Loyola of Los Angeles
Entertainment Law Review

Volume 24 | Number 3 Article 4

6-1-2004

Internet Pop-Up Ads: Your Days Are Numbered - The Supreme Court of California Announces a Workable Standard for Trespass to Chattels in Electronic Communications

Geoffrey D. Wilson

INTERNET POP-UP ADS: YOUR DAYS ARE NUMBERED!

THE SUPREME COURT OF CALIFORNIA ANNOUNCES A WORKABLE STANDARD FOR TRESPASS TO CHATTELS IN ELECTRONIC COMMUNICATIONS

I. INTRODUCTION

The recent California Supreme Court decision in *Intel Corp. v. Hamidi*[1] could prove to be the undoing of the Internet's newest and most intrusive form of advertising: the pop-up advertisement.[2]

Utilizing a theory of trespass to chattels, Intel Corporation brought suit against its former employee, Kourosh Kenneth Hamidi, to enjoin him from using the company's e-mail list to contact Intel employees with mass e-mails.[3] On six occasions spanning almost two years, Hamidi sent over 30,000 e-mails criticizing Intel's employment practices to numerous employees on Intel's electronic mail system.[4] Hamidi did not breach any computer security barriers in order to communicate with Intel employees.[5] He offered to, and did, remove from his mailing list any recipient who so wished.[6] Hamidi's communications to individual Intel employees caused neither physical damage nor *functional disruption* to the *company's computers*, nor did his communications at any time *deprive Intel of the use of its computers*.[7] The contents of the messages, however, caused

1. 71 P.3d 296 (Cal. 2003).

2. *See generally id.* (Pop-up ads generally cause functional disruption, dispossession, and loss of use or control over computer systems for a period of time. As such they fit the definition of trespass to chattels that the Intel court announces in this decision.).

3. *Id.* at 299–300.

4. *Id.* at 299.

5. *Id.* at 301.

6. *Id.*

7. *Intel*, 71 P.3d at 301 (emphasis added).

discussion among employees and managers, and according to Intel, this intrusion fulfilled the requirements of trespass to chattels.[8] However, the court in *Intel* held:

> After reviewing the decisions analyzing unauthorized electronic contact with computer systems as potential trespasses to chattels, we conclude that under California law the tort does not encompass, and should not be extended to encompass, an electronic communication that neither *damages* the recipient computer system nor *impairs its functioning*. Such an electronic communication does not constitute an actionable trespass to personal property, i.e., the computer system, because it does not *interfere with the possessor's use or possession* of, or any other legally protected interest in, *the personal property itself*.[9]

In holding that the tort of trespass to chattels should not include electronic communications that neither damage nor impair the recipient computer system,[10] California's highest court has laid out a blueprint for the destruction of the Internet pop-up. Confusing as it might seem, by defining what trespass to chattels is *not*, the court established a test which can be used to define what trespass to chattels has become in the Internet age.[11]

After years of refinement the personal computer became part of many American's lives; as connection speeds become faster, the Internet is quickly achieving the same level of popularity. In an age where the question is more likely "do you have a wireless broadband connection to the Internet at home?" as opposed to "do you have access to the Internet at home?" personal interaction with the Internet is becoming more and more prevalent. As people venture onto the Internet in ever greater numbers, so do advertisers, and their tactics grow ever more intrusive.[12] Part II of this comment discusses the effect that Internet advertising, especially the Internet pop-up, has had on individual Internet users. Part III discusses the legal approach of taming the Internet and other related electronic mediums with remedies such as copyright, trademark, and the shockingly ineffectual statutes that have led to the reintroduction of the ancient common law tort of trespass to chattels to modern Internet law.

---

8. *Id.*

9. *Id.* at 300 (emphasis added).

10. *Id.*

11. *Id.*

12. *See Development of Internet*/WWW.AD, *at* http://www.ciadvertising.org/SA/fall_02/adv391K/jeong/page4_2.html (last visited Mar. 11, 2004) [hereinafter *Development of Internet*/WWW.AD].

Part IV provides a synthesis of modern Internet law and a forward-looking view of its application to the most invasive form of Internet advertising yet: the pop-up and its progeny. Specifically, the discussion centers around how the rise of invasive advertising such as the pop-up and the evolution of the tort of trespass to chattels have converged, resulting in the simultaneous zenith of an odious form of advertising and a legal solution for it. The question is how far will advertisers be able to go without trespassing to your chattels? Part V concludes that they may have already gone too far.

