2005

Contracting Spyware by Contract

Jane K. Winn
University of Washington School of Law

Symposium on Spyware: The Latest Cyber-Regulatory Challenge

Contracting Spyware by Contract[1]

20 Berkeley Tech. L.J. 1345 (2005)

Jane K. Winn

Abstract

The question of what constitutes "spyware" is controversial because many programs that are "adware" in the eyes of their distributors may be perceived as "spyware" in the eyes of the end user. Many of these programs are loaded on the computers of end users after the end user has agreed to the terms of a license presented in a click-through interface. This paper analyzes whether it might be possible to reduce the volume of unwanted software loaded on end users' computers by applying contract law doctrine more strictly. Unwanted programs are often bundled with programs that the end user wants, but the disclosure that additional programs will be downloaded is usually buried deeply within dense form contracts. Even though this makes it difficult for end users to recognize that they are agreeing to have multiple programs installed at once and that some of those programs may be objectionable, US courts are unlikely to invalidate those disclosures. This is because in business to consumer online contracting cases in the US, courts have tended to be very deferential to the intentions of the merchants in designing the contract interfaces. In the EU, by contrast, such conduct by software distributors would not be binding on consumers. Under unfair contract terms laws in place in EU member states, consumer objections to bundled software could not be overridden by terms hidden in standard form contracts.

1. Introduction: From Goodware to Badware[2] to Somewhere In Between

Does contract law provide consumers whose computers are clogged with spyware any tools to defend themselves against this onslaught of unwanted software? The answer is likely to be no, as courts have shown themselves generally willing to enforce online contracts notwithstanding questions about what consumers actually knew or intended when the contract was formed. Although at one extreme it is easy to identify "badware" – viruses, Trojan horses and other clearly malicious programs – and at the other, it is equally easy to identify "goodware" – popular shareware or freeware applications – there is considerable uncertainty about what end users really think about many programs. Furthermore, software that some commentators label pernicious "spyware" is considered to be comparatively benign "adware" by others, making it hard to be certain what an individual consumer would think of the program in question and whether the consumer would agree to contract for it.[3]

---

1. Professor & Director, Shidler Center for Law, Commerce & Technology, University of Washington School of Law *at* http://www.law.washington.edu/Faculty/Winn/. Many thanks to my research assistant Andrew Braff for all his help.

2. Thanks to my colleague Bill Covington for suggesting these terms to characterize the two ends of the spectrum of applications that have been labeled spyware.

3. Weatherbug is perceived by some to be a legitimate piece of software and adware/spyware by others. *Compare* PC Hell: How to Remove Weatherbug *at* http://www.pchell.com/support/weatherbug.shtml (Aug. 17, 2005) *with*

In evaluating online contracts, courts generally have shown more deference to the intent of the merchants who design the contract interfaces than to the expectations of consumers using them. In the event any consumers claim software was loaded on their computers without authorization, that deference toward the intent of the online interface designer is likely to protect distributors of programs that deliver "targeted marketing"[4] to consumers using a click-through contract interface.

In order for contract law to provide a meaningful constraint on the distribution of spyware programs, a major revision of current contract law would be required. Legislation pending in Congress in 2005 proposes to do just that: require explicit notice and consent from end users before spyware can be loaded onto their computers.[5] Assuming such a strategy might actually have an impact on the volume of spyware distributed,[6] it remains unclear whether such a piecemeal, ad hoc approach is a sensible approach to contract law reform. A similar strategy of narrowly targeted sector-specific reforms has been used in U.S. information privacy law for the last two decades with disastrous results;[7] it is not clear that such a strategy would be any more successful when applied to contract law. By contrast, the more general regulatory approach taken in the EU Unfair Contract Terms Directive[8] could be used both to block the use of misleading contract interfaces to legitimate the distribution of spyware and to provide critical scrutiny of merchant designed contracting interfaces generally.

The label "spyware" has been applied to a wide range of software applications, and it is difficult to identify an authoritative definition of spyware which would clarify the scope of the problem.[9] Because an in-depth analysis of competing definitions of spyware is beyond the scope of this paper, this paper will take the following definition from the Federal Trade Commission 2004 Federal Register Notice:

> [Spyware is] software…that aids in gathering information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge.[10]

Weatherbug Frequently Asked Questions: Is Weatherbug spyware or adware? *at* http://www.weatherbug.com/aws/support/faq_spyware.htm (last visited Aug. 18, 2005).

4. "Targeted marketing" consists of making "the right offer to the right customer at the right time." *See* Affiliate Program Glossary, *available at* http://affiliatetip.com/affiliate_glossary.php (last visited May 1, 2005).

5. "Securely Protect Yourself Against Cyber Trespass Act' or the 'Spy Act,' H.R. 29, 109th Cong. (2005).

6. This would be in contrast to the CAN SPAM Act, which one year after enactment "clearly has had no meaningful impact on the unrelenting flow of spam that continues to clog the Internet and plague inboxes." Keith Regan, "CAN-SPAM Gets Mixed Report Card for First Year," MacNewsWorld.com, Jan. 3, 2005, *at* http://www.macnewsworld.com/story/39354.html.

