware in the greater context of the Internet's general development. It also addresses the debate over the definition of "spyware" and the importance of the perceived grant of consent in that debate. Part I ends by categorizing the various negative attributes of spyware on consumers' computers, including deceptive installations, impaired computer performance, difficulty of removal, and the privacy concerns of spyware.[3] Part II analyzes the various existing and proposed laws that may apply to spyware. These include: (1) the current federal laws governing wiretapping, acquisition of stored communications, and unauthorized computer access; (2) the common law torts of trespass and invasion of privacy; and (3) the proposed federal and state laws related specifically to spyware. Part II demonstrates that virtually every single existing and proposed statute, as well as common law doctrines, incorporates consent as an element which can defeat liability.[4] Part III differentiates between nontransactional consent and transactional consent and discusses cases that analyze the relevance of a contract in determining consent to various activities that would otherwise be actionable. Though this Article recognizes that contractual consent can provide a defense in many circumstances, Part III discusses cases that articulate public policy limits on that consent.[5]

---

[3] *See infra* notes 8-100 and accompanying text.

[4] *See infra* notes 101-45 and accompanying text.

[5] *See infra* notes 146-273 and accompanying text.

Part IV addresses the problems of contract-based consent to spyware. It discusses the means of typical contractual assent through the EULA and highlights the realities of the spyware bargain by comparing them to a "real [offline] world" example of the bargain. Part IV then analyzes the viability of contractual consent to spyware in light of *Restatement (Second) of Contracts* section 211(3), the unconscionability doctrine, and the general doctrine of disfavoring contracts that contravene public policy. The results of this analysis are that the assent that consumers grant to spyware is flawed. Moreover, the public policy concern of privacy compels a conclusion that the law should prohibit such contracts in the consumer context. In the absence of such prohibitions, however, the current proposals for regulation of spyware should include additional procedural safeguards to protect the privacy and dignity interests of the consumers who bind themselves to these bargains.[6] The Article concludes with a brief summary of proposals.[7]

I. SPYWARE: HISTORY AND BACKGROUND

A. The Early, Safer Days of the Internet

In the early days of the World Wide Web, surfing the web and downloading files was a much safer proposition than it is today.[8] For one thing, the Internet was a much less populated space. Viruses emerged as a threat during this period, but users were relatively safe unless they were extremely active in the Usenet newsgroups or were foolish enough to open a file attached to an e-mail from an unknown source.[9] However, as the population of the Internet increased, larger commercial actors took notice and began to seek ways to market products and services to web users.[10] Advertisers began to covet information on consumer's web browsing habits for purposes of developing "marketing profiles."[11] Unless the user volunteered her preferences in survey form, the only other manner to obtain this

---

[6] *See infra* notes 274-410 and accompanying text.

[7] *See infra* note 411 and accompanying text.

[8] *See* Mike Tonsing, *Protect Yourself from Spyware*, FED. LAW., Nov./Dec. 2002 ("While it used to be the case that downloading a program from a reputable source was a fairly safe proposition, cyberia has become a more hostile environment than it used to be.").

[9] *See* E. Tenn. State Univ., *Avoiding Spyware*, http://www.etsu.edu/oit/helpdesk/spyware (last visited Jan. 26, 2006).

[10] *Id.*

[11] *Id.*

information, it seemed, was by surreptitious means because the idea of requesting consumer consent to online surveillance had not yet emerged as a proposed business model.

One of the most important developments in online information collection was cookies. Cookies are text files placed on a user's hard drive by a particular website or group of related websites.[12] Cookies were originally created to allow user-specific customizations of the Internet browsing experience. They allow a user's computer to "remember" things such as website passwords and shopping cart information for commercial websites.[13] As stated in a recent case involving cookies:

> A cookie is a piece of information sent by a web server to a web browser that the browser software is expected to save and to send back whenever the browser makes additional requests of the server (such as when the user visits additional webpages at the same or related sites). . . . Cookies are widely used on the internet by reputable websites to promote convenience and customization. Cookies often store user preferences, login and registration information, or information related to an online "shopping cart." Cookies may also contain unique identifiers that allow a website to differentiate among users.[14]

Gradually, websites began using cookies for advertising purposes. A website places the cookie on the user's computer hard drive, and then the cookie collects data about the consumer's use of that particular site. By technical design, cookies are "domain-specific" — they can only collect data from browsing on pages within a particular website.[15] Therefore, for instance, Wal-Mart.com could place a cookie on a consumer's hard drive, but could only collect data about the consumer's activity within pages on Wal-Mart.com. Once the user went to, for example, Amazon.com, the Wal-Mart.com cookie would have no surveillance capability. In this regard, cookies are somewhat like the virtual equivalents to video cameras in real, brick and mortar stores — they are cyberspace analogs to a real landowner exercising her right to observe things that occur on her own property. Further, cookies are now

---

[12] *See* Viktor Mayer-Schönberger, *The Cookie Concept*, http://www.cookiecentral.com/c_concept.htm (last visited Jan. 26, 2006).

[13] *Id.*

[14] *In re* Pharmatrak, 329 F.3d 9, 14 (1st Cir. 2003).

[15] *See* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1227-28 (1998).

completely controllable in all browsers — a user can fully exclude them if she wants to and can also easily delete them all (though she may find that browsing is somewhat labored without allowing some cookie access).[16] As discussed below, these relatively benign and noninvasive characteristics do not apply to spyware.

B. The Advent of Spyware

Eventually, advertisers sought to overcome the domain-specific limitations of cookies and instead develop a means by which they could follow consumers wherever they went on the Internet. Thus, the concept of spyware was born. Some believe that the participants in a 1995 Usenet group first used the term "spyware" to refer derisively to aspects of Microsoft's software applications and business practices.[17] Later, "spyware" came to refer to surveillance products such as spy cameras and microphones.[18] Software applications known as spyware were originally used for activities such as marital surveillance to discover infidelity.[19] The first widely-known "bundled" spyware application appeared on the Internet in 1999.[20] A freeware game called "Elf Bowling" became very popular, but the subsequent discovery that the application collected information about its users and reported it back to Nsoft, its distributor, surprised many users.[21] Hence, the current spyware model was realized. Some software providers, seemingly fearing that a traditional pricing model would fail, began choosing a three-party transaction instead, whereby the provider bundles the application with spyware. The advertising revenue compensated the provider for its product, thus allowing the provider to present its product to users for "free."

Some spyware distributors have clearly illegitimate, malevolent motives. These perpetrators bundle spyware with "free" software, with the sole purpose of obtaining credit card account numbers, social security numbers, or other personally-identifying information about the

---

[16] *See* David Whalen, *The Unofficial Cookie FAQ*, § 1.1, http://www.cookiecentral.com/faq/#1.1 (last visited Jan. 26, 2005).

[17] *See Chapter 2: The History of Spyware*, http://www.pcsecuritynews.com/spyware_history.html (last visited Jan. 26, 2006) [hereinafter *The History of Spyware*].

[18] *Id.*

[19] *See, e.g.*, John Borland, *'Spyware' Steps Out of the Shadows*, CNET NEWS.COM, Nov. 19, 2003, http://news.com.com/2100-1032_3-5108965.html.

[20] *See The History of Spyware*, *supra* note 17.

[21] *Id.*

owner of the computer.[22] This type and use of the software is designed for purposes of identity theft — the perpetrators have, as their sole or primary purpose, the theft of personal financial information which allows them to make fraudulent purchases on the victim's credit.[23] Although in many instances existing law protects the consumer from such losses,[24] the consumer's financial institutions nevertheless sustain the damage. Such malevolent uses of spyware are sometimes rightly referred to as "malware."[25]

Another, arguably more legitimate, form of spyware is often referred to as "adware." Adware is spyware which is installed in one of the manners described above, but for marketing purposes.[26] The software, once installed, monitors all of the consumer's Internet browsing activities, including, but not limited, to purchases made online.[27] The principal purpose of the adware's surveillance is to deliver advertising, usually in the form of "pop-up ads," of products calculated to be desirable to the consumer based on the extensive surveillance of that consumer's web browsing.[28] The adware companies refer to this process as "contextually based marketing." Notably, adware companies do obtain purported consent from consumers more often than is the case with "malware," but they do not universally obtain such consent before beginning surveillance. It is this purportedly consent-driven "spyware bargain" that is the focus of this Article.

C. *The Problem of Definition*

The term "spyware" has generated much controversy but is surprisingly immune to precise definition, at least by way of agreement within the industry. Jerry Berman, the President of the Center for Democracy and Technology, stated that spyware is comprised of "software ranging from 'keystroke loggers' that capture every key typed on a particular computer; to advertising applications that track users'

---

[22] MARCIA S. SMITH, CONG. RESEARCH SERV., SPYWARE: BACKGROUND AND POLICY ISSUES FOR CONGRESS 2 (2005), *available at* http://www.cdt.org/righttoknow/crsreports/RL32076_20050518.pdf (last visited Jan. 26, 2006).

[23] *Id.*

[24] *See* 15 U.S.C. § 1666i (2005).

[25] Another term that has been used for stand-alone programs designed for clandestine surveillance is "snoopware." *See* CTR. FOR DEMOCRACY & TECH., GHOSTS IN OUR MACHINES (2003), *available at* http://www.cdt.org/privacy/031100spyware.pdf.

[26] Smith, *supra* note 22, at 2.

[27] *Id.*

[28] *Id.*

web browsing; to programs that hijack users' system settings."[29] Berman noted that the means of installation of these programs are often veiled in secrecy, manifesting a lack of respect for consumers' dominion over their computers and their connections to the Internet.[30] Another definition of "spyware" is "any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes."[31]

Internet merchants argue vociferously about which applications deserve the "spyware" label.[32] One Internet source claims that "[i]f you ask 10 experts what the term Spyware describes[,] you will get 10 very different answers."[33] This, in fact, has been one of the problems for industry and law enforcement in deciding how to regulate the spyware problem.[34] The Federal Trade Commission ("FTC") held a conference to discuss the spyware epidemic on April 19, 2004.[35] The definitional problem was the very first subject tackled by the conference participants.[36] The FTC panel on defining "spyware" articulated three primary challenges to achieving consensus on the subject.[37] The first issue is knowledge of the program and consent to its installation.[38] Although everyone at the conference agreed that the law should label software as "spyware" only if the program was surreptitiously downloaded in a manner designed to circumvent the user's knowledge and consent, there was substantial disagreement about how a program could or should obtain effective consent.[39] The primary method to obtain user consent is disclosure in a EULA.[40] However, there is significant

---

[29] *Id.* at 1 (citing testimony to Senate Committee on Commerce, Science, and Transportation, Subcommittee on Communications, Mar. 23, 2004).

[30] *Id.*

[31] Webopedia, Definition of "Spyware," http://www.webopedia.com/TERM/s/spyware.html (last modified Feb. 18, 2005).

[32] *See* Robert Vamosi, *Who You Callin' Spyware, Spyware?*, CNET NEWS.COM, Mar. 15, 2005, http://reviews.cnet.com/4520-3513_7-5759896-1.html.

[33] *See* Anti-Spyware-Software.net, Definition of the Term Spyware (July 12, 2004), http://www.anti-spyware-software.net.

[34] *See* FED. TRADE COMM'N, SPYWARE WORKSHOP — MONITORING SOFTWARE ON YOUR PC: SPYWARE, ADWARE, AND OTHER SOFTWARE (2005), *available at* http://www.ftc.gov/os/2005/03/050307spywarerpt.pdf. This report is a summary of the proceedings of the FTC spyware conference that was held on April 19, 2004. *Id.*

[35] *Id.* at 1.

[36] *Id.* at 2.

[37] *Id.* at 3.

[38] *Id.*

[39] *Id.*

[40] *Id.*

disagreement about the desirability or effectiveness of this method in obtaining meaningful consent from the consumers who download such software.[41] The second impediment to defining "spyware" is whether the law should limit the term to software that monitors computer use or instead also apply the term to other types of software.[42] There seems to be a consensus, however, that surveillance is the sine qua non of spyware.[43] Finally, the panel discussed the issue of whether and to what extent the law should require some manifestation of harm before attaching the "spyware" label.[44] Some panelists argued that any installation is a trespass which is per se harmful, while others argued for a requirement of some additional harm.[45]

The consent issue is at the heart of the spyware debate. As mentioned above, there is a class of software known as "adware" — marketing software that providers often bundle with other applications — that monitors the user's Internet browsing and delivers "contextually relevant" ads.[46] These ads are usually in the form of pop-ups, though the Internet marketing industry is in a constant state of flux.[47] Adware providers dispute that their applications are spyware, insisting that users have received notice and consented to the installation.[48] Others, however, contend that the pervasive surveillance activities of adware make it just as undesirable as all other types of spyware, regardless of the technical presence of a long and complex EULA that purports to provide notice and a means for obtaining the consumer's consent. The FTC panel concluded that a definition of the term "spyware" would be important to future efforts by industry and government alike to address the problem.[49] It further offered a working definition for purposes of the workshop: "[S]oftware that aids in gathering information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge."[50] The FTC definition,

---

[41] *Id.*

[42] *Id.*

[43] *Id.*

[44] *Id.*

[45] *Id.*

[46] *Id.*

[47] *See* Anick Jesdanun, *Controversial Adware Firm Claria Wants to Cozy Up to Web Surfers*, SILICONVALLEY.COM, Aug. 1, 2005, http://www.siliconvalley.com/mld/siliconvalley/news/editorial/12276380.htm (describing Claria's plans for new adware that does not use pop-up ads).

[48] FED. TRADE COMM'N, *supra* note 34, at 4.

[49] *Id.*

[50] *Id.*

however, was viewed as a starting point, not a final definition.[51]

On the other hand, some observers believe that the spyware/adware distinction is spurious. Ben Edelman, perhaps the foremost researcher of spyware in the United States, stated:

> From the perspective of users whose computers are infected, there is nothing hard about (defining spyware). . . . If you have adware or spyware on your computer, you want it gone. Maybe the toolbar is Mother Theresa, but it's Mother Theresa sitting in your living room uninvited and you want her gone also. . . . You don't need a committee of 50 smart guys in D.C. sipping ice tea in order to decide that.[52]

Many people, fed up with the epidemic of spyware and adware, say that it is not the software's given label, but rather "what you don't want on your PC that matters."[53] In considering recently proposed spyware legislation, a U.S. Congressperson remarked, in an analogy of spyware's intrusive tactics to the "real" world: "If somebody walks in my house without my knowledge, without my permission, they're trespassing. I don't understand, I really don't understand, why we're having a . . . debate about this issue that everyone is outraged about."[54]

Recently, in the face of growing public pressure, the Center for Democracy and Technology convened the Anti-Spyware Coalition ("ASC").[55] The ASC describes itself as a "group dedicated to building a consensus about definitions and best practices in the debate surrounding spyware and other potentially unwanted technologies."[56] The ASC is composed of anti-spyware software companies, academics, and consumer groups.[57] The ASC noted that, in response to the spyware

---

[51] *Id.*

[52] Ryan Singel, *Giving New Meaning to 'Spyware,'* WIRED NEWS, July 12, 2005, http://www.wired.com/news/privacy/0,1848,68167,00.html.

[53] Maurice McElroy, *Spyware? Adware? Does It Really Matter?* (July 22, 2005), http://www.answersthatwork.com/Tasklist_pages/article_july05.htm.

[54] Michael Cowden, *Congress Promises Anti-Spyware Law*, CBS MARKETWATCH.COM, Apr. 29, 2004, http://www.marketwatch.com/news/story.asp?guid=%7BCCCD507B-F3D4-4A9A-A5ED-C76547E69783%7D&siteid=google&dist=google&cbsReferrer=www.google.com.

[55] The coalition maintains a website. *See* Anti-Spyware Coalition Homepage, http://www.antispywarecoalition.org (last visited Feb. 27, 2006).

[56] *See id.*

[57] As of August 4, 2005, the ASC members consisted of the following: Aluria, AOL, Computer Associates, Dell, Inc., EarthLink, F-Secure Corporation, HP, ICSA Labs, Lavasoft, McAfee Inc., Microsoft, Panda Software, PC Tools, Safer-Networking Ltd., Symantec, Tenebril, Trend Micro, Webroot Software, Websense, Yahoo! Inc., Center for Democracy & Technology, National Center for Victims of Crime, Samuelson Law,

epidemic, "[m]any find themselves trapped in a cyclical battle against programs that install themselves without warning, open dangerous security holes and reinstall themselves after they've been deleted."[58] As a result, the ASC released a series of spyware-related definitions, which were opened to public comment. The ASC defined "adware" and "spyware," respectively, as follows:

> **Adware:** A type of *Advertising Display Software*, specifically certain executable applications whose primary purpose is to deliver advertising content potentially in a manner or context that may be unexpected and unwanted by users. Many Adware applications also perform tracking functions, and therefore may also be categorized as *Tracking Technologies*. Some consumers may want to remove Adware if they object to such tracking, do not wish to see the advertising caused by the program, or are frustrated by its effects on system performance. . . . [S]ome users may wish to keep particular adware programs if their presence subsidizes the cost of a desired product or service or if they provide advertising that is useful or desired. . . .
>
> **Spyware:** The term Spyware has been used in two ways. In its narrow sense, Spyware is a term for *Tracking Software* deployed without adequate notice, consent, or control for the user. In its broader sense, Spyware is used as a synonym for what the ASC calls "Spyware and Other Potentially Unwanted Technologies."
>
> In technical settings, ASC uses the term Spyware only in its narrower sense. . . . However, we understand that it is impossible to avoid the broader connotations of the term in colloquial or popular usage, and we do not attempt to do so. For example, we refer to the group as the Anti-Spyware Coalition and vendors as makers of anti-spyware software, even recognizing that their scope of concern extends beyond tracking software.[59]

The ASC also released several other helpful definitions in this area, all of which it has opened up for public comment. Debate on the propriety of

---

Technology & Public Policy Clinic at Boalt Hall, UC Berkeley School of Law, The Canadian Internet Policy and Public Interest Clinic, and The Cyber Security Industry Alliance. *Id.*

[58] Anti-Spyware Coalition, Anti-Spyware Coalition Definitions and Supporting Documents Webpage, http://www.antispywarecoalition.org/documents/definitions.htm (last visited Jan. 30, 2006).

[59] Anti-Spyware Coalition, Glossary Webpage, http://www.antispywarecoalition.org/documents/glossary.htm (last visited Jan. 30, 2006).

these and other definitions is sure to continue. For now, however, the ASC definitions of "spyware" and "adware" are probably the most authoritative to date and the closest to a "standard definition" for reference purposes in any discussion.

D. Negative Aspects of Spyware

Regardless of definition, many believe that spyware has now become "public enemy number one."[60] Whether the surveillance-enabled software is labeled "malware," "spyware," or "adware," it has profound effects on a range of issues that threaten the future of e-commerce on the Internet.[61] One negative attribute of many types of spyware is that the more malevolent types install themselves through deception. The more legitimate adware programs are "bundled" with applications desired by the consumer, with some type of disclosure included at the time of installation.[62] One of the most common ways to obtain spyware is by downloading and installing any one of the several popular file-sharing programs, such as KaZaa, BearShare, or Limewire.[63] However, spyware can also be distributed by an attachment to an e-mail or directly from a webpage (a "drive-by download") through browser vulnerabilities, either clandestinely or through the use of deceptive message prompts.[64] Regardless of how spyware is installed, surveys indicate that consumers and businesses are not aware that their computers are infected with spyware.[65] A survey of Internet users, conducted by America Online and the National Cyber Security Alliance and released in October 2004,

---

[60] Paul Myer, *Spyware, Adware, and Unaware*, SECURITY MAG., June 22, 2005, http://www.storagesearch.com/8e6tech-art1.html.

[61] Smith, *supra* note 22, at 2-3 (citing *Hearing Before the S. Comm. on Commerce, Science, and Transportation*, 109th Cong. (2005) (testimony of David Moll, CEO, Webroot Software, Inc.), *available at* http://www.commerce.senate.gov/hearings/testimony.cfm?id=1496&wit_id=4255).

[62] *Id.*, at 2-3.

[63] CTR. FOR DEMOCRACY & TECH., *supra* note 25, at 9-10. Some of the peer-to-peer file sharing companies, including KaZaa, offer two versions of the software — one "free" version supported by adware and one "commercial" version that the user must pay for, but is claimed to be free of adware. *Id.* This practice apparently commenced only after these companies suffered negative publicity upon the public's discovery of the presence of adware being bundled with the programs. *Id.*

[64] FED. TRADE COMM'N, *supra* note 34, at 5-6; *see also* CTR. FOR DEMOCRACY & TECH., *supra* note 25, at 5 (describing one company, nCase, which "has been accused of deceiving users into granting permission to download and install the application by presenting potentially deceptive or confusing pop-ups on various websites or by taking advantage of poorly configured security settings in users' browsers (a practice known as 'drive-by downloads')").