II. PROBLEMS WITH POP-UPS

What is a pop-up? The definition and commentary provided by marketingterms.com, an online dictionary, defines a pop-up ad as: "[a]n ad that displays in a new browser window."[13] Information pop-up windows come in many different shapes and sizes, typically in a scaled-down browser window with only the "Close," "Minimize," and "Maximize" commands.[14] "There is strong resentment by some Web surfers towards pop-up ads."[15] In fact, by its very definition pop-up ads are revealed as synonyms for annoying.[16] One could argue that this form of advertising is the most despised on the web.

The Internet began as an ad-free zone, but as it has become more widely used, advertising has sprung up all over the web.[17] Many advertisers use the form of a "banner ad" that is basically akin to a poster on the background of a website. Dictionary.com refers to banner ads as "[a]ny of the annoying graphical advertisements that span the tops of way too many Web pages."[18] Typically the banner ad also has a "hyperlink"

13. MARKETINGTERMS.COM, *at* http://www.marketingterms.com/dictionary/pop_up_ad/ (last visited Mar. 3, 2004) [hereinafter MARKETINGTERMS.COM]. A browser is an application program that provides a way to look at and interact with all the information on the World Wide Web. The word "browser" originated prior to the internet as a generic term for user interfaces that allow you the ability to browse, navigate through and read, text files online. Perhaps the first widely used web browser was Netscape Navigator. Microsoft followed with its Microsoft Internet Explorer. Online services, such as America Online, originally had their own browsers, however almost all now offer the Netscape or Microsoft browser. *Id.* http://searchwebservices.techtarget.com/sDefinition/0,,sid26_gci211708,00.html (last visited on November 16, 2003).

14. 1ADCLICK.COM, *at* http://www.1adclick.com/ac/pops.html (last visited Mar. 29 2004).

15. MARKETINGTERMS.COM, *supra* note 13.

16. *Id.*

17. *See Development of Internet*/WWW.AD, *supra* note 12.

18. DICTIONARY.COM, *at* http://dictionary.reference.com/search?q=banner%20ad (last visited Mar. 29, 2004).

that will direct the web browser to the electronic document or file to which the banner ad is connected.[19]

While these banner ads may be annoying, they do not spring onto the screen unannounced, obstructing your work, as Internet pop-ups do. Banner ads are stationary, and while they may occupy a large area of a site, they are only of consequence when they are actively clicked on by a visitor to the website.[20] In contrast, when a pop-up ad pops up, users are forced to stop whatever they are doing and close the newly created browser window.[21] "Marketers often do not realize the ill-will generated by pop-ups because it is easier to click the 'close' button than send an e-mail to complain."[22]

Online advertisers using pop-up advertisements may feel that their messages are getting through because their methods of measuring success are overly inflated. When online advertisers measure their online success in advertising rates, they often use the standard of "hits," or user clicks on their web pages, often through banner ads or pop-ups.[23] This measurement, called a "click-through rate," is relied on by some advertisers to show that their message is getting through to potential consumers.[24] However, when a pop-up gets in the way of something that a potential consumer actually intends to click on, "[w]hat can often be seen is an above-average click-through rate from 'false positives.'"[25]

A. The Pop-Up Ad Backlash

A common sentiment surrounding pop-up ads is that no one buys anything from pop-up advertisers, so why do advertisers use them?[26] Advertisers use pop-up ads because they feel they can create a large amount of them, relatively inexpensively, that have the potential of reaching millions of customers.[27] Some argue that instead of using the

19. Tom Harris, *How Banner Ads Work*, HOWSTUFFWORKS.COM, *at* http://money.howstuffworks.com/banner-ad.htm (last visited Mar. 11, 2004).

20. *See id.*

21. *See* John Borland, *Napster Clones Spy on P2P Users*, CNET NEWS.COM *at* http://news.zdnet.co.uk/internet/security/0,39020375,2086554,00.htm (posted May 15, 2001).

