

Too Many Open Windows? Exploring the Privacy Implications of Pop-Up Ads

Emily Woodward Deutsch*

IT IS ALL BUT IMPOSSIBLE these days to traverse the World Wide Web without encountering a smorgasbord of online advertisements. One form of internet advertising that has attracted particular notoriety and spawned considerable controversy is the pop-up. Typically resembling a small electronic billboard containing a link to an advertiser's corporate web site, a pop-up ad may be affiliated with the web page. Conversely, the pop-up may have no relationship with the web page, other than appearing at the same time that a user accesses the page. This second category of pop-ups is enabled by software that a user downloads on his computer, often in exchange for other software that the user wants for his personal use. Once downloaded, this software, known as "adware" or, more derisively, "spyware," interacts with the user's internet browser and triggers a pop-up to appear in response to existing data on the browser or key terms that the user enters. Pop-up ads, and the opposition they engender, raise new doubts about the sanctity of privacy in the internet age. This paper seeks to address whether these controversial ad placement practices constitute protected speech under the United States' First Amendment or whether they unlawfully invade the privacy of individual internet users who frequent popular web sites. Underlying the concerns surrounding pop-ups is the broader public policy issue of how the internet threatens the privacy of individuals and corporate entities by calling into question customary, "real-world" conceptions of what constitutes private or privileged space. As this paper purports to show, it is all too easy for constitutional violations to occur if real-world notions of privacy are trampled online in the private sector.

IL EST DE NOS JOURS à vrai dire impossible de traverser le World Wide Web sans se heurter à tout un assortiment de publicités en ligne. Une forme de publicité sur Internet particulièrement bien connue, qui soulève une grande controverse, est la fenêtre en incrustation. Cette fenêtre, qui typiquement ressemble à un petit tableau d'affichage électronique, comporte un lien vers le site Web de l'entreprise qui fait la publicité. La fenêtre en incrustation peut être associée ou non à une page Web. Si elle ne l'est pas, la fenêtre apparaît simplement au moment où l'utilisateur a accès à une page. Cette seconde catégorie de fenêtre en incrustation est activée par un logiciel que l'utilisateur télécharge sur son ordinateur, souvent en échange d'un autre logiciel qu'il ou elle veut utiliser personnellement. Une fois téléchargé, ce logiciel, appelé « logiciel de publicité » ou de façon dérisoire « logiciel espion », interagit avec le navigateur Internet de l'utilisateur et fait apparaître les fenêtres en incrustation en réponse à des données existantes du navigateur ou à des mots clés entrés par l'utilisateur. Les fenêtres en incrustation, et l'opposition qu'elles soulèvent, créent des doutes quant au caractère sacré de la vie privée à l'ère de l'Internet. Cet article cherche à explorer si ces pratiques de publicité controversées constituent une forme de discours protégé par le premier amendement de la Constitution des États-Unis ou elles constituent une atteinte illégale à la vie privée des utilisateurs d'Internet individuels qui consultent les sites Web populaires. Derrière ces préoccupations concernant les fenêtres en incrustation se pose la question plus large de la politique publique relativement à la menace à la vie privée des individus et des personnes morales créée par l'Internet. Cela nous invite à remettre en question les notions coutumières du « monde réel » de ce qui constitue l'espace privé ou privilégié. Comme cet article tente de le démontrer, il est trop facile de conclure à des atteintes au droit constitutionnel si les notions de vie privée du monde réel sont bafouées en ligne dans le secteur privé.

399	1. INTRODUCTION
402	2. EVOLUTION OF ONLINE ADS
402	2.1. <i>Banners and Sponsors Make Way for Classifieds, Search and Email</i>
403	2.2. <i>New Ad Forms Breed Increased Egalitarianism in Internet Marketplace</i>
404	2.3. <i>Peculiar, Unpopular, but Popping Up All Over the Web</i>
407	3. FREEDOM OF THE PRESS...AND THE POP-UP?
407	3.1. <i>Online Commercial Speech Deserving of New Protection</i>
409	3.2. <i>'Here's the Catch': Protection Not Absolute</i>
412	4. PRIVACY GUARANTEED?
412	4.1. <i>Constitutional Safeguards</i>
412	4.2. <i>Privacy in the Private Sector</i>
413	5. AN EMERGING MARKET: USER PRIVACY LAWSUITS
413	5.1. <i>Real Property and Unauthorized Access Claims</i>
414	5.2. <i>Intellectual Property Claims</i>
415	6. A HARD SELL: DEFENDING CORPORATE PRIVACY INTERESTS
416	6.1. <i>The "Cons" Have Their Day: News Sites Sink Teeth Into Claria's Commercial Speech Claims</i>
420	6.2. <i>The "Pro" Side Bites Back: WhenU Wins Legal Battle Against Corporate Foe</i>
421	7. BEYOND THE COURTROOM: ALTERNATIVE TREATMENTS FOR THE PAIN OF POP-UPS
421	7.1. <i>"There Ought to Be a Law..."</i>
422	7.2. <i>Going High-Tech</i>
424	8. CONCLUSION

Too Many Open Windows?

Exploring the Privacy Implications of Pop-Up Ads

Emily Woodward Deutsch

1. INTRODUCTION

THE INTERNET, IN ITS EVOLUTION from Cold War innovation¹ to worldwide information network,² has forever changed the way goods and services are exchanged. It has opened up a new electronic marketplace, freed from the constraints of the physical world, in which merchants of all sizes and profit margins are able to advertise across a myriad of electronic data networks. These new avenues of information have spurred tremendous commercial growth, but they also have tested the traditional protections for commercial speech³ against countervailing rights of privacy.

Fueled by a growing and increasingly diverse cache of users, the internet has demonstrated its potential to serve as an equalizing force for retailers, from mom-and-pops stores to Fortune 500's.⁴ Electronic commerce tools have enabled small-scale, provincial enterprises to penetrate their local markets as never before, while connecting to national and global markets that were previously the sole domains of major corporations. For example, by placing an ad on *Newsday.com*,⁵ a consignment store owner on New York's Long Island is

-
1. See Daniel Brenner, Monroe E. Price & Michael Meyerson, "Internet and Cable" in *Cable Television* (2001) at p. 18.01[1] (detailing the evolution of the internet from ARPANET, a computer network developed in the late 1960s and funded by the US Department of Defense's Advanced Research Projects Administration, which was designed to support the central command and control structure for the US armed forces during the Cold War).
 2. See Kevin Werbach, "Digital Tornado: The Internet and Telecommunications Policy" OPP Working Paper Series (1997), <http://www.fcc.gov/Bureaus/OPP/working_papers/oppwp29.pdf> at p. 10.
 3. Commercial speech has been defined as "speech about who is selling what, at what price, and for what reason." The most common form of commercial speech is advertising. David H. Remes, "Commercial Speech: Past Present and Future" in Elizabeth A. McNamara, Anke E. Steinecke & Matthew A. Leish, eds., *Internet Publishing* (2000) at pp. 169-170.
 4. The title "Fortune 500s" refers to the top 500 companies ranked each year by *Fortune*, <<http://www.fortune.com/fortune/fortune500>>.
 5. Web site of New York daily newspaper, *Newsday*, serving communities of Queens, Nassau and Suffolk Counties, <<http://www.newsday.com/>>.

able to reach potential new customers in the region who prefer to get their local news online. At the same time, he or she can access customers in Northern Virginia, Southern California and South Korea, who may have never seen *Newsday* in print, but who stumbled upon the website through one of many internet search engines. In this way, the internet has taken the provincial merchant's window on the world and expanded it to a level that puts him or her on par with retailers hundreds of times their size.

In other advertising ventures, however, the internet has proven less effective in closing the logistical and financial gaps that have long put large businesses at an advantage over smaller ones. As in the physical world, major corporations have continued to attract a more expansive and diverse consumer base online than their lesser-known competitors. These large commercial entities have sustained their real world market edge in cyberspace by dominating the advertising spots that appear on a handful of websites, which generate the lion's share of all online ad revenue.⁶

The disparity within online advertising has inspired some entrepreneurial internet advertisers to develop strategies aimed at companies that either have been shut out of major news and e-commerce sites or have failed to fully penetrate this market. These advertisers have made their niche providing ads that are viewable to users when they click on pages of major websites. Though not connected to the sites themselves, such ads are tailored to fit the underlying content. For example, an advertiser may display an ad for the University of Phoenix online⁷ in the browser of an internet user who has clicked on the Education section of *Washingtonpost.com*.⁸ The ad appears in a separate window from the section-related material. Nevertheless, the user may assume that the ad is a component of the site, given that one appears simultaneously with the other and contains similar content. This arguably deceptive method of advertising is appealing to companies that want their ads to appear affiliated with the major web sites, and thus take advantage of those sites' name recognition and credibility.

Alternatively, an advertiser may adopt the more brazen scheme of displaying ads for no-name companies in windows that overlap with the websites of their big name competitors. For example, an ad for an obscure rent-a-truck outfit may open in a user's browser window when he accesses the U-Haul, Inc.⁹ website. In this instance, the user is unlikely to confuse the two companies. However, he or she still might opt to give their business to the lesser-known one, particularly if it charges considerably less than U-Haul for what appears, in its ad, to be the same services.

-
6. Six web sites—MSN, AOL, Yahoo!, Overture, Lycos and CNET—have made up more than half the online ad market during the period from January 2000 to June 2003. eMarketer, *Advertising Spending* (July 2003), <<http://www.emarketer.com>> [*Advertising Spending*].
 7. New York-based advertiser WhenU.com Inc. regularly displays ads for the University of Phoenix online, a web-based university, <<http://www.phoenix.edu>>, on users' screens when they click on *Washingtonpost.com* and other web sites.
 8. Web site of *The Washington Post*, <<http://www.washingtonpost.com>>.
 9. U-Haul Inc., <<http://www.uhaul.com>>, sued WhenU.com for targeting ads for rival moving companies to appear on users' computer screens when they clicked on the U-Haul web site.

Not surprisingly, these sorts of ad placement practices are seen as trespassing by major website owners, as well as by the companies that pay top dollar to post advertisements on their sites. Likewise, many internet users rue the extra layers of ads as intrusions on the content they wish to access. Technology experts, moreover, warn that the software triggering the ads—a form of spyware¹⁰ called adware¹¹—has the potential to undermine the privacy safeguards that many major website owners guarantee their consumers and advertising clients.