[65] Smith, *supra* note 22, at 1.

revealed that 80% of all computers tested had spyware or adware installed on them.[66] Even more notably, 89% of these computer users were completely unaware of the presence of the surveillance software on their computers.[67]

Perhaps the most commonly publicized problem with spyware is the practical effects it has on the technical performance of a computer.[68] In a consumer "spyware alert," the FTC recently itemized a list of ill effects caused by spyware: (1) numerous pop-up ads, (2) a hijacked browser — a browser program that goes to websites other than those directed by the operator, (3) changes to the browser's home page, (4) unanticipated toolbars, (5) unanticipated icons in the Microsoft Windows system tray at the bottom of the desktop screen, (6) certain keys being rendered inoperable, (7) random, haphazard error messages, and (8) slowed computer performance, sometimes resulting in crashes.[69] These ill effects of spyware frustrate Internet users and lessen consumer confidence in commercial activity and communication conducted on the Internet.[70] In addition, the practical problems of spyware are not limited to consumers — businesses also suffer. Companies incur expenses when they expend effort to eradicate spyware from their employees' computers.[71] Further, computer slowdowns and crashes, although a mere annoyance or inconvenience from a purely consumer perspective, translate into productivity reductions and thereby incur profit losses from a business perspective.[72] Moreover, certain types of keylogging malware installed on a company's workstations would allow commercial surveillance that could result in the theft of trade secrets and other confidential corporate data.[73]

---

[66] AMERICA ONLINE & NAT'L CYBER SECURITY ALLIANCE, AOL/NCSA ONLINE SAFETY STUDY (Oct. 2004), *available at* http://www.staysafeonline.info/pdf/safety_study_v04.pdf.

[67] *Id.*; *see also* Michael D. Lane, Comment, *Spies Among Us: Can New Legislation Stop Spyware from Bugging Your Computer?*, 17 LOY. CONSUMER L. REV. 283, 283 (2005) ("The unfortunate reality is that many consumers are unaware that spyware exists, much less that it can cause serious problems.").

[68] Though performance is the most publicized problem, this Article submits that privacy is the much more serious problem with spyware.

[69] FED. TRADE COMM'N, FTC CONSUMER ALERT (July 2005), *available at* http://www.ftc.gov/bcp/conline/pubs/alerts/spywarealrt.pdf.

[70] Smith, *supra* note 22, at 5 (quoting testimony of Howard Beales, director of FTC's Bureau of Consumer Protection, before House Energy and Commerce Committee, April 29, 2004).

[71] *Id.*

[72] *Id.*

[73] *Id.*

Legitimate computer industry leaders are all too aware that spyware causes serious disruption in the operation of computers. At the FTC conference, a Microsoft representative reported that spyware caused 50% of all reported customer computer crashes.[74] A Dell representative reported that more than 25% of its customer service calls concerned spyware complaints.[75] Spyware has this effect on computers because it greatly increases the number of tasks a computer is requested to perform simultaneously, which can place great strains on a computer's processing power.[76] In some instances, spyware is installed such that any attempt to remove it will result in the loss of a consumer's Internet connection.[77] Spyware is also notorious for "browser hijacking," which refers to a range of effects, including changing the user's home page, inserting bookmarks, and altering search requests made on an Internet search engine.[78] Quite often, such hijacking confuses consumers into blaming some other application or their Internet provider, which only exacerbates the problem.[79] Finally, finding spyware and removing it invariably involve time and costs — some users must reformat their hard drives, which erases all data, and some users even decide that it is easier to simply discard their infected computer and purchase a new one.[80]

Another hallmark of spyware applications is the difficulty in removing them once installed.[81] There are many layers to this seemingly designed difficulty. First, spyware programs will often prevent Windows from registering the program, which would otherwise allow the typical uninstall process through the Add/Remove Programs feature.[82] Second, spyware programs frequently do not come associated with an uninstaller

---

[74] FED. TRADE COMM'N, *supra* note 34, at 8.

[75] *Id.*

[76] *Id.* A panelist at the FTC conference stated that, whereas the ordinary number of processes running on a Windows-based machine is 30 to 40, a computer infected with spyware can often have over 600 such processes running at the same time. *Id.*

[77] *Id.*

[78] *Id.* at 9; *see also* CTR. FOR DEMOCRACY & TECH., *supra* note 25, at 3.

[79] CTR. FOR DEMOCRACY & TECH., *supra* note 25, at 3.

[80] FED. TRADE COMM'N, *supra* note 34, at 8-9. The technical problems associated with spyware, while often dismissed as somewhat minimal in comparison to the privacy and consent issues, are often quite real. Take, for example, the case of Tim Binger, the owner of a heating and cooling company in Lansing, Michigan. His business computers crashed, and he was forced to bring them to a computer repair store for service. The store technicians discovered an astounding 15,324 pieces of spyware on his computers. Binger was out of business for two full days while the problem was resolved. David Eggert, *Legislature Tackles Spyware Epidemic, but Effectiveness Doubted*, DETROIT NEWS, Mar. 5, 2005, *available at* http://www.detnews.com/2005/technology/0503/05/polit-108073.htm.

[81] FED. TRADE COMM'N, *supra* note 34, at 7.

[82] *Id.*

which will remove the program.[83] Third, spyware programs notoriously have as many as 4000 files installed as part of the application and may insert up to 2000 changes in the registry on the computer, which greatly complicates any attempted manual removal of the application.[84] Fourth, many spyware programs will actually alter the file names and folder names on a constant basis, so as to evade detection and removal.[85] Finally, many spyware programs leave behind information on the computer known as a "trickler."[86] If the user deletes the trickler, then the computer will surreptitiously redownload the program and reinstall it on the user's computer.[87]

Aside from the practical, computing process effects of spyware lies the most insidious concern — privacy:

> You are being watched. Monitored. Every move you make is being recorded, logged. Your personal tastes and desires, your friends, travel plans, favorite TV shows, and newspapers. Perhaps more disturbing, this information is stored into databases, sold and shared with nameless and countless others. And you have no idea. . .
>
> This isn't a high-tech spy novel — it's the reality of cyberspace, where the vast majority of Internet users have their privacy surreptitiously violated on a regular basis. This invasion into your personal "private" life is made possible by varieties of software, insidiously installed on your computer when you're web-connected, and commonly referred to as "Spyware."[88]

Spyware obviously represents a significant privacy threat to Internet users.[89] It is always watching the users on whose computers it is installed.[90] Spyware programs can obtain financial information that a consumer desires to be kept confidential.[91] Such software is also a

---

[83] *Id.*

[84] *Id.* The registry is the "the basic configuration file for most computers with a Windows-based operating system." *Id.*

[85] *Id.*

[86] *Id.* at 8.

[87] *Id.*

[88] Michael L. Baroni, *Spyware Beware*, ORANGE COUNTY LAW., Apr. 2005, at 36.

[89] *See* CTR. FOR DEMOCRACY & TECH., *supra* note 25, at 1 (describing overview of various types of spyware and adware applications, and noting that many of them "represent a significant privacy threat").

[90] Brad Slutsky & Sheila Baran, *Just a Tad Intrusive? Spyware and the Internet*, BUS. LAW TODAY, Nov./Dec. 2004, *available at* http://www.abanet.org/buslaw/blt/2004-11-12/baram.shtml.

[91] FED. TRADE COMM'N, *supra* note 34, at 9.

ubiquitous agent of constant surveillance — every single thing a consumer does online is monitored.[92] Though the monitored activity includes sites necessary for "contextual marketers," such as e-commerce shopping activity, the spyware is also capable of monitoring consumers' visits to financial, medical, political, and religious sites and even individual chat rooms where private conversations take place. The marketing companies that distribute spyware often promise software providers to deliver the ability to "see a 360-degree view of the user's behavior — 24 hours a day, 7 days a week."[93] The amount of personal, private information transmitted to the marketing companies that distribute spyware is extensive and can be contrary to expectations of the consumers who download bundled applications.[94] In short, spyware can allow hackers and marketing companies to monitor all of a consumer's online activity. As one website states:

> Spyware can track the keystrokes you make, websites you visit, the keyword terms you use in search engines, the items you buy online, the emails you send and receive, your Instant Message dialog, and worst of all they can even record your credit card number, personal identification numbers, and all of your computer and Internet passwords.[95]

These bits of personal information are stored indefinitely because the cost of memory has become cheaper and cheaper — some companies that collect personal data online have claimed to possess over 100 million consumer profiles.[96]

---

[92] *Id.* at 10.

[93] CTR. FOR DEMOCRACY & TECH., *supra* note 25, at 4-5 (citing statements apparently once made on website of 180 Solutions, provider of adware applications).

[94] *See* Benjamin Edelman, *Methods and Effects of Spyware: Response to FTC Call for Comments* (Mar. 19, 2004), http://www.benedelman.org/spyware/ftc-031904.pdf. Edelman is a Harvard student who is one of the foremost researchers of spyware in the United States. He provides an extensive, detailed explanation of how spyware is installed and how it operates, available at his website, http://www.benedelman.org.

[95] *See* Webman Studios, About Adware, Spyware and Adware, Spyware Removal Tools Webpage, http://www.webman.com.au/adware-spyware.html (last visited Jan. 30, 2006). This data is amassed by the marketing companies in an astonishing amount. One of the biggest online marketers, a company called Claria (formerly known as Gator), now possesses the seventh largest "decision support" database in the entire world. Edelman, *supra* note 94, at 5 (citing Matthew Hicks, *Survey: Biggest Databases Approach 30 Terabytes*, EWEEK.COM, Nov. 8, 2003, *available at* http://www.eweek.com/article2/0%2C1895%2c1377106%2C00.asp).

[96] Jefferson Lankford, *Big Brother Is Watching You*, ARIZ. ATT'Y, July/Aug. 2004, at 8.

All of these concerns over spyware disillusion Internet users.[97] The public's intolerance of spyware grows every day.[98] As New York Attorney General Elliot Spitzer said recently regarding a high-profile case against adware provider Intermix, Inc.: "People are fed up with adware and spyware. They feel as though they've lost control of their computers and they want something to be done."[99] Indeed, a recent study released by the Pew Internet & American Life Project concluded that the prevalence of spyware and related privacy-intruding technologies affects the way people use the Internet and undermines their confidence in it as a medium of communication and commerce.[100] In many ways, therefore, the spyware epidemic is a threat to the future viability of the Internet as a means of conducting commerce with consumers.

II. THE EXISTING AND PROPOSED LAWS GOVERNING SPYWARE: CONSENT AS A COMMON ELEMENT

As the spyware epidemic has exploded, consumers, lawyers, government, industry, and academics have all struggled to determine whether and to what extent existing law may already apply to spyware and adware practices.[101] However, seemingly everyone assumes that contractual consent is a complete obstacle to consumer relief. This Part catalogs several of the existing statutes and doctrines that could potentially apply to spyware, as well as proposed laws related to spyware, and highlights the presence of consent as a common defense to the application of these laws. To aid discussion, this Article divides the laws into three broad areas: (1) existing federal surveillance and unauthorized use law, (2) existing tort law, and (3) proposed (or recently enacted) spyware-specific law.

---

[97] Sarah Gordon, *Elusive Intruders: Spyware & Adware*, LAW PC, May 15, 2005, at 8.

[98] *Id.*

[99] Michael Gormley, *Crusader Looks to Zap Net Spyware*, CONTRA COSTA TIMES, May 22, 2005, at f4, *available at* http://www.contracostatimes.com/mld/cctimes/11710696.htm.

[100] *See generally* PEW INTERNET & AMERICAN LIFE PROJECT, SPYWARE: THE THREAT OF UNWANTED SOFTWARE PROGRAMS IS CHANGING THE WAY PEOPLE USE THE INTERNET (2005), *available at* http://www.pewinternet.org/pdfs/PIP_Spyware_Report_July_05.pdf (collecting empirical data of consumers' online experiences and activities, and observing that many have begun taking precautions and are also in "fear" of potential threats online).

[101] *See, e.g.*, Brian Livingston, *Is Spyware Illegal Under Existing Laws?*, DATAMATION, May 24, 2005, http://itmanagement.earthweb.com/columns/executive_tech/article.php/3507261.

A. Existing Statutory Surveillance and Unauthorized Use Law

There is a well-developed body of statutory provisions in federal law that governs electronic surveillance and unauthorized use of computers. Of course, when Congress originally promulgated these laws it did not have either the Internet or spyware specifically in mind. Moreover, while these laws do address private conduct, they primarily concern law enforcement efforts.[102] Nevertheless, they "present an intuitive fit for responding to the regulatory challenges of spyware, because those statutes bar the unauthorized acquisition of electronic communications and related data in some circumstances."[103] Consent is a defense to all of these laws, however.

For instance, the Wiretap Act[104] establishes criminal liability and/or civil penalties for anyone who "intentionally intercepts, endeavors to intercept, or procures any person to intercept or endeavor to intercept, any wire, oral, or electronic communication."[105] Though there are some potential problems with whether and to what extent Internet communications such as browsing activity or e-mails can be "intercepted,"[106] there does not seem to be any real dispute that they are "electronic communications."[107] This is true even though the addition of this definition preceded popular use of the Internet by several years.

One of the defenses to liability under the Wiretap Act, however, is consent. Specifically, the Wiretap Act provides the following in relevant part:

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

---

[102] *See generally* Patricia L. Bellia, *Spyware and the Limits of Surveillance Law*, 20 BERKELEY TECH. L. J. 1283 (2005) (detailing difficulties in applying federal surveillance statutes to spyware).

[103] *Id.* at 1284.

[104] *See* 18 U.S.C. §§ 2510-2522 (2000 & Supp. II 2002).

[105] 18 U.S.C. § 2511(1)(a).

[106] *See generally* Bellia, *supra* note 102, at 1301-05 (describing how Wiretap Act's requirement of capturing communications "in transmission" presents potential problems when information is detected at point of storage along interconnected computers in networks that make up Internet).

[107] "Electronic communication" is defined in the statute 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." 18 U.S.C. § 2510(12).

> or where one of the parties to the communication has given prior consent to such interception. . . .[108]

This consent exception applies to instances of purely private conduct and thus could arguably apply to a contractual transaction involving spyware. That is, in the face of claims that its software's surveillance of a consumer's browsing activity violates the Wiretap Act, an adware company that obtained consumer consent to a EULA could argue it is immune from liability because of the consent provision of 18 U.S.C. § 2511(2)(d).

The Stored Communications Act[109] is a companion statute to the Wiretap Act. Congress enacted this Act in 1986 to expand law enforcement's ability to obtain data or communications that were in storage and thus could not be "intercepted" during live transmission.[110] The Stored Communications Act creates criminal and/or civil liability for anyone who "intentionally accesses without authorization a facility through which an electronic communication service is provided" or who "intentionally exceeds an authorization to access that facility" and by either of these actions "thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system . . . ."[111] This last requirement itself alludes to the "authorization" of a party to access a computer facility.[112]

As with the Wiretap Act, however, there is an express consent defense in the Stored Communications Act. Specifically, the consent provision provides that a person is not liable under the Act for retrieval of a stored communication from an "electronic communications service" that was authorized "by a user of that service with respect to a communication of or intended for that user."[113] Thus, so long as the user either sent the electronic communication or the sender intended the user to receive it, it would seem that such user has the statutory power to consent to any retrieval of her communications. Therefore, in the face of claims that its software's surveillance of browsing activity violates the Stored Communications Act, an adware company could assert a consent defense similar to that under the Wiretap Act. That is, it could argue that

---

[108] 18 U.S.C. § 2511(2)(d).

[109] *See* 18 U.S.C. §§ 2701-2711 (2000 & Supp. II 2002).

[110] *See* Bellia, *supra* note 102, at 1291 n.40 (citing S. REP. NO. 99-541, at 8 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3562 (describing e-mail systems); H.R. REP. NO. 99-647, at 22 (1986) (same)).

[111] 18 U.S.C. § 2701(a).

[112] *Id.*

[113] *Id.* § 2701(c)(2).

it is immune from liability under the authorization provision of 18 U.S.C. § 2701(c)(2).

Also important here is the Computer Fraud and Abuse Act ("CFAA"), passed by Congress in 1984.[114] Unlike the Wiretap Act and Stored Communications Act, which relate to wrongfully appropriated content, the CFAA focuses more on the wrongfully appropriated access to a computer itself.[115] Several provisions of the CFAA could potentially apply to purely private spyware- or adware-related transactions. For instance, section 1030(a)(2) of the CFAA provides criminal liability for whoever "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer if the conduct involved an interstate or foreign communication."[116] Unlike the Wiretap Act and the Stored Communications Act, the CFAA does not contain a separate consent provision as a defense. However, the fact that the CFAA only penalizes "unauthorized" computer access presupposes that any consent or authorization which has been given to the accessing entity will create a defense to liability under the CFAA.[117] This could pose a problem for litigants seeking to sue spyware or adware providers under the CFAA. A provider could argue that the user's consent to installation of the program makes the provider's access to the user's computer "authorized." Unlike the Wiretap Act and the Stored Communications Act, however, any such authorization under the CFAA would have to come from the computer user herself, rather than the mere one-party consent that is sanctioned under the Wiretap Act and the Stored Communications Act.

---

[114] *Id.* § 1030.

[115] *See* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1615-17 (2003).

[116] 18 U.S.C. § 1030(a)(2). Subsection (a)(2) also refers to unauthorized access to "information contained in a financial record of a financial institution, or of a card issuer . . . , or contained in a file of a consumer reporting agency on a consumer . . . ," as well as unauthorized access to "information from any department or agency of the United States." *Id.*

[117] *See* Bellia, *supra* note 102, at 35 n.174 ("Because the CFAA requires a showing that any access to a computer was without authorization or exceeded authorized access, it raises a consent or authorization [issue] similar to the Wiretap Act and the [Stored Communications Act].").

B. Tort Theories that May Apply to Spyware

Tort law provides another potential doctrine for consumers aggrieved by spyware, adware, or related wrongful online activity. Though many different torts could be potentially considered for such action,[118] this Article focuses on the two most likely ones: trespass and invasion of privacy. As is the case with the federal statutes on surveillance and unauthorized use, consent is a defense to liability for these torts.

1. Trespass

Many commentators, and some litigants, have looked to trespass law for a possible remedy for wrongful actions online or involving access to computers generally.[119] Since a computer is undoubtedly personal property, trespass to chattels has been proffered as a potential theory to use for wrongful online activity. Section 217 of the *Restatement (Second) of Torts* provides that "[a] trespass to a chattel may be committed by intentionally . . . using or intermeddling with a chattel in the possession of another."[120] Section 218 of the *Restatement* provides, in relevant part, that "[o]ne who commits a trespass to a chattel is subject to liability to the possessor of the chattel if, but only if . . . the chattel is impaired as to its condition, quality, or value, or . . . harm is caused to some person or thing in which the possessor has a legally protected interest."[121] It is fairly easy to envision application of the trespass to chattels doctrine to the practice of unwanted spyware access on a computer. In fact, unauthorized computer access, such as by remotely-installed spyware, resembles a trespass in many ways.[122] The unwanted installation of spyware onto the user's computer can certainly be said to be an intentional act by the distributor of the spyware to use or intermeddle with the consumer's computer and processing power. The same can be said for the surreptitious data collection and transmission back to the

---

[118] Conversion and nuisance are two torts that other commentators have previously considered, but which this Article will not discuss. *See generally* Dan L. Burk, *The Trouble with Trespass*, 4 J. SMALL & EMERGING BUS. L. 27 (2000) (discussing trespass liability for computer-related activity); Orin Kerr, *The Limits of Computer Conversion:* United States v. Collins, 9 HARV. J. L. & TECH. 205 (1996) (discussing conversion liability for computer-related activity).

[119] *See, e.g.*, Lane, *supra* note 67 at 295-98; *see also* Kerr, *supra* note 118, at 212 ("It is trespass . . . that provides the common law framework best suited to prevent computer system abuse."); Michael R. Siebecker, *Cookies and the Common Law: Are Internet Advertisers Trespassing on Our Computers?*, 76 S. CAL. L. REV. 893, 911-29 (2003).

[120] RESTATEMENT (SECOND) OF TORTS § 217 (1965).

[121] *Id.* § 218.

[122] *See* Kerr, *supra* note 115, at 1606.

spyware distributor. Moreover, such acts by the spyware companies arguably meet the impairment element of section 218 because the infusion of spyware onto the computer impairs the condition or quality of the user's computer in the form of slower performance, crashes, and data acquisition.