22. MARKETINGTERMS.COM, *supra note* 13.

23. *See id.*

24. *Id.*

25. *Id.*

26. *See* Kelly Sitch, *Internet Ads Dream for Advertisers, Nightmare for Surfers*, THE DIGITAL COLLEGIAN, March 4, 2003 *at* http://www.collegian.psu.edu/archive/2003/03/03-04-03tdc/03-04-03dscihealth-05.asp.

27. *See id.*

number of ads an advertiser creates that are viewed by customers as the measure of an ad's success, often using over inflated "click through rates," that advertisers can get a better picture of the effectiveness of pop-up advertising by paying attention to conversion rates and return on investment (ROI).[28] However, as advertisers set their Internet spending budgets, they seem to use pop-ups as the "go to" form of new Internet advertising, even if the practice yields small return on investment.[29] Companies may still see the investment required to spit out pop-up ads as very small compared to other forms of mass advertising, thus, many companies will continue to use pop-ups as their preferred form of advertisement.[30]

The problem is that many members of the online community despise pop-ups,[31] and hundreds of articles have been written about the problems that pop-ups create. "Pop-ups Must Die" is a site dedicated exclusively to the problems of pop-ups and serves as a clearing house for anti pop-ups articles and sites.[32] Just a few of the listings are as follows:

- *AOL Pops Pop-Ups*, CLICKZ (March 12, 2003);
- *Are Pop-Up Ads Killing Themselves?*, E-COMMERCE TIMES (October 28, 2002);
- *Earthlink Joins Movement to Kill Pop-Up Ads*, USA TODAY (August 19, 2002);
- *Pop-Up Warfare: Is Peace Possible?*, CLICKZ (August 15, 2000);
- *The Pop-Up Ad Campaign From Hell*, SALON.COM (May 7, 2002);
- *Google Distances Itself From Pop-Ups*, CNET NEWS.COM (January 29, 2002);
- *Hate Pop-Up Ads? Here's How to Burst Their Bubbles*,

28. MARKETINGTERMS.COM, *supra* note 13. (Conversion rates in this case are the percentage of visitors to a site who make a purchase, ROI in this case would be the total financial benefit of the pop-up ads minus their total cost.).

29. *See*, Jim Rapoza, *Pop-up Ads Bad For Business*, EWEEK.COM, *at* http://www.eweek.com/article2/0,1759,1545511,00.asp (posted Mar. 8, 2004). *See also*, Anne Chan, *The Efficacy of Pop-ups and the Resulting Effect on Brands – A White Paper by Bunnyfoot Universality*, BUNNYFOOT.COM, http://www.bunnyfoot.com/popup/bunnyfoot_popup.pdf (last visited April 1, 2004).

30. *See generally id.*

31. *See generally Pop-ups Must Die*, *at* http://www.4degreez.com/popupsmustdie/ (last visited Mar. 3, 2004) [hereinafter *Pop-ups Must Die*] (website containing information for Internet users that are against pop-up ads).

32. *Id.*

ZDNET (August 17, 2001);

- *Noxious Pop-Up Ads are Gaining Respect*, MEDIA LIFE (April 4, 2001);
- *Consumers Combat Pop-ups With Software, Tricks*, CNET (February 5, 2001);
- *GeoCitizens Bristle at Pop-up Ads*, CNET (December 18, 1997).[33]

Since their arrival, pop-ups have been controversial and the volume of articles advocating their elimination, despite their brief time in existence, clearly establishes their despised nature.[34] Many of these article titles themselves reveal their authors' distaste for this form of advertising and the reasons for their hatred of pop-ups are fairly straight forward.[35] Simply put, pop-up ads are unwanted and unrequested, disrupt the effectiveness of the systems they appear on, and waste users' time.

In addition to the sheer volume of articles which have been published from the pop-up ads inception, there seems to be an overwhelming negative response to the very nature of pop-up ads.[36] The following excerpt from the website "Pop-ups Must Die," represents common complaints and exemplifies the degree of frustration experienced by many Internet users:

Question (by an Internet user):

> "Why do you care if there are Pop-up ads? It's not like they are killing you or anything . . ."