This paper focuses on the privacy and privacy-related concerns raised by the particular ad form, known as the pop-up,¹² which has become the primary vehicle for unauthorized advertising on the internet. Part 2 traces the rise of the pop-up as an affordable and user-friendly alternative to the various other ad forms that populate the online marketplace. Part 3 examines the degree to which pop-ups and other online ads are protected under the US Constitution as commercial speech. Notwithstanding such protections, part 4 considers whether pop-ups may be unlawful on privacy grounds. Part 5 investigates the privacy implications of pop-ups from the perspective of the individual internet users who frequent highly trafficked web sites. Part 6 looks at how these ads may violate the rights of the companies that own and manage these websites, paying close attention to the recent litigation brought against two of the most prolific suppliers of unauthorized pop-up displays, Claria Corporation¹³ and WhenU.com, Inc.¹⁴ Part 7 investigates methods outside the court system for restricting pop-ups, and discusses the long-term ramifications these strategies may have on civil liberties in cyberspace. The paper concludes with an assessment of public attitudes regarding the risks posed by pop-ups against the ads' perceived value as catalysts of competition and growth.

-
10. "Any software that covertly gathers user information through the user's internet connection without his or her knowledge, usually for advertising purposes." *Webopedia*, s.v. "spyware." <<http://www.webopedia.com/TERM/s/spyware.html>>.
 11. *Ibid.*, s.v. "adware," <<http://www.webopedia.com/TERM/A/adware.html>>. Adware is software which enables pop-up ads, and has been used interchangeably with "spyware." However, companies that hold themselves out as solicitors of adware have been adamant that internet users elect to use their software, in contrast to spyware, which, they argue, consumers don't ask for and which runs on applications that consumers don't know they have. See Karl Bode, "Don't Call Gator 'Spyware' or They'll See You in Court" *Broadband Reports* (22 October 2002), <<http://www.dslreports.com/shownews/34679>>.
 12. "A type of window that appears on top of (over) the browser window of a Web site that a user has visited. In contrast to a pop-under ad, which appears behind (in back of) the browser window, a pop-up is more obtrusive as it covers other windows, particularly the window that the user is trying to read. Pop-up ads are used extensively in advertising on the Web, though advertising is not the only application for pop-up windows." *Webopedia*, s.v. "pop-up ad," <http://www.webopedia.com/TERM/P/popup_ad.html>. While this paper focuses on the privacy implications surrounding pop-up ads, the same arguments may be applied to pop-upners.
 13. Founded in 1998, Claria Corporation is an online marketing firm based in Redwood City, California. It was known as Gator Corporation until October 2003, <<http://www.claria.com>>.
 14. Founded in 2000, WhenU Inc. is an online marketing firm, and competitor of Gator, based in New York, NY, <<http://whenu.com>>.

*

2. EVOLUTION OF ONLINE ADS

2.1. Banners and Sponsors Make Way for Classifieds, Search and Email

AT THE HEIGHT OF THE E-COMMERCE boom, banner ads¹⁵ and paid sponsorships¹⁶ were the dominant vehicles of online advertising, accounting for 46.8 percent and 28.5 percent, respectively, of all online ad revenue.¹⁷ Displayed on the pages of major news and corporate web sites, these ad spots offered companies high rates of user traffic per ad. For example, in March 2002, banners displayed on the web pages of NYTimes.com achieved more than 193 million page views, banners on Washingtonpost.com received more than 99 million page views, and banners on USATODAY.com received more than 98 million page views.¹⁸ Because the prices of these ads were also high—and remain so today, with Washingtonpost.com, for example, charging between US\$5,000 and US\$50,000 per banner per month¹⁹—their popularity was concentrated among the top cross-media advertisers: large companies that advertise in more than one forum, such as print and online or online and television, and can afford to pay higher rates per ad than their competitors.²⁰

Not surprisingly, given their costliness, banners and sponsorships were hit hard by the dot-com bust of recent years, when even the largest companies scaled back their online advertising. In the last few years, they have seen their shares of the online ad market drop by 17.4 percent and 10.2 percent, respectively,²¹ amid growth in other online ad sectors, particularly online classifieds,²² paid search engines,²³ and email advertisements.²⁴

15. This term refers to static or hyperlinked ads, which companies pay web site owners to display on their sites. See "Definitions of Online Advertising Vehicles that PricewaterhouseCoopers Supplies to U.S. Publisher Web Sites that Report Data" in eMarketer, *Online Advertising Tactics: Trends, Stats and Best Practices for Using Banners, Rich Media, Search, Sponsorships, E-mail, Classifieds and More* (16 July 2003), <<http://www.emarketer.com>> [*Online Advertising Tactics*].
16. Online ad vehicle in which a company pays to sponsor all or part of a web site in exchange for right to post targeted ads in certain areas of the site.
17. See *supra* note 6 at p. 22 and p. 142.
18. Memorandum in Support of Plaintiffs' Motion for Preliminary Injunction at p. 5, *Washingtonpost.Newsweek Interactive Co. LLC v. Gator Corp.*, CV 02-909-A (ED Va 2002), injunction granted by *Washingtonpost.Newsweek Interactive Co., LLC v. Gator Corp.*, 2002 U.S. Dist. LEXIS 20879 (ED Va 2002) [*Washingtonpost.Newsweek Interactive*].
19. See Washingtonpost.com's *Online Media Kit*, <<http://www.washingtonpost.com/wp-adv/mediakit/adinfo/display/front.htm>>.
20. The larger companies that have traditionally dominated advertising seem to take more to traditional banner formats, according to Nielsen//NetRatings' study of the top 100 cross-media advertisers, with 29% of impressions coming from that format among the top 100 cross-media advertisers. See *Online Advertising Tactics*, *supra* note 15 at p. 28.
21. See *ibid.* at p. 22, p. 142.
22. Online ad vehicle similar to print Yellow Pages directory, in which advertisers pay web site owners fees to list specific products or services. See *ibid.*
23. *Ibid.* Interactive online ad model in which users enter words or phrases to view listings for online companies. Advertisers pay web sites supporting search engine, such as Yahoo! or Google, to list and/or link their company site domain names to specific search terms.
24. *Ibid.* Banner ads, links or advertiser sponsorships that appear in email.

Compared to banners and sponsorships, these up-and-coming ad forms are not featured as prominently on heavily trafficked sites—and, thus, do not benefit from the same levels of click-throughs per ad.²⁵ Nevertheless, they have achieved profitability in light of their relative inexpensiveness. This quality has made them less susceptible to spending downturns than other online ad forms.²⁶ Moreover, it has enabled them to attract a higher volume of advertisers and thereby take advantage of the growing numbers of advertisers and consumers equipped to do business online.²⁷

2.2. New Ad Forms Breed Increased Egalitarianism in Internet Marketplace

The smaller-scale ad models have proven particularly attractive to small businesses, a “huge market that otherwise wouldn’t even play the online advertising game.”²⁸ These mom-and-pop drycleaners, hardware stores, and plumbing contractors, to offer just a few examples, could never afford to put up thousands of dollars for a single banner ad or web site sponsorship, but are able to advertise in the online classifieds, at an average cost of US\$1.18 per action.²⁹ Even more affordable are email and paid search, costing, on average, just US\$0.50 per action and US\$0.29 per action, respectively.³⁰

By attracting a wider cross-section of advertisers, classifieds, paid search engines and email ad forms have obtained an advantage over their competitors in generating appeal among a wide spectrum of consumers. For example, only 13 percent of internet users claim to be annoyed by email subscription-based advertising, compared with 53 percent who are annoyed by banner ads.³¹ Unlike the banner ad, which promotes one brand of a particular product that may appeal to some consumers but not others, these less costly ad vehicles typically attract multiple advertisers that produce the same good or offer the same service. They offer consumers the opportunity to evaluate different brands of the same goods and services to determine which ones best suit their diverse needs

-
25. The click-through rate (CTR) is the average number of click-throughs an online ad receives per hundred user impressions, expressed as a percentage. It remains the most common metric for online ad effectiveness. More than 94 percent of US ad executives still use CTR's to plan or measure online advertising. See “How Online Advertising and Marketing Sway Sales” in eMarketer, *Online Advertising Essentials: What Marketers Need to Know about Online Audiences, Dayparts, Branding, Direct Response, Context, Advertisers and Publishers* (June 2003), <<http://www.emarketer.com>> at p. 113.
 26. Since total online advertising spending peaked in 2000, revenue for online classified ads has grown from 7.4 percent to 15 percent of all online ad revenue. For paid search engines, the increase has been from 1.3 percent to 15.4 percent, and for email advertising, from 2.7 percent to 4 percent. *Supra* note 6 at p. 64, p. 66, p. 69.
 27. Projections from the online market analyst firm eMarketer say the total number of internet users in the United States will increase from 162 million in 2003 to 171.4 million by 2005, but online ad spending per internet user will drop from US\$41.23 to around US\$40.00, pointing to an increase in the number of online commercial transactions and a decrease in the cost per transaction in that period. *Ibid.* at p. 172, p. 180.
 28. Tom Hespos, *MediaPost*, quoted in “Ad Tactics: What Are the Online Ad Vehicles?”, *Online Advertising Tactics*, *supra* note 15.
 29. Online ad metric based on user taking some specifically defined action in response to an ad, such as registering on the advertiser's web site. *Advertising Spending*, *supra* note 6 at p. 78.
 30. *Ibid.*

and interests. This practice, known as comparative shopping,³² has long been standard operating procedure in the real world marketplace, with supermarkets and mass-merchandise retailers offering consumers a vast array of selections from daily staples, such as coffee and cold medications, to big-ticket items, such as computers and home entertainment systems. In the print advertising sector, comparative shopping methods have influenced the layout of newspaper classifieds and yellow page directories, in which competing products and services are listed together for consumers to research and evaluate. On the internet, these methods operate in much the same way that they do in print, but are more closely tailored to users' tastes and preferences. For example, using the search capabilities of online classifieds, a consumer can pick the area and price range of a product he or she is interested in buying, instead of "churning laboriously through page after page of fine print"³³ in the yellow pages. Search engines, likewise, enable a consumer to "indicate an interest in a specific area"³⁴ by entering key words, and then view ads for products in that area. Finally, targeted marketing emails, which a user must give his permission to receive,³⁵ provide the consumer with ads targeted to the preferences he or she stated when that user opted to receive the email.

2.3 Peculiar, Unpopular, but Popping Up All Over the Web

The pop-up is fundamentally different from other online ad forms, and its distinctiveness has made it both a hotbed of controversy and a hot marketing tool. Unlike other ads, which are hosted by the sites on which they appear, a pop-up is controlled by a remote advertiser³⁶ and appears in its own unique window on an internet user's screen. The pop-up, which typically resembles a small electronic billboard containing an embedded link to an advertiser's corporate web site, appears in a window that overlaps with the content on a web page that a user is trying to access.