Like the federal surveillance and unauthorized use statutes, however, consent is an issue in trespass to chattels cases. Specifically, section 252 of the *Restatement* provides that "[o]ne who would otherwise be liable to another for trespass to a chattel or for conversion is not liable to the extent that the other has effectively consented to the interference with his rights."[123] Section 892 relates to consent as a defense for all torts under the *Restatement* and provides:

> Consent is willingness in fact for conduct to occur. It may be manifested by action or inaction and need not be communicated to the actor. . . . If words or conduct are reasonably understood by another to be intended as consent, they constitute apparent consent and are as effective as consent in fact.[124]

Section 892A confirms that the presence of effective consent eliminates any liability on the part of the alleged trespasser.[125] Thus, if a consumer brought suit for trespass to chattels against a spyware vendor who had obtained the consumer's purported contractual assent to installation of the spyware, the vendor would potentially have a consent defense to the trespass action. The same would apply to the vendor if the consumer had brought suit under the CFAA, the Wiretap Act, or the Stored Communications Act.

With respect to allegedly wrongful online activity such as spyware, trespass to chattels is the only trespass action which has been seriously discussed among commentators and courts. However, the traditional trespass action, which refers to injuries against land rather than chattels, may also be important here. One is liable for trespass if she intentionally enters upon land owned by another or causes anything to enter upon such land.[126] Furthermore, the injury is the invasion itself — liability

---

[123] RESTATEMENT (SECOND) OF TORTS § 252 (1965).

[124] *Id.* § 892 (1979).

[125] *See id.* § 892A (providing, in pertinent part, that "[o]ne who effectively consents to conduct of another intended to invade his interests cannot recover in an action of tort for the conduct or for harm resulting from it").

[126] *See id.* § 158 (1965) ("One is subject to liability to another for trespass, irrespective of whether he thereby causes harm to any legally protected interest of the other, if he intentionally . . . enters land in the possession of the other, or causes a thing or a third person to do so . . . .").

obtains regardless of whether any actual harm is caused.[127] This ability, under land-based trespass doctrine, for the tort to be committed by the causing of *things* to enter upon someone else's land has interesting implications for spyware and other wrongful online activity. Spyware and other unwanted code, when installed upon a consumer's computer, is arguably a "thing" that enters the computer, which is almost invariably inside the consumer's home. Thus, the spyware vendor has caused a "thing" (spyware program) to enter upon the land (home) of the consumer (via the consumer's computer, which is on the land). Hence, it is theoretically conceivable to argue that spyware is a trespass to land as well as to chattels. However, as with trespass to chattels and to land, and generally most torts, consent is a defense.[128] Therefore, any spyware vendor sued in trespass would have recourse to consent as a defense in the event a EULA was presented to the consumer and assent was manifested by "clicking through."

2. Invasion of Privacy

Whereas resort to trespass comports with the physical nature of spyware's ill effects, invasion of privacy addresses the pernicious nature of its intrusion into consumers' private lives and their activities. "Privacy" has been defined as "the right to be let alone."[129] The right to privacy as an actionable tort has its formal origin in an 1890 *Harvard Law Review* article by Samuel Warren and Louis Brandeis, *The Right to Privacy*.[130] It has since been compartmentalized into four basic categories of offenses.[131] Hence, section 652A of the *Restatement (Second) of Torts* provides that invasion of privacy is actionable and that one's privacy can be invaded in any of the following four ways: (1) "unreasonable intrusion upon the seclusion of another," (2) "appropriation of the other's name or likeness," (3) "unreasonable publicity given to the other's private life," or (4) "publicity that unreasonably places the other in a false light before the public."[132] Of these four possibilities, the intrusion upon one's seclusion is probably the most applicable to most instances of privately occurring spyware and adware. Section 652B of

---

[127] *Id.*

[128] *Id.* § 167 (stating that *Restatement's* general rules on consent set forth in sections 892-892D are applicable to trespasses to land).

[129] *Id.* § 652A cmt. A (1977).

[130] *See generally* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

[131] *See* William Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960).

[132] RESTATEMENT (SECOND) OF TORTS § 652A (1977).

the *Restatement* states the principle with respect to the seclusion offense: "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."[133] As the comments to section 652B indicate, no publicity is necessary for this offense.[134] Further, the comments discuss the manner in which the intrusion upon one's seclusion may be accomplished:

> The invasion may be by physical intrusion into a place in which the plaintiff has secluded himself, as when the defendant forces his way into the plaintiff's room in a hotel or insists over the plaintiff's objection in entering his home. It may also be by the use of the defendant's senses, with or without mechanical aids, to oversee or overhear the plaintiff's private affairs, as by looking into his upstairs windows with binoculars or tapping his telephone wires. It 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, or compelling him by a forged court order to permit an inspection of his personal documents. The intrusion itself makes the defendant subject to liability, even though there is no publication or other use of any kind of the photograph or information outlined.[135]

It is easy to map a potential cause of action for invasion of privacy in terms of intrusion upon one's seclusion over the typical facts and circumstances surrounding spyware. The spyware distributor is intruding into the consumer's seclusion by viewing her online activities at every moment, right in the privacy of her own home. "One's home is his castle, and one's private life is a precious possession which cannot be wrested from him."[136] Thus, the constant, ubiquitous surveillance effected by spyware located on a consumer's computer could quite arguably be held to be actionable as an invasion of privacy.

---

[133] *Id.* § 652B.

[134] *Id.* § 652B cmt. a ("The form of invasion of privacy covered by this Section does not depend upon any publicity given to the person whose interest is invaded or to his affairs. It consists solely of an intentional interference with his interest in solitude or seclusion, either as to his person or as to his private affairs or concerns, of a kind that would be highly offensive to a reasonable man.").

[135] *Id.* § 652B cmt. b.

[136] Louis Nizer, *The Right of Privacy, A Half Century's Developments*, 39 MICH. L. REV. 526, 560 (1941).

As with all torts, however, it appears that consent is a defense in most cases of invasion of privacy. Interestingly, the defense of consent to the "intrusion upon seclusion" type of invasion of privacy does not readily appear in the *Restatement*. Rather, the only consent to invasion of privacy referred to by the *Restatement* has to do with consent to the publication of information.[137] Because the intrusion upon seclusion tort does not require any publication at all, however, it would not appear that this publication-based method of consent, akin to consent in defamation cases, would be applicable. Nevertheless, most jurisdictions that have adopted the tort hold that consent is either a defense or, rather, that the absence of consent is itself an element of the tort.[138] Therefore, in the face of a consumer's suit for invasion of the right of privacy, a spyware company could attempt to argue that any contractually granted consent serves as a defense to such suit.

C. *Recently Proposed and Enacted Spyware-Specific Legislation*

Given the currency of the spyware problem, legislatures across the country are beginning to entertain proposed measures to regulate spyware.[139] Moreover, in the 109th Congressional session in 2005, at least four highly publicized spyware-specific proposals were pending in Congress. These proposals were based on Congress's recognition of "the devastating damage that [spyware] can inflict on individuals and businesses, [and the fact that] they also undermine the confidence that citizens have in using the Internet."[140] The proposals were the Securely Protect Yourself Against Cyber Trespass Act ("SPY ACT"),[141] the Internet Spyware Prevention Act of 2005 ("I-SPY"),[142] the Software Principles Yielding Better Levels of Consumer Knowledge Act ("SPY BLOCK

---

[137] *See* RESTATEMENT (SECOND) OF TORTS § 652F (1977). Section 652F provides that "[t]he rules on absolute privileges to publish defamatory matter stated in §§ 583 to 592A apply to the publication of any matter that is an invasion of privacy." *Id.*

[138] *See* DAVID A. ELDER, PRIVACY TORTS § 2:12 (2002) ("Although some decisions refer to consent to an intrusion as a defense, the preferable perspective, as in the case of intentional torts generally, is that consent, whether express or implied, negates the existence of the tort itself." (citing Engman v. Sw. Bell Tel. Co., 631 S.W.2d 98, 100-02 (Mo. Ct. App. 1982); Leggett v. First Interstate Bank of Oregon, 739 P.2d 1083, 1086 (Or. Ct. App. 1987); *Waiver or Loss of the Right of Privacy*, 57 A.L.R. 3d 16 (1975))).

[139] The National Conference of State Legislatures website has a list of the jurisdictions which have passed, or are considering, spyware-related proposals. National Conference of State Legislatures, 2005 State Legislation Relating to Internet Spyware Webpage, http://www.ncsl.org/programs/lis/spyware05.htm (last visited Jan. 11, 2006).

[140] Internet Spyware Prevention Act of 2005, H.R. 744, 109th Cong. § 4 (2005).

[141] Spy Act, H.R. 29, 109th Cong. (2005).

[142] H.R. 744.

Act"),[143] and the Enhanced Consumer Protection Against Spyware Act of 2005.[144] It is presently unknown whether any of these bills will become law, and they vary in their specific definitions and treatment of the spyware problem. However, they all directly or indirectly provide for an improved "notice and consent" regime for consent-based adware or spyware installations.[145] This reflects the inertia associated with acceptance of the consent-based "spyware/adware bargain." Hence, existing surveillance, trespass, and invasion of privacy law, as well the currently pending federal spyware-specific proposals, operate on the same fundamental premise. This premise is that a consumer may, if she knowingly chooses, validly consent to the installation and execution of spyware on her computer, even if the software conducts continual surveillance of her online activities.

III. CASES DISCUSSING THE RELATIONSHIP OF CONTRACT TO CONSENT TO SURVEILLANCE, TRESPASS, OR OTHER HARMS

As discussed in the previous part, virtually all existing or proposed laws applicable to spyware contain an element of consent, either as a defense or the nonexistence of which is one of the prima facie elements of the offense.[146] The manner of consent and the means by which it is applied to avoid liability varies considerably across the statutes and

---

[143] Spy Block Act, S. 687, 109th Cong. (2005).

[144] Enhanced Consumer Protection Against Spyware Act of 2005, S. 1004, 109th Cong. (2005).

[145] *See* S. 1004, § 8 (declaring it unlawful to intentionally access, without authorization, protected computer "by causing a computer program or code to be copied onto the protected computer, and intentionally us[ing] that program or code in furtherance of another Federal criminal offense" or by using program to "intentionally impair the security protection of the protected computer"); S. 687, § 2 (declaring unlawful installation of any software by nonauthorized user where installation either conceals itself or denies user any opportunity to give consent to program being installed); *Id.* § 3 (prohibiting installation of software with "surreptitious information collection feature," which is defined in part as software that collects and transmits data without providing clear and conspicuous notice to user and without giving user opportunity to prevent installation and operation of software); H.R. 744, § 2 (making it violation to intentionally access, without authorization, protected computer "by causing a computer program or code" to be copied onto protected computer, and intentionally us[ing] that program or code in furtherance of another Federal criminal offense"); H.R. 29, § 3 (providing for notice screen to consumers indicating that software will collect and transmit information about consumer, and requiring agreement to statement before installation may proceed).

[146] *See supra* notes 101-45 and accompanying text; *see also* Lane, *supra* note 67, at 298 ("[T]he question is obscured in cases where spyware notice is buried deep within end user license agreements, forcing courts to first deal with whether this constitutes consent.").

doctrines discussed in the previous Part.[147] One of the types of consent that the wrongdoer may obtain is simultaneous, or near-simultaneous, "nontransactional" consent. By "non transactional," I simply mean that the consent obtained is not part of a transaction — a contract, a bargained-for exchange of some kind. To take an example from the tort law of trespass, if a person comes to your front door and asks to come inside for a moment to visit and you agree, the visitor is not guilty of trespass by entering onto your property in the manner discussed.[148] In this example, there was no bargained-for exchange between you and the visitor. Your consent was simply requested at the moment of the visitor's proposed invasion of your house, and you simultaneously agreed to it, indicating your consent. This eliminates any liability of the visitor.[149] This type of immediate, contemporaneous, nontransactional consent is fairly universal and will apply to most of the statutes and other doctrines discussed in the previous part,[150] in addition to

---

[147] When there is no consent involved, this Article assumes that the installation and operation of spyware for purposes of surveillance and monitoring on a consumer's computer violates existing law or soon will under any of the federal proposals, if enacted.

[148] *Cf.* RESTATEMENT (SECOND) OF TORTS § 167 cmt. a, illus. 1 (1965) ("A, a sheriff, comes to B's house to search for contraband liquor. He tells B that he has forgotton [sic] to bring his search warrant. B nevertheless tells him to come in. A's entry is by consent of B and is not a trespass.").

[149] *See id.* § 892A(1) (1979) ("One who effectively consents to conduct of another intended to invade his interests cannot recover in an action of tort for the conduct or for harm resulting from it.").

[150] In cases under the Wiretap Act, 18 U.S.C. §§ 2510-2522 (2000 & Supp. II 2002), the situation comes up frequently in the context of a potential informant granting the government consent to record conversations with another person under investigation. *See, e.g.*, United States v. Davanzo, 699 F.2d 1097, 1100 (11th Cir. 1983); United States v. Jones, 693 F.2d 343, 346 (5th Cir. 1982). Consent to surveillance under the Wiretap Act, however, can also be granted to a private party. *See, e.g.*, Griggs-Ryan v. Smith, 904 F.2d 112, 118 (1st Cir. 1990) (holding tenant consented to all recordings of home phone calls where landlord informed tenant several times that she was making such recordings). There appear to be no cases decided under the Stored Communications Act, 18 U.S.C. §§ 2701-2711 (2000 & Supp. II 2002), that deal with such simultaneous, nontransactional consent to acquisition of data. There are also comparatively few cases on the consent/authorization issue under the CFAA, 18 U.S.C. § 1030 (Supp. 2002), but there is at least one case that suggests a contemporaneous, nontransactional authorization. *See* Davies v. Afilias Ltd., 293 F. Supp. 2d 1265, 1273 (M.D. Fla. 2003) (holding that Internet domain name registrant did not violate CFAA by registering certain names with registering entity, in part, because entity provided registrants with authorization codes that allowed him to access system).

There are not very many reported cases on consent in the context of consent to the privacy tort of intrusion upon seclusion. There is at least one case where a court appeared to conclude that express consent was given, which defeated a claim of invasion of privacy. *See* Hall v. Heavey, 481 A.2d 294, 593-94, 597 (N. J. Super. Ct. App. Div. 1984) (holding that customer of grocery store had no claim for invasion of privacy caused by store employee searching through customer's pocketbook, where customer admitted that she had

trespass.[151] This type of consent, being beyond the purview of contract law, is not the focus of this Article. For that reason, and for the reason that such nontransactional, contemporaneous consent seems fairly unlikely in the current context of spyware and consent to surveillance upon one's own online activities (except for perhaps in the context of law enforcement or employment relationships), this Article does not address it any further. Rather, it focuses on "transactional" consent, or consent deemed to arise by virtue of having entered into a contractual exchange.

A. Cases Where Contractual Consent Is Exceeded

In the computer/online context, there is now considerable authority for the proposition that certain activity is *not* consented to or authorized, by virtue of someone having *exceeded* the authority which was otherwise granted in a contract. These appear to be mostly trespass and CFAA cases. A couple of cases will illustrate the proposition. In *EF Cultural Travel BV v. Zefer Corp.*,[152] Explorica (a start-up travel company) used "scraper" software designed by Zefer to access a competitor's website and rapidly glean the competitor's prices for a variety of travel packages that Explorica then used to undercut the competitor's prices.[153] The

---

consented to allow search upon accusation of shoplifting). "Undoubtedly, [however] the more common type of consent in intrusion or trespass cases is the implied variety." DAVID A. ELDER, PRIVACY TORTS § 2:12, at 2-128 (2002). In the words of one court: "Frequently, perhaps more than otherwise, the consent will be implied rather than expressed. Consent may be implied from custom, local or general, from usage or from the conduct of the parties, or some relationship between them." *Id.* (quoting Engman v. Sw. Bell Tel. Co., 631 S.W.2d 98, 101 (Mo. Ct. App. 1982)). There are several examples of cases holding that a person impliedly consented to the invasion of his or her privacy by intrusion upon seclusion. *See, e.g.*, Moffett v. Gene B. Glick Co., 621 F. Supp. 244, 283 (N.D. Ind. 1985), *overruled on other grounds by* Reeder-Baker v. Lincoln Nat'l Corp., 644 F. Supp. 983 (N.D. Ind. 1986) (holding that plaintiff consented to invasion of privacy by discussing personal and intimate relationship at place of employment); Wolf v. Regardie, 553 A.2d 1213, 1218 (D.C. 1989) (holding that plaintiff consented to invasion of privacy by disclosing confidential facts to person who then disclosed those facts to other persons).

Obviously, there are not yet any decisions under any of the proposed, or enacted, spyware-specific laws regarding the interpretation of "consent" under those statutes. In a theoretical case, it would seem plausible, however, that contemporaneous, nontransactional consent, if given (and untainted by fraud, misunderstanding, or other circumstances), would be held to be a defense under any of those statutes, however unlikely such a scenario might be.

[151] *See supra* notes 148-49 and accompanying text.

[152] EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58 (1st Cir. 2003).

[153] *Id.* at 60. In an earlier companion case against EF Cultural, the competitor whose website was "scraped" for data, the court described this technological process in some detail:

competitor, EF Cultural, complained about access to its website in this manner and filed suit against both Explorica and Zefer, alleging violations of the CFAA[154] and the federal Copyright Act.[155] During the litigation, Zefer filed for bankruptcy, and, thus, the case only proceeded against Explorica initially.[156] The principals of Explorica were former employees of EF Cultural and were subject to confidentiality agreements that prohibited the disclosure of certain EF Cultural codes and trade information they provided to Zefer for use in designing the scraper. The First Circuit therefore affirmed the finding that there was a substantial likelihood that Explorica's actions constituted "unauthorized access" of EF Cultural's computer (which, in turn, operated the website) under the CFAA, and accordingly affirmed the district court's injunction preventing Explorica from further accessing the website in that manner.[157]

When the automatic stay in Zefer's bankruptcy was lifted, EF Cultural resumed the litigation against Zefer.[158] Unlike the principals of Explorica, Zefer was not contractually bound by the terms of the confidentiality agreement, but rather dealt with EF Cultural at arms' length.[159] Nevertheless, the First Circuit ultimately affirmed the

---

> The scraper has been likened to a "robot," a tool that is extensively used on the Internet. Robots are used to gather information for countless purposes, ranging from compiling results for search engines such as Yahoo! to filtering for inappropriate content. The widespread deployment of robots enables global Internet users to find comprehensive information quickly and almost effortlessly. Like a robot, the scraper sought information through the Internet. Unlike other robots, however, the scraper focused solely on EF's website, using information that other robots would not have. Specifically, Zefer utilized tour codes whose significance was not readily understandable to the public. With the tour codes, the scraper accessed EF's website repeatedly and easily obtained pricing information for those specific tours. The scraper sent more than 30,000 inquiries to EF's website and recorded the pricing information into a spreadsheet.

EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 579 (1st Cir. 2001).

[154] 18 U.S.C. § 1030 (2005).

[155] *Zefer*, 318 F.3d at 60 (citing 17 U.S.C. §§ 101-1332 (2000)).

[156] *Zefer*, 318 F.3d at 61. After Zefer filed for bankruptcy, the automatic stay prevented the litigation against Zefer from continuing. *Id.* (citing 11 U.S.C. § 362(a)(1) (2000)).

[157] *Explorica*, 274 F.3d at 583-84.

[158] *Zefer*, 318 F.3d at 60.

[159] *Id.* at 61. The court also rejected an argument by EF Cultural that Zefer must have known that all of the information it received from Explorica about the website was confidential. *Id.* at 61-62. Although Explorica's provision of the codes to Zefer greatly speeded the process of designing the scraper, the court noted that anyone, including Zefer, could have obtained the codes by simply reviewing the pages within EF Cultural's website. *Id.*

injunction on the basis that since Explorica was enjoined from accessing the EF Cultural website with the scraper, Zefer was not authorized to assist Explorica in violating the district court's injunction.[160] As part of its argument that the injunction should be independently affirmed as to Zefer, EF Cultural claimed that Zefer's access to the website through the high-speed scraper program was "unauthorized access" under the CFAA because such use was prohibited by the terms of use of the website itself.[161] The court rejected this argument, not because the terms of use on a website would not be operative, but because EF Cultural had no such terms posted on its website at the time of Zefer's access using the scraper.[162] Indeed, the court conceded the potential efficacy of such a notice, if posted on the website:

> The issue, then, is whether use of the scraper "exceed[ed] authorized access." A lack of authorization could be established by an explicit statement on the website restricting access. (Whether public policy might in turn limit certain restrictions is a separate issue.) Many webpages contain lengthy limiting conditions, including limitations on the use of scrapers. However, at the time of Zefer's use of the scraper, EF had no such explicit prohibition in place, although it may well use one now. . . .
>
> . . . .
>
> If EF wants to ban scrapers, let it say so on the webpage or a link clearly marked as containing restrictions.[163]

---

[160] *Id.* at 63 ("[A]n injunction properly issued against a named party means that anyone else with notice is precluded from acting to assist the enjoined party from violating the decree or from doing so on behalf of that party." (citing FED. R. CIV. P. 65(d); G. & C. Merriam Co. v. Webster Dictionary Co. Inc., 639 F.2d 29, 34-35 (1st Cir. 1980))).