7. *See, e.g.*, DANIEL J. SOLOVE & MARC ROTENBERG, INFORMATION PRIVACY LAW 58 (2003); Will Thomas DeVries, *Protecting Privacy in the Digital Age*, 18 BERKELEY TECH. L.J. 283, 285 (2003)

8. Council Directive 93/13 EEC of 5 April 1993 on Unfair Terms in Consumer Contracts, 1993 O.J. (L 95) 29.

9. *See, e.g.*, SpywareGuide, which described over 1,500 programs that met its definition of spyware in May 2005, states "There are a lot of differing opinions on what the definitions of Parasiteware Spyware, Adware and Malware should be." *See* Intro to Spyware *at* http://www.spywareguide.com/txt_intro.php (last visited May 1, 2005) (listing parasiteware, adware. spyware, malware, page hijackers and dialers as various types of software that may be covered by the term spyware.); *see also*, Consumers Union, Press Release: Consumer Reports Investigates How to Protect Against Spam, Spyware and Phishing, August 9, 2004 ("Spyware isn't a single type of software. The term covers a diverse range of applications.") *available at* http://www.consumersunion.org/pub/core_product_safety/001305.html (last visited May 1, 2005).

10. Notice Announcing Public Workshop and Requesting Public Comment, 69 Fed. Reg. 8538 (February 24, 2004).

Not all distributors of programs covered by this definition of spyware use contracting interfaces to help manage their relationship with those consumers whose computers run their software. Distributors of software that includes viruses or other malware that permit the software developer to commit identity theft or to access the end user's financial accounts without authorization can distribute their programs with interfaces that do not require the cooperation of the end user and so have no reason to ask the end user to assent to the download. The following discussion will address only those software distributors that include contracting interfaces in their distribution systems.

There are many popular "shareware" or "freeware" programs[11] that provide unambiguous benefits to end users who manifest assent to their end user license agreements by using a click-through interface.[12] Because end users' understanding of a program's function and the users' level of interest in granting programs access to their computers is uncertain, many targeted marketing or adware programs fall somewhere in between the extremes of universally detested and virulent spyware and acclaimed and popular freeware. While many end users might welcome targeted comparison shopping information about products they are actively seeking, they also may hate popup ads. End users might not understand either the specific quid pro quo that a particular targeting marketing company is offering (e.g., free access now to desirable content in return for exposure to popup ads in the future), or the mechanism by which that quid pro quo is enforced (e.g., adware applications loaded on the end user's computer).

This paper focuses only on those ambiguous cases where a merchant has a plausible claim that consumers have consented to the collection of personal information in exchange for some product or service, but consumers have a plausible claim that there was no consent. The application of contract law to spyware programs in this ambiguous, intermediate position between goodware and badware produces uncertain outcomes, in part because the intent of the end user in contracting or downloading is uncertain. The recent trend in contact cases toward liberalizing contract formation doctrine, in effect removing obstacles to the greater use of new technologies, makes it unlikely that contract law might be used to establish a framework within which more explicit consent must be sought before the collection of personal information could begin. While courts may be unwilling to invalidate clickwrap agreements that legitimate the distribution of adware programs that many find annoying, such deference has limits. Thus, there is no reason to expect that judicial deference to online contracts will extend so far as to legitimate the distribution of clearly malicious programs that support fraudulent or criminal activities.

2. Interpreting Ambiguous Online Contracting Interfaces

Targeted marketing firms that collect personal information in exchange for providing products or services to consumers use contracting interfaces similar to those used by other online merchants: click-through interfaces that seek blanket assent to standard form contracts. What

11. "Shareware is software that is distributed free on a trial basis with the understanding that the user may need or want to pay for it later." Whatis.com definition. "Freeware... is programming that is offered at no cost and is a common class of small applications available for downloading and use in most operating systems." Whatis.com definition.

12. *See, e.g.*, the contracting interfaces for the most popular free software downloads listed at http://www.download.com/ (last visited May 1, 2005).

often distinguishes the online contracting processes used marketing firms such as Claria and WhenU is that consumers may not realize that when they click "I agree" in response to what appears to be a standard end user license agreement (EULA),[13] they are licensing a bundle of different applications, and included in that bundle are programs that have been labeled spyware by consumer advocates.[14] Consumers may intend to download a single application and end up instead downloading several programs, including some they do not want, either by inadvertence, because the desired application is not available without the extra programs, or because the different programs have actually been combined into one. The problem of inadvertent or qualified assent is exacerbated by the fact that many adware programs are difficult to locate and remove because they are not listed in the "Add/Remove Programs" function provided by Microsoft Windows operating systems.[15]

Before asking whether assent to the terms of adware EULAs should be treated differently than assent to other Internet contracts, it may be useful to consider the current state of Internet contracting doctrine generally. Whether assent to an offer to form a contract has been manifested is a fact-specific inquiry. The Restatement provides that manifestation of assent may be by written or spoken words or by other acts or by failure to act but the conduct in question must be intentional or the actor must have reason to know conduct will be treated as assent by other party. In the absence of such a manifestation of assent, then the contract may be voidable for fraud, duress, mistake or any other invalidating cause.[16] The manifestation of mutual assent to any exchange ordinarily takes the form of an offer or proposal by one party followed by an acceptance by the other party or parties;[17] however, a manifestation of mutual assent may be made even though neither offer nor acceptance can be identified and even though the moment of formation cannot be determined.[18] The application of these principles that guide the inquiry into

---

13. Use of adware distributed by Claria (formerly known as Gator) is governed by an end user license agreement accessible at the website for Gain Publishing; *see, e.g.*, Gain Publishing Privacy Statement and End User License Agreement 7.0 issued December 2004, *available at* http://www.gainpublishing.com/global/help/app_privacy/app_ps_v70.html (last visited May 1, 2005). WhenU distributes a wide variety of direct marketing programs that are considered spyware by others, including SaveNow, WhenUShop, WeatherCast, ClockSynch and PriceBandit. Copies of the end user license agreement for each product can be accessed at http://www.whenu.com/support.html (last visited Aug. 17, 2005); the contract interface used is described at http://www.whenu.com/how_whenu_works_dl.html (last visited May 1, 2005).