The pop-up may be associated with the web page it overlaps—indeed, many news and corporate sites function as advertisers for pop-ups appearing on pages of their sites—or it may have no relationship with the page, other than appearing at the same time on the user's screen. This second category of pop-ups is enabled by adware,³⁷ which a user downloads on their computer, often in exchange for other software that the user wants for his personal use. Video and

31. *Online Advertising Tactics*, *supra* note 15 at p. 158.

32. See Declaration of John A. Deighton, In Support of WhenU.com Inc.'s Opposition to Plaintiffs' Motion for Preliminary Injunctive Relief at p. 8, *1-800-Contacts, Inc. v. WhenU.com Inc.*, CV 02-8043 (SD NY 2003).

33. *Advertising Spending*, *supra* note 6 at p. 66.

34. *Ibid.* at p. 64.

35. Targeted emailed marketing is a separate online ad form from unsolicited mass email, or spam. See *Online Advertising Tactics*, *supra* note 15 at p. 195.

36. This term refers to a program or a type server that manages and maintains ad banners for a web site or collection of web sites. See NetLingo.com, s.v. "ad server software," <<http://www.netlingo.com/lookup.cfm?term=ad%20server%20software>>.

37. *Supra* note 11.

audio file-sharing programs³⁸ are two examples of popular software that users commonly download from the internet that have been known to be bundled with adware. Once downloaded, adware interacts with the user's computer and triggers pop-ups to appear in response to disparate types of commercial data, which the user encounters while surfing the Web.

Frequently, the data that trigger adware are other online ads; for example, a banner for U-Haul may activate a pop-up for a rival moving company.³⁹ Alternatively, the adware may trigger pop-ups corresponding to key words in an article that the user has downloaded, as in the example of the Washingtonpost.com Education article cited in the introduction of this paper.

Regardless of whether it is triggered by adware or is part of the JavaScript⁴⁰ code of a particular web site, a pop-up can be highly annoying to the user, especially if he is not aware of having done anything to trigger the ad that is obscuring his view of a web page. In many instances, online users are left to "wonder what [they] have done to warrant the punishment of seizure of [their] computer screens by pop-up advertisements for secret web cameras, insurance, travel values, and fad diets, to name a few of the more popular pop-up ads."⁴¹

Critics of adware warn that the software poses an even greater threat to privacy than the majority of users realize. In addition to triggering intrusive pop-up ads, "adware applications have been known to secretly snoop around areas of [a user's] computer they don't belong, including [the user's] browser history."⁴²

Pop-up advertisers Claria and WhenU carry assurances on their web sites that users' personal information is neither collected without their express consent nor used for purposes other than responding to users' concerns and routine troubleshooting.⁴³ Such assurances are misleading, say adware critics. They warn that, in fact, the software that a user downloads from these companies

38. *Supra* note 18. See Declaration of Benjamin G. Edelman, where he testified that "Gator Corp. bundles a software program that it calls 'OfferCompanion' together with its Gator digital wallet software program, so that persons who download the Gator application onto their personal computers automatically have OfferCompanion downloaded and installed onto their personal computers. In addition, when a person downloads certain popular free software programs, such as Kazaa or AudioGalaxy, OfferCompanion is automatically downloaded and installed onto their personal computer. Because OfferCompanion is bundled with other software programs and downloaded automatically with those other software programs, even sophisticated computer users frequently do not know that OfferCompanion has been installed on their personal computers." *Ibid.*

39. *Supra* note 9.

40. JavaScript is a programming language used to insert interstitial moving text and images within the static content of web sites. See *Internet Marketing Reference*, s.v. "java script," <<http://www.marketingterms.com/dictionary/javascript/>>.

41. Jason A. Cody, "Just WhenU Thought It was All Over, Gator's Kin Pops Up and Slides Out of Dangerous IP Waters (for the Most Part): A Review of 2 Online Pop-Up Advertisers and 4 Internet Law Decisions" (2004) 7 *PGH Journal Technology Law & Policy* 3, <http://www.pitt.edu/~sorc/techjournal/articles/Vol7_Cody.pdf>.

42. "The Trouble with Spyware & Advertising - Supported Software" *Counter Exploitation* (2004), <<http://cexx.org/problem.htm>> ["Trouble with Spyware"].

43. See Claria Web Site Privacy Statement & Terms of Use, <<http://www.claria.com/help/privacy/>> and WhenU Consumer Privacy Policy, <<http://www.whenu.com/about.html>>.

exists as an *independent, executable program on [the user's] system*, and has the capability to do anything any program can do, including monitor keystrokes, arbitrarily scan files on [user's] hard drive, snoop other applications such as word-processors and chat programs, read [the user's] cookies, change [user's] default homepage, interface with [user's] default Web browser to determine what Web sites [user is] visiting, and monitor various aspect of [the user's] behavior.⁴⁴

Moreover, "[a]ll the information obtained by the spyware can be used by the spyware author for marketing purposes, or sold to other companies for a profit."⁴⁵

While the risks posed by adware driven pop-ups may not be fully understood by most internet users, the ads still have managed to generate an enormous amount of negative feedback. According to an April 2003 study released by the internet marketing group PlanetFeedback, 83 percent of users find pop-ups annoying, an even more unfavorable rating than the 77 percent of users who are annoyed by spam.⁴⁶

Given their unpopularity, it may seem counterintuitive that the market for pop-ups is increasing at a rate of nearly 100 percent, according to Nielsen/NetRatings.⁴⁷ Even more surprisingly, the cost of an individual pop-up, which averages between US\$15 and US\$35 per thousand impressions, registers at more than twice that of a banner ad, which averages between US\$3 and US\$7 per thousand impressions.⁴⁸

One explanation for why pop-ups have remained in demand, despite their annoying attributes, is that their average click-through rate—the traditional and still most widely used metric for measuring ad effectiveness on the internet—far surpasses those of other ad forms.⁴⁹ As the vice president of ad sales for NYTimes.com concedes, "our advertisers are still finding great value to the [pop-ups] and obviously some of our users find them attractive enough to click on them."⁵⁰

For companies that can ill afford to operate their own high profile web sites, or pay to advertise on NYTimes.com and its ilk, the pop-up represents an even more valuable marketing tool. It provides such companies the opportunity to display ads in the context of an almost limitless array of web pages, thus enabling them to take advantage of a user's predisposition toward certain content.

44. "Trouble with Spyware," *supra* note 42 [underlining added by author].

45. *Ibid.*

46. "Internet Advertising Not Well Trusted," *Marketing Vox* (23 April 2003), <http://www.marketingvox.com/archives/2003/04/24/internet_advertising_not_well_trusted/>.

47. *Online Advertising Tactics*, *supra* note 15 at p. 131.

48. *Ibid.*

49. *Ibid.* at p. 135.

50. *Ibid.*

★

3. FREEDOM OF THE PRESS...AND THE POP-UP?

3.1. Online Commercial Speech Deserving of New Protection

THE EMERGENCE OF POP-UPS and other online ad forms, which serve the interests of large numbers of advertisers and consumers, suggests that internet advertising is worthy of the First Amendment⁵¹ protection that governs commercial speech in print.

The grounds for First Amendment-protected commercial speech were set forth in *Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council, Inc.*,⁵² a 1976 United States Supreme Court case. Justice Blackmun, writing for the Court, held that licensed pharmacists were entitled to advertise the price of prescription drugs, regardless of the risk of ensuing price competition.⁵³ Such advertising, the Court emphasized, constituted protected speech because it facilitated an exchange of “truthful speech proposing lawful transactions” between advertisers and consumers “about who is selling what, at what price, and for what reason.”⁵⁴ The Court further stated that it was in the best interest of society at large for consumers to have enough information to make intelligent and well-informed decisions in a free enterprise system. While the Court acknowledged the risks of protecting speech that could ultimately lead to harm for consumers, it was adamant about the “impermissibility of keeping consumers ignorant for their own protection.”⁵⁵

The Court’s rationale has been extended to ads appearing on consumer web sites⁵⁶ and solicited email ads.⁵⁷ As with their print counterparts, these online ad vehicles meet the requirements for protected speech under the First Amendment. They facilitate free and truthful information exchange, which benefit advertisers as well as consumers, by opening the channels of online commercial speech to a wide spectrum of advertisers—not just those with the deepest pockets—and by keeping consumers informed of the wide range of market choices available in ways that suit their tastes and preferences.⁵⁸

51. US Const. amend. I, <<http://www.law.cornell.edu/constitution/constitution.billofrights.html#amendmenti>>, states, “Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.”
52. 425 U.S. 748, <<http://justia.us/us/425/748/case.html>>, 96 S. Ct. 1817, 48 L. Ed. 2d 346 (1976) [*Virginia State Board of Pharmacy*].
53. *Ibid.* at p. 765.
54. Remes, *supra* note 3 at pp. 171-173.
55. *Ibid.* at p. 74.
56. See e.g. *Knoll Pharm. Co. v. Sherman*, 57 F. Supp. 2d 615 at p. 618 (D Ill 1999) (enjoining state law banning pharmaceutical company from advertising its products on nationally and regionally distributed newspapers and magazines, on cable television and on a consumer web site on the internet as part of its Meridia advertising program).
57. Unsolicited email ads, pejoratively labeled as junk email or spam, also have been defended under the First Amendment, though their suitability for free speech protection remains fiercely contested. See David L. Hudson Jr., “Internet & First Amendment Issues: Spam” *First Amendment Centre* (29 June 2004), <<http://www.firstamendmentcenter.org/speech/internet/topic.aspx?topic=spam>>, which cites First Amendment attorney Kurt Wimmer’s remarks that “even unsolicited email messages constitute speech.”
58. See CATO Institute, “Free Speech & First Amendment Issues/Media Ownership & Broadcasting Issues,” <<http://www.cato.org/tech/inetfreespeech.html>>.

Likewise, the advertisers that specialize in pop-ups have invoked the spirit of the First Amendment by defending their advertising practices using arguments that hearken to the doctrine of commercial speech proffered in *Virginia State Board of Pharmacy*.⁵⁹ Just as the Court in that case found that the First Amendment protected an advertiser's interest in speaking and a consumer's interest in receiving truthful information about a particular product, WhenU and Claria have claimed that their use of pop-ups constitutes protected speech because it provides advertisers increased access to consumers and offers consumers information enabling them to make more intelligent purchasing decisions.