[161] *Id.* at 62-63.

[162] *Id.* at 62.

[163] *Id.* at 62-63. The court noted, as an example of such an explicit restriction on the commercial use of a website, the following which was contained on America Online's site as of January 14, 2003:

> [Y]ou may print or download one copy of the materials or content on this site on any single computer for your personal, non-commercial use, provided you keep intact all copyright and other proprietary notices. Systematic retrieval of data or other content from this site to create or compile, directly or indirectly, a collection, compilation, database or directory without written permission from America Online is prohibited.

Id. at 62 n.3 (citing AOL Anywhere Terms and Conditions of Use, http://www.aol.com/copyright.html (last visited Jan. 14, 2003)).

Thus, the court assumed that the terms of access posted on a website would rise to the level of a contractual or quasi-contractual exchange whereby EF Cultural could allow users to visit its website in exchange for the users' agreement to abide by the terms and restrictions on such access. Exceeding such access would be unauthorized access and thereby a violation of the CFAA, among other potential violations.

Another example of this type of reasoning under the CFAA, as well as trespass law, is *America Online, Inc. v. LCGM, Inc.*[164] In *America Online*, America Online ("AOL") complained about LCGM's harvesting of e-mail addresses of AOL subscribers and its submission of unsolicited bulk e-mail advertising LCGM's various pornographic websites to the e-mail addresses.[165] AOL alleged that this activity, known derisively as "spam" in the industry,[166] violated its terms of service, which barred "both members and nonmembers from sending bulk e-mail through AOL's computer systems."[167] AOL alleged that LCGM's bulk e-mail activity consumed capacity on its computers, impaired AOL's e-mail system which required repair, damaged AOL's goodwill, and actually resulted in lost customers and lost profits.[168] Thus, AOL sued LCGM under the CFAA, the Lanham Act, and various state law doctrines including trespass to chattels.[169] As to the CFAA claim, the court found that LCGM was subject to AOL's terms of use because it was itself an AOL

---

[164] Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444 (E.D. Va. 1998).

[165] *Id.*

[166] This is, of course, not to be confused with the processed meat product, SPAM. Sure enough, the meat product SPAM has its own website, located at http://www.spam.com. One might assume that the nickname "spam" for bulk unsolicited e-mail is derived from a perhaps unfavorable view of this enduring meat product. The SPAM website, however, states: "Use of the term "spam" was adopted as a result of the Monty Python skit in which our SPAM meat product was featured. In this skit, a group of Vikings sang a chorus of 'spam, spam, spam' . . . in an increasing crescendo, drowning out other conversation. Hence, the analogy applied because [unsolicited bulk e-mail] was drowning out normal discourse on the Internet." *See* SPAM Corp., *SPAM and the Internet*, http://www.spam.com/ci/ci_in.htm (last visited Jan. 30, 2006); *see also* Webopedia, Definition of "Spam," http://www.webopedia.com/TERM/s/spam.html (last visited Jan. 30, 2006) ("There is some debate about the source of the term, but the generally accepted version is that it comes from the Monty Python song, 'Spam spam spam spam, spam spam spam spam, lovely spam, wonderful spam' . . . . Like the song, spam is an endless repetition of worthless text.")

[167] *Am. Online*, 46 F. Supp. 2d at 448.

[168] *Id.* at 449.

[169] *Id.* at 446. The Lanham Act claims concerned AOL's allegation that LCGM's use of "aol.com" in its e-mails gave the false appearance of AOL's official involvement with the project and that such use would damage AOL's interest in the value of its brand name and marks. *Id.* at 449-50. The court concluded that AOL had proven its Lanham Act claims of false designation of origin and dilution. *Id.*

member.[170] Though the AOL terms of service were obviously designed to allow LCGM some access to AOL's computer systems as a subscriber, the court found that LCGM's "actions [in sending unsolicited bulk e-mail] violated AOL's Terms of Service, and as such was [sic] unauthorized" under the CFAA.[171]

The court subsequently addressed AOL's claim that LCGM's actions were independently actionable on trespass to chattels grounds.[172] The court defined a "trespass to chattels" as "when one party intentionally uses or intermeddles with personal property in rightful possession of another without authorization."[173] Further, the court noted that, in order for LCGM to be liable for such trespass, AOL must have shown that the chattel had been impaired as to its "condition, quality, or value."[174] The court found it sufficient, for trespass purposes, that LCGM's e-mails were an intentional use of AOL's computer systems (its chattels) and that the "transmission of electrical signals through a computer network [was] sufficiently 'physical' contact to constitute a trespass to property."[175] Although AOL's terms of service allowed ordinary use of e-mail over the system, it specifically prohibited the sending of unsolicited bulk e-mail.[176] Therefore, the court held that LCGM's contact with AOL's computer systems exceeded the authorization granted to LCGM in its AOL subscription contract and therefore constituted a trespass to chattels.[177] *Zefer* and *America Online* thus illustrate the proposition that contract language can set the bounds for authorized access to a computer

---

[170] *Id.* at 450. In fact, LCGM admitted that it used its AOL membership to harvest the AOL e-mail addresses that were later "spammed." *Id.*

[171] *Id.*

[172] *Id.* at 451-52. The court applied Virginia's common law trespass to chattels doctrine in its analysis. *Id.*

[173] *Id.* (citing Am. Online, Inc. v. IMS, 24 F. Supp. 2d 548 (E.D. Va. 1998)); RESTATEMENT (SECOND) OF TORTS § 217(b) (1965).

[174] *Id.* at 452 (citing *IMS*, 24 F. Supp. 2d at 548); RESTATEMENT (SECOND) OF TORTS § 217(b).

[175] *Id.* (citing CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1021 (S.D. Ohio 1997)). In *CompuServe*, under similar facts, the court stated: "To the extent that defendants' multitudinous mailings demand the disk space and drain the processing power of plaintiff's computer equipment, those resources are not available to serve [plaintiff] subscribers. Therefore, the value of that equipment to [plaintiff] is diminished even though it is not physically damaged by defendants' conduct." *Id.* (citing *CompuServe*, 962 F. Supp. at 1022).

[176] *Id.*

[177] *See id.* Other similar cases exist, but these are sufficient to make the point. *See, e.g.*, Hotmail Corp. v. Van$ Money Pie, Inc., No. C-98 JW PVT ENE, 1998 WL 388389, at *7 (N.D. Cal. Apr. 16, 1998) (holding that use of e-mail account for purposes of sending spam was potentially trespass to chattels); *CompuServe, Inc.*, 962 F. Supp. at 1021-22 (same).

system.[178] Exceeding such bounds will often constitute a trespass to chattels or a violation of the CFAA as to the owner of the computer.[179]

B. Cases Discussing Consent to "Cookie" Surveillance by Contract Between a Host Website and a Third Party Surveillance Agent

Zefer and *America Online*, and the cases similar to them, discuss the issue of consent and authorization via contract in the converse: the scope of contract language was exceeded and therefore the contract helped establish that the plaintiffs did not consent to or authorize the actual actions taken by the defendants in those cases. On the other hand, some recent online cases in the "cookie" context demonstrate by tangential reference the use of contracts for affirmative consent to access to computer systems.[180] In *In re DoubleClick, Inc., Privacy Litigation*, DoubleClick was an online marketing company which contracted with over 11,000 various websites to provide them with "banner advertisements."[181] DoubleClick served as an intermediary between companies that wanted to advertise on the Internet generally and those "host" websites that were willing to sell advertising space.[182] Specifically, DoubleClick "promise[d] client Web sites that it [would] place their banner advertisements in front of viewers who match[ed] their demographic target."[183] So, for instance, DoubleClick might have promised a golfing supply company that it would make sure its golf club ads were displayed to users that were known to have purchased golf clubs and related products in the past.[184] DoubleClick accomplished this through cookies, meaning that whenever a user visited a DoubleClick-

---

[178] Orin Kerr has proposed that simple breach of contract, or exceeding contractual authority to access a computer system, alone should not be sufficient to constitute unauthorized access. *See* Kerr, *supra* note 115, at 1600. Instead, he suggests that some circumvention of code-based restrictions, such as "hacking" into the system or cracking in with stolen passwords, should be required under such statutes as the CFAA. *Id.*

[179] *Id.*

[180] *See In re* Pharmatrak, Inc., 329 F.3d 9, 19-21 (1st Cir. 2003), *remanded to* 292 F. Supp. 2d 263 (D. Mass. 2003); *In re* Toys R Us, Inc., Privacy Litig., No. 00-CV-2746, 2001 WL 34517252, at *5, *7 (N.D. Cal. Oct. 9, 2001); Chance v. Avenue A, Inc., 165 F. Supp. 2d 1153, 1160-62 (W.D. Wash. 2001); *In re* DoubleClick, Inc., Privacy Litig., 154 F. Supp. 2d 497, 510-11 (S.D.N.Y. 2001).

[181] *DoubleClick*, 154 F. Supp. 2d at 502. "Banner advertisements are so named because they generally resemble flags or banners, in that they tend to be long and narrow and their width often spans a significant part of a Web page." *Id.* at 502 n.6 (citing Amended Complaint ¶ 60, *DoubleClick*, 154 F. Supp. 2d. (No. 00-Civ-0641)

[182] *Id.* at 502.

[183] *Id.*

[184] *Id.*

affiliated website, a cookie was transferred to the hard drive of the user's computer.[185] Gradually, so that DoubleClick could build a marketing profile of the user, the cookie collected "information . . . such as names, e-mail addresses, home and business addresses, telephone numbers, searches performed on the Internet, Web pages or sites visited on the Internet. . . ."[186] Then, when a user visited a host website that dealt with DoubleClick, the host site would sense the presence of a DoubleClick cookie on the user's hard drive and alert DoubleClick's website to the host site's communication with the user.[187] DoubleClick's servers would then intercept the communication between the user and the host website, access and read the marketing profile data contained in the cookie located on the user's hard drive, and finally select and display a targeted banner advertisement on the host webpage as it was displayed to the user on her computer.[188]

The plaintiffs in *DoubleClick* were a class of individual computer users who had had DoubleClick cookies deposited on their hard drives, and thus, their online communications had been intercepted by the cookies for marketing profile reasons.[189] The plaintiffs sued DoubleClick under the Stored Communications Act, the Wiretap Act, the CFAA, and various state law causes of action, including invasion of privacy and trespass to property.[190] The district court analyzed these claims in response to DoubleClick's motion to dismiss.[191] The court first analyzed the plaintiffs' claims under the Stored Communications Act. It initially determined that at least some of DoubleClick's activities did arguably constitute the acquisition of stored communications under the Act.[192] The court next analyzed DoubleClick's claim under section 2701(c)(2) of

---

[185] *Id.* It is crucial to note the importance that the website be "affiliated" with DoubleClick. This is because, normally, cookies are domain-specific — a website can only deposit a cookie that will read information on that website, not others. *See* Whalen, *supra* note 16, §3.3 ("The server issuing the cookie must be a member of the domain that it tries to set in the cookie. That is, a server called www.myserver.com cannot set a cookie for the domain www.yourserver.com. The security implications should be obvious. If *Domain* is not set explicitly, then it defaults to the full domain of the document creating the cookie.").

[186] *DoubleClick*, 154 F. Supp. 2d at 503.

[187] *Id.* at 503-04. The case has an extremely detailed and complicated, but very helpful technical discussion of the entire process. It discusses how a targeted banner ad is selected and displayed for any particular computer user. *See id.* at 503-05. It further explains how deposited cookies conduct the information collection to build a user's marketing profile to allow DoubleClick to select appropriately targeted advertisements. *Id.*

[188] *Id.* at 503-04.

[189] *Id.* at 500 n.1.

[190] *Id.* at 500.

[191] *Id.*

[192] *Id.* at 507-09.

the Act — namely, that the Act is not applicable to "conduct authorized . . . by a user of that [wire or electronic communications] service with respect to a communication of or intended for that user."[193] Crucially, the individual plaintiffs' consent, as the consumers browsing the Internet sites, was irrelevant. As to the "communications" between such users and the host websites, all that was necessary for DoubleClick to prevail was to show that the applicable host website, which was one of the parties to the online communications between it and the individual computer user, had authorized DoubleClick to acquire the communications of the user to the website.[194] Examining the "technological and commercial relationships" DoubleClick had with its affiliated websites, the Court found that the websites had clearly authorized DoubleClick's conduct.[195] Given the intricate code that was required to facilitate the interaction between the websites, DoubleClick, and the end user visiting the sites, the court found that it was implausible to make any other conclusion but that the websites had explicitly authorized DoubleClick's acquisition of the browsing communications.[196] Strangely, the court discussed no direct evidence of the express contractual relationship which surely existed between DoubleClick and the websites. However, it clearly concluded "that the DoubleClick-affiliated web sites consented to DoubleClick's access of plaintiffs' communications to them."[197] The court made the same conclusion with respect to the Wiretap Act claim — that the websites were parties to the communications with the plaintiffs and clearly consented to DoubleClick's interception of those electronic communications, precluding DoubleClick's liability under the Wiretap Act.[198] The court disposed of the other claims on grounds other than

---

[193] *Id.* at 507 (quoting 18 U.S.C. § 2701(c)(2) (2005)).

[194] *Id.*

[195] *Id.* at 510.

[196] *Id.*

[197] *Id.* at 511.

[198] *Id.* at 514. The consent provision of the Wiretap Act is 18 U.S.C. § 2511(2)(d), which provides:

> It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any state.

Id. (quoting 18 U.S.C. § 2511(2)(d)). Most of the court's opinion on the Wiretap Act focused on the part of the provision that eliminates the defense of consent where the intercepting

consent.[199] Other cookie cases have reached similar results as the court did in *DoubleClick*,[200] indicating that the one-party consent granted by the host websites is sufficient to eliminate the liability of the cookie-enabled surveilling entity.

Some superficial similarity exists between cookie cases like *DoubleClick* and the typical spyware scenario, but the differences should be immediately apparent. Both scenarios involve online monitoring of individual users of the Internet. The *DoubleClick* case even involved "contextual marketing," much as the typical "legitimate" spyware scenario does. Moreover, in the cookie cases, there is often clearly manifested, contractual consent to the monitoring by one of the parties to the online Internet communications, usually the host websites that have consented to third party monitoring. The similarities seemingly end there, however. The differences are more profound. For one, spyware involves operating application code located on a user's computer, rather than benign text files as in the case of cookies. Thus, there is a usage of system resources in spyware not present with cookies. Second, unlike the domain-specific limitations of cookie monitoring, spyware is ubiquitous — it invades the user's privacy twenty-four hours a day, seven days a week, so long as the computer is turned on, no matter when and where the user browses on the Internet. Third, the "legitimate" spyware companies claim that there is two-party consent for the operations — between the spyware distributor and the individual user, who has supposedly granted consent for ubiquitous, constant online

---

party acts for the purpose of committing a crime or a tort. *Id.* at 514-19. The court, after a lengthy discussion of authorities, concluded that, although DoubleClick may arguably have committed torts by its conduct, that was not its intent. *Id.* at 518. Rather, DoubleClick's intent was to execute "a highly-publicized market-financed business model in pursuit of commercial gain." *Id.*

[199] The court dismissed the plaintiffs' CFAA claims, but only on the grounds that the plaintiffs had not proven that they met or exceeded that Act's damage thresholds. *Id.* at 519-26. For purposes of the litigation, DoubleClick did not contest the fact that its actions constituted unauthorized access of the plaintiffs' computers. *Id.* at 520. As for the plaintiffs' state law claims, including invasion of privacy and trespass, the court declined to assert supplemental jurisdiction because it dismissed all of the federal claims on which the plaintiffs had based federal jurisdiction. *Id.* at 526 (citing 28 U.S.C. § 1367(c)(3) (1994)). Accordingly, the court dismissed these state law claims. *Id.*

[200] *See In re* Toys R Us, Inc., Privacy Litig., No. 00-CV-2746, 2001 WL 34517252, at *7 (N.D. Cal. Oct. 9, 2001); Chance v. Avenue A, Inc. 165 F. Supp. 2d 1153, 1162 (W.D. Wash. 2001). *But see In re* Pharmatrak, Inc., 329 F.3d 9, 20 (1st Cir. 2003), *remanded to* 292 F. Supp. 2d 263 (D. Mass. 2003) (holding that consent granted by pharmaceutical websites to Pharmatrak to intercept web browsing communications between pharmaceutical websites' customers and websites was exceeded because personally-identifying information was collected and though websites had consented to interceptions, they had authorized Pharmatrak to retrieve only nonpersonally identifying information).

surveillance of her every move on the Internet, with no generally specified termination to the invasion. The cookie cases, by contrast, do not involve the consent of the user at all. Further, the contract which forms the basis for consent to the cookie surveillance of the individual users — a contract between two sophisticated, commercial actors (the host website and the third party ad provider such as DoubleClick) — does not involve the consumer computer user at all. In addition, the individual is the one with privacy interests at stake because the online browsing activity is her private, personal information, whereas it is simply valuable "customer data" from the business perspective of the host website. Thus, the cookie contract cases do not implicate the prospect of a consumer contracting away her own privacy rights like the spyware scenarios do. Accordingly, the cookie cases cannot support the practice of spyware contractually consented to by the user. The intrusion is far more invasive, and clear contractual consent must be established if the spyware distributors' position is to be vindicated.

C. *Cases Discussing Contractual Consent to Surveillance, Trespass, or Other Harms by the Harmed Individual*

The cases discussed thus far in this part involved some aspects of consent to invasions or harm of some kind from a contractual perspective. The cases did not, however, involve consent obtained by contract from the actual "victim" of the invasion — a contract signed by an individual, which purports to directly sanction the other contracting party to invade her interest in land or property or monitor her activities. This is, of course, the type of consent that spyware distributors claim that they obtain from the individual users who agree to install such programs. Such direct contractual-consent cases do not appear with any great degree of frequency in the published case reporters, but a few that do appear may be instructive.

The only reported case discussing this type of direct contractual consent in the "surveillance" context, at least under the federal Wiretap Act and the Stored Communications Act, is *American Computer Trust Leasing v. Jack Farrell Implement Co.*[201] In this case, American Computer Trust Leasing ("ACTL") sued two agricultural equipment dealers for payments owed under computer leases and software licenses that the dealers had entered into with ACTL and various affiliated companies,

[201] Am. Computer Trust Leasing v. Jack Farrell Implement Co., 763 F. Supp. 1473, 1494-95 (D. Minn. 1991), *aff'd and remanded by* 967 F. 2d 1208 (8th Cir. 1992).

including the equipment manufacturer.[202] The computer network installed in the dealers' offices was designed to allow all dealers to be able to communicate with each other and the manufacturer and "provide dealers with capabilities in the area of parts ordering, inventory tracking, accounting, customer record keeping, warranty records and whole goods ordering."[203] The dealers defaulted under the computer contracts, so ACTL and/or related companies eventually deactivated the software through the online connections established between it and the dealers.[204] This caused the dealers to lose valuable business records data.[205] ACTL sued the dealers for payment under the contract, but the dealers alleged a host of theories by counterclaim, including claims that ACTL and related companies had violated the Wiretap Act and the Stored Communications Act by wrongfully accessing their computers and misappropriating their business data.[206] The court, however, rejected these claims, citing the consent exceptions in both Acts and stating that these Acts "[do] not outlaw the authorized use of computer data and thus ha[ve] no applicability to the present case because both defendants allowed [an ACTL affiliate] access to their computer systems pursuant to their contracts with [the ACTL affiliate.]"[207] The dealers acknowledged that they were aware that ACTL and its affiliates could access their computers and data and were contractually empowered to do so.[208] The dealers could not recover under these Acts, the court reasoned, because

---

[202] *Id.* at 1480.

[203] *Id.*

[204] *Id.* at 1492.

[205] *Id.* The dealers complained that ACTL wrongfully failed to provide a "conversion tape" containing their data, which would have allowed the dealers to import their business data into a new computer system they had purchased from one of ACTL's competitors. *Id.* The court, however, refused to impose any liability on ACTL for the failure to provide a tape, as there was no requirement to do this in the contract between the parties. *Id.*

[206] *Id.* at 1494-95. The exact nature of the alleged wrongful activity was fairly murky. It appears that the dealers pleaded that ACTL and related affiliates "wrongfully gained access to defendants' computer systems and misappropriated their property," presumably their business records. *Id.* When pressed at the summary judgment level for greater specificity, the dealers were unable to meaningfully do so:

> [D]efendants proffer no evidence that their wire communications were actually intercepted or disclosed. They merely allege that [an ACTL affiliate] somehow got into their computer systems and used this access to snoop for unspecified purposes. The only evidence to support this allegation is that the indicator lights on the computer systems would sometimes be illuminated.