14. *See, e.g.*, Tatiana Serafin, *Mr. Manners*, FORBES, July 26, 2004, at 133 ("The Federal Trade Commission held workshops on spyware in April, knocking companies (read Claria and WhenU) for failing to disclose how their software programs glom on to PCs and how they misbehave thereafter.").

15. *Id*.

16. Restatement (Second) of Contracts § 19.

17. Restatement (Second) of Contracts § 24 states that an offer is defined as the manifestation of willingness to enter into a bargain, so made as to justify another person in understanding that his assent to the bargain is invited and will conclude it.

18. Restatement (Second) of Contracts § 22; *accord* U.C.C. § 2-204:

> (1) A contract for sale of goods may be made in any manner sufficient to show agreement, including conduct by both parties which recognizes the existence of such a contract.
> (2) An agreement sufficient to constitute a contract for sale may be found even though the moment of its making is undetermined.
> (3) Even though one or more terms are left open a contract for sale does not fail for indefiniteness if the parties have intended to make a contract and there is a reasonably certain basis for giving an appropriate remedy.

U.C.C. § 2-204.

whether a contract has been formed to standard form contracts raises troubling, unresolved issues about the meaningfulness of the assent.[19] The Restatement's provisions addressing the use of standard form contracting attempt to balance the pervasive use of forms with the desire to preserve some vestige of concern about the character of the assent to the contents of forms.[20]

The apparent conflict between the freedom of choice ideology embedded in contract doctrine and the magnitude of the constraints imposed on consumer choice by standard form contracts does not appear to be any more acute in the online environment than it has been in traditional markets.[21] There does not appear to be any clear evidence that consumers are less able to deal with click-through contracting interfaces than they were able to deal with traditional paper standard form contracts, or that legitimate merchants use click-through interfaces to take advantage of consumers any more often than they did with printed form contracts. Furthermore, the question remains whether the presence of a discernable assent should really be the criteria for distinguishing between enforceable and unenforceable contracts formed using new contracting systems.[22]

While it may be difficult to ascertain whether courts are more or less deferential to merchants seeking enforcement of contracts formed with new contracting systems than they were toward merchants in traditional markets, it is not difficult to ascertain the overall trend of deference to merchant interface design choices in the face of consumer objections.[23] Because spyware is delivered exclusively in online environments, the debate surrounding the enforceability of "shrinkwrap"[24] "pay now, terms later"[25] contracts is not relevant here.[26] The

---

19. Contract scholars have recognized for nearly a century that the use of standard form contract is widespread but at the same time fails to conform to classical 19th century freedom of contract principles and debated strategies for dealing with this contradiction. *See* Nathan Isaacs, *The Standardizing of Contracts*, 27 YALE L. J. 34 (1917); Friedrich Kessler, *Contracts of Adhesion - Some Thoughts About Freedom of Contract*, 43 COLUM. L. REV. 629 (1943); W. David Slawson, *Standard Form Contracts and Democratic Control of Law-Making Power*, 84 HARV. L. REV. 529 (1971).

20. Restatement (Second) of Contracts § 211 provides:

> (1) Except as stated in Subsection (3), where a party to an agreement signs or otherwise manifests assent to a writing and has reason to believe that like writings are regularly used to embody terms of agreements of the same type, he adopts the writing as an integrated agreement with respect to the terms in the writing.
> (2) Such a writing is interpreted wherever reasonable as treating alike all those similarly situated, without regard to their knowledge or understanding of the standard terms of the writing.
> (3) Where the other party has reason to believe that the party manifesting such assent would not do so if he knew that the writing contained a particular term, that term is not part of the agreement.

Restatement (Second) of Contracts § 211.

21. Robert A. Hillman & Jeffrey J. Rachlinski, *Standard-Form Contracting in the Electronic Age*, 77 N.Y.U. L. REV. 429, 432-34 (2002).

22. Clayton P. Gillette, *Rolling Contracts as an Agency Problem*, 2004 WIS. L. REV. 679, 681 (2004) (arguing that it is possible to determine whether a contract should be enforced without reference to intent).

23. *See, e.g.*, James J. White, *Autistic Contracts*, 45 WAYNE L. REV. 1693 (2000) (noting the trend with approval); Jean Braucher, *Delayed Disclosure in Consumer E-Commerce as an Unfair and Deceptive Practice*, 46 WAYNE L. REV. 1805, 1807 (2000) (noting the trend with disapproval).

24. *See generally* Robert W. Gomulkiewicz, *Getting Serious About User-friendly Mass Market Licensing For Software*, 12 GEO. MASON L. REV. 687 (2004).