WhenU, for example, has argued that pop-ups, like online classifieds, search engines and targeted emails, "give the little competitor and the late-to-market company a chance to compete by giving them a presence close to the moment of purchase. Without such advertising like that supplied by WhenU, entrenched market leaders will likely wield more pricing power than with such advertising."⁶⁰ Regarding pop-ups' benefit to consumers, WhenU has noted that "significant numbers of consumers hosting the WhenU software acquired the software in an affirmative effort to learn about competing offers," and that the resulting "free play of competition brings learning and with learning comes protection against intelligent purchasing decisions."⁶¹

For its part, Claria, when it was known as Gator, padded its own website with testimonials from industry experts in defence of its advertising practices.⁶² These testimonials echo the defences WhenU raised by asserting that pop-up ads are integral to maintaining an abundance of advertising voices on the internet and providing consumers with sufficient choices to make informed purchases. One testimonial on the Gator site, for example, emphasized that "[the web site owners] that are suing Gator...do not have [end-users'] interests at heart. Instead, they are trying to create legal precedents that will be used to give them unprecedented control over your [personal computer]."⁶³ Another warned that "a decision against Gator would give web site owners 'far more control over the end user than is appropriate',"⁶⁴ while a third noted that "a ruling against Gator would be a ruling against consumer choice. It would set a dangerous precedent that could affect consumers' rights to display content on the access devices in the ways they like."⁶⁵

59. *Virginia State Board of Pharmacy*, *supra* note 52.

60. *Advertising Spending*, *supra* note 6 at p. 14.

61. *Ibid.*

62. See "Gator Company Info.: What the Industry is Saying" available at Electronic Frontier Foundation, "Gator Archive" (January 2003), <<http://www.eff.org/IP/gator>> [Gator Archive].

63. *Ibid.*

64. Decker & Lewis, "Gator Goes on the Attack in 'Pop-Up' Internet Ad War" *Bloomberg News* (8 November 2002), cited in "Over Two Million Internet Users Respond to Consumer Rights Issue" *News Room, Claria Corp.* (18 November 2002), <<http://www.claria.com/companyinfo/press/releases/pr021118.html>>.

65. Tom Hespos, "Let's Not Kid Ourselves - It's About Consumer Control" *Online Spin* (26 November 2002), <<http://forum.abestweb.com/showthread.php?t=29864>>.

3.2. 'Here's the Catch': Protection Not Absolute

While the First Amendment has emerged as a powerful sword for commercial speech, its swath of indemnity has not been all-encompassing. Just four years after *Virginia Board of Pharmacy*, the Supreme Court narrowed the scope of its commercial speech doctrine in *Central Hudson Gas & Electric Corp. v. Public Service Commission of New York*.⁶⁶ The majority in this case adopted a four-part test for determining whether commercial speech should be protected under the First Amendment.

For commercial speech to come within that provision, it at least must concern lawful activity and not be misleading. Next we ask whether the asserted governmental interest is substantial. If both inquiries yield positive answers, we must determine whether the regulation directly advances the governmental interest asserted, and whether it is not more extensive than is necessary to serve that interest.⁶⁷

Central Hudson empowered agencies and legislative bodies to enact statutes and regulations against certain forms of speech that otherwise would merit protection, by virtue of "enhancing 'the flow of commercial information',"⁶⁸ under *Virginia Board of Pharmacy*. Indeed, several laws proscribing spam have been successfully defended in state and federal court using the various prongs of the *Central Hudson* test. In *State v. Heckel*,⁶⁹ the Washington Court of Appeals invoked the first part of this test in upholding a state law that prohibited "misrepresentation in the subject line or transmission path of any unsolicited commercial email message sent from a computer located in Washington."⁷⁰ The court reasoned that "[b]ecause the Act is narrowly tailored to regulate only deceptive commercial speech,"⁷¹ it applied only to spam that was inherently misleading. In this way, the law met "the appropriate standard in determining when commercial speech is constitutionally protected,"⁷² under part one of *Central Hudson*.

The Washington state court's interpretation of *Central Hudson* could easily be extended to uphold provisions targeting pop-up ads, according to one legal expert involved in litigation against pop-up providers.⁷³ As with the particular spam in question in *Heckel*, the pop-ups delivered by "the Gators and

66. 447 U.S. 557, <http://supct.law.cornell.edu/supct/html/historics/USSC_CR_0447_0557_ZS.html>, 100 S.Ct. 2343, 65 L. Ed. 2d 341 [*Central Hudson*].

67. *Ibid.* at p. 566.

68. *Illinois Association of Realtors v. Bellwood*, 516 F. Supp. 1067 at p. 1069 (N D Ill 1981) [*Illinois Association of Realtors*.] citing *Virginia Board of Pharmacy*, *supra* note 52 at p. 1827.

69. 122 Wn. App. 60, <<http://search.mrsc.org/nxt/gateway.dll/supreme/143wn2d/143wn2d0824.htm>>, 93 P.3d 189(2001) [*Heckel*].

70. *Ibid.* at p. 63.

71. *Ibid.* at p. 72.

72. *Ibid.*

73. Interview with Clifford Sloan, General Counsel, Washingtonpost.Com (July 2003). Washingtonpost.com is one of several major news web sites that filed suit against Gator for its unauthorized pop-up displays.

WhenUs have no First Amendment defence under *Central Hudson*, he argues, "because what they are doing constitutes unlawful and misleading activity, period."⁷⁴

For their part, Gator and WhenU deny that their pop-up ads either violate the law or mislead users. To the contrary, as noted above, these companies maintain that their pop-ups enable users to make more intelligent purchasing choices. They further argue that users are no more likely to be misled by their ads than by other forms of targeted advertising, which are common and accepted in the real world. Parts 5 and 6 describe these arguments in more detail in the context of the recent legal actions brought against Gator and WhenU.

Ultimately, the ability of pop-up ad companies to successfully rebut charges that their practices are unlawful and misleading may not be enough to exempt them from regulation. Indeed, whereas the Washington court of appeals in *Heckel* confined its analysis of the state's *Commercial Electronic Mail Act* to its prohibition of misleading speech, which the court found to be unprotected under prong one of the *Central Hudson* test, other courts have relied upon the other three parts of this test in upholding regulations that go beyond the Washington state law to target more benign forms of online commercial speech. For example, in *White Buffalo Ventures, LLC v. The University of Texas at Austin*,⁷⁵ the US District Court for the Western District of Texas ruled that anti-spam policies at the University of Texas (UT) were constitutionally valid. The district court held that, while the plaintiff's spam was "neither misleading nor unlawful" on its face, it was nonetheless subject to prohibition under the university's tough anti-spam policies. The court noted that these policies

...easily survive a constitutional challenge under *Central Hudson*.... UT has asserted a substantial government interest—namely managing and blocking the unsolicited commercial email the university computer system receives that ties up memory space on UT servers, expends UT resources in responding to user complaints, and disrupts the work of UT students, faculty and staff.

...

While UT's system for stopping spam, which involves commercial filters, responding to user complaints, and installing ISP-specific filters, could not [b]e considered perfectly tailored in that it most likely blocks some solicited email and misses some spam, it is sufficiently tailored in light of the quantity of users and spam with which it deals and in light of the technology currently available. As such, UT's policies do not run afoul of *Central Hudson* and the Court will not enjoin UT from blocking White Buffalo's email messages to utexas.edu since White Buffalo will not commit to stop spamming utexas.edu addresses.⁷⁶

74. *Ibid.*

75. 2004 U.S. Dist. LEXIS 19152, (WD Tex) (Lexis) available at National Association of College and University Attorneys, <http://www.nacua.org/documents/WhiteBuffaloVentures_v_UofTexasAustin_b.pdf> [*White Buffalo*].

76. *Ibid.* at p. 16, p. 20.

It is too soon to tell whether the district court's rationale in *White Buffalo* will be adopted by higher-level federal courts. Nevertheless, the decision seems to set a clear precedent for courts to extend considerable deference to policymakers' efforts to restrict online commercial speech, which a high proportion of internet users may find annoying, but which is not demonstrably unlawful or misleading. Given the hostility that many internet users harbour toward pop-up ads—forms of online commercial expression which, as aforementioned, have been found to annoy an even higher percentage of users than spam—it seems likely that new laws targeting these ad forms will be awarded deference by the courts, regardless of whether or not they are proven to be unlawful or misleading.

Of course, to satisfy the requirements of *Central Hudson*, policymakers must demonstrate a sufficiently compelling reason to regulate commercial speech. Arguably, the fact that such speech is found to be annoying by its intended recipients is not a substantial enough interest to justify regulation, absent other underlying factors.

In the case of pop-up ads,⁷⁷ as with spam,⁷⁸ the core interest put forth in support of regulation is internet user privacy. Privacy is an interest that has been used in the past to justify regulations targeting various forms of commercial speech, such as restrictions on telemarketing solicitation of accident victims,⁷⁹ unsolicited advertisements to fax machines,⁸⁰ and door-to-door solicitations.⁸¹ As discussed in the next section, concerns about the privacy risks posed by pop-up ads are rooted in theories of privacy that have been recognized, to varying degrees, under Constitutional, statutory and common law.

-
77. See e.g. Dannielle Cisneros, "Do Not Advertise: The Current Fight Against Unsolicited Advertisements" (2003) *Duke Law & Technology Review* 0010, <<http://www.law.duke.edu/journals/dltr/articles/2003dltr0010.html>>, at para. 18 warned that "without regulation of the newer forms of advertising including pop-up advertising and spam, the interruptions will simply shift form and not be eradicated...The right to privacy should not be outweighed by an advertiser's right to sell his product by forcing a captured audience (in a movie theater, online or in an email inbox) to be inundated with sales pitches."
78. See e.g. Credence E. Fogo, "The Postman Always Rings 4,000 Times: New Approaches to Curb Spam" (2000) 18 *John Marshall Journal of Computer & Information Law*. 915 at p. 930, argued that courts are more likely to show deference toward "an anti-spam regulation, which protects both privacy and property. Even if a ban covered commercial speech that was not false, misleading, or illegal, prohibiting the practice of sending hundreds of thousands of unsolicited commercial messages [i.e., spam], at a huge expense to the recipients and countless third parties with a highly detrimental effect that threatens the survival of a medium that has become increasingly necessary to the smooth functioning of commerce, would serve an important governmental interest." See also Beth I. Z. Boland, Daniel B. Trinkle & Christine M. Baker, "'Initial Interest Confusion' and the Use of Metatags and Keyed Banner Ads in Internet Trademark Law" (2001) 45 *Boston Bar Journal* 6 at p. 21.
79. See e.g. *Capobianco v. Tennessee Board of Chiropractic Examiners*, 377 F.3d 559, <<http://www.ca6.uscourts.gov/opinions.pdf/04a0237p-06.pdf>> (6th Cir 2004); and *Anderson Courier Service v. Texas*, 104 S.W. 3d 121 (CA Texas, 3d Dist 2003).
80. See e.g. *Minnesota v. Sunbelt Communications and Marketing*, 282 F. Supp. 2d 976 (D Minn 2002).
81. See e.g. *Cleveland Home Improvement Council v. City of Bedford Heights*, 113 Ohio App. 3d 814, 682 N.E.2d 667 (CA Ohio, 8th App Dist 1996).