Id.

[207] *Id.* at 1494.

[208] *Id.*

the dealers consented to the computer access by their contracts, and this was sufficient to preclude liability.[209] However, there was not actually any direct evidence of surveillance by ACTL.[210]

There are other cases, outside the computer context, that discuss the existence of a contract as indicative of consent that precludes liability, particularly in the trespass context. For instance, in *Rawls & Associates v. Hurst*,[211] a contract for several parcels of real estate was entered into subject to the occurrence of several conditions, including the approval of certain zoning restrictions.[212] During the pendency of the contract, the proposed purchaser placed several items on the property, including a mobile home, construction equipment, and other materials.[213] When the sellers tendered a deed to the purchasers, there was an error in the legal description of the property, and so the buyers rejected the deed and requested a corrected one be sent.[214] The sellers refused and instead claimed, among other things, that the buyers were trespassing on their property by virtue of having the various construction items located on the property.[215] This was in spite of the fact of the pending contract, as well as the fact that the sellers had been well aware of the presence of these items for several months without complaint.[216] The purchasers filed an action for specific performance of the contract to sell the realty, and the sellers counterclaimed for trespass and breach of contract.[217] The court granted summary judgment in favor of the purchasers and denied the sellers' claims. The court reasoned that the sellers' clear consent to the purchasers' presence on the land by virtue of the contractual relationship precluded claims of trespass. In addition, the sellers gave implied consent derivable from their prior knowledge of, and failure to object to, the purchasers' physical presence on the land.[218] Thus, the fact that the sellers had contracted to allow the purchasers to acquire the land

---

[209] *Id.* at 1495. On the same basis, the court also considered and rejected the dealers' claims that ACTL and its affiliates should be liable under a Minnesota statute that was substantially similar to the Wiretap Act. *Id.* at 1494 n.31 (citing MINN. STAT. ANN. § 626A.02 (West 2003)). That statute also contained a consent exception. *Id.*

[210] *Id.* at 1494-95.

[211] Rawls & Associates v. Hurst, 550 S.E.2d 219, 224 (N.C. Ct. App. 2001).

[212] *Id.* at 221.

[213] *Id.* at 224. The other materials were construction materials, construction waste, and dumpsters. *Id.*

[214] *Id.* at 222.

[215] *Id.*

[216] *Id.* at 224.

[217] *Id.* at 222.

[218] *Id.* at 224.

in question precluded them from subsequently claiming that the purchasers' presence on the land was a trespass.

Another interesting example of consent by contract is *Geddes v. Mill Creek Country Club, Inc.*[219] In *Geddes*, the plaintiff was a landowner who complained of errant golf balls entering his property from an adjacent golf course (his property adjoined the fairway on the fourteenth hole of the course).[220] The plaintiff sued the defendant golf course for trespass and nuisance.[221] The golf course pled the affirmative defense of estoppel, based on a contract between the golf course and the plaintiff arranging for the construction of the fairway adjacent to the plaintiff's property.[222] The contract — negotiated between the golf course and the plaintiff at the time the construction of the course was being planned — provided for several things, including the construction of an eight-foot chain link fence on the adjoining border at the course's expense, landscaping along such fence, and several other accommodations to the plaintiff, all in exchange for the plaintiff's agreement not to protest the golf course's development.[223] The plaintiff had actually chosen his property to be adjacent to a fairway as opposed to other choices including adjoining residences and a bicycle path.[224] Though the plaintiff claimed ignorance that errant golf balls on his property would be an inevitable consequence of being adjacent to a fairway, the court rejected this claim and took judicial notice of the fact that some errant golf balls were known to have been a probability.[225] Therefore, the court applied the elements of

---

[219] Geddes v. Mill Creek Country Club, Inc., 751 N.E.2d 1150 (Ill. 2001).

[220] *Id.* at 1152.

[221] *Id.*

[222] *Id.* at 1152-53.

[223] *Id.* at 1153-54.

[224] *Id.* at 1153.

[225] *Id.* at 1158-59. For this proposition, the court cited a number of other cases, which make for entertaining reading by anyone who has ever ventured out onto a golf course. The court stated, in response to plaintiff's claim:

> This contention lacks merit. That golfers do not always hit their golf balls straight is a matter of common knowledge; it is a fact that needs no supporting evidence, a principle that needs no citation of authority. Courts have long acknowledged this axiom . . . . This condition is as natural as gravity or ordinary rainfall. We repeat: it is a matter of common knowledge that golfers do not always hit their shots straight. Defendants knew it.

Id. ("'It is well known that not every shot played by a golfer goes to the point where he intends it to go. If such were the case, every player would be perfect and the whole pleasure of the sport would be lost.'" (quoting Campion v. Chicago Landscape Co., 14 N.E.2d 879, 886 (Ill. 1938))); *Id.* (citing Patton v. Westwood Country Club Co., 247 N.E.2d 761, 763 (Ohio Ct. App. 1969) ("It is generally known that the average golfer does not

equitable estoppel and concluded that the plaintiff's entry into the contract was sufficient to estop him from complaining of trespass or nuisance.[226] The court did not not phrase its reasoning explicitly in terms of consent. The court did not even discuss whether the plaintiff had shown a prima facie case of trespass or nuisance notwithstanding the estoppel defense. However, the case's end result is tantamount to a finding that the plaintiff consented to any trespass or nuisance that otherwise may have occurred.

The consent to invasive harms granted in a contract has limits from a public policy perspective, however. There is a series of cases concerning a seller's or lessor's rights to enter a debtor's premises to retake possession of an item of personal property after default that is illuminating for present purposes. One such case is *Fassitt v. United T.V. Rental, Inc.*[227] In *Fassitt*, the plaintiff leased a phonograph player from the defendants, in return for weekly rental payments.[228] The plaintiffs defaulted on their rent payments ten months after execution of the lease, and the defendants arranged for agents to repossess the phonograph.[229] Notably, no judicial process was utilized, and the defendants' agents entered the plaintiffs' home when no one but the eleven-year-old daughter was present and proceeded to take the phonograph without obtaining consent at the time (though they did leave a business card with the eleven-year-old).[230] The plaintiffs sued for trespass, and the defendants claimed that contractual consent had been given by virtue of a clause in the phonograph rental contract that provided as follows:

> OWNER'S RIGHT TO ENTER AND TAKE POSSESSION: The owner and its agents, upon the termination of this agreement, are specifically authorized to enter upon any premises where the property may be found and to take possession of and remove the property without liability, and owner and its agents are hereby released and discharged from any claim or cause of action in or relating to entry and taking possession and renter agrees to indemnify owner and its agents for all costs, expenses, and damages

always hit the ball straight.")). Based on this obvious fact about golf shots, the court noted that "it is a matter of common knowledge that on practically all golf courses, including those constructed on vast acreages where the fairways are wide and well separated by rough and shrubs, a golfer can slice or hook a ball off of the fairway." *Geddes*, 751 N.E.2d at 1158 (quoting *Campion*, 14 N.E.2d 879).

[226] *Id.* at 1159.

[227] 297 So. 2d 283 (La. Ct. App. 1974).

[228] *Id.* at 284.

[229] *Id.* at 285.

[230] *Id.*

> occurring directly or indirectly from or related to the taking possession and the removal of said property.[231]

The court conceded that the case turned on the question of whether the plaintiffs, by agreeing to the contract term cited above, had effectively consented to any trespass that the defendants would subsequently commit.[232] The court observed that the clause was tantamount to a contractual waiver of the plaintiffs' right to privacy that otherwise existed in the sanctity of their own home.[233] Unsurprisingly, then, the court declined to enforce the provision and therefore recognized the defendants' liability for trespass:

> Public policy cannot condone the use in a sale or lease contract of a provision irrevocably authorizing entry into a debtor's or lessee's home without judicial authority or without the owner's consent at the time of entry. We decline to construe the quoted provision, incorporated into a printed from [sic] contract as a necessary condition of the agreement, as irrevocable permission to enter a private home at any time, day or night, occupied or unoccupied, under any circumstances. Law and order cannot allow such a construction, which would tend to encourage breaches of the peace.[234]

Hence, the court ignored the alleged contractual consent to entry into the plaintiffs' home and granted recovery in trespass to the plaintiffs, notwithstanding the contractual provision.[235]

Nine years later, the Lousiana Court of Appeal reached a similar decision in *St. Julien v. South Central Bell Telephone Co.*[236] In that case, the local telephone company entered a customer's apartment without consent and without anyone being present, in order to take possession of a telephone, due to the telephone bill being in arrears.[237] Instead of a contractual provision, the entry was allegedly authorized by a state tariff filed of record in favor of the telephone utility.[238] The plaintiffs filed suit for invasion of privacy.[239] The appeals court, in reversing a trial court

---

[231] *Id.* at 286.
[232] *Id.* at 287.
[233] *Id.*
[234] *Id.*
[235] *Id.* at 287-88.
[236] 433 So. 2d 847 (La. Ct. App. 1983).
[237] *Id.* at 848-49.
[238] *Id.* at 849.
[239] *Id.* at 848.

decision denying the plaintiffs' invasion of privacy claim, discussed the historical and constitutional lineage of the privacy right and its close affinity with the staunch protection the law has traditionally afforded to the sanctity of a person's home.[240] The defendant argued on appeal that the plaintiffs had impliedly consented to the entry by contracting for telephone service.[241] However, the court first noted the absence of any contract in the evidence, so no such terms were before the court.[242] Second, the court cited *Fassitt* and strongly suggested that any such contract, even if it existed, would not be enforceable:

> [Defendant] made no showing whatsoever that the [plaintiffs] ever voluntarily, intelligently, and knowingly granted the right to enter their home while they were away and search for and take a phone. Nor is there even the slightest suggestion that such an agreement would be the product of meaningful bargaining and subsequent meeting of the minds. Even if defendant had satisfied the aforesaid evidencing requirements, their position would likely fail.[243]

In so holding, the *St. Julien* court cited the public policy rationale that had been voiced by the *Fassitt* court, essentially stating that such a contract granting irrevocable "consent" to entry into the home without contemporaneous consent would be void as against public policy because of privacy concerns.[244]

Fassitt and *St. Julien*, both Louisiana cases from a civil law jurisdiction, seem to be in accord with the rest of the country in this regard. They relate, by analogy, to the law of secured transactions and the right of a secured creditor to enter the debtor's premises and retake possession of collateral upon default. Such a right existed at common law before the promulgation of article 9 of the Uniform Commercial Code ("U.C.C."). Under that common law principle, one of the defenses to liability for trespassing onto land was granted to either a conditional seller or the holder of a chattel mortgage (the pre-U.C.C. precursor to a security interest in personal property) who had a right to immediate possession of an item of personal property and "to enter land in the possession of the [debtor], for the purpose of taking possession of the thing and removing it from the land."[245] The entry, however, was required to be at

---

[240] *Id.* at 849-52.

[241] *Id.* at 853.

[242] *Id.*

[243] *Id.*

[244] *Id.* (quoting Fassit v. United T.V. Rental, Inc., 297 So. 2d 283, 287 (La. Ct. App. 1974)).

[245] RESTATEMENT (SECOND) OF TORTS § 183 (1965).

a reasonable time and to be conducted in a reasonable manner.[246] The article 9 codification of this principle is set forth in section 9-609 of the U.C.C., which provides that "[a]fter default, a secured party may take possession of the collateral . . . without judicial process, if it proceeds without breach of the peace."[247] This duty of a secured party not to breach the peace in taking possession of collateral upon default, moreover, is not waiveable by contract between the parties under section 9-602(6).[248]

Although the U.C.C. mandates that secured creditors may not breach the peace when repossessing collateral, it does not define the term "breach of the peace."[249] Rather, the U.C.C. leaves the definition and development of this concept to the courts.[250] Indeed, the duty not to breach the peace in this context has been present for as long as the law has recognized some right of certain parties, including secured creditors, to retake possession of personal property upon default.[251] Though creditors regularly contract for the right to enter a debtor's premises to retake possession upon default, courts typically hold that the creditors have this right absent the contractual provision.[252] Section 9-609 of the U.C.C. specifically provides this as well.[253] Courts have defined the contours of the breach of peace limitation, both prior to and since the enactment of article 9 of the U.C.C. Certain principles are now fairly well established. Most clearly, the standard unequivocally prohibits the

---

[246] *Id.*; *see also* § 183 cmt. e ("An entry in the nighttime or in time of serious illness or other misfortune may be at an unreasonable time.").

[247] U.C.C. § 9-609 (2000).

[248] U.C.C. § 9-602(6) ("The debtor or obligor may not waive or vary the rules stated in the following listed sections: . . . (6) Section 9-609 to the extent that it imposes upon a secured party that takes possession of collateral without judicial process the duty to do so without breach of the peace . . . .").

[249] U.C.C. § 9-609 cmt. 3 (2002).

[250] *Id.*

[251] *See generally* Eugene Mikolajczyk, Comment, *Breach of Peace and Section 9-503 of the Uniform Commercial Code — A Modern Definition for an Ancient Restriction*, 82 DICK. L. REV. 351 (1978). Article 9 of the U.C.C. was revised by the National Conference of Commissioners on Uniform State Laws to have an effective date in all 50 states of July 1, 2001. *See* U.C.C. § 9-701; *id.* § 9-701 cmt. (2002). At the time of the revision, section 9-503 was renumbered, without substantial change, into section 9-609 in the revised article 9. *See* U.C.C. § 9-609 cmt. 1.

[252] *See* RESTATEMENT (SECOND) OF TORTS § 183 reporter's notes (1965) (citing Blackford v. Neaves, 205 P. 587 (Ariz. 1922); C.I.T. Corp. v. Reeves, 150 So. 638 (Fla. 1933); C.I.T. Corp. v. Short, 115 S.W.2d 899 (Ky. 1938); Heath v. Randall, 58 Mass. (4 Cush.) 195 (1849); Day v. Nat'l Bond & Inv. Co., 99 S.W.2d 117 (Mo. Ct. App. 1936); Proctor v. Tilton, 17 A. 638 (N.H. 1888); Westerman v. Or. Auto. Credit Corp., 122 P.2d 435 (Or. 1942); Abel v. M.H. Pickering Co., 58 Pa. Super. 439 (1914); Willis v. Whittle, 64 S.E. 410 (S.C. 1909)).

[253] *See* U.C.C. § 9-609.

use of actual force or violence in the retaking of personal property.[254] Also, most courts have denounced the use of threats or intimidation to assist in retaking possession, since such means are likely to incite violence.[255]

Another line of cases has held that a debtor's voiced objection to the creditor's proposed repossession of the collateral may make the creditor's continued repossession efforts a breach of the peace.[256] "This principle is based upon the 'potential for violence' definition of breach of peace in that an objection by the debtor will serve as the foundation for a possible violent confrontation if the objection is ignored."[257] The breach of peace will be deemed to occur if the repossession continues over the debtor's objection, even if no violence materializes.[258] Moreover, any such protestation by the debtor at the time of the attempted repossession will render any prior contractual consent to repossession a nullity, such that continued action by the creditor after such fact will be a breach of peace.[259] This doctrine essentially imposes an additional "contemporaneous consent" requirement for private repossession to be valid, notwithstanding the technical presence of purported contractual consent in advance. As noted by one commentator:

> It is consistent with the underlying policy to find . . . that a consent given contemporaneously with the possession is effective and, on the other hand, that one given weeks or months before in . . . the security agreement is ineffective. In the former case, the debtor fully appreciates the consequences of his consent and has no time in

---

[254] *See* Mikolajczyk, *supra* note 251, at 355-56; *see also* RONALD A. ANDERSON, ANDERSON ON THE UNIFORM COMMERCIAL CODE § 9-609:6R (1981).

[255] *See* Mikolajczyk, *supra* note 251, at 356-57; *see also* ANDERSON, *supra* note 254, § 9-609:6R (citing Deavers v. Standbridge, 242 S.E.2d 331 (Ga. Ct. App. 1978) (holding that "the blocking-in of debtor's automobile accompanied by the use of offensive and insulting language was found sufficient to raise a question of fact as to whether the secured party's actions constituted a breach of peace")).

[256] *See* Mikolajczyk, *supra* note 251, at 363-66; *cf.* ANDERSON, *supra* note 254, § 9-609:6R ("Case law is clear that if the debtor threatens to physically prevent the repossession, the secured party must not proceed with the repossession. The debtor must, however, do more than order the secured party to cease the repossession. Similarly, if the secured party has already taken possession of the collateral, the mere objection by the debtor will not convert a peaceful repossession into a breach of the peace. Along the same lines, a debtor's threats during an earlier repossession attempt will not convert a later peaceful repossession into one involving a breach of the peace." (citations omitted)).

[257] Mikolajczyk, *supra* note 251, at 364.

[258] *Id.* (citing Crews & Green v. Parker, 68 So. 287 (Ala. 1915); Manhattan Credit Co. v. Brewer, 341 S.W.2d 765 (Ark. 1961); Ben Cooper Motor Co. v. Amey, 287 P. 1017 (Okla. 1930)).

[259] Mikolajczyk, *supra* not 251, at 364.

> which to change his mind. That is not so in the latter case. . . . [T]he contemporaneous consent affords substantial protection against violence, while an earlier written consent does not. Since the goal of the breach of peace restriction is to prevent violence, . . . the distinction is appropriate.[260]

There is some inherent murkiness in the line between a sufficiently voiced objection that renders any subsequent act a breach of peace and purely internal dissatisfaction with the prospect of repossession, which will not be sufficient.[261] However, for present purposes, it suffices to note that if the debtor voices a sufficient objection contemporaneously with the proposed repossession, then a court can deem the debtor's prior contractual consent to repossession inadaquate to preclude the creditor's liability in trespass or conversion.

One other area of case law development on the breach of peace formulation deserves mention here — the extent to which repossession clauses in sales or security contracts are sufficient to authorize a subsequent entry into the debtor's premises to effect the repossession. Here again, the courts have developed contours of protection depending on the sanctity of the area invaded. Most clearly, courts have repeatedly held that entry into an individual debtor's home, absent contemporaneous consent (which is impossible to obtain when the debtor is absent), will constitute a breach of the peace per se.[262] The reason for such a strong rule is to honor and protect the private and sacrosanct nature of the individual home as a refuge from the outside world, though the prevention of potential retaliatory violence is also a factor.[263] Though technically these cases have required the creditor to "break" into the residence for a violation to occur, the cases have been quite liberal in finding breakings, allowing such things as turning a

---

[260] *Id.* at 365 (quoting James J. White, *Representing the Low Income Consumer in Repossessions, Resales and Deficiency Judgment Cases*, 64 NW. U. L. REV. 808, 815 n.24 (1970)).

[261] Mikolajczyk, *supra* note 251, at 365 (citing McWaters v. Gardner, 69 So.2d 724, 726 (Ala. Ct. App. 1954) (holding employer's expressed wish that creditor wait until debtor-employee return was insufficient protest); Benschoter v. First Nat'l Bank, 542 P.2d 1042, 1050 (Kan. 1975) (noting son's request that creditor wait until his father's return would be sufficient protest); Luthy v. Philip Werlein Co., 112 So. 709, 709 (La. 1927) (noting daughter and son informed creditor that he would have to wait to see their father); Kirkwood v. Hickman, 78 So. 2d 351, 352 (Miss. 1955) (noting daughter-in-law of debtor informed creditor that he would have to wait until debtor returned home)).

[262] *See* Mikolajczyk, *supra* note 251, at 358-59; *see also* ANDERSON, *supra* note 254, § 9-609:6R ("Any breaking in, or entering of, a house or other closed premises, including a fenced-in area, constitutes a breach of the peace.").

[263] *See* Mikolajczyk, *supra* note 251, at 358.

doorknob on an unlocked door to suffice.[264] Another leading commentator on the U.C.C. has stated that "[a]ny breaking in, or entering of, a house or other closed premises, including a fenced-in area, constitutes a breach of the peace."[265] Notably, the same degree of protection has not been afforded to areas outside the debtor's residences,[266] such as driveways, or to lands owned by commercial enterprises.[267] This distinction makes sense, for though the law should certainly give some protection to commercial enterprises, the same privacy and security issues facing individual debtors are not present with commercial actors.[268] The cases prohibiting entry into an individual's home, absent contemporaneous consent, are replete with admonitions about the special protection afforded a person's home, notwithstanding any prior contractual consent granted to a lender. For example, the Alabama Supreme Court once stated that "[t]he law guards with jealous care the sacredness of every man's dwelling, and his lawful possession of property against invasion or disturbance, otherwise than by proceedings taken under the sanction and through the agency of public justice."[269] The Iowa Supreme Court has similarly noted that "[a]n agreement permitting a family's home to be broken open and entered for the purpose of forcibly taking possession of property therein is contrary

---

[264] *See id.* at 359 ("In applying this test courts have held that the breaking need not be violent to fall within the scope of the . . . prohibition [against breaching the peace]. A breach of the peace has been found in cases in which the entry was affected by turning the knob of a closed but unlocked door, by raising a closed but unlocked window, or by using a key found under a doormat." (citing Girard v. Anderson, 257 N.W. 400 (Iowa 1934); Kemmitt v. Adamson, 46 N.W. 327 (Minn. 1890); M.J. Rose Co. v. Lowery, 169 N.E. 716 (Ohio 1920); Lyda v. Cooper, 169 S.E. 236 (S.C. 1933))).