25. *See generally* Gillette, *supra* note 22 (using the term "rolling contracts" to describe "pay now, terms later" contracts).

best indication of how courts would likely respond to consumer complaints about the enforceability of adware EULAs will come from cases addressing the enforceability of "clickwrap" and "browsewrap" agreements. Clickwrap contract interfaces require some explicit manifestation of assent by the consumer to form a contract; in most cases, the consumer is asked to select between graphical representations of "I accept" and "I decline" by clicking on the chosen alternative.[27] Browsewrap terms and conditions are usually found behind a hyperlink marked something like "Legal" or "Terms" or "Use of this site signifies your acceptance of the Terms and Conditions." Because end users must seek out browsewrap terms in order to learn their contents, there is considerable disagreement over whether browsewrap interfaces can be used to form contracts at all.[28] However, the mere fact that some courts have been willing to entertain the idea that an online contract could be formed without any apparent manifestation of assent by the end user is an important development in this area.[29]

The first cases holding explicitly that a click-through interface design could be used to form a binding contract appeared in 1998.[30] In all, more than a dozen cases have been decided upholding the enforceability of contracts formed using click-through interfaces.[31] In only a few cases have courts refused to enforce specific terms contained within contracts formed using a click-through interface, and the terms at issue have been found to violate a public policy of the forum state or to be unconscionable. In one, a court refused to enforce a choice of forum term that would have required a Massachusetts resident to file suit in Virginia, which does not generally permit class action law suits, because it found that to do so would in effect deprive Massachusetts consumers of any right to challenge the merchant's performance under the contract.[32] In *Comb v. PayPal, Inc.*, a federal district court refused to enforce an arbitration agreement contained in a clickwrap agreement after the merchant presented inadequate evidence

---

26. *See* Gillette, *supra* note 22 at 685-88 (summarizing the debate); *see also* Christina L. Kunz, Maureen F. Del Duca, Heather Thayer & Jennifer C. Dubrow, *Click-Through Agreements: Strategies for Avoiding Disputes on Validity of Assent*, 57 BUS. LAW. 401 (2001) (ABA Working Group on Electronic Contracting Practices report).
27. *Id*.
28. *See* Christina L. Kunz, John E. Ottaviani, Elaine D. Ziff, Juliet M. Moringiello, Kathleen M. Porter, & Jennifer C. Debrow, *Browse-Wrap Agreements: Validity of Implied Assent in Electronic Form Agreements*, 59 BUS. LAW. 279 (2003) (ABA Working Group on Electronic Contracting Practices report).
29. *See generally id*.
30. The first appears to have been Hotmail Corp. v. Van Money Pie, Inc., 1998 WL 388389, 47 U.S.P.Q.2d 1020 (BNA) (N.D. Cal. Apr. 16, 1998) (preliminary injunction to stop spammer from using Hotmail's e-mail service because no e-mail account could be set up without clicking through online registration agreement prohibiting the sending of unsolicited commercial e-mail); a close second seems to have been Groff v. America Online, 1998 WL 307001 (R.I. Super. 1998) (no authorization to proceed with class action lawsuit when all members of putative class would have had to click through online registration agreement with choice of forum clause pointing to a different jurisdiction).
31. Caspi v. Microsoft Network, L.L.C., 732 A.2d 528 (N.J. Super. Ct. App. Div. 1999); *In re* RealNetworks, Inc. Privacy Litig., 2000 U.S. Dist. LEXIS 6584 (N.D. Ill., 2000); Lieschke v. RealNetworks, Inc., 2000 U.S. Dist. LEXIS 1683 (N.D. Ill., 2000); America Online v. Booker, 781 So. 2d 423 (Fla. Dist. Ct. App. 2001); Barnett v. Network Solutions, 38 S.W.3d 200 (Tex. App. 2001); Forrest v. Verizon Communs., Inc., 805 A.2d 1007 (D.C. 2002); Moore v. Microsoft Corp., 741 N.Y.S.2d 91, (App. Div. 2002); Net2phone, Inc. v. Superior Court, 135 Cal. Rptr. 2d 149 (Ct. App. 2003); DeJohn v. .TV Corp. Int'l, 245 F. Supp. 2d 913 (N.D. Ill. 2003); Davidson & Assocs. v. Internet Gateway, 334 F. Supp. 2d 1164, 1170 (E.D. Mo., 2004); Mortgage Plus, Inc. v. DocMagic, Inc., 2004 U.S. Dist. LEXIS 20145 (D. Kan., 2004).
32 Williams v. America Online, 2001 Mass. Super. LEXIS 11 (February 8, 2001); *accord* Scarcella v. America Online, 798 N.Y.S.2d 348 (Civ. Ct. 2004) (refuses to enforce AOL forum selection clause when alterative is small claims court); *but see* Celmins v. America Online, 748 So. 2d 1041 (Fla. Ct. App. 1999); America Online v. Booker, 781 So. 2d 423 (Fla. Ct. App. 2001) (enforcing the same term against Florida residents).

of what contract terms had actually been displayed to the plaintiffs when they enrolled in the service or that those terms had subsequently been validly modified to include an arbitration term and the plaintiffs alleged deplorable misconduct on the part of the merchant.[33]

Given the strong trend in recent cases favoring the enforcement of clickwrap agreements in the absence of a conflict between a requirement of a term in the contract and a fundamental public policy of the forum, or evidence of misconduct so egregious that it might rise to the level of unconscionable, courts are likely to find that adware EULAs are enforceable contracts. Most recent clickwrap cases deal with consumer objections to the level of service provided by online service providers, and a consumer might try to distinguish a service contract under which a consumer gains access to e-mail and the Internet generally from an agreement under which a consumer gains access to comparison advertising presented in the form of annoying pop-up ads. However, in the absence of any evidence of serious misuse of personally identifiable information by the adware company, the distinction is unlikely to be persuasive.