Answer (by Pop-ups Must Die):

> Nothing seems so bad that we can't make it worse. I got on the Web in October of 1994. Back then there were NO ADS! None, nada, zip, zero, not even ONE! (Just a bunch of crappy gray homepages) I saw the rise of advertising on the Internet. And to tell you the truth it's only getting worse. One idiot came up with Pop-up ads and soon all the marketing people followed like a bunch of lemmings towards the cliff! I wouldn't be so bothered

33. MARKETINGTERMS.COM, *supra* note 13. The above titles have been bulieted for effect as it is not only easier on the eyes to read titles on individual lines, but also causes the reader to pause and fully appreciate each title and its authors point of view when the title is set out on its own line.

34. *See generally id.* (discussing numerous articles describing pop-up ads as vile creations).

35. *Id.*

36. *See generally, Pop-ups Must Die*, *supra* note 31 (discussing websites where those who hate pop-up advertising can learn about pop-ups and communicate their feelings about them.).

> if they weren't so obtrusive! Ads in and of themselves don't even phase me. I live in America - land of opportunity and advertising. I just don't like having to STOP what I am doing and close a window, just so I can turn around and do it again 30 seconds later. It slows me down.[37]

Perhaps the most legally significant question that one can draw from such an exchange is "how?" Namely, *how* do the pop-ups slow the user down? The Internet user exclaims that he does not like to "STOP what [he] is doing and close a window, just so [he] can turn around and do it again 30 seconds later."[38] As the pop-up window appears on the desktop, it causes the user to stop and close the window. In effect, pop-ups cause the *user's* computer to display a message over the work the user is doing, forcing the user to stop his or her work in order to address a message that someone else has caused to be placed on the user's system.[39] This is not only annoying to the user, but also affects the computer itself.

Specifically, Internet pop-ups can cause connections to slow down and often cause the user to inadvertently open a link to a website that may expose the computer to viruses, software bugs, or even more pop-ups.[40] For example, "mouse-trapping" occurs when an Internet user becomes "trapped" as a nearly infinite number of pop-up ads, generated from as little as one unintended click, stream onto his computer causing the computer to crash or forcing the user to take immediate action to end the onslaught of advertisements.[41] While unscrupulous practitioners of the mouse-trapping technique create ads that spawn pop-ups from a single click on a pop-up window, other programs do not even require that much.

For example, computer programs, like SaveNow, actually store information on a user's computer and then provide precisely tailored information to other computers on the net in order to generate content specific advertisements.[42] Thus, if a user was visiting a travel website such as Orbitz.com and about to make a purchase, an ad generated by SaveNow would pop up on the desktop and present information about comparable

37. *Id.*

38. *Id.*

39. *See* MARKETINGTERMS.COM, *supra* note 13.

40. *See*, Brian McWilliams, *Privacy Concerns Raised Over Adbot Software*, CLICKZNEWS, February 24, 2000 *at* http://clickz.com/news/article.php/12_309951 (discussing how adbots can "potentially [make] systems unreliable and open security holes.").

41. NETLINGO.COM, *at* http://www.netlingo.com/lookup/cfm?term=mousetrapping (last visited Mar. 3, 2004). Mouse-trapping occurs "when a site uses browser tricks to keep a user captive . . . by disabling the back button or by generating repeated pop-up windows." *Id.*

42. *See* WHENU.COM, *at* http://www.whenu.com/about_savenow.html (last visited Mar. 3, 2004) [hereinafter WHENU.COM].

deals on another competing website such as Hotwire.com.[43]

Furthermore, programs such as SaveNow are problematic since many users may have downloaded the program without even knowing it.[44] This occurs because file sharing software such as "BearShare" can contain hidden programs like SaveNow that cause the user's computer to communicate with other computers without the user's knowledge, often resulting in decreased computer performance.[45] "'SaveNow is buggy and tends to screw up your network connection,' Manish Vij, a BearShare user and founder of Web design firm Net Studio," wrote in an e-mail to News.com.[46] "'Every time I launch a browser, SaveNow keeps trying to run and makes my network connection flaky.'"[47] The program utilizes the user's system resources to run its own pop-up ads which impair system performance and reduces a user's control over his system.[48] Even providers of SaveNow at WhenU.com acknowledge that there are system performance problems associated with the software as it results in "sustained . . . CPU usage."[49]

"The advertising software has prompted some discussion on bulletin boards online and drawn criticism from people who say the extra programs are privacy violations and can hurt computer performance."[50] Users such as Vij find that their systems are affected by problematic programs that generate pop-ups and other types of advertising, monopolizing their time and wasting their system resources by running ad after unsolicited ad.[51]

B. Pop-Up Ads, the Next Generation

Often users will surf the web and then realize that there is an inordinate amount of advertising that has piled up on their desktop.[52] One

43. *See id.*

44. *See* Bob Sullivan, *Are You Being Watched Online*, MSNBC.COM, *at* http://www.msnbc.msn.com/*id*/3475956/ (last visited Mar. 5, 2004).