[265] ANDERSON, *supra* note 254, § 9-609:6R (citing Madden v. Deere Credit Servs., Inc. 598 So. 2d 860, 865-67 (Ala. 1992) (breaking into locked premises is breach of peace); Bloomquist v. First Nat'l. Bank, 378 N.W.2d 81, 81 (Minn. Ct. App. 1985) (entering into locked premises by removing window pane without debtor's permission is breach of peace); Martin v. Dorn Equip. Co., 821 P.2d 1025, 1025 (Mont. 1991) (cutting lock on gate and thereby entering closed premises is breach of peace)).

[266] ANDERSON, *supra* note 254, § 9-609:6R ("In contrast, taking property from a driveway or other open area, even though technically trespassing, will not generally, by itself, make the repossession involve a breach of the peace." (citing Hester v. Bandy, 627 So. 2d 833 (Miss. 1993))).

[267] *See* Mikolajczyk, *supra* note 251, at 359-61 (citing Wirth v. Heavey, 508 S.W.2d 263 (Mo. Ct. App. 1974); Cherno v. Bank of Babylon, 282 N.Y.S.2d 114 (N.Y. Sup. Ct. 1967)).

[268] *See* Kirkwood v. Hickman, 78 So. 2d 351, 356 (Miss. 1955) ("The important factors of the sanctity of a private home from invasion by others, and the right of privacy require, we think, a different rule as to the right of repossession from that applied in those cases not involving a private residence.").

[269] Evers-Jordan Furniture Co. v. Hartzog, 187 So. 491, 493 (Ala. 1939).

to good public policy and void to that extent."[270] The South Carolina Supreme Court adds that "[a] man's home is his castle and no outsider has the right to enter the home in the absence of the occupants without the permission, express or implied, of the occupants, and if one does so he becomes a trespasser. . . ."[271] On the basis of this special protection for people's homes, the Ohio Supreme Court has ruled:

> The insertion in a mortgage of a clause whereby a mortgagor purportedly consents in advance to a breaking and entering is an attempt to confer upon a mortgagee an extraordinary privilege not enjoyed by an absolute owner and is not needed for the reasonable protection of the mortgagee's investment. The existence of the privilege is a threat to the peace and contrary to public policy. A contractual provision purporting to authorize a breaking is, therefore, void.[272]

The creditors in the cases cited immediately above were found liable for trespass, even though there purportedly was prior contractual consent to entry for purposes of retaking the collateral. Thus, notwithstanding prior contractual consent, it seems clear under secured transactions law that courts require a creditor to obtain additional, contemporaneous consent if the creditor contemplates retaking the collateral by entering the debtor's enclosed premises. This furthers the public policy goal of protecting the sanctity and privacy of a person's residence. Thus, under secured transactions law, prior contractual consent or privilege to enter the debtor's premises is not sufficient. If the creditor plans to enter the debtor's home, then he must obtain subsequent, contemporaneous consent at the time of entry. For reasons of public policy, the prior contractual consent does not authorize any and all future entries into the home.[273]

IV. THE PROBLEM WITH CONTRACT-BASED CONSENT TO SPYWARE

The preceding part illustrates that courts have been willing to accept that, in some instances, contractual arrangements can indicate consent to

---

[270] Girard v. Anderson, 257 N.W. 400, 402-03 (Iowa 1934).

[271] Childers v. Judson Mills Store Co., 200 S.E. 770, 774 (S.C. 1939).

[272] Hileman v. Harter Bank & Trust Co., 186 N.E.2d 853, 854-55 (Ohio 1962).

[273] At least one court has noted that such provisions may even be unconscionable as well. *See* Kosches v. Nichols, 327 N.Y.S.2d 968, 970 (Civ. Ct. 1971) ("Needless to say, the clauses giving the seller the right to enter a debtor's residence and seize the goods without a court order are unconscionable.").

particular types of invasions.[274] However, in other instances, most notably with contracts purporting to grant advance consent to trespass for purposes of repossession of collateral, courts have been unwilling to infer contemporaneous consent to invasions based on such contracts.[275] Presently, distributors of spyware and adware insist that the legitimate uses of such technology — those that obtain customer "consent" before installation and operation of such surveillance software — are perfectly lawful and valid, based primarily on the presence of such purported contractual consent at the inception of the transaction.[276] The purpose of this final part is to analyze these claims in light of both the foregoing discussion and basic contract law principles and to determine whether such contractual consent to spyware can be substantiated.

A. The Consent-Granting Contract: The End User License Agreement

As an initial manner, some description of the technical means by which most "legitimate" spyware and adware companies obtain purported contractual consent is instructive. The examples of the EULAs presented to users before download and installation of programs containing spyware are too numerous to count, but one example should suffice. Ben Edelman, perhaps the world's foremost and certainly the most famous technical spyware researcher, has outlined numerous examples of EULAs and spyware installation and bundling practices on his website, http://www.benedelman.org.

On his website, Edelman outlines the process for downloading and installing KaZaa, the popular peer-to-peer file sharing program.[277] A

---

[274] *See supra* notes 146-226 and accompanying text.

[275] *See supra* notes 227-73 and accompanying text.

[276] *See* FED. TRADE COMM'N, *supra* note 34, at 3-4; *see, e.g.*, Press Release, The Gator Corporation (July 1, 2002), *available at* http://www.claria.com/companyinfo/press/releases/pr070102.html ("'Consumers have opted to receive free software in return for occasionally receiving these advertisements,' said Gator Corporation CEO Jeff McFadden. 'The 22 million PCs that comprise the Gator Advertising and Information Network (GAIN) are owned and operated by 22 million consumers, not by a handful of website publishers. What happens on these users' screens is the users' business and choice, not the plaintiffs.'"). The discussion of spyware or adware surreptitiously installed on a consumer's computer, without any attempt to notify or obtain contractual consent, seems to many to be clearly wrongful, but is beyond the realm of contract law and, in any event, will not be discussed further in this Article.

[277] *See* Ben Edelman, Claria License Agreement Is Fifty Six Pages Long Webpage (Dec. 1, 2004), http://www.benedelman.org/spyware/claria-license. Edelman's documentation of the installation process and EULA was related to the version of KaZaa that was available as of June 2, 2004. *Id.* In August 2005, KaZaa stopped bundling its application with the GAIN software from Claria (formerly Gator) and instead began bundling it with a different adware program. However, Edelman's documentation is sufficient for present purposes.

consumer who decides that she wants the program can go to KaZaa's website to download it.[278] After downloading the file, she opens it for purposes of initializing the installation. Shortly after commencing the installation process, a notification box pops onto the user's screen, which says, among other things: "KaZaa Media Desktop is a free download supported by advertising from . . . The GAIN Network."[279] At the bottom, directly under the sentence that says "Sharman Networks respects your privacy,"[280] the notification box says: "I agree to the KaZaa Media Desktop End User License Agreement and Altnet Peer Points Manager Package End User License Agreements."[281] Under this text is a box where the user can signal her agreement by placing a checkmark. If the user clicks the checkmark and clicks "Next," a new notification box will appear.[282] This box has the following statement at the top: "This free copy of KaZaa Media Desktop is supported by advertising delivered by the GAIN Network and other partners. The GAIN Network delivers online advertisements which are selected in part based on how you surf the Web."[283] Then, the opening lines of the GAIN End User License Agreement are presented.[284] However, in order to read the entire license, the user must traverse some fifty-six of these screens.[285] At any point, the user may instead commence installation of the KaZaa program and all bundled applications including the GAIN adware simply by checking the box at the bottom of the screen that indicates that the user has read and agreed to the GAIN license.[286] The license is 5541 words long.[287]

Contained within that license agreement, which virtually no user bothers to read,[288] are the provisions by which the user purportedly authorizes herself to be subject to surveillance for "targeted marketing" purposes. The following are some of the relevant excerpts from the license:

---

[278] *See id.*

[279] *See id.* This is likely the first time that the user, who thinks she wants KaZaa, has heard of the GAIN Network.

[280] Sharman Networks is the owner of the KaZaa website and software application. *See* Sharman Networks, About Sharman Networks Webpage, http://www.kazaa.com/us/about/sharman.htm (last visited Mar. 20, 2006).

[281] Edelman, *supra* note 277.

[282] *Id.*

[283] *Id.*

[284] *Id.*

[285] *Id.*

[286] *Id.*

[287] *Id.* Edelman notes that, by contrast, the U.S. Constitution is 4616 words long. *Id.*

[288] Shaun B. Spencer, *Reasonable Expectations and the Erosion of Privacy*, 39 SAN DIEGO L. REV. 843, 895 (2002).

> GAIN Publishing ('GP') and the GAIN Network provide personal computer users with a valuable proposition: the ability to obtain Kazaa Media Desktop software, valued at up to $30, free-of-charge or at a reduced cost in exchange for users' agreement to accept advertising and other promotional messages delivered by the GAIN Network to users' personal computers. . . .
>
> While we don't know the identity of Subscribers, the GAIN AdServer and GP collect and use the following kinds of anonymous information:
>
> -Some of the Web pages viewed
>
> -The amount of time spent at some Web sites
>
> -Standard web log information and system settings (excluding IP addresses and system settings)
>
> -Non-personally identifiable information on Web pages.[289]
>
> When running on a computer, the GAIN AdServer regularly communicates with GP servers, and in some cases, third party servers, among other reasons, to:
>
> 1.maintain/update the GAIN AdServer;
>
> 2.facilitate installing and removing the GAIN-Supported Software or the GAIN AdServer;
>
> 3.retrieve content and ads for display;
>
> 4.facilitate various GAIN AdServer features as contained in this Privacy Statement; and/or
>
> 5.collect anonymous Subscriber computer usage information as contained in this Privacy Statement.[290]

---

[289] Edelman, *supra* note 277. The EULA also states: "For more information, http://www.gainpublishing.com/help/psdocs/kmd/60/datause.html, incorporated herein by reference, provides a more detailed description of the information collected by GP and how it is used." *Id.* The webpage referred to notes that while IP Addresses are supposedly not stored, they are obviously collected. *Id.* Moreover, the EULA fails to state that the GAIN software inventories are software installed on the user's computer. *Id.*

[290] *Id.* The EULA also requires that the user only delete the program (if she chooses to do so) by using "authorized" methods, which apparently consist primarily of the Windows Control Panel "Add/Delete Programs" function; not authorized, notably, is the use of third-party spyware removal programs. *Id.* Moreover, the EULA prohibits the user from attempting to monitor the GAIN software's surveillance and communication activities through the use of "packet sniffer" programs designed for this purpose. *Id.*

Thus, by clicking that she has accepted this EULA from KaZaa, bundled with the GAIN software, the user has ostensibly struck a bargain. She will receive a program she sought for "free." Of course, "[i]n a sense, [she] is paying, but the coin is privacy, not money."[291] Hence, in return the consumer "agrees" that all of her online activity may now be continuously subject to monitoring and surveillance. However, the EULA language may not impress upon the user the fact that her computer is now watching her on a twenty-four seven basis.[292] "The installation screens do not say that, for as long as the software is running, it will monitor the URL of every site the user visits and report that information back to a Claria database."[293] In fact, this is all for the sake of receiving only the advertisements she is purportedly likely to desire, as opposed to the unfavorable ones for which she has no desire. In the words of one article on the GAIN software, it "collects far too much information about user activity, and is far too cavalier about disclosing what it collects."[294]

The arrangement possesses the superficial appearances of a contractual bargain — the user has received consideration in the form of a desired application (KaZaa) and in exchange has supposedly agreed to have the GAIN software continuously monitor her online activities. In fact, the typical software EULA is, despite use of the term "license," simply a contract.[295] Moreover, the process of indicating assent to contract/license terms by clicking online with a mouse, rather than writing a signature on a piece of paper, has become an accepted legal mechanism for contract formation.[296] A contract formed in this manner is generally referred to as a "clickwrap" agreement.[297] Courts generally

---

[291] Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2072 (2004) (quoting Cade Metz, *Spyware — It's Lurking on Your Machine*, PC MAG., Apr. 22, 2003, at M7).

[292] *See* Janet Kornblum, *Spyware Watches Where You Surf*, USATODAY.COM, Mar. 10, 2002, http://www.usatoday.com/tech/news/2002/03/11/stealthware.htm.

[293] Mitch Wagner, *Review: Claria Software — Unsafe at Any Speed*, TECHBUILDER.ORG, Aug. 1, 2005, http://www.techbuilder.org/views/showArticle.jhtml?articleId=167100181.

[294] *Id.*

[295] *See* L.K. KUTTEN, COMPUTER SOFTWARE PROTECTION: LIABILITY, LAW, FORMS § 9:2 (2005); *see also id.* § 9:7 ("Software license agreements are first and foremost contracts."). The fact of "licensing" the software is pragmatic, since it is not exactly like the sale of goods: "The developer wishes to clearly state that only the right to use the software is included and that no rights are granted to the underlying intellectual work." *Id.* § 9:6.

[296] *See generally* Christina L. Kunz et al., *Click-Through Agreements: Strategies for Avoiding Disputes on Validity of Assent*, 57 BUS. LAW. 401 (2001) (analyzing case law involving click-through or "clickwrap" consent, and evaluating trends).

[297] *See id.* at 401; *see also* Mark E. Budnitz, *Consumers Surfing for Sales in Cyberspace: What Constitutes Acceptance and What Legal Terms and Conditions Bind the Consumer?*, 16 GA. ST. U.

uphold the initial manifestation of assent in clickwrap agreements so long as the terms are reasonably viewable before assent is manifestable by clicking, users are not mechanically able to proceed without the terms being presented and available for review, and a clear choice between assent and nonassent is given.[298] This is equally true, as a general proposition, with respect to standard form contracts initiated online that users agree to through clickwrap methods, even though such contracts contain "electronic boilerplate" that may be unfavorable to the user.[299] Notwithstanding the acceptance of clickwrap agreements, existing contract doctrine should allow such "e-consumers" to assert defenses to the contract formation or enforcement where appropriate.[300] Defenses should include, for example, unconscionability, fraud, and similar doctrines.[301] That is to say, "existing contract doctrine can sensibly resolve disputes arising in electronic contracts."[302] Accordingly, the normal rules of contract law should apply to contracts whose terms include purported consent to continual surveillance, as in the case of spyware. Engaging in an analysis of such consensual spyware contracts, under appropriate contract doctrines, is the purpose of this Part of the Article.

B. Clarifying the Spyware Issues: A "Virtual" Perspective

Highlighting the actual realities of the spyware bargain significantly aids the doctrinal analysis of contract law. The development of the Internet has led to the metaphor of cyberspace as an actual space, though virtual and abstract.[303] We all think of cyberspace as a place: we go on

---

L. REV. 741, 745 (2000) ("Because a contract is formed through the consumer's various clicks on the mouse as she proceeds through various steps in the online shopping process, these agreements are known as 'click-through' contracts."). There is a related type of online contract, where a user is bound by the terms that are printed or available on the website itself, without having to manually click through such terms to indicate direct exposure to them. These are known as "browsewrap" agreements, but are not the focus of this Article. *See id.* at 763; Christina L. Kunz et al., *Browse-Wrap Agreements: Validity of Implied Assent in Electronic Form Agreements*, 59 BUS. LAW. 279, 279-80 (2003).

[298] *See* Kunz et al., *supra* note 296, at 402-16.

[299] *See generally* Robert A. Hillman & Jeffrey J. Rachlinski, *Standard-Form Contracting in the Electronic Age*, 77 N.Y.U. L. REV. 429 (2002) (noting that there is no compelling reason to treat standard-form contracts in online context as legally different from standard-form contracts in offline context).

[300] *See id.* at 486-95.

[301] *See id.*

[302] *Id.* at 486.

[303] *See* Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 CAL. L. REV. 439, 446 (2003).

the "web," we "surf" the Internet, we "visit sites," we "access a homepage," and we "hang out in chat rooms."[304] Scholars and judges have begun to refer to wrongful online activity directed toward a victim's computer as "trespass."[305] In the words of one commentator:

> Cyberspace is a place that conforms to our understanding of the physical world, with private spaces such as websites, email servers, and file servers, connected by the public thoroughfares of the network connections. Viewed through the filter of the cyberspace as place metaphor, computer trespass does not just infringe on one's right to use the personal property of one's computer system. Instead, the action becomes a trespass against a form of quasi land that exists online. Trespasses to land have always been considered more serious than the equivalent actions against personal property. For example, an action lies against the most trivial trespass to land, whereas trespasses to chattels have always required serious damage.[306]

This illustrates the view that cyberspace is "virtual land" that can be considered invaded just as physical real estate can be in the real world.

In fact, this struggle to reconcile the virtual characteristics of the Internet with its real characteristics have begun to draw serious analytical attention. As Professor Orin Kerr has noted:

> The Internet's facts depend on whether we look to physical reality or virtual reality for guidance. We can model the Internet's facts based on virtual reality, looking from the perspective of an Internet user who perceives the virtual world of cyberspace and analogizes Internet transactions to their equivalent in the physical world. Alternatively, we can model the facts based on the physical reality of how the network operates [i.e., the computer, the cables, the phone lines].[307]

Kerr has claimed that the "virtual reality" of the Internet experience creates a "problem of perspective" in discussing issues of law and the Internet.[308] This problem is deciding whether to view Internet law issues from the "virtual reality" perspective or from the "actual reality" perspective.[309] The decision is critical because the difference in

---

[304] *Id.* at 453.

[305] *See id.* at 475-88.

[306] *Id.* at 481-82.

[307] Orin S. Kerr, *The Problem of Perspective in Internet Law*, 91 GEO. L.J. 357, 357 (2003).

[308] *Id.*

[309] *Id.*

perception can result in different legal outcomes.[310] As Kerr notes, neither claim is inherently superior — both perspectives may be "perfectly viable, depending on the circumstances."[311]

Kerr colorfully uses the 1999 sci-fi movie *The Matrix* as a perfect illustration of the problem of perspective.[312] In the movie, "the Matrix" is a vast computer network to which virtually all humans are neurally connected while lying in a vegetative state.[313] The Matrix obtains all humans' energy, while employing a computer-generated virtual reality to keep them occupied and unaware of the realities of their physical circumstances. In the movie, Neo — the lead character played by Keanu Reeves — is contacted by and joins a rebel group that is disconnected from the network and now seeks to destroy it. However, during the movie, Neo and the others must continually go back and forth between the virtual, Matrix-induced reality (by hooking back up to the network) and the actual reality (by disconnecting from the network).[314]

This, Kerr argues, is not so unlike the current Internet. While online, users shop, receive, and send mail and go to chat rooms, all the while oblivious to how it all technically works.[315] On the other hand, the external reality of the Internet is that it is a series of computers, connected by wires and cables, which communicates by various standard protocols.[316] For example, when a user goes to Amazon.com to buy a book, she is in reality accessing the website through her browser over the phone lines (or cable wires) and through IP address locations, while she is simply sitting in front of a computer.[317] However, from her virtual reality perspective, it is as though she is driving down the street and walking into a real, brick and mortar store.[318] Kerr concludes that, though there may be some disagreement on the issue, the "advance of technology" and increasingly "lifelike" virtual realities created by the Internet and other technologies may well appropriately require courts to acknowledge the virtual perspective in addressing subsequent legal disputes.[319]

---

[310] *Id.*

[311] *Id.* at 357-58.

[312] *Id.* at 359-61 (citing THE MATRIX (Warner Brothers Pictures 1999)).

[313] *Id.* at 359.

[314] *Id.*

[315] *Id.* at 360.

[316] *Id.*

[317] *Id.* at 363.

[318] *See id.*

[319] *See id.* at 405.

Viewing the spyware bargain from the virtual perspective sharpens the relevant issues into focus. This helps overcome the problem of perspective regarding the spyware bargain by sharply drawing attention to the underlying reality of the invasive surveillance involved and away from the seemingly benign conclusion that "it's just another program on your computer." The online version of the spyware transaction usually has the user acquiring a modestly valued software application, such as KaZaa, a computer game, or a weather program, for "free." In exchange, the user allows the installation of additional software that monitors all online activity and delivers advertisements based on that user's "marketing profile," which develops based on the aggregation of the surveillance data. A contract is thereby formed. The spyware then "spies" on the user — every shopping website, every e-mail, every chat room, every medical website, every religious website, every political website, every pornographic website. No matter where the user "goes" online, the spyware records the activity and transmits it back to the software provider. All of this is usually from the user's computer in the comfort of her own home.