One distinction between most clickwrap agreements with online service providers and adware companies is that, while consumers may rarely read and understand the terms of the online service provider's form contract before manifesting assent to it, and thus may find quite a few of the terms contained in the form surprising, they are likely to have a reasonably accurate idea of what the other party to the contract will provide. In the adware context, consumers may not have an accurate idea of what the other party will provide if the adware programs are bundled with other programs and the bundling is disclosed only in the form contract. Many consumers know they are downloading at least one program they want, but generally do not understand that their access to that program is conditioned on accepting a second program that will monitor their online conduct and transmit information about them to a third party so that relevant comparison ads can be shown to them in the future.[34] In other words, consumers are paying for access to the programs or services they want by using their personal information and displays of comparison ads as currency.

Anecdotally, many consumers apparently believe that licenses to online content or access to online services are being granted in return for nothing more than a release of liability from the consumer to the provider. Given the popularity of such business models during the dot-com bubble, it might be difficult to say that such consumer expectations are unreasonable. However, few cases considering the enforceability of clickwrap agreements consider whether consumer claims to be surprised by arbitration agreements or choice of forum clauses that make it prohibitively expensive for consumers to sue online merchants are reasonable. It seems likely, therefore, that the need to avoid frustrating reasonable consumer expectations about the online environment will lay adequate grounds to refuse enforcement of adware EULAs.

Although several courts have held that browsewrap interfaces do not establish manifestation of assent to contract terms,[35] not all that have considered the issue have so held.[36]

---

33. 218 F. Supp. 2d 1165, 1171 (N.D. Cal. 2002).
34. Ben Elgin, *Guess What -- You Asked For Those Pop-Up Ads*, BUSINESS WEEK, June 28, 2004, at 94.
35. Ticketmaster Corp. v. Tickets.com, 2000 U.S. Dist. LEXIS 12987, 18 (C.D. Cal. 2000); Specht v. Netscape, 306 F.3d 17 (2nd Cir. 2002); *In re* Northwest Airlines Privacy Litigation 2004 U.S. Dist. LEXIS 10580 (D. Minn. 2004).
36. Pollstar v. Gigmania Ltd., 170 F. Supp. 2d 974 (E.D. Cal. 2000) (refusing summary judgment dismissing contract claims); Register.com, Inc. v. Verio, Inc., 126 F.Supp 2d 238 (S.D.N.Y. 2000) (holding that contract was formed by posted terms even without click-though interface where evidence showed that defendant had actual knowledge of terms); Ticketmaster Corp. v. Tickets.com, 2003 U.S. Dist. LEXIS 6483; Copy. L. Rep. (CCH) P28,607 (2003) (reviewing a revised Ticketmaster interface and refusing Tickets.com summary judgment dismissing contract claims).

While this split in the cases hardly justifies advising a client that embedding the terms of a contract behind an obscure hyperlink may result in an enforceable contract, courts' unwillingness to uniformly reject such a suggestion as preposterous demonstrates the depth of the deference that courts show to those who develop innovative contracting interfaces with what appears to be cavalier disregard for established contract law doctrine. Closer examination of the cases reveals that all three cases holding either that browsewrap might be the basis of a contract – or at least that summary judgment against the party advancing that argument would be premature – involve business-to-business contracts, not business-to-consumer contracts. Furthermore, in all three cases the party claiming that a browsewrap interface can be used to form a contract also had strong claims that the defendant should also be held liable for unfair competition. If the cases holding that browsewrap might be enough to form a contract are in substance disguised unfair competition cases, then consumers finding fault with the ambiguity of adware EULA contract interfaces should be able to distinguish those cases. But because adware distributors appear to be happy to use click-through interfaces, this distinction is unlikely to help many consumers who object to the adware on their computers.

3. Liability under Other Forms of Online Market Regulation

Because it seems unlikely that contract law will provide much protection to consumers from unwanted adware, the possibility that other doctrines that regulate market conduct could provide a shield should be explored. However, a review of unfair competition, deceptive trade practices, electronic surveillance, and computer fraud laws provides little more hope for disgruntled consumers than contract law does.

Both federal and state unfair competition laws provide competitors a cause of action to object to improper conduct by merchants on behalf of consumers rather than providing consumers with a direct cause of action. Section 43(a) of the Lanham Act created a federal law of unfair competition; in 1988 its scope was expanded by the Trademark Law Revision Act, which codified more than two decades of case law. Section 43(a) prohibits the use in commercial advertising of any word, term, name, symbol or device or false or misleading statement of fact that misrepresents the nature, characteristics or quality of goods, services or commercial activities.[37] Section 2 of the Restatement (Third) of Unfair Competition Law provides that "one who, in connection with marketing of goods or services, makes a representation relating to the actor's own goods, services, or commercial activities that is likely to deceive or mislead prospective purchasers to the likely commercial detriment of another" may be liable to the other. As with § 43(a), the appropriate remedy in the absence of a showing of specific harm to a competitor is injunctive relief.[38] Companies whose customers are shown comparison ads by means of adware may well have an unfair competition claim against the adware company or its customer whose comparison ad is displayed, but consumers would not be able to bring suit in their own names if no competitor was willing to act.