*

4. PRIVACY GUARANTEED?

4.1. *Constitutional Safeguards*

THE RIGHT TO PRIVACY is not expressly recognized in the US Constitution.⁸² Nevertheless, the Supreme Court has identified certain zones of privacy implicit in the Bill of Rights, such as the right to associate in the First Amendment, the right to prohibit the quartering of soldiers in homes in times of peace in the Third Amendment, the right to be free from unreasonable search and seizures under the Fourth Amendment, and the right against self-incrimination in the Fifth Amendment.⁸³ While such rights apply only to actions taken by the state, the spirit of these Constitutional protections has given rise to similar causes of action, or torts, against private actors.⁸⁴

4.2. *Privacy in the Private Sector*

William L. Prosser identified four primary privacy torts in his landmark 1960 article, "Privacy."⁸⁵ These torts include the right against intruding (physically or otherwise) upon the solitude of another in a highly offensive manner, publicizing highly offensive private information about someone which is not of legitimate concern to the public, publicizing a highly offensive and false impression of another, and using another's name or likeness for some advantage without the other's consent.⁸⁶ The torts have been upheld in numerous federal and state court decisions, and have been incorporated in the statutes of several states.⁸⁷

Other torts have emerged in statutes and case law that protect privacy-related interests, including the torts of trespass, intentional infliction of emotional distress, and defamation.⁸⁸ As with the main privacy torts, these causes of action relate to harm caused by private actors.

Companies are not entitled to privacy rights per se.⁸⁹ However, like individuals, companies are subject to protection under laws encompassing privacy-related interests. These include real property laws governing conversion

82. Ellen Alderman & Caroline Kennedy, *The Right to Privacy* (New York: Random House, 1997) at p. 52.

83. See e.g. *Griswold v. Connecticut*, 381 U.S. 479, <<http://justia.us/us/381/479/case.html>> (1965) (recognizing right of privacy implicit in First, Third, Fourth and Fifth Amendments).

84. See generally, American Law Institute, *Restatement (Second) of Torts* (St Paul, Minn: American Law Institute Publishers, 1977).

85. William L. Prosser, "Privacy" (1960) 48 California Law Review 383.

86. *Ibid.* at p. 389 (defining rights against intrusion, public disclosure of private facts, false light and appropriation).

87. *Ibid.* at p. 386 (describing privacy torts recognized in 47 states).

88. Alderman & Kennedy, *supra* note 82 at p. 52.

89. See e.g. *Pacific Gas & Electric Co. v. Public Utilities Com.*, 475 U.S. 1, <<http://justia.us/us/265/403/case.html>>, 89 L. Ed. 2d 1 (1986) at p. 34 [*Pacific Gas*], citing *First Nat'l Bank v. Bellotti*, 435 U.S. 765 (1978) at p. 779, where the court stated that "the two constitutional liberties most closely analogous to the right to refrain from speaking—the Fifth Amendment right to remain silent and the constitutional right of privacy—have been denied to corporations based on their corporate status."

and trespass to chattel,⁹⁰ as well as intellectual property laws governing copyright,⁹¹ trademarks,⁹² and fair use.⁹³

*

5. AN EMERGING MARKET: USER PRIVACY LAWSUITS

5.1. *Real Property and Unauthorized Access Claims*

TO DATE, FEW INTERNET USERS have leveraged their outrage at pop-up ads into legal causes of action. In a rare lawsuit brought in 2003, a user in Texas claimed that DIRECTV's pop-up ads constituted trespass to chattels⁹⁴ and unauthorized access to his computer.⁹⁵ The US District Court for the Western District of Texas disagreed. Although the court conceded that "to interfere wrongfully with the use or possession of property is a trespass to chattel," it held that such interference must cause "actual damage to the property or *depriv[e] the owner of its use for a substantial period*," in order for liability to incur.⁹⁶ The court likewise proceeded to strike down the user's claim that DIRECTV had violated the *Computer Fraud and Abuse Act*,⁹⁷ the federal statute governing unauthorized access to computers, by "knowingly and with intent to defraud access[ing] this protected computer without authorization or exceeded authorized access...appropriating [user's] time and attention without authorization and use of his computer resources."⁹⁸ The court responded that there simply was no precedent for including pop-up ads within the scope of "access" under the statute.⁹⁹

The district court's ruling suggests that pop-up ads, which generally appear in windows on a user's screen for only a few seconds, are too ephemeral in nature to violate contemporary laws governing trespass and other forms of unauthorized access, as such torts were created to protect interests in *real*

90. See Dan Burk, "The Trouble With Trespass" (2000) 4 *Journal of Small & Emerging Business Law* 27, <<http://www.isc.umn.edu/research/papers/trespass-ed2.pdf>>. Trespass to chattel is an archaic trespass tort prohibiting substantial interference with personal property ("chattel"). See Electronic Freedom Foundation, "EFF Analysis of Trespass to Chattels Legal Theory," <http://www.eff.org/Spam_cybersquatting_abuse>.
91. "Copyright subsists in original works of authorship fixed in any tangible medium of expression. Literary works (including computer programs), musical works, dramatic works, pictorial, graphic and sculptural works, motion pictures and other audiovisual works, and sound recordings are all protected by U.S. copyright law." *Legal Definitions.com*, s.v. "copyright," <<http://www.legal-definitions.com/copyright.htm>>.
92. "A trademark is a distinctive sign which identifies certain goods or services as those produced or provided by a certain entity or person. The trademark is protected for a period of 20 years, indefinitely renewable." *Legal Definitions.com*, s.v. "trademark," <<http://www.legal-definitions.com/IP/trademark.htm>>.
93. Fair use is a copyright concept that permits third parties to use portions of copyrighted materials for purposes of commentary and criticism. See, for example, Stanford University Libraries, *Copyright & Fair Use*, ch. 9, <http://fairuse.stanford.edu/Copyright_and_Fair_Use_Overview/chapter9/index.html>.
94. Archaic trespass tort prohibiting substantial interference with personal property ("chattel"). See "EFF Analysis of trespass to Chattels Legal Theory," *supra* note 90.
95. *DIRECTV Inc. v. Jae Sun Chin*, 2003 U.S. Dist LEXIS 15815 (WD Tex) (Lexis) [*DIRECTV*].
96. *Ibid.* at para. 6 [first emphasis added].
97. *Computer Fraud and Abuse Act*, 18 U.S.C., s. 1030, <http://www4.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00001030----000-.html>.
98. *Ibid.* at (a)(4).
99. *DIRECTV*, *supra* note 95 at para. 7.

property, rather than those in the virtual realm of cyberspace where pop-ups dwell.

Nevertheless, additional suits targeting pop-up ad providers on grounds of trespass and unauthorized access grounds are possible in the future, in the wake of related claims brought against spammers. While not entirely successful, legal action taken against spammers has established a precedent for using property-based claims and unauthorized computer access claims to target noxious commercial speech.¹⁰⁰

5.2. Intellectual Property Claims

Though hard to pin down in the literal sense, pop-ups have not escaped scrutiny. In a recent spate of litigation, pop-up ads have been alleged to violate intellectual property statutes governing copyright, trademark and fair use.¹⁰¹ These lawsuits have been brought by companies, rather than individuals, which is not surprising, given that intellectual property law, as previously noted, is largely geared towards protecting the proprietary interests of corporations.¹⁰²

On one hand, individual users seem to have a good case against invasive pop-ups if they prove by a preponderance of evidence that the adware triggering these ads was as invasive as many critics allege. This article has discussed how sophisticated forms of adware can monitor and intercept users' personal information. The personal information intercepted can include information inputted during commercial transactions online, or when registering to use certain web sites, including NYTimes.com, Washingtonpost.com and other public and subscription sites that require logins.¹⁰³ Such invasive collecting of users' personal information, if properly documented, could implicate several of the privacy torts, including intrusion, public disclosure of private facts and appropriation.¹⁰⁴

Conversely, however, courts still could reject claims against pop-up providers in favor of the counter argument that users who elect to download software from such providers must assume any subsequent risk of privacy invasion. In prior litigation, WhenU and Claria both pleaded that users voluntarily download their software in order to avoid liability.¹⁰⁵ Regardless of such pleas, it is unlikely that many users would consent to the downloading of such software if they fully understood how invasive it could be. Courts might nonetheless hold

100. See e.g. *Compuserve Inc. v. Cyber Promotions*, 962 F. Supp. 1015, 25 Media L. Rep. 1545 (SD Ohio 1997) at p. 1022 [*Compuserve* cited to F.Supp] (granting preliminary injunction against a bulk e-mailer on a theory of trespass to chattels); *America Online v. IMS*, 24 F. Supp. 2d 548 (ED Va 1998), at p. 550 [*America Online*] (relying on the reasoning in *Compuserve* to find that a bulk e-mailer "injured AOL's business goodwill and diminished the value of its possessory interest in its computer network"); *Intel Corp. v. Hamidi*, 114 Cal. Rptr. 2d 244, 94 Cal. App. 4th 325 (Cal Ct App 2001) rev'd 71 P.3d 296, 30 Cal. 4th 1342 (Cal 2003) (holding that under California law, the tort of trespass to chattels does not encompass an electronic communication that neither damages the recipient computer system nor impairs its functioning, but leaving the door open for suits against electronic communications that are demonstrably harmful).

101. *Supra* notes 91-93.

102. Benjamin Edelman, "Methods and Effects of Spyware: Response to FTC Call for Comments" (19 March 2004), <<http://www.benedelman.org/spyware/ftc-031904.pdf>>.