Consider now an "offline" analogy of this transaction. Instead of KaZaa, the consumer wants to acquire a toaster or perhaps a scientific calculator. The consumer could buy one of these items for a modest price, say, ten to fifteen dollars. Instead, however, a company approaches the consumer and makes the following proposition. The company will provide the calculator free of charge. All the consumer has to do in return is allow one of the company's "surveillance agents" to move into the consumer's house and follow the consumer wherever she goes, day or night, for whatever purpose. The consumer is told that the surveillance agent will report the data he gathers back to the company, which will then mail to the consumer advertising circulars targeted to the consumer's apparent interests. Somewhat wary but ready for the free calculator, the consumer agrees. She brings the calculator home and begins using it. A couple of hours later, there is a knock on the door. It is the surveillance agent, dressed in a black suit and sunglasses. The consumer shows the agent in, and he places a desk in the corner of the living room, takes out a notepad, and sits down. A bit unnerved, the consumer decides to go to the bookstore across town. The agent follows her in his car and into the store, up and down the aisles, writing down every book and other product she touches. He also notes when she orders a decaf latte at the coffee stand in the corner of the bookstore. When the consumer leaves the bookstore, she goes by a convenience store to buy a home pregnancy testing kit. Meanwhile, the agent follows

and notes everything. Then the consumer goes to her local church to participate in a prayer ceremony. The agent follows and documents it all. The consumer then leaves and stops by a friend's house for a visit. The agent enters the house behind her and listens to record every word spoken. Finally, the consumer leaves and goes back to her house, where the agent follows and enters in. The next day, the consumer checks her mailbox and finds brochures on latte makers, baby products, abortion clinics, adoption agencies, and a new church being built two blocks from her house. The agent, of course, is looking over her shoulder while she is checking her mail. And so on it goes.

Would anyone knowingly make such a deal in the offline world where perspective is more firmly based?[320] Has anyone ever even heard of such a deal in the offline world — where the primary consideration offered by the consumer is the purported contractual consent to trespass and invasion of privacy, to allow herself to be continuously monitored and subject to surveillance indefinitely? That is, has anyone heard of such a deal before the advent of spyware and adware?[321] Surely not. This Article is not alone in its view of the realities, however "virtual" they may be, of the typical spyware transaction. One software executive has said that "spyware is the cyber-age equivalent of someone trespassing into your home."[322] Representative Joe Barton recently stated, in a similar vein: "If somebody walks in my house without my knowledge,

---

[320] Not everyone expresses such skepticism. One cryptographer suggested that "were McDonald's to offer free Big Macs in exchange for DNA samples, there would be lines around the block." Andrew J. McClurg, *A Thousand Words Are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling*, 98 NW. U. L. REV. 63, 129 (2003) (citing Bernice Kanner, *One Person's Privacy Is Another's Free Goody*, SAN DIEGO UNION-TRIB., Aug. 21, 2001, at 4). Though dismayed, McClurg concludes that "[i]f people validly consent to invasions of their privacy, there is little room for objection by others." McClurg, *supra*, at 129. Notably absent from this discussion, however, is any mention of public policy limitations on such contracts.

[321] *Cf.* I ♥ HUCKABEES (Twentieth Century Fox 2004) (involving plot where the protagonist hires "existential detectives" to spy on him in his house, at work, and everywhere he goes in order to help solve the coincidences occurring in his life); *see also* Jen Harris, *A Great Film's Infinite Nature*, YALE DAILY NEWS.COM, Oct. 29, 2004, *available at* http://www.yaledailynews.com/article.asp?AID=27030; Megan Lehmann, *Smart with Sartre*, N.Y. POST, Oct. 1, 2004, at 45, *available at* http://nypost.com/movies/29445.htm (describing this movie as "zany," "bizarre," and a "hyperactive farce"). Thanks to my colleague Jason Gillmer for the discussion on the movie. Perhaps, though, this further illustrates my point of the absurdity of knowingly contracting primarily for oneself to be spied upon.

[322] Smith, *supra* note 22, at 9-10 (quoting *Hearing Before the S. Comm. on Commerce, Science, and Transportation*, 109th Cong. (2005) (testimony of David Moll, CEO, Webroot Software, Inc.), *available at* http://commerce.senate.gov/hearings/testimony.cfm?id=1496&wit_id=4255).

without my permission, they're trespassing."[323] As Ben Edelman described: "Maybe the [spyware] is Mother Theresa, but it's Mother Theresa sitting in your living room uninvited and you want her gone also."[324] Senator Conrad Burns, one of the sponsors of the SPY BLOCK Act introduced in Congress in the 2005 session, has said that the legislation is needed to "protect . . . computer users from those potentially devastating spies and the programs they want to install."[325] His cosponsor, Senator Wyden, stated: "Millions of Americans use computers daily to pay their bills, research medical conditions and to shop online, and no one should have to worry that with each click of a mouse their every move in cyberspace is being watched."[326] Yet another commentator has stated that "[s]tealth data collection is like having a telemarketer listen in on the speakerphone while you eat dinner with your family."[327] Still, many observers seem to dismiss the invasive nature of spyware. This may be based in part on the perspective problem highlighted by Professor Kerr. But, if anything, the threat of surveillance is greater online than it is in real space.[328] Hence, the spyware scenario should be addressed for what it is in every virtual sense of how it invades consumers' privacy and dominion. It is a purported contractual consent to constant surveillance and monitoring that starts from inside users' homes on their computer and follows them wherever they go on the World Wide Web. Only if the problem of perspective is overcome can the spyware bargain be correctly addressed.

C. *An Analysis of the Purported Spyware Bargain Under Existing Contract Theories*

With the clarified perspective on the reality of the "spyware bargain" in place, the following section turns to whether contract law can countenance such a bargain. For purposes of this analysis, this Article assumes that the spyware distributor has described the actual surveillance practices of the software somewhere in the EULA. Indeed,

---

[323] Cowden, *supra* note 54.

[324] Ryan Singel, *Giving New Meaning to 'Spyware,'* WIRED NEWS, July 12, 2005, *available at* http://www.wired.com.

[325] Press Release, Senator Conrad Burns, Burns, Wyden Introduce SPY BLOCK Act (Mar. 21, 2005), *available at* http://burns.senate.gov/index.cfm?FuseAction=PressReleases.Detail&PressRelease_id=1290&Month=3&Year=2005.

[326] *Id.*

[327] Spencer, *supra* note 288, at 895 n.313 (quoting Howard Millman, *How to Keep Vendors from Quietly Violating Your Privacy*, N.Y. TIMES, Jan. 18, 2001, at G9).

[328] Kang, *supra* note 15, at 1269 (basing this conclusion on computer processibility of surveillance data collected).

without such a description of what the software is actually going to do, contract and other law has little difficulty concluding that any access and surveillance would be unauthorized.[329] However, even if the EULA describes such surveillance practices, there are strong reasons to either disapprove of users' contractual consent or at least subject it to serious limits.

1. *Restatement (Second) of Contracts* Section 211(3)

Electronic boilerplate has flourished in the world of online contracting, with standard-form contracts in the form of EULAs predominating.[330] This has certainly been the case with spyware and adware EULAs; usually the details and extent of the surveillance capabilities of the software to be installed are inserted in the EULA's "fine print." Section 211 of the *Restatement (Second) of Contracts* addresses the effect of parties' adoption of a standardized writing as their contract.[331] Subsection (1) of section 211 provides that such documents have presumptive contractual validity, so long as the parties manifested assent and the terms are indeed "standard." Essentially, the consumer must "[have] reason to believe that like writings are regularly used to embody terms of agreements of the same type."[332] Consumers downloading and agreeing to EULAs for applications bundled with spyware are likely to satisfy this prong of the rule because the "clickwrap" method usually manifests assent sufficiently.[333] Moreover, the "standardization" expectation is particularly applicable in the context of downloaded software. Such applications are usually obtained by clicking on a link on a website, which is universally the same for everyone who visits the site. Thus, there can be no serious question that clickwrap assent to a EULA for spyware can meet the assent manifestation requirements of section 211(1). As an initial matter, therefore, section 211 presupposes a consumer's duty to read all terms in a contract, with the concomitant effect that the consumer is thereby bound by such terms.[334]

Section 211's reach does not end there, however. Subsection (3) provides: "Where the other party has reason to believe that the party manifesting such assent would not do so if he knew that the writing

---

[329] *See supra* notes 152-79 and accompanying text (describing "exceeded authorization" e-mail cases).

[330] Hillman & Rachlinski, *supra* note 299, at 467-68.

[331] *See* RESTATEMENT (SECOND) OF CONTRACTS § 211 (1981).

[332] *Id.* § 211(1).

[333] *See generally* Kunz et al., *supra* note 296, at 414.

[334] *See* Hillman & Rachlinski, *supra* note 299, at 458.

contained a particular term, the term is not part of the agreement."[335] In this provision, the "other party" is typically the commercial enterprise that prepared the standardized form, and the assent-manifesting party is the individual customer or consumer.[336] Thus, stated another way, subsection (3) provides that if a commercial enterprise has a good idea that its customer would not agree to the standardized contract if she was aware of one or more of its terms, those objectionable terms will be excised from the agreement. The standard is fairly high — section 211 presupposes that most consumers will not read most of the language in standardized contracts, so mere lack of actual knowledge of the objectionable terms is not enough.[337] However, section 211(3) is a device to prevent companies from abusing the fact that consumers do not read standardized contracts. Thus, consumers "are not bound to unknown terms which are beyond the range of reasonable expectation."[338] Section 211's comments further explain:

> [A] party who adheres to the other party's standard terms does not assent to a term if the other party has reason to believe that the adhering party would not have accepted the agreement if he had known that the agreement contained the particular term. Such a belief or assumption may be shown by the prior negotiations or inferred from the circumstances. Reason to believe may be inferred from the fact that the term is bizarre or oppressive. . . .[339]

An argument can certainly be made that purported contractual arrangements such as spyware EULAs, which include consent to continual online surveillance and monitoring, are candidates for nonenforcement under section 211(3). It is highly doubtful that any user actively seeks to have such surveillance-enabled software placed on her computer for its own sake. Rather, the consumer is only thinking of getting the desired application, such as KaZaa or a computer game. True freeware still exists on the Internet, as well as "trial versions" of programs or shareware, which allow the downloading of a program for limited purposes, with payment required to get the full version.[340] Thus,

---

[335] RESTATEMENT (SECOND) OF CONTRACTS § 211(3).

[336] *See id.* § 211 cmts. a, b, f.

[337] *Id.* § 211 cmt. b ("A party who makes regular use of a standardized form of agreement does not ordinarily expect his customers to understand or even to read the standard terms.").

[338] *Id.* § 211 cmt. f.

[339] *Id.*

[340] *See, e.g.*, CNET Networks, Search for Shareware Programs and Free Software Webpage, http://www.shareware.com (last visited Feb. 28, 2005).

it certainly is not a given that consumers always know there "must be a catch" in the form of consent to constant surveillance. In short, consumers do not usually expect spyware. This is further evidenced by the recent survey of Internet users mentioned in Part I.D.[341] That survey revealed that 80% of all computers tested had spyware or adware installed on them; even more notably, 89% of these computer users were completely unaware of the presence of the surveillance software on their computers.[342] The fact that 89% of these users were completely unaware of the spyware on their computers supports an inference that the installation of such software — if it had been discussed in a EULA to which the consumer manifested some type of superficial assent — was clearly beyond the range of reasonable expectation, in terms of the operation of *Restatement* section 211(3).

The actual language of section 211(3) requires proof that the company has reason to know that if the consumer knew the term was in the contract, the consumer would not agree.[343] Thus, in the spyware scenario, a consumer would need to prove that the spyware distributing company with whom the consumer made the "deal" had reason to believe that the consumer would not have assented to the EULA if she had known that surveilling spyware or adware was part of the EULA and thus the contract. Though there have been no cases to date on this issue, a recent empirical study addressed this and other questions concerning spyware.[344] The study confirmed that spyware exists on almost 90% of all computers connected to the Internet.[345] It also stated that most users consider "spyware-like functionality" to be unacceptable.[346] However, due in large part to the "perspective problem," many users lack knowledge or awareness of the actual risks of certain applications because they lack technical knowledge of how the Internet works.[347] The study, which tracked users' installation of various programs containing spyware, confirmed that consumers typically ignore the EULAs altogether and instead quickly click in order to

---

[341] AMERICA ONLINE & NAT'L CYBER SECURITY ALLIANCE, *supra* note 66.

[342] *Id.*

[343] RESTATEMENT (SECOND) OF CONTRACTS § 211(3).

[344] Nathaniel Good et al., Stopping Spyware at the Gate: A User Study of Privacy, Notice and Spyware (July 6, 2005) (unpublished manuscript presented at Symposium on Usable Privacy and Security (SOUPS)), *available at* http://www.sims.berkeley.edu/~jensg/research/paper/grossklags-spyware_study.pdf.

[345] *Id.* at 1.

[346] *Id.* at 2.

[347] *Id.* at 3 ("Consumers often lack knowledge about risks and modes of technical and legal protection.").

commence the installation.[348] Perhaps most importantly, the study showed that once users were informed that they had installed programs with spyware on them, the regret factor was high.[349] Pop-up ads, slowed computer performance, and privacy issues caused these regrets.[350] In many cases, users under the study said that they would not have installed the program had they known it contained spyware.[351] In one case concerning an application called "Weatherscope" which contained spyware, thirty out of thirty-one users said that they would not have installed the program had they known it contained spyware. This illustrates the direct applicability of section 211(3) to the spyware situation — many users would not install applications if they knew that the EULA authorized the installation of surveillance-enabled spyware. If users accounted for their "virtual perspective" and were more directly cognizant of the realities of the constant surveillance that EULAs authorize, then their reluctance to install such applications would only increase.[352] Under the terms of section 211(3), therefore, there is an argument to be made that the contract term requiring the spyware should be unenforceable.

2. Unconscionability

A broader doctrine related to section 211(3) is the doctrine of unconscionability.[353] The unconscionability doctrine is set forth in section 2-302 of the U.C.C., which applies to contracts for the sale of goods and authorizes courts to refuse to enforce contracts that contain terms that are deemed to be unconscionable.[354] The doctrine has been liberally applied outside the sale of goods context and is also set forth in the *Restatement* section 208, which provides substantially the same rule.[355] The purpose of the doctrine of unconscionability is to prevent oppression and unfair surprise.[356] Under the doctrine as it has been developed, courts have followed an analytical framework proposed by Arthur

---

[348] *Id.* at 8.

[349] *Id.* at 8-9.

[350] *Id.* at 8.

[351] *Id.* at 8-9 ("Users remarked that they would remove programs that had popups. 'If I had known this had popups wouldn't have installed it.'").

[352] *See supra* notes 301-28 and accompanying text.

[353] *See* RESTATEMENT (SECOND) OF CONTRACTS § 211 cmt. f (1981) ("This rule is closely related to the rule against unconscionable terms . . . .").

[354] U.C.C. § 2-302 (2003).

[355] RESTATEMENT (SECOND) OF CONTRACTS § 208.

[356] U.C.C. § 2-302 cmt. 1.

Leff.[357] Leff's framework requires separating the unconscionability inquiry into two distinct phases: (1) procedural unconscionability, which measures the voluntariness and quality of the manifested assent, and (2) substantive unconscionability, which measures the relative fairness of the substantive terms of the contract.[358]

Unconscionability, like *Restatement* section 211(3), quite often is utilized in analyzing the enforceability of standard-form agreements.[359] Determining whether a contract is procedurally unconscionable involves factors such as "sneaky drafting strategies, such as hiding offensive terms in fine print, . . . or incomprehensible terms."[360] Courts also consider disparity in bargaining power, as well as the fact that the contract is one of adhesion offered on a "take it or leave it" basis.[361] EULAs for spyware-containing software bundles arguably fall into this category of procedural unconscionability. The technical intricacies of the software's surveillance capabilities are usually contained in the "fine print," as evidenced by the fact that virtually no one who has spyware on their computer knows that they have it.[362] Had the users understood that the EULA contained references to the installation of spyware, it would not have surprised them to subsequently learn that their computers were infected with it. Moreover, online EULAs that accompany software downloads are uniquely adhesion contracts, more so than in the traditional context, because with a downloaded program there is literally no way to interact with and bargain with a real person. Therefore, the clickwrap functionality of manifesting assent — the user literally cannot install the software mechanically without manifesting assent by mouse click — is quintessentially indicative of unequal bargaining power. There is not even a pretense of the potential for dickering or the customization of terms. This, coupled with the adverse surveillance effects of spyware and near universal surprise at consumers' discovery of its presence on their computers, makes the case for procedural unconscionability.

The case for substantive unconscionability follows closely after the case for procedural unconscionability. "Substantive unconscionability

---

[357] *See* Hillman & Rachlinski, *supra* note 299, at 456 (citing Arthur Allan Leff, *Unconscionability and the Code — The Emperor's New Clause*, 115 U. PA. L. REV. 485, 486-87 (1967)).

[358] *See id.* at 456-57.

[359] *See id.* at 457-58.

[360] *See id.* at 456-57.

[361] *See* Williams v. Walker-Thomas Furniture Co., 350 F.2d 445, 449 (D.C. Cir. 1965).

[362] *See supra* note 66-67 and accompanying text.

encompasses manifestly unjust terms, such as terms that are immoral, conflict with public policy, deny a party substantially what she bargained for, or have no reasonable purpose in the trade."[363] Further, when there is a gross disparity in the terms of the contract, courts will often apply the unconscionability doctrine.[364] Sometimes, courts describe the unenforceability of contracts that "shock the conscience," but this is not required.[365] These factors all have potential applicability in the context of spyware bargains. Viewed from the "virtual" perspective outlined by Professor Kerr, the disparity of terms between the spyware distributor and the consumer seems immense. A consumer gets a modestly priced application[366] and, in return, grants the distributor the right to follow her every move on the Internet — to "spy" indefinitely on her wherever she goes. Moreover, there is typically no contractually specified end to the surveillance — it continues indefinitely, theoretically for years. The problem of perspective, in the case of individual sharing of personal and private details of one's life, results in what Michael Froomkin has called "privacy myopia."[367] That is, consumers simply are often unable to perceive the value of yielding their privacy in the context of a transaction dealing in that privacy.[368] As a result, consumers are almost invariably badly outdone in the bargaining process when they exchange privacy for some software because the danger of gross miscalculations of relative value in the bargaining process is great.[369] This can change, however, once the problem of perspective is recognized. Courts should also factor in the transaction's extreme "take it or leave it" characteristics coupled with the often impenetrable maze of language contained in most spyware-related EULAs. If the purported spyware bargain is seen for what it truly is, then courts should be more willing to find substantive unconscionability.

---

[363] Hillman & Rachlinski, *supra* note 299, at 457.

[364] *See, e.g.*, Sosa v. Paulos, 924 P.2d 357, 360-61 (Utah 1996).

[365] Hillman & Rachlinski, *supra* note 299, at 457-58.

[366] Though this Article presents no direct evidence to support this conclusion, there is little doubt as a market matter that software applications that are sufficiently desired by the consuming public may easily charge a fair price which consumers are willing to pay. Those on the marginal fringes of desirability are often the ones that are offered for "free," bundled with spyware.

[367] *See* A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1501-05 (2000).

[368] *See id.*

[369] *See id.*

3. Public Policy and Privacy Concerns

As discussed above, *Restatement* section 211(3), or possibly the unconscionability doctrine, could be utilized for purposes of invalidating contractual consent to spyware. This list of potential contract defenses for spyware-containing EULAs is not, however, a necessarily exhaustive one.[370] However, perhaps the most straightforward way to deal with purported contractual consent to surveillance by spyware is simply to analyze such contracts under the rubric of privacy as a public policy concern. As discussed earlier, all of the current legislative efforts toward spyware and many of the industry participants simply assume that consent in the form of a EULA clickwrap is sufficient to legitimize the practice of indefinite online surveillance.[371] However, given the privacy concerns at stake, it is worth considering whether contract doctrine should be utilized to countenance the bargain of software in exchange for indefinite surveillance.