Because spyware involves the transmission of personal information without the knowledge or consent of the person whose information is being sent, and because federal deceptive trade practices law has been the foundation of Federal Trade Commission efforts to

37. 15 U.S.C. § 1125(a)(1).
38. Restatement (Third) of Unfair Competition Law § 35.

increase the level of protection given to personal information,[39] federal deceptive trade practices law actions seem like a promising strategy to help consumers fight back against unwanted adware programs. By 2005, however, the FTC had announced only one spyware enforcement action.[40] Because many states have enacted "Little FTC Acts" with provisions similar to Section 5 of the FTC Act that are enforced by state attorneys general or that grant a private cause of action to consumers, consumers may have better luck fighting spyware with state deceptive trade practices law than with federal.

In 1968, Congress enacted the Wiretap Act to establish a framework within which police would be permitted monitor telephone communications. In 1986, Congress revised the statute to include electronic communications,[41] which is now known as the Electronic Communications Privacy Act (ECPA).[42] The second title of the ECPA also added an entirely new regulatory program, the Stored Communications Act, which covers access to certain stored communications.[43] The ECPA applies not only to government monitoring of electronic communications, but also to monitoring by private parties. The ECPA generally prohibits anyone other than the sender and intended recipient of a message from intercepting it in transit, accessing it after it has been stored, or disclosing its contents. The ECPA restricts the ability of both government agents and private parties to monitor electronic communications.

An important exception to the application of the ECPA exists where one of the parties to the communication has consented to the monitoring.[44] The scope of this exception for monitoring consented to by one of the parties to an electronic communication has recently been the subject of considerable controversy in the context of Internet commerce. If a website operator monitors the activities of visitors to its site and also posts a privacy policy explaining the scope of the personal information it collects and the uses to which it puts that information, then even though the visitor may not have expressly consented to the collection of the information, the visitor has been provided with notice. Many website operators permit third parties to post banner ads on their sites, and many of the providers of banner ads also monitor the conduct of visitors to the website hosting the ad and collect personal information about those visitors, which is later analyzed to permit more accurate targeting of advertisements. If the providers of banner ads place "cookies" on the hard drives of visitors to websites hosting the ads, the visitors may be unaware of the fact that someone other than the operator of the website is monitoring their online activity and furthermore may not know how to discover the identity of the banner ad provider or learn its privacy policies.

The Computer Fraud and Abuse Act (CFAA)[45] addresses unauthorized access and misuse of computers and computer networks. The CFAA prohibits various forms of unauthorized

---

39. Section 5 of the FTC Act provides "Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce are hereby declared unlawful." 15 U.S.C. § 45(a)(1) (2000). Since the late 1990s, the FTC has been encouraging online businesses to disclose their privacy practices and taking enforcement actions based on its deceptive trade practices authority against online businesses that fail to do what their privacy policies say. *See* FTC descriptions of all the enforcement actions it has taken against online businesses for failing to follow their posted privacy policies, *available at* http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html (last viewed Aug. 18, 2005).
40. FTC v. Seismic Entm't Prods., 2004 U.S. Dist. LEXIS 22788 (D.N.H., 2004); FTC Press Release, October 12, 2004, *available at* http://www.ftc.gov/opa/2004/10/spyware.htm (last viewed May 1, 2005).
41. Electronic Communications Privacy Act, Pub. L. No. 99-508, 100 Stat. 1848 (1986).
42. Codified at 18 U.S.C. §§ 2510-2522 (2005).
43. Codified at 18 U.S.C. §§ 2701-2711 (2005).
44. 18 USC § 2511(3)(b)
45. 18 U.S.C. § 1030.

access of "protected computers." In 1996, the definition of "protected computer" was considerably expanded: now any unauthorized interference with a computer with access to the Internet may be a federal crime.[46] The CFAA prohibits unauthorized access or exceeding authorized access to obtain information from a protected computer,[47] accessing a protected computer with intent to defraud or obtain anything of value,[48] or intentionally harming a protected computer.[49]

An in depth exploration of the application of these statutes to spyware generally is provided in "Spyware and the Limits of Surveillance" by Patricia Bellia.[50] Some recent attempts to use these statutes as the basis for class action lawsuits based on allegations of online privacy violations indicate that their application to unwanted adware in particular may not prove to be very helpful.[51]

If the consumer could claim that unwanted adware running on a computer substantially interfered with the consumer's use of that computer, then it might be possible to make out a trespass to chattels claim.[52] Once again, while there is considerable uncertainty surrounding the scope of such a claim in light of conflicting case law, the trend in recent cases has been for courts to be more skeptical of such claims and to ask computer owners to tolerate more unwanted interference with the use of computers connected to the Internet.[53]

4. Regulatory Alternatives to Contract Doctrine

Because none of the obvious alternatives to liability for breach of contract seem any more likely to give consumers an effective legal remedy against the unwanted distribution of adware, many law reform proposals have been offered. Given that "unfair competition" is the body of law that addresses overzealous competition among merchants, perhaps what is needed is a new doctrine of "unfair marketing" that protects online consumers against overzealous marketing by online merchants. A claim of unfair marketing of adware might be defended by a showing that the adware company had clearly and explicitly disclosed to the consumer what the consumer would be giving up in exchange for whatever product or service the consumer intended to accept. In fact, that was more or less the approach taken in Congress in 2005 when H.R. 29, the Securely Protect Yourself Against Cyber Trespass Act, or "Spy Act," was introduced.[54]