45. *See* John Borland, *Napster Clones Spy on P2P Users*, CNET NEWS.COM *at* http://news.zdnet.co.uk/internet/security/0,39020375,2086554,00.htm (posted May 15, 2001).

46. *Id.*

47. *Id.* Users of SaveNow have noted that the program contacts SaveNow servers often, in order to retrieve content from SaveNow and store that content on *their own personal computer. Id.* "[T]he desktop application checks for the presence of new browser windows *every 3 seconds*, which results in sustained (but very low) CPU usage." WHENU.COM, *supra* note 42 (emphasis added).

48. *See id.* Borland, *supra* note 45.

49. *See id.* WHENU.COM, *supra* note 42.

50. Borland, *supra* note 45.

51. *See id.*

52. *See generally id.*

possibility is that a user visited a site while surfing and that site launched pop-up windows in the background.[53] These ads are known in the advertising industry as "pop-unders."[54] Other web pages trigger pop-ups when a user leaves that site.[55] Essentially, even after a user leaves a site they chose to visit, the pop-ups or pop-unders remain on their system, often slowing the system as they communicate with the site from which they came.[56] These advertising programs can be launched as a pop-up or pop-under or, even more insidiously, transported in a program that a user downloads for other non-related purposes.

Newer pop-up ads and their progeny are now often packaged in other software. For example, many computer users have inadvertently downloaded a pop-up producing program with their free file-sharing software.[57] This packaging causes even more egregious interference with a user's control over his own computer.[58] A recent article that has criticized pop-ups speaks about greater problems to come: "Dubbed 'adware,' or 'spyware' by their critics, these software programs run in the background even when the original file-swapping [sharing] software isn't operating, popping up advertisements while people surf online, and sometimes quietly uploading information about a Web surfer's habits."[59]

"The programs have sparked a swell of protest from some people computer-savvy enough to figure out what software is running on their machines and what it is doing."[60] This type of pop-up has been dubbed "Spyware" because it often spies on the user's Internet activity without his knowledge.[61] Spyware and Stealth advertising components that are

---

53. *See generally* Jeffrey Benner, *Spyware, In a Galaxy Near You*, WIRED NEWS, *at* http://www.wired.com/news/technology/0,1282,49960,00.html. (last posted Jan. 24, 2002).

54. *Id.* A pop-under ad is "[a]n ad that displays in a new browser window behind the current browser window . . . the sneakier relative of the pop-up ad. While pop-up ads are often shown (and closed) instantly, pop-under ads linger behind the current browser window, appearing only after other windows have been closed." *at* http://www.marketingterms.com/dictionary/pop_under_ad/ (last visited April 1, 2004).

55. *See, About the Pop-up Blocker*, GOOGLE.COM, *at* http://toolbar.google.com/popup_help.html (last visited Mar. 3, 2004).

56. McWilliams, *supra* note 40.

57. *Id. See also* Borland, *supra* note 45.

58. Borland, *supra* note 45.

59. *Id.*

60. *Id.*

61. NETLINGO.COM, *supra* note 41 *at* http://www.netlingo.com/lookup.cfm?term=spyware. "Software that gathers information about a user as he or she navigates around the Web, it is intended to track surfing habits in order to build marketing profiles." These programs may also transmit information about your habits to the company's Website. Borland, *supra* note 45. "Spyware is cause for public concern about privacy on the Internet." NETLINGO.COM, *supra* note 41.

installed by some "shareware" products (and sometimes legitimately purchased commercial software) may collect personal information from the user's computer.[62] These "adbots" are usually tied to a shareware program the user has downloaded and installed like a music-sharing or other media-sharing program.[63] One of the latest scandals over spyware involves a mysterious and particularly insidious program that tracks surfing, delivers pop-up ads, and is even capable of collecting credit card information.[64] How can advertisers justify such extreme measures? Some argue that it is necessary to subsidize the cost of their "free," or inexpensive, software.