103. *Ibid.*

104. Interview of Benjamin Edelman by Emily Woodward, 20 April 2004.

105. Benjamin Edelman, "Pending Suits Against Designers of Spyware" (June 2002), <<http://www.benedelman.org/spyware/#suits>>.

that users assumed the risk associated with downloading software. Indeed, this stance was taken by Judge Lee of the US District Court for the Eastern District of Virginia in his September 2003 order granting summary judgment to WhenU against U-Haul.¹⁰⁶ Although this case was decided against a corporation, rather than an individual user, the following portion of Judge Lee's opinion leaves little doubt that an individual also would be unlikely to prevail in a claim against pop-up ads:

The average computer user who conducts a web search for the U-Haul web site would expect the U-Haul web site to appear on their computer screen; however, in this case, the computer screen fills with the advertisement of a U-Haul competitor...While at first blush this detour in the user's web search seems like a siphon-off of a business opportunity, the fact is that the computer user consented to this detour when the user downloaded WhenU's computer software from the Internet. In other words, the user deliberately or unwittingly downloaded the pop-up advertisement software.¹⁰⁷

★

6. A HARD SELL: DEFENDING CORPORATE PRIVACY INTERESTS

MANY CORPORATE WEB SITES that require users to enter personal information carry notices on their registration pages promising that information entered will be used solely for the purpose of monitoring site traffic.¹⁰⁸ Such guarantees—and, with them, much of the credibility of these self-described secure web sites—would be undermined if courts were to side with adware critics regarding the extensive spying capabilities of such software.¹⁰⁹

However, while websites themselves could be liable to users if a court of law determined that a user's personal information had been intercepted by a third party without their consent, it is doubtful the websites could assert claims on behalf of their users against the entities responsible for the interception.¹¹⁰ Instead, the website's only grounds for legal recourse is likely to remain in the intellectual property realm.

106. *U-Haul International, Inc. v. WhenU.com Inc.*, 279 F. Supp. 2d 723 (ED Va 2003)[U-Haul].

107. *Ibid.* at p. 725.

108. See e.g. [Washingtonpost.com](http://www.washingtonpost.com), <<http://www.washingtonpost.com>>. This web site includes a pop-up window guaranteeing that "the 'cookie' set by a web site can only be read by that site. This means that your 'cookie' will only be used by [washingtonpost.com](http://www.washingtonpost.com) to store small bits of information regarding your visit to the site." A "cookie" is a small piece of information that a site can store within a user browser.

109. Interview of Benjamin Edelman by Emily Woodward; Benjamin Edelman, email to Emily Woodward (19 April 2004). Edelman, a noted adware critic and expert witness in several lawsuits involving WhenU and Gator, expressed the belief that at least certain adware programs had the capability of monitoring and collecting user data mandated by secure web sites. He added that "there's basically nothing web sites can do to stop it, other than push for legislation, educate consumers about the problem, etc.—but no obvious self-help for web sites to block the data collection."

110. The Supreme Court has granted third-party standing in privacy claims. See e.g. *Miller v. Albright*, 523 U.S. 420, <<http://supct.law.cornell.edu/supct/html/96-1060.20.html>>, (1998) at p. 449 (*Miller* cited to U.S.) where the Court stated that privacy concerns may provide a compelling explanation for a third party's absence from litigation citing *Carey v. Population Services International*, 431 U.S. 678 (SD NY 1977) at p. 684. However, third party standing has not been extended to claims of privacy invasion involving speech on the internet. See *United States v. Reilly*, U.S. Dist. LEXIS 6005 at para. 13 (SD NY 2003) (Lexis) which ruled against third-party standing for individuals in matters relating to the interstate transportation of obscene material via an interactive computer service.

As indicated in the previous section, numerous commercial websites have filed suit against WhenU and Gator on intellectual property grounds.¹¹¹ While early efforts proved effective in halting unauthorized displays of pop-up ads, recent unsuccessful attempts to pursue pop-up ad providers have raised new doubts relating to the usefulness of litigation in this area.

WhenU has been sued by U-Haul, 1-800 Contacts, Overstock.com and Weight Watchers.¹¹² Claria has been the defendant in actions commenced by the New York Times, the Washington Post, Hertz Rent-a-Car, Wells Fargo, L.L. Bean and Extended Stay America among others.¹¹³ While only two cases will be discussed, similar charges have been filed in other cases.

6.1. The "Cons" Have Their Day: News Sites Sink Teeth Into Claria's Commercial Speech Claims

In August 2002, the US District Court for the Eastern District of Virginia enjoined Claria (then known as Gator) from using its adware to trigger pop-up ad displays in the vicinity of the plaintiffs' web sites. In this case, each plaintiff was a news conglomerate operating a site on the internet.¹¹⁴

The plaintiffs' first claim was that Claria's pop-up ads infringed their registered trademarks in violation of the *Lanham (Trademark) Act*,¹¹⁵ a statute which prohibits the "use in commerce of "any reproduction, counterfeit, copy or colorable imitation of a registered mark in connection with the sale, offering for sale, distribution, or advertising of any goods or services on or in connection with which such use is likely to cause confusion, or to cause mistake, or to deceive."¹¹⁶

To prevail on a claim of trademark infringement, a plaintiff is required to show ownership of a valid, protectable mark and proof that a defendant used the mark in commerce in a way likely to cause confusion.¹¹⁷ Accordingly, the plaintiffs in this action submitted to the court certificates of registration for each of their registered trademarks. They then argued that Claria's adware triggered pop-up ads on the page views that feature plaintiffs' trademarks, thereby creating an

111. See e.g. *Washingtonpost.Newsweek Interactive Company v. The Gator Corporation*, 2002 U.S. Dist. LEXIS 20881 (ED Va 2002) (Lexis); *U-Haul*, *supra* note 106.

112. Benjamin Edelman, "Documentation of Gator Advertisements and Targeting" *Berkman Center for Internet & Society, Harvard Law School* <<http://cyber.law.harvard.edu/people/edelman/ads/gator/>>.

113. See e.g., *1-800 Contacts, Inc. v. WhenU.com, Inc.*, 2005 U.S. App. LEXIS 12711 (2d Cir 2005), available at EFF.com, <http://www.eff.org/legal/cases/1800contacts_v_whenU/decision.pdf>, *Gator.com Corp. v. L.L. Bean, Inc.*, 398 F.3d 1125, <[http://www.ca9.uscourts.gov/coa/newopinions.nsf/955C2E6DC12A870688256E84006DDEDF/\\$file/0215035o.pdf?openelement](http://www.ca9.uscourts.gov/coa/newopinions.nsf/955C2E6DC12A870688256E84006DDEDF/$file/0215035o.pdf?openelement)> (9th Cir 2005); *Wells Fargo & Co. v. WhenU.com, Inc.*, 293 F. Supp. 2d 734, <http://www.mied.uscourts.gov/_opinions/Edmundspdf/NGE03cv71906WhenU.pdf> (D Mich 2003); *Hertz Corp. v. Gator Corp.*, 250 F. Supp. 2d 421 (D NJ 2003); *Washingtonpost.Newsweek Interactive*, *supra* note 18.

114. The plaintiffs involved in this action were Washington Post Newsweek Interactive Company, Gannett Satellite Information Network, Media West-GSI, the New York Times Company, the Boston Globe Newspaper Company, Dow Jones, Smartmoney, the Chicago Tribute Interactive, Condenet, American City Business Journals, Cleveland Live and Knight Ridder Digital. See *Washingtonpost.Newsweek Interactive*, *supra* note 18.

115. Plaintiff's Memorandum in Support of Preliminary Injunction at 19, *Gator* (CV 02-909-A). *Lanham (Trademark) Act*, 15 U.S.C. s.1114(1)(a) (2002) <http://www.law.cornell.edu/uscode/html/uscode15/usc_sec_15_00001114----000-.html>.

116. *Ibid.*

117. *Ibid.*

unauthorized association between the two, and giving users visiting the sites the impression that the ads were sponsored or approved by the trademark owners.¹¹⁸ As evidence of user confusion, the plaintiffs included the results of a consumer survey in which 66 percent of respondents believed the ads were authorized by the plaintiffs.¹¹⁹

Claria responded that its ad placement practices did not involve use of the plaintiffs' marks in commerce.¹²⁰ It argued that its pop-ups neither appeared on the plaintiffs' web pages, nor altered their appearance in any way. Rather, Claria maintained that, because the pop-ups appeared in a window separate from the content on the plaintiffs' web sites, the ads constituted no more of an infringement to the plaintiffs than an open email or Instant Messenger window, which would likely overlap with the content on the plaintiffs' sites.¹²¹ Claria's second argument concerned the likelihood of user confusion about the origin of its pop-up ads, a concern it argued was misplaced. According to Claria, "Confusion as to the origin of the product being advertised is the appropriate inquiry, not whether there is confusion as to the origin of the advertisement."¹²² Claria then argued that each of its pop-ups clearly indicated the source of the product being advertised. As pointed out by one legal scholar, this argument fails as a defence for a particular type of trademark infringement known as initial interest confusion, "a bait-and-switch-type of confusion over a trademarked name that might attract a consumer's interest in a competitor or competitor's goods—and can be actionable just as when confusion arises at the point of sale."¹²³ Under this doctrine, which Claria ignored in its defence, the advertiser would be liable for trademark infringement if its pop-ups left internet users with the impression, when they initially viewed the ads, that they were affiliated with the plaintiffs' sites. As evidence that this was, in fact, the case, the plaintiffs pointed to the results of their survey—showing that 66 percent of respondents believed there was an association between their sites and the pop-up ads.¹²⁴

Initial interest confusion also was the key issue in the plaintiffs' next claim, which alleged that Claria's pop-ups constituted unfair competition in violation of section 43(a) of the *Lanham (Trademark) Act*, which provides broader protection than the rule against trademark infringement by prohibiting the "use of any word, term, name, symbol or device, or any combination thereof...which is likely to cause confusion...as to the origin, sponsorship, or approval of his or her goods, services, or commercial activities by another."¹²⁵

The plaintiffs' burden of proof for unfair competition was slightly different than for their trademark infringement claim. For unfair competition, they were

118. Plaintiff's Complaint, Gator (CV 02-909-A), available at <http://www.gdclaw.com/fstore/documents/Media/WP_Complaint.pdf> at p. 33.

119. *Ibid.*

120. *Washingtonpost.Newsweek Interactive*, *supra* note 111.

121. *Ibid.*

122. *Ibid.* at p. 18.

123. Boland, Trinkle & Baker, *supra* note 78 at p. 6.

124. *Supra* note 118.