---

46. 18 U.S.C. § 1030(e)(2).
47. 18 U.S.C. § 1030(a)(2).
48. 18 U.S.C. § 1030(a)(4).
49. 18 U.S.C. § 1030(a)(5).
50 20 Berkeley Tech. L.J. 1283 (2005).
51. *In re* Doubleclick Privacy Litig., 154 F. Supp. 2d 497, 519-20 (S.D.N.Y. 2001); *In re* Intuit Privacy Litig., 138 F. Supp. 2d 1272, 1279-81 (C.D. Cal. 2001).
52. Trespass to chattels is defined as the unauthorized, intentional, and substantial use of or intermeddling with another's tangible personal property. RESTATEMENT (SECOND) OF TORTS §§ 217–218 (1965).
53. Trespass was found in Thrifty-Tel, Inc. v. Bezenek, 46 Cal. App. 4th 1559 (1996); CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015 (S.D. Ohio 1997); eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058 (N.D. Cal. 2000); Register.com, Inc. v. Verio, Inc., 126 F.Supp 2d 238 (S.D.N.Y. 2000); EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58 (1st Cir. 2003). No trespass was found in Ticketmaster Corp. v. Tickets.com, 2003 U.S. Dist. LEXIS 6483; Copy. L. Rep. (CCH) P28,607 (2003); Intel Corp. v. Hamidi, 30 Cal. 4th 1342 (2003); Southwest Airlines Co. v. FareChase, Inc., 318 F. Supp. 2d 435 (N.D. Tex. 2004); Nautical Solutions Mktg. v. Boats.com, 2004 U.S. Dist. LEXIS 6304 (M.D. Fla. 2004).
54. The 109th Congress Spy Act is similar to the 108th Spy Act that passed overwhelmingly in the House but stalled in the Senate.

The Spy Act's "notice and consent" approach[55] to dealing with unwanted adware appears to be drawn more from tort law than from contract law, which is consistent with an unfair competition approach. As a narrowly targeted response to the problem of unwanted adware, the Spy Act may well have a material impact on the business models and software designs of legitimate adware distributors.[56] If the Spy Act is characterized as a narrowly targeted reform of contract law, however, its likely impact will be much less positive. U.S. information privacy law is now in shambles after decades of narrowly focused, piecemeal legislation; the notice and consent approach taken in various information privacy statutes has achieved only modest success.[57] Perhaps narrowly focused, piecemeal legislation to reform contract law is better than nothing it if can help stem the rising tide of spyware being loaded on consumers, but it is no substitute for a more general reappraisal of the current state of contract law as it applies to online transactions.

In contrast, the EU Directive on Unfair Contract Terms was promulgated in 1993 and provides a very successful example of a reorientation of contract law following such a general reappraisal.[58] Member States were expected to pass laws implementing its provisions by the end of 1994. The Directive provides that contract terms not individually negotiated will be deemed unfair if they create a significant imbalance, to the consumer's detriment, between the rights and obligations of the contracting parties.[59] If a contract term is drafted in advance and the consumer has no influence over the substance of the term, then it is always considered not to be individually negotiated, and hence subject to review based on substantive fairness.[60] An annex to the directive contains an expansive list of terms that may be deemed unfair.[61] The nature of

---

55. Spy Act section 3 provides that it is unlawful to transmit an adware program to a computer or execute adware software on a computer unless the consumer is provided with a clear, explicit notice that personal information will be collected and provided an opportunity to consent to that function; the end user can easily identify the adware program and remove it, and when advertisements are displayed, the adware company is identified as the source of the ad.

56. By contrast, distributors of nefarious or fraudulent spyware are unlikely to be any more deterred by the Spy Act than distributors of fraudulent spam e-mails have been deterred by the CAN SPAM Act.

57. *See* Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 826-28 (2000) (discussing the shortcomings of the informed consent model of information privacy protection).

58. Council Directive 93/13 EEC, *supra* note 8; *see generally*, James R. Maxeiner, *Standard-Terms Contracting in the Global Electronic Age: European Alternatives*, 28 YALE J. INT'L L. 109 (2003).

59. Council Directive 93/13 EEC, *supra* note 8 at art. 3.

60. *Id*. at art. 2.