Though parties generally have the freedom to contract as they wish, this is not universally true. When there is a sufficiently important societal interest involved, courts have refused to enforce contracts concerning the implicated subject matter on public policy grounds.[372] Thus, section 178(1) of the *Restatement (Second) of Contracts* provides: "A promise or other term of an agreement is unenforceable on grounds of public policy if legislation provides that it is unenforceable or the interest in its enforcement is clearly outweighed in the circumstances by a public policy against the enforcement of such terms."[373] The sources of such public policy can be the Constitution, statutes enacted by the legislature, or case law. "[W]hether there is a prior expression or not the courts can refuse to enforce any contract which they deem to be contrary to the best interests of citizens as a matter of public policy."[374] On account of public policy, a wide range of subjects have been deemed to be beyond the range of permissible contract, including contracts to perform illegal acts, such as selling human organs;[375] contracts to commit torts;[376] contracts in

---

[370] Arguments could possibly be made under theories such as mistake or misunderstanding, among others, though the obstacles would likely be higher than under section 211(3) or unconscionability. *See* RESTATEMENT (SECOND) OF CONTRACTS § 153 (1981) (addressing unilateral mistake by one party); *id.* § 20 (misunderstanding by parties as to meaning of mutual assent).

[371] *See supra* notes 139-45 and accompanying text.

[372] *See* RESTATEMENT (SECOND) OF CONTRACTS ch. 8, Introductory Note.

[373] RESTATEMENT (SECOND) OF CONTRACTS § 178(1).

[374] Anaconda Fed. Credit Union v. West, 483 P.2d 909, 911 (Mont. 1971).

[375] *See* 6 WILLISTON ON CONTRACTS § 12:4 (4th ed. 1990); *see also* 42 U.S.C. § 274e(a) (2005) ("It shall be unlawful for any person to knowingly acquire, receive, or otherwise

restraint of trade, such as excessively constraining covenants not to compete;[377] and contracts to charge excessive interest on loans.[378] Thus, for instance, no matter how much a consumer may be willing to pay 45% interest on a home mortgage loan, such a contract would be almost universally condemned under the usury laws.

With the purported spyware bargain, the countervailing public policy is privacy.[379] There is no existing or proposed legislation providing that the practice is unenforceable if purported consumer consent is obtained, so the analysis must turn on the law and policy behind the right to privacy. The common law right to privacy in the United States originates from a law review article written in 1890 by Samuel Warren and Louis Brandeis.[380] The article articulated the basis for what would become the tort of invasion of privacy.[381] Warren and Brandeis wrote the article in response to invasive press coverage of their families,[382] but it was also broadly in response to the threats imposed by technological innovation. "[N]umerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"[383] Thus, they argued at the onset of the article that such technological innovations require that courts consider fashioning new doctrines to ensure the balance of protection for individuals. "That the individual shall have full protection of person and property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection."[384] The Warren and Brandeis article focused on the right to prevent certain private facts from exposure, but the invasion of privacy tort was later

---

transfer any human organ for valuable consideration for use in human transplantation if the transfer affects interstate commerce.").

[376] *See* RESTATEMENT (SECOND) OF CONTRACTS § 192.

[377] *See* 6 WILLISTON ON CONTRACTS §§ 13:1-28.

[378] *See id.* § 20 (usury).

[379] *See* Kang, *supra* note 15, at 1202-05 (describing three clusters of privacy concerns: (1) spatial privacy, which is concern for preventing intrusion into physical space; (2) decisional privacy, such as set forth in *Roe v. Wade*; and (3) informational privacy, which Kang describes as "an individual's claim to control the terms under which personal information — information identifiable to the individual — is acquired, disclosed, and used").

[380] Warren & Brandeis, *supra* note 130.

[381] *See, e.g.*, Howard v. Antilla, 294 F.3d 244, 247-48 (1st Cir. 2000) ("It is rare that the pedigree of a whole breed of common law tort claims can be traced with pinpoint accuracy. But in the case of common law claims for invasion of the right of privacy, most sources agree that the broad contours of these legal theories were first outlined by Samuel Warren and Louis Brandeis in the pages of the *Harvard Law Review*.").

[382] *See* ROBERT ELLIS SMITH, THE LAW OF PRIVACY EXPLAINED § 1.03 (1993).

[383] Warren & Brandeis, *supra* note 130, at 195.

[384] *Id.* at 193.

expanded to include a right of freedom from intrusion upon seclusion.[385]

The privacy interest, of course, is not limited to the interests of tort law. From the law enforcement perspective, it has been enshrined in the Constitution in the form of the Fourth Amendment requirement that citizens be secure in their persons and homes against unreasonable searches and seizures.[386] Moreover, the U.S. Supreme Court has recognized a broad right of privacy provided by the Constitution and has even classified it as a "fundamental" right.[387] This right has been recognized by the Supreme Court, in light of the various zones of privacy which are guaranteed by the Constitution.[388] One of these zones of privacy that has been consistently acknowledged and protected is the "sanctuary of the home."[389] In *Rowan v. U.S. Post Office Department*, the Court stated that "[t]he ancient concept that 'a man's home is his castle' into which 'not even the king may enter' has lost none of its vitality."[390] The fundamental nature of the right to be free from privacy intrusions in one's own home was also recognized by the Court in *Stanley v. Georgia*.[391] Unwanted surveillance has also been said to be "in tension with human dignity."[392] Therefore, the right of privacy in one's own home has long been recognized and even resides in the rarefied air of fundamental rights protected by the Constitution.

The fact that one may contractually consent to most things, including even a surrender of one's privacy by surveillance-enabled spyware that trespasses into the home, has not been seriously challenged. Thus, all current proposals for spyware legislation have assumed consent as a defense.[393] However, privacy is a fundamental right of constitutional proportions, and the degree to which it may be frivolously contracted away bears some scrutiny. The cases discussed above, which seemed to allow contractual consent to various trespasses, all concerned a bargained-for exchange in which the trespass was incidental to the

---

[385] *See* Prosser, *supra* note 131, at 389-90.

[386] U.S. CONST. amend. IV.

[387] *See* Roe v. Wade, 410 U.S. 113, 152 (1973).

[388] *See* Griswold v. Connecticut, 381 U.S. 479, 483-84 (1965).

[389] *See* Rowan v. U.S. Post Office Dep't, 397 U.S. 728, 738 (1970).

[390] *Id.* at 737.

[391] Stanley v. Georgia, 394 U.S. 557, 564-65 (1969).

[392] Kang, *supra* note 15, at 1260; *see also* Schwartz, *supra* note 291, at 2086 ("If information privacy is a civil liberty, it may make no more sense to propertize personal data than to commodify voting rights." (quoting *Need for Internet Privacy Legislation: Hearing Before the S. Comm. on Commerce, Science, and Transportation*, 108th Cong. (2001); Electric Privacy Info Center & Junkbusters, *Pretty Poor Privacy: An Assessment of P3P and Internet Privacy* (June 2000), http://epic.org/reports/prettypoorprivacy.html).

[393] *See supra* notes 139-45 and accompanying text.

transaction.[394] So, for instance, in *American Computer Trust Leasing v. Jack Farrell Implement Co.*,[395] the court declined to find violations of the Wiretap Act for alleged incursions onto the plaintiff's computer because online access to it was part of the contractual arrangement between the plaintiff owner and the defendant computer vendor. The contract was primarily for the sale or lease of the computer and the maintenance of certain business records, not for trespass and intrusion onto the computer.[396] Further, in *Geddes v. Mill Creek Country Club, Inc.*,[397] the contract was primarily for the allowance of the construction of a golf course adjacent to the property.[398] The subsequent alleged intrusion onto the plaintiff's property in the form of errant golf balls was neither a serious intrusion nor a primary component of the contract.[399] Other cases of clear consent to trespass and invasion of privacy can be offered: one has no trespass or privacy claim against a plumber who enters the consumer's home to fix a leaky pipe. No doubt there has been an invasion, but it was clearly consented to. However, allowance of the plumber's invasion was not the primary consideration flowing from the consumer — payment of money was. Allowance of the invasion was merely a practical necessity.

What these cases do not involve is a contract where the *primary* consideration flowing from the consumer was the grant of an indefinite license to enter into her home and subject her to constant surveillance or even constant trespass. Such consent is indirectly addressed by the chattel repossession cases under article 9 of the U.C.C. and prior law.[400] Those cases involved contract clauses which granted the vendor or secured creditor the right to repossess personal property upon default and even to enter the debtor's home to effect the repossession if necessary. As this Article has demonstrated, however, these purported contractual consents to entry and invasion are not enforceable.[401] The courts have developed at least the following principles which are applicable here: (1) public policy simply will not condone the granting of an indefinite license to enter one's own home to obtain property, even

---

[394] *See supra* notes 201-26 and accompanying text.

[395] Am. Computer Trust Leasing v. Jack Farrell Implement Co., 763 F. Supp. 1473, 1494 (D. Minn. 1991), *aff'd and remanded*, 967 F.2d 1208 (8th Cir. 1992).

[396] *Id.*

[397] Geddes v. Mill Creek Country Club, Inc., 751 N.E.2d 1150 (Ill. 2001).

[398] *Id.* at 1155.

[399] *Id.*

[400] *See supra* notes 227-73 and accompanying text.

[401] *See id.*

if there is purported contractual consent; (2) rather, the invader must obtain subsequent, contemporaneous, actual consent before entering, or otherwise the entry is not countenanced; and (3) the consumer may voice her objection at the time of entry, and this will result in the prohibition of any further entry, notwithstanding any prior contractual consent.[402]

Thus, based on these general privacy principles and the sanctity of one's home, it can be argued that spyware contracts that obtain purported consent to surveillance should be unenforceable as being against the public policy favoring privacy. Unlike contracts where the invasion is a merely incidental aspect of the bargain, under the spyware bargain the full consideration flowing from the consumer is the allowance of unfettered, continuous online surveillance of the consumer, which could conceivably include all of the most private aspects of the consumer's life. The invasion effected by the spyware is a "virtual" trespass into the consumer's home — the usual location of the consumer's computer used for web browsing. There is not any "announcement" by the spyware that it is about to enter, as there is in the repossession cases. Rather, the invasion and surveillance are continuous and largely hidden from the typical consumer once the initial "click" occurs when the software is downloaded.[403] The entry into a consumer's home is not countenanced when the issue is repossession of collateral. Quite arguably, neither should the virtual entry into one's home be countenanced when the issue is the gathering of surveillance. Further, since this is the entire consideration flowing from the consumer in the bargain, unlike a secured loan where the consumer is also making payments on the loan in exchange for having received the item of personal property, the issue of simply declaring the bargain unenforceable becomes one worthy of consideration.

This Article is not alone in asserting this opinion. Though largely unaddressed to date by legal commentators, several industry participants have come to a similar conclusion. For instance, Dr. John R. Levine, the author of several consumer books on the Internet, including *The Internet for Dummies*,[404] *Internet Privacy for Dummies*,[405] and *Fighting Spam for Dummies*,[406] has stated the following in response to recent

---

[402] *See id.*

[403] *See* Schwartz, *supra* note 291, at 2068 ("[A]dware and spyware operate in an environment in which consumers generally lack any awareness that their computers are 'phoning home' to the companies who are tracking their online behavior.").

[404] JOHN R. LEVINE ET AL., THE INTERNET FOR DUMMIES (9th ed. 2003).

[405] JOHN R. LEVINE ET AL., INTERNET PRIVACY FOR DUMMIES (2002).

[406] JOHN R. LEVINE ET AL., FIGHTING SPAM FOR DUMMIES (2004).

proposed legislation regarding spyware:

> One could argue that in principle this problem [of spyware] could also be addressed by better disclosure, but I believe there are public policy reasons that it's not a good idea to let people sell their privacy rights. The law has long forbidden certain kinds of consumer transactions (selling parts of one's own body, for example) as contrary to the public interest, even if the consumer wishes to enter into such a transaction voluntarily and with full notice. I believe that there are sound reasons to treat the sale of one's privacy as contrary to public privacy. The value of one's privacy is great, and the amounts offered in exchange for it are rarely large. Once one's privacy is traded away, it is difficult or impossible to regain, and the implications of giving it up are frequently far greater than what a consumer would foresee.[407]

Thus, a plausible argument can be made that contracts where the primary source of consideration is the consumer's consent to allow indefinite surveillance of all of her online activities, as in the case of spyware contracts, are too invasive in nature and of sufficient privacy concern so as to be void under public policy. Consumers do not know that spyware gets on their computers, as the model of contractual assent is deeply flawed. They cannot get it off their computers, the spyware fouls up the performance of their computers, and it generates annoying pop-up ads. Of much greater concern, the spyware conducts continual surveillance of the consumer's online activities. Adware advocates insist that the surveillance, development of a "marketing profile," and resultant delivery of "desired ads" is a net social benefit, but this is a highly dubious claim. Even if it were completely true, however, the negative attributes of spyware as perceived by the public, combined with the privacy-invasive nature of the surveillance functions of the spyware, compel the conclusion that the "spyware bargain" should be banned as violative of public policy. Of course, as a practical matter, the dollar amounts involved in individual cases may present cost-benefit problems with bringing litigation. Class actions are a possibility, but federal legislation that bans such contracts is the easiest route to implementing any such public policy concerns.

Thus, spyware and adware, in its surveillance form, should be banned. However, recognizing that this would be a dramatic change from current industry practices, there is a first step that could be taken. It may be

---

[407] FTC Spyware Workshop, *Written Comments by Dr. John Levine* (Mar. 2004), http://www.ftc.gov/os/comments/spyware/040319levine.pdf.

helpful to analogize to repossession cases which do not countenance an advance, contractual license to enter a consumer's home. Rather, in situations where a seller or secured creditor wishes to enter a consumer's home in order to repossess personal property, the contemporaneous consent of the consumer must be obtained — the prior contractual grant of consent is ignored as a public policy matter.[408] Like secured creditors, spyware operators seek advance contractual consent to "enter" a consumer's home by invading the home computer. Also, like secured creditors, they seek to obtain valuable property, namely the surveillance data obtained as a result of the constant monitoring of the consumer's web browsing activities. Unlike the secured creditor context, however, spyware operators only obtain consent at the initial transaction stage, usually in the form of click-assent to a EULA. However, this is not sufficient, given the privacy concerns at stake and the danger that most consumers are not aware of the surveillance that is continually transpiring (notwithstanding their prior manifestation of assent). Public policy should dictate additional procedural safeguards designed to further ensure ongoing consumer consent to the spyware surveillance, if it is to be countenanced at all. Thus, as a matter of code requirements for the spyware, the software should be required to periodically "knock and announce" before "entering" the consumer's home/computer and transmitting the private surveillance data.[409] This should be required as a matter of privacy and consumer dignity, just as it is in the "offline" world, as illustrated by the repossession cases. A periodic notification screen on the consumer's computer, which itemizes all web browsing activity that has been monitored, would be helpful. The screen should clearly display this content to the consumer in an easy-to-read form, so that the consumer understands the degree of surveillance that has been collected. Then, to ensure privacy and dignity and to ameliorate the effect of the invasive nature in which the data has been harvested, the software should ask whether the consumer consents on that occasion to

---

[408] *See supra* notes 227-73 and accompanying text.

[409] *See* Spencer, *supra* note 288, at 910-11 ("Consumer privacy legislation should further combat information asymmetry by requiring every business to obtain the consumer's express consent each time it wishes to share personal data about that consumer with a third party. Businesses could send notice via e-mail or post card, giving consumers the option to grant or deny permission via e-mail, Web site, or toll-free telephone number. The notices would have to disclose the identity of the third party. Although some consumers are dimly aware that their data is shared, most have no conception of how pervasive the data web is. Merely receiving notice of each instance of data sharing would raise awareness among consumers, and the opportunity to deny permission would add to the process an aspect of meaningful consent that is notably absent today.").

the data being transmitted. Further, the consumer should have a "line item" veto right over the excision of certain data being transmitted, as well as the right to completely deny consent to any of the data being transmitted. This process should occur frequently, perhaps as often as once a week or maybe even more often, and the notifications should clearly identify themselves as being produced by the surveillance-enabled spyware program installed on the consumer's computer. Short of an outright ban on spyware, these measures should be implemented in any current or future efforts at regulating the spyware practice. These measures are needed in order to vindicate the privacy concerns at issue.[410]

CONCLUSION

The purpose of this Article has been to question the propriety of sanctioning spyware's consumer-consent driven paradigm. In this paradigm, the individual consumer contractually consents to allow installation of spyware as the primary consideration in a bargain to obtain certain desired software applications. The spyware's purpose is to effect continual, unending surveillance of all of the consumer's online browsing activities on the Internet. To date, many have accepted the contractual consent to this arrangement without serious question. This is illustrated by the element of consent throughout all laws and doctrines that potentially apply to spyware, as well as by remarks by certain industry participants in the ongoing public spyware debate. This, however, may be largely because of the perspective problem about online activity, as recently highlighted by Professor Kerr. Taking the surveillance more literally for what it is — comparing it, for example, to real world surveillance effected from inside a person's home by a real person — draws the objectionable nature of the surveillance into sharper focus. Many, if not most, consumers would be unlikely to enter into such a bargain knowingly if they were fully aware of the degree of privacy that the bargain compels them to surrender in exchange for a modestly valued software application. For this reason, section 211(3) of the *Restatement (Second) of Contracts* would probably invalidate most purported consumer consents to EULAs that provide for the installation

[410] Paul Schwartz recently made a similar suggestion in a slightly different context. *See generally* Schwartz, *supra* note 291 (proposing hybrid alienability model for sale of personal information so that, as to information consented to be collected by consumer, further consent must be obtained by original collecting entity before that entity may sell information to third party).

and surveillance of such spyware. Moreover, there is also an argument that such agreements are unconscionable, even if the consumer was aware of the relative values exchanged, because gaining a desired software application in exchange for granting the right to effect surveillance for an indefinite period of time is not a fair bargain.

More significantly, however, the invasive nature of the spyware bargain is such an affront to privacy concerns that it implicates public policy. One response to these privacy concerns is simply to declare such bargains void as against public policy. This result can be easily defended based on the negative attributes of spyware, the often deceptive mode of installation, the great peril that abuse of the software's surveillance ability would cause, and the fact that the assent to such a bargain by the consumer is often flawed. The foremost basis, however, is that privacy is such a paramount concern that society has decided that it does not want to encourage consumers to frivolously bargain away their fundamental dignity and privacy, all in the name of obtaining software and a few advertisements. Of course, to be effective, any such prohibition and enforcement would likely have to occur on a federal legislative level, since individual lawsuits against spyware distributors would be problematic from a cost-benefit perspective.

A more immediate response to the spyware bargain which should occur is the implementation of additional procedural safeguards to the transactions than are currently employed in the industry or that are contemplated in any of the current spyware-specific legislative proposals. The impetus for these safeguards comes from a review of the law of secured transactions and, specifically, repossession of personal property from inside a consumer's home. In that context, a creditor must receive contemporaneous consent to invade the consumer's house and retrieve the item of personal property, regardless of any prior contractual consent that may have been given to such entry. Public policy has clearly articulated that such prior contractual consent is ineffectual, and the sanctity of the consumer's home dictates that contemporaneous consent must be obtained prior to the creditor's entry. Because surveillance-enabled spyware is on a consumer's computer inside her home and is continually obtaining surveillance data and seeking to transmit it back to the spyware distributor, similar policy implications are present. Currently, no proposed legislation requires any consumer consent other than that obtained at the initial transaction phase, when the consumer grants "click through" consent to the EULA. Afterwards, unless the consumer is extraordinarily adept, she is thereafter completely unaware of the degree of surveillance and transmission of her data.

Public policy should require that spyware be modified to require frequent notifications to the consumer that do the following: (1) provide extensive detail about all web browsing data, including specific websites that have been harvested by surveillance; (2) provide the name of the spyware entity which has collected the surveillance data; and (3) request contemporaneous permission from the consumer to allow the surveillance data to be transmitted back to the company. The permission could be granted in full, denied in full, or granted in part with permission denied as to certain selected website information that the consumer does not wish to share. Matters of convenience may dictate that the spyware company space these notifications apart so that they are not too great an imposition. Weekly occurrences seem like an appropriate duration between notices and requested consent, though reasonable minds could differ on the appropriate frequency. If the spyware bargain is to be countenanced at all, then these additional procedural safeguards should be implemented as a matter of public policy.

The privacy implications of spyware are great. As in 1890, when Warren and Brandeis wrote their famous article concerning the right to privacy, "recent inventions and business methods call attention to the next step which must be taken for the protection of the person."[411] In 2006 and beyond, one of the new business methods is spyware, which effects constant surveillance of a consumer's web browsing in exchange for a modestly valued software application. Though the Internet's incursions into consumers' privacy have already been substantial, attempts to obtain their contractual consent to ubiquitous constant online surveillance on computers in their own homes should be the point at which policy intervenes. Courts should decline to countenance such consent under contract doctrine or at least insist on additional procedural safeguards than are currently present. This is necessary to protect the dignity and privacy concerns of consumers.

[411] Warren & Brandeis, *supra* note 130, at 195.

***