125. *Lanham Act*, *supra* note 115 at 1125(a)(1).

required to show that user confusion resulted from a particular word, term, name or symbol used in the pop-up ads, or from a particular device of the defendants. The plaintiffs argued that Claria's so-called "pop-up advertising scheme" constituted a device that gave rise to user confusion.¹²⁶ However, the plaintiffs did not specify what this scheme entailed; *i.e.*, whether it pertained to the pop-up ads themselves or the adware triggering them. Claria, in its response to the complaint, argued that the meaning of the word "device" under Section 43(a) was limited to "symbols used as source identifiers"—for example, registered trademarks—and that it had not used any such device to confuse users.¹²⁷

The plaintiffs' third argument was that Claria's pop-up ads diluted their registered trademarks. The claim of trademark dilution refers to the eroding of a trademark in the mind of the public through unauthorized use of the mark.¹²⁸ While such unauthorized use could be to sell a competing product—*e.g.*, using a Coca-Cola trademark in an advertisement for Pepsi—it need not be.¹²⁹

To prevail on their claim of trademark dilution, the plaintiffs needed to show that 1) their marks were famous 2) the defendant had made commercial use of the marks in commerce 3) the use of the marks had begun after they became famous and 4) the use of the mark diluted the quality of the marks in identifying and distinguishing goods and services.¹³⁰

Having dealt with the first three elements of this claim in their trademark infringement argument, the plaintiffs concerned themselves with establishing that Claria's commercial use of their trademarks tarnished the goodwill users bore toward the marks.¹³¹ Tarnishment, as a basis for trademark dilution, occurs when a famous mark is associated with another product or context that is degrading and unwholesome.¹³² The plaintiffs alleged that such tarnishment occurred when Claria altered the look and feel of their web sites with its pop-up ads, thereby annoying users who visited the sites and disparaging their goodwill toward the plaintiffs.¹³³ Moreover, the plaintiffs noted that Claria's contextual ad placement practices posed a risk of tarnishment, if ads offensive to the users were displayed. As an example, the plaintiffs noted that Claria's software could potentially trigger an advertisement for a flight training school ad to appear in a window overlapping a web page containing an article about the September 11, 2001 tragedies.¹³⁴

126. *Supra* note 118 at p. 22.

127. *Ibid.* at pp. 17-18.

128. Frank Schecter, "The Rational Basis of Trademark Protection" (1927) 40 Harvard Law Review 813.

129. *Ibid.* at p. 820.

130. See *e.g.* *Panavision Int'l, L.P. v. Toepfen*, 141 F.3d 1316, <<http://www.ca9.uscourts.gov/cao/newopinions.nsf/04485f8dcbd4e1ea882569520074e698/f05d3f7623c90f5488256e5a007188ef>>, 46 U.S.P.Q.2d (BNA) 1511 (9th Cir 1998) at p. 1324 (*Panavision* cited to F.3d) citing the Federal Trademark Dilution Act, 15 U.S.C. s. 1125(c), <http://www.law.cornell.edu/uscode/html/uscode15/usc_sec_15_00001125----000-.html>.

131. *Supra* note 118 at p. 32.

132. See *e.g.* *Bally Total Fitness Holding Corp. v. Faber*, 29 F.Supp. 2d 1161, 50 U.S.P.Q.2D (BNA) 1840 (CD Cal 1998) at p. 1166 [*Bally Total Fitness* cited to F.Supp.] in which the plaintiff argued that the defendant had tarnished its mark by associating it with pornography.

133. *Supra* note 118 at p. 32.

134. *Ibid.*

A true-life example of such an alleged tarnishment involved Claria's competitor, WhenU. WhenU's adware triggered ads for pornography to appear when users entered the URL of a well-known safe-sex web site.¹³⁵

In responding to the trademark dilution charge, Claria relied on its earlier defence against the trademark infringement claim that its pop-up ads did not constitute use of the plaintiff's marks in commerce.

The plaintiffs also alleged that Claria's use of pop-ups constituted a violation of the US *Copyright Act*.¹³⁶ They argued that Claria was liable for direct contributory infringement for its role in transmitting authorized pop-ups to users' computers, from which they were displayed over the content of the plaintiffs' web sites, as well as contributory copyright infringement, for providing users with the tools—*i.e.*, the software—to alter the appearance of the plaintiffs' web sites on their computers.

In proving their copyright claims, the plaintiffs were required to show ownership of the intellectual property in question—in this case, a valid copyright—and to prove that the defendant both played a role in the copying of the elements of the plaintiffs' web sites, and facilitated copying on the part of users. The plaintiffs argued that this unlawful copying occurred when the Claria pop-ups were juxtaposed on each of their web sites. They maintained that the combination of the ads and the underlying site content constituted an unlawful "derivative work," based on the original site consisting of "editorial revisions, annotations, elaborations or other modifications."¹³⁷ "[U]nauthorized editing of the underlying work...would constitute an infringement of the copyright in that work similar to any other use of a work that exceeded the license granted by the proprietor of the copyright."¹³⁸

Claria, in appealing the district court order granting the plaintiffs a preliminary injunction, argued that the plaintiffs' allegations that it prepared and enabled users to prepare derivatives of the plaintiffs' copyrighted work was unfounded. "Software that users install on their computers and which subsequently opens a separate, independently controllable window containing advertising on that user's computer screen does not abridge, condense, recast, transform or adapt the web page in the underlying window any more than laying one document partially over another alters or modifies the underlying document."¹³⁹

Because the plaintiffs' case against Claria was subsequently settled under confidential terms in February 2003, it failed to set a binding legal precedent as to whether the defendant's use of pop-ups and the adware that triggered them was inherently unlawful. In fact, the practice of delivering pop-ups via adware has been upheld as not violating intellectual property laws in a number of subsequent court decisions.

135. See <http://www.allaboutsex.org/pop-up_ads.html>.

136. U.S. *Copyright Act*, 17 U.S.C. 106, <http://www.law.cornell.edu/uscode/html/uscode17/usc_sup_01_17.html>.

137. *Supra* note 118.

138. *Ibid.*

139. *Ibid.*

*6.2. The "Pro" Side Bites Back:
WhenU Wins Legal Battle Against Corporate Foe*

Less than a year after ordering the injunction on behalf of the news website plaintiffs, the district court in Virginia reversed its position and granted summary judgment in favor of WhenU in a case brought by U-Haul involving near-identical charges of trademark infringement, unfair use, trademark dilution and copyright infringement.¹⁴⁰ While the exact reason for the different outcomes in these two cases is unclear, it appears that the counsel for WhenU took notice of, and learned from, Claria's unsuccessful defence effort. WhenU's defence in several respects improved upon Claria's core argument that pop-ups, and the adware that triggered them, were neither connected to the plaintiff's web sites, nor likely to leave a user with the mistaken impression that they were affiliated. First, WhenU noted that all of its pop-ups contained disclaimers stating, "This is a WhenU offer and is not sponsored or displayed by the web site you are visiting."¹⁴¹ Next, WhenU pointed out that its pop-ups carried their own brand names as well as the trademarks of WhenU's advertisers.¹⁴² Third, WhenU stated that each of its ads contained the standard marking of a Windows software application: a "?" symbol that, if clicked on, would open to the website of a particular advertiser.¹⁴³ In each of these ways, the ads made it apparent to the consumer that they were "distinct from the consumer's internet browsing application and clearly not generated by the web site the consumer initially visited."¹⁴⁴

To further demonstrate that its pop-ups were patently distinct from the content on U-Haul's web site, WhenU likened its ad placements to common contextual marketing practices in the physical world. The advertiser stated that its tactics were analogous "to those of big-city vendors who wear poster boards or distribute fliers for goods or services outside a competitor's store."¹⁴⁵ Moreover, WhenU argued that, just as the court would not find a "vendor distributing coupons for Blimpie's outside a Subway sandwich shop," to infringe Subway's trademarks or copyrights, it should not find a WhenU pop-up for Ryder Moving Co., which appeared alongside a window to the U-Haul web site, to constitute trademark or copyright infringement. In this way, WhenU provided the Court with an understanding of the nature of pop-ups that was far more tangible and benign than the explanation given by Claria.

140. Order, *U-Haul v. WhenU.com Inc.*, CV 02-1469-A (ED Va 2002).

141. Affidavit of Avi Naider in support of WhenU.com's Motion for Partial Summary Judgment at 19, *WhenU.com Inc.* (CV 02-1469-A).

142. *Ibid.*

143. *Ibid.*

144. *Ibid.*

145. Interview of Beth Kallett, General Counsel, WhenU.com Inc. by Emily Woodward (9 July 2003).

★

7. BEYOND THE COURTROOM: ALTERNATIVE TREATMENTS FOR THE PAIN OF POP-UPS

7.1. "There Ought to Be a Law..."

IN THE MONTHS FOLLOWING WhenU's win against U-Haul, federal courts in Michigan and New York sided with the pop-up advertiser against similar claims of copyright infringement brought by 1-800 Contacts Inc.¹⁴⁶ This trend suggests that corporate websites targeted by WhenU and its ilk may have exhausted their remedies at law.

Perhaps it is not surprising, then, that alternative methods of restricting pop-ups and adware have begun to crop up, most significantly in proposed legislation at the federal and state levels. Bills that would entitle users to receive more information about adware prior to downloading, and would require pop-up advertisers to modify the software with uninstall capabilities, currently are pending in the US Senate and House of Representatives.¹⁴⁷ In addition, the state legislatures of Iowa, New York, and Virginia have introduced measures to protect internet users' privacy rights by curbing the dissemination of adware and other forms of spyware.¹⁴⁸

California and Utah, meanwhile, have led the nation in opposing these invasive technologies by becoming the first states to enact law¹⁴⁹ prohibiting the installation of any form of spyware on a third party's computer without consent. However, the ultimate effectiveness of these pioneering anti-spyware laws appears limited, at best.

California's *Computer Spyware Act*, signed into law by Governor Arnold Schwarzenegger in September 2004, has already been faulted by spyware critics for failing to address many of the fraudulent and unfair trade actions currently practiced by spyware companies and for preempting other laws that, while not specifically developed to address spyware, nonetheless offer users greater protection against these programs.¹⁵⁰

146. See *1-800 Contacts Inc. v. WhenU.com Inc.*, 309 F. Supp.2d 467; 69 U.S.P.Q.2D (BNA) 1337 (SD NY 2003). In this dual-edged decision, the district court granted summary judgment to WhenU on the basis of the copyright infringement claim, but ruled in favor of the defendant on the trademark infringement and cybersquatting claims.