61. The terms listed in the annex include:

> (a) excluding or limiting the legal liability of a seller or supplier in the event of the death of a consumer or personal injury to the latter resulting from an act or omission of that seller or supplier;
>
> (b) inappropriately excluding or limiting the legal rights of the consumer vis-à-vis the seller or supplier or another party in the event of total or partial non-performance or inadequate performance by the seller or supplier of any of the contractual obligations, including the option of offsetting a debt owed to the seller or supplier against any claim which the consumer may have against him;
>
> (c) making an agreement binding on the consumer whereas provision of services by the seller or supplier is subject to a condition whose realization depends on his own will alone;
>
> (d) permitting the seller or supplier to retain sums paid by the consumer where the latter decides not to conclude or perform the contract, without providing for the consumer to receive compensation of an equivalent amount from the seller or supplier where the latter is the party cancelling the contract;

the goods or services covered by the contract, the circumstances surrounding the drawing up of the contract, and the other terms in the contract or in another contract to which it relates will be taken into account in assessing the unfairness of a term.[62] Contract terms offered to consumers in writing must always be drafted in plain language and where there is doubt as to the meaning of a term, the interpretation most favorable to the consumer will prevail.[63] In the event that terms in a consumer contract are found to be unfair, those terms will not be binding on consumers, although the remainder of the contract will be enforceable.[64]

Adware clickwrap agreements would likely be unenforceable under the law of EU member states on the grounds that consumers are normally required to agree to the contract terms before having any real opportunity to become acquainted with them. However, the list of unfair terms in the Annex to the Directive are merely suggestive and not in any way limiting. As a result, a court in an EU member state might find that contract terms are unfair and thus

---

(e) requiring any consumer who fails to fulfil his obligation to pay a disproportionately high sum in compensation;
(f) authorizing the seller or supplier to dissolve the contract on a discretionary basis where the same facility is not granted to the consumer, or permitting the seller or supplier to retain the sums paid for services not yet supplied by him where it is the seller or supplier himself who dissolves the contract;
(g) enabling the seller or supplier to terminate a contract of indeterminate duration without reasonable notice except where there are serious grounds for doing so;
(h) automatically extending a contract of fixed duration where the consumer does not indicate otherwise, when the deadline fixed for the consumer to express this desire not to extend the contract is unreasonably early;
(i) irrevocably binding the consumer to terms with which he had no real opportunity of becoming acquainted before the conclusion of the contract;
(j) enabling the seller or supplier to alter the terms of the contract unilaterally without a valid reason which is specified in the contract;
(k) enabling the seller or supplier to alter unilaterally without a valid reason any characteristics of the product or service to be provided;
(l) providing for the price of goods to be determined at the time of delivery or allowing a seller of goods or supplier of services to increase their price without in both cases giving the consumer the corresponding right to cancel the contract if the final price is too high in relation to the price agreed when the contract was concluded;
(m) giving the seller or supplier the right to determine whether the goods or services supplied are in conformity with the contract, or giving him the exclusive right to interpret any term of the contract;
(n) limiting the seller's or supplier's obligation to respect commitments undertaken by his agents or making his commitments subject to compliance with a particular formality;
(o) obliging the consumer to fulfill all his obligations where the seller or supplier does not perform his;
(p) giving the seller or supplier the possibility of transferring his rights and obligations under the contract, where this may serve to reduce the guarantees for the consumer, without the latter's agreement;
(q) excluding or hindering the consumer's right to take legal action or exercise any other legal remedy, particularly by requiring the consumer to take disputes exclusively to arbitration not covered by legal provisions, unduly restricting the evidence available to him or imposing on him a burden of proof which, according to the applicable law, should lie with another party to the contract.

Unfair Contract Terms Directive Annex.

62. Council Directive 93/13 EEC, *supra* note 8 at art. 4.
63. *Id*. at art. 5.
64. *Id*. at art. 6.

unenforceable if they purport to permit a software distributor to load several software programs at once without clearly disclosing that more than one program is being loaded, or to load an adware program on a computer without clearly explaining its functions.

The Unfair Contract Terms Directive takes the opposite approach of current U.S. contract law: instead of a presumption of deference to whatever novel contract interface the merchant has developed, the Directive substitutes a presumption that the merchant will be bound to a contract based on the reasonable expectations of the consumer. Under such a standard for contract formation, it would be easy to predict that objectionable adware products would not be protected by click-through contract interfaces. Furthermore, even adware distributors that clearly and explicitly disclosed their business models – which is all that proposed U.S. legislation such as the Spy Act would require – might find that some elements of those business models would not be permitted notwithstanding the full disclosure if the behavior that the contract purports to authorize is not actually fair to consumers.

5. Conclusion

Adware distributors believe that consumers want the comparison advertisements they provide. Many others believe that such programs are simply another form of spyware, and that consumers would not accept such programs on their computers if adware distributors were required to disclose the purpose and functions of the software clearly and explicitly. If existing contract law doctrine regarding the formation of contracts were applied rigorously and consistently, then contract law might provide an effective mechanism for determining which description of reality is more accurate. However, whatever rigor and vitality applicable contract law doctrine might have possessed has already been dissipated by courts trying to accommodate a wide range of innovation in contracting systems. As a result, courts reviewing the contracting interfaces used by adware distributors in light of current law are unlikely to demand that they make clear and explicit disclosures before claiming that consumers have consented to running their software.

Law reform efforts aimed at filling this apparent gap in contract doctrine appear narrowly targeted at problems associated with a particular technology – spyware – and so are unlikely to have any impact on the balance of power between merchant and consumer under contract law doctrine generally. This piecemeal, sectoral approach to the reform of contract law is reminiscent of the U.S. approach to information privacy law, which has proved to be a dismal failure. One alternative to a narrowly targeted, ad hoc approach to controversies in contract law triggered by specific technological innovations would be to address the balance of power between merchant and consumer more generally, following the approach taken in the EU Unfair Contract Terms Directive. However, the pronounced U.S. proclivity for market-oriented rather than regulatory approaches to new commercial practices makes it very unlikely that such an approach would be tried in the U.S.