Software manufacturers claim that in order to provide certain software to users at little or no cost, sneaking ad generating software into software with a totally unrelated purpose is one of the least intrusive methods they can use to recoup the cost of offering their software for free.[65] Many forms of media-trading or playing software are initially offered for free but contain hidden pop-up projecting software.[66] Internet users who have unwittingly downloaded a program with a hidden advertising purpose complain about poor system performance and the barrage of ads it creates every time they are online.[67] "[T]he companies defend themselves saying there are worse alternatives [like spyware] and they need some revenue sources if they are to continue to offer their products for free."[68]

Another type of pop-up comes in a form often indistinguishable from a user's typical program.[69] Internet sites warn about this type of spam called "Messenger Service Spam."[70] It "looks like all the usual crud you receive in your email (enlarge your whang, herbal Viagra, university diplomas, mortgage etc.), but appears on your desktop in its own window

62. *See* Borland, *supra* note 45.

63. *See* McWilliams, *supra* note 40. In his description of what adbots are, and some of the problems associated with them, McWilliams explained that "adbot software pulls down banners from a server on the Internet, caches them on the user's hard disk, and then display[s] them in a special window in the utility or application." Adbot manufacturers have been accused of uploading pages of "user information back to the [adware] company, including a list of all installed software on the PC and any multimedia clips downloaded by the user." Another concern is "the always-on nature of their technology." Some adbot critics have problems with programs unnecessary to the user (adbots) constantly running in the background potentially causing "systems to be unreliable and opening security holes." *Id.* Users have reported ". . . system lock-ups and browser crashes," even after uninstalling the ad-supported program. *Id.*

64. Benner, *supra* note 53.

65. *See* Borland, *supra* note 45.

66. *Id.*

67. *Id.*

68. *Id.*

69. *Adware - Spyware and now "Trash Apps,"* MULTI.CO.NZ SYSTEMS CONSULTANCY, *at* http://www.multi.co.nz/software/adware.html (last visited Mar. 26, 2004).

70. *Id.*

while you're online."[71] "Messenger Service Spam" results from spammers "exploiting Windows Messaging,[72] a service present on Windows NT/2000/XP machines."[73] Internet spammers find weaknesses in programs running on the user's computer system and exploit these programs in order to send messages the user must close manually.[74] So many Internet users have grown to hate this particular type of pop-up[75] that special sites have posted links to pages that have instructions on how to "turn this service off and thwart the spammers."[76]

In fact, many of the problems involving websites and pop-up windows have been addressed by private parties.[77] As "[m]any web sites —even very prominent sites—are now using unwanted and unrequested pop-up windows [w]hen surfers arrive or even depart,"[78] some Internet users and websites have taken action. Some have gone so far as to rank other sites based on the number of pop-ups on that site.[79] Top9, a website that ranks other sites based on criteria including the number of pop-ups that site produces, suggests: "[i]f you experience a pop-up on our TOP9.com pages that we have not designated, please let us know!"[80] Other sites provide programs that block most pop-ups.[81] Clearly, it seems that Internet users will go to great lengths to avoid pop-ups.

---

71. *Id.*

72. "Windows Messenger is a technology that gives users the ability to identify people online and to exchange messages with them in real time." *See, e.g.,* NETLINGO.COM, *at* http://www.netlingo.com/lookup.cfm?term=instant+messaging (last visited Mar. 28, 2004).

73. MULTI.CO.NZ SYSTEMS CONSULTANCY, *supra* note 69. In October 2001 Microsoft merged its two Windows operating system lines for consumers and businesses into their current offering, Windows XP. XP is the evolution of Microsoft's efforts to create the world's most used user interface. MICROSOFT.COM *Windows Products and Technologies History, Windows Desktop Products History at* http://www.microsoft.com/windows/WinHistoryDesktop.mspx. (last visited Mar. 3, 2004) [hereinafter *Windows History*].

74. *See About the Pop-up Blocker,* GOOGLE.COM, *at* http://toolbar.google.com/popup_help.html (last visited Mar. 3, 2004).

75. *See generally* McWilliams *supra* note 40 (citing Internet users concerns about pop-ups).