147. US, Bill, H.R.2929, *Safeguard Against Privacy Invasions Act* ("SPY"), 108th Cong., 2004, <<http://thomas.loc.gov/cgi-bin/query/C?c108:/temp/~c108Twhbqu>>, introduced by Rep. Mary Bono (D-Cal) would require, *inter alia*, that advertisers using Spyware technology obtain the permission of internet users prior to installing this software and provide mechanisms for disabling the software following installation. The Software Principles Yielding Better Levels of Consumer Knowledge ("SPY BLOCK") Act, introduced 27 February 2004, by Sen. Conrad Burns (R-Mont) and Sen. Ron Wyden (D-Ore), is intended, *inter alia*, to regulate the unauthorized installation Spyware and other invasive software, and require more effective disclosure to users of certain computer software features that may pose a threat to user privacy.

148. Benjamin Edelman, "Proposed State Legislation," <<http://www.benedelman.org/spyware/#suits>>.

149. See *Consumer Protection Against Computer Spyware Act*, Cal. S.B. 1436 (2004), <http://www.leginfo.ca.gov/pub/03-04/bill/sen/sb_1401-1450/sb_1436_bill_20040928_chaptered.html>; *Spyware Control Act*, Ut. H.B. 323 (2004), <<http://www.le.state.ut.us/~2004/bills/hbillenr/hb0323.htm>>.

150. Erin Joyce, "A Hobbled Anti-Spyware Law" *Internet News* (1 October 2004), <<http://www.internetnews.com/commentary/article.php/3416391>>; Benjamin Edelman, "California's Toothless Spyware Law" (29 September 2004), <<http://www.benedelman.org/news/092904-1.html>>.

Utah's *Spyware Control Act* proved to be even more problematic. Though scheduled to take effect May 3, 2004, implementation of the act was stayed to allow time for a state court to hear WhenU's argument for a preliminary injunction against the statute.¹⁵¹ WhenU, seemingly emboldened by its victories in the courts, had filed suit against the state of Utah on April 12, 2004, alleging that the *Spyware Control Act* interferes with its First Amendment speech rights.¹⁵² The court suspended the law June 22, 2004, and subsequently denied the Utah state government's bid for reconsideration.¹⁵³ Surprisingly, even mainstream internet companies, including AOL, Amazon, Google, Microsoft and Yahoo, opposed the Utah spyware ban, claiming that it would block their own seemingly benign and beneficial internet communications software.¹⁵⁴ Their fears were unfounded, according to one leading internet software expert who has embraced the law as a measured approach to curbing the "growing array" of invasive software "that gets installed on users' computers, often without their knowledge, consent, and/or informed consent, and performs functions users dislike, often including tracking or transmitting personal information [and] displaying targeted advertisements."¹⁵⁵

A common argument among advocates of the Utah law, and related legislation designed to limit unauthorized displays of pop-up ads, is that regulation of online advertising, though unprecedented in the United States, is justifiable under the scarcity principle.¹⁵⁶ The scarcity principle, which has served as the basis for government's hands-on regulation of broadcast and cable media in contrast to its hands-off approach to print,¹⁵⁷ recognizes the need for federal oversight of limited communications resources. According to legislative advocates, online ad space constitutes a limited resource, because of internet users' limited threshold for ads, particularly pop-ups. The website owners affected by the pop-ups concur, warning that the proliferation of such ads, "if left unchecked, would erode the attractiveness of advertising on [their] web sites and disrupt or potentially destroy [their] ability to sell advertising, imperiling [their] economic viability."¹⁵⁸

7.2. Going High-Tech

Critics of pop-up regulation argue that, notwithstanding the problems posed by these ads and the software that enables them, it is still premature for either government or the courts to take steps to restrict their growth. Alternatively,

151. See Complaint, *WhenU Inc. v. Utah*, 04-0907578 (Salt Lake Co, Utah, 12 April 2004).

152. *Ibid.*

153. Utah Reply Memorandum in Support of Reconsideration, *WhenU Inc. v. Utah*, 04-0907578 (Salt Lake Co, 30 July 2004) denied 28 September 2004.

154. Ross Fadner, "Top Web Businesses Oppose Utah Spyware Law" *Media Daily News* (15 March 2004), <http://www.mediapost.com/dtls_dsp_news.cfm?newsID=242077>.

155. Benjamin Edelman, "A Close Reading of Utah's Spyware Control Act" (February 2004), <<http://www.benedelman.org/spyware/#suits>>.

156. Interview of Benjamin Edelman by Emily Woodward (16 July 2003).

157. See Ithiel de Sola Pool, *Technologies of Freedom* (Cambridge, MA: Harvard University Press, 1984) at p. 6.

158. *Supra* note 118.

critics assert that the tensions created by pop-ups are best handled through the cultivation of new protective technologies, such as pop-up ad blockers,¹⁵⁹ and through regulatory efforts within the internet community. However, a large number of ad blocking tools currently on the market have proven to be ineffective against the particular pop-ups triggered by adware,¹⁶⁰ while online community policing efforts against the invasive use of pop-ups are still in their infancy.¹⁶¹

A major drawback to treating invasive pop-ups with similarly high-tech remedies is that it places the burden of safeguarding internet users' privacy rights on the online community, rather than on traditional governmental instruments charged with privacy enforcement. Already, relying upon the private sector to protect internet users has proven risky. In the past year, two companies have been accused of installing spyware on users' computers, only to then turn around and sell their victims anti-spyware software.¹⁶² More generally, the erosion of privacy protections in the public sector has come under fire by civil liberties advocates and organizations such as the American Civil Liberties Union (ACLU). According to the head of the ACLU's Technology and Liberty Program, "Americans are facing major new threats to their privacy each day and they should be able to look to their [federal and] state governments for assistance in preserving their privacy."¹⁶³

Ironically, by tolerating a hands-off governmental approach to invasive pop-ups, internet users and web sites could find themselves subject to increased monitoring at the hands of federal and state agencies. As noted by Professor Jeffrey Rosen, "people's subjective expectations of privacy tend to reflect the amount of privacy they subjectively experience."¹⁶⁴ Applying this rationale to pop-ups, it would seem that the more the online community is willing to bear responsibility for the privacy risks posed by invasive pop-up advertising, the more government agencies may permit, and even contribute to, these sorts of intrusions in the future. Indeed, the United States federal government already has begun expanding its surveillance authority, both on- and off-line, through

159. A number of internet service providers, led by Microsoft Corp., have introduced software to block pop-up ads on internet user's screens. See e.g. Stephanie Olsen "Internet Explorer to Stomp Pop-ups" *CNETNews* (10 November 2003), <<http://news.com.com/2100-1032-5105139.html>>.

160. "2004 Anti-Spyware Software Report" *TopTenReviews* (2004), <<http://www.anti-spyware-review.toptenreviews.com/index.html>>.

161. At the time this article was written the Internet Advertising Bureau (IAB), the dominant private-sector organization serving the interests of online commercial advertisers, had only just introduced its first set of self-regulating guidelines governing the display of pop-up and pop-under ads. See "IAB Issues Pop-Up Ad Guidelines for Industry Comment" *Interactive Advertising Bureau* (29 April 2004), <http://www.iab.net/news/pr_2004_4_29.asp> .

162. David McGuire, "FTC Files First Federal Lawsuit Against Spyware" *Washington Post* (13 October 2004), <<http://www.washingtonpost.com/wp-dyn/articles/A28179-2004Oct12.html>>.

163. See "ACLU Asks Attorney General John Ashcroft to Enforce Driver's License Information Privacy Law in Florida," *American Civil Liberties Union of Florida* (8 April 2003), <http://www.aclufl.org/news_events/archive/2003/dlprivacy040803.cfm>.

164. Jeffrey Rosen, *The Unwanted Gaze* (New York: Random House, 2000) at p. 60.

recent legislation, most notably the 2001 *Patriot Act* and its spin-offs.¹⁶⁵ Agencies also are experimenting with their own forms of spyware as a prophylactic measure to thwart misuse of their online data.¹⁶⁶

*

8. CONCLUSION

THE FATE OF POP-UPS ultimately will depend on whether individuals and businesses allow their personal and proprietary information to be compromised in exchange for a more cost-efficient and diverse online marketplace. In what is essentially a match of privacy versus capitalist interests, the internet will either persist in redefining commercial speech—testing the limits of what constitutes “ad space”—or it will yield to increased regulation at the hands of the courts, legislative bodies, the internet community, or a combination thereof.

For the present, most internet users and commercial websites seem resigned, however reluctantly, to the tradeoff between privacy and commercialism. Indeed, this article has addressed how, despite their complaints about pop-ups, few internet users have seriously attempted to protect their personal property interests from invasive ads. Their inaction may have much to do with the fact that, as Professor Rosen notes, “[m]ost people don’t care about privacy until they have something to hide, and there’s no reason to believe that consumers wouldn’t voluntarily transfer property rights in their personal data to commercial web sites in exchange for product discounts and other conveniences.”¹⁶⁷ Even if a court were to rule that adware-driven pop-ups are as invasive as critics allege, Professor Rosen’s observations suggest that internet users may continue to click on these ads—in large enough numbers for the advertisers to turn a profit—and chalk up any subsequent privacy loss as the cost of doing business online.

Against this swell of user indifference and willingness on the part of many companies to confuse or mislead in order to boost their profits, it is perhaps little wonder that the efforts of a handful of large websites, legislators and online privacy advocates have done little to stop the flood of unauthorized pop-up ad displays.

165. The United States Congress in October 2001 passed the *United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act* (USA *Patriot Act*) of 2001, Pub. Law No: 107-56, <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107.pdf>. The act consisted of several time-limited provisions which significantly increased the surveillance and investigative powers of law enforcement agencies in the United States. The Bush Administration began campaigning to renew the Act in early 2004. See e.g., “Remarks by the President on the USA *Patriot Act*” *Whitehouse.gov* (20 April 2004), <<http://www.whitehouse.gov/news/releases/2004/04/20040420-3.html>>. For further discussion of the expansion of the government’s surveillance authority under *Patriot Act* provisions, see Susan Murray, “‘Queer Eye’ for Big Brother” *Washingtonpost* (28 January 2004), <<http://www.washingtonpost.com/ac2/wp-dyn/A54703-2004Jan27>>.

166. Richard M. Smith, “Is currency anti-copying software government-mandated ‘spyware’?” *ComputerBytesman* (22 January 2004), <<http://www.computerbytesman.com/privacy/anticopy.htm>>.

167. Rosen, *supra* note 164 at p. 181.