76. *See, e.g., About the Pop-up Blocker,* GOOGLE.COM, *at* http://toolbar.google.com/popup_help.html (last visited Mar. 3, 2004). *See also, Adware - Spyware and now "Trash Apps,"* MULTI.CO.NZ SYSTEMS CONSULTANCY, *at* http://www.multi.co.nz/software/adware.html (last visited Mar. 26, 2004) (discussing instant messenger spam).

77. *See, e.g., Avoid the Pop-ups!* TOP9.COM *at* http://www.top9.com/popups/ (last visited Mar. 3, 2004).

78. *Id.*

79. *See id.*

80. *Id.* (emphasis added).

81. *See About the Pop-up Blocker,* GOOGLE.COM, *at* http://toolbar.google.com/popup_help.html (last visited Nov. 20, 2003).

III. TRESPASS TO CHATTELS, EVOLUTIONS

Trespass to chattels is experiencing a rebirth in modern day policy via Internet advertising.[82] Commentators describe this tort as "a centuries-old . . . theory that languished for years in the dusty archives of obscure legal doctrines learned and then promptly forgotten in the first year of law school, which has unexpectedly found new life courtesy of the Internet."[83]

> Dubbed by Prosser [perhaps the foremost legal scholar on the subject of tort law], the 'little brother of conversion,' the tort of trespass to chattels allows recovery for interferences with possession of personal property 'not sufficiently important to be classed as conversion, and so to compel the defendant to pay the full value of the thing with which he has interfered.'[84]

Prosser gives an example of an early case "where the defendant merely interferes without doing any harm – as [w]here, for example, he merely lays hands upon the plaintiff's horse, or sits in his car. . . ."[85] While acknowledging a division among legal scholars, Prosser admits that "[b]y analogy to trespass to land there might be a technical tort in such a case. . . ."[86] This ancient tort is recognized as falling short of conversion, as in the examples above; however, "the defendant's interference must, to be actionable, have caused some injury to the chattel or to the *plaintiff's rights in it*."[87]

Under California law, trespass to chattels "lies where an intentional interference with the possession of personal property has proximately caused injury."[88] In cases of interference with possession of personal property not amounting to conversion, "the owner has a cause of action for trespass or case, and may recover only the actual damages suffered by reason of the impairment of the property or the loss of its use."[89]

Generally, in modern American law, "trespass remains as an occasional remedy for minor interferences, resulting in some damage, but not sufficiently serious or sufficiently important to amount to the greater

---

82. Tamara Loomis, *Internet Trespass: Companies Turn to an Old Tort for a New Reason*, 227 N.Y. LAW J. Jan. 10, 2002, at 5.

83. *Id.*

84. Intel Corp. v. Hamidi, 71 P.3d 296, 302 (Cal. 2003) (citations omitted).

85. *Id.* at 303.

86. PROSSER AND KEETON ON THE LAW OF TORTS § 14 (W. Page Keeton et. al. eds., 5th ed. 1984).

87. *Intel*, 71 P.3d at 302 (emphasis added).

88. Thrifty-Tel, Inc. v. Bezenek, 54 Cal. Rptr. 2d 468, 473 (1996).

89. Zaslow v. Kroenert, 176 P.2d 1, 7 (Cal. 1946) (emphasis added).

tort" of conversion.[90] Trespass to chattels was resurrected earlier in the twentieth century to combat the rise of junk faxes.[91] If the trend of Internet advertising continues, the tort may be called upon for what may become its greatest purpose yet: the elimination of unsolicited pop-up advertising on the Internet.

A. Internet Case Law

This section reviews the success of the tort of trespass to chattels in combating mass e-mail spam, highlights the failure of statutes in addressing the problems created by pop-ups, and suggests trespass to chattels might be the solution. In modern Internet law, several cases[92] have been essential in setting the stage for the fact that suddenly "[a]n arcane 18th century legal doctrine is . . . the darling of cyberspace."[93] These cases have laid out the principle that the same trespass rules that apply to land and personal property also apply to computer systems, considered chattel.[94] Similarly, these rules also apply to the electronic transmissions over the Internet from one computer to another.[95] Specifically, recent cases have focused on the requirement that, in order for electronic transmissions over the Internet to rise to the level of an actionable trespass, the rule "should not be extended to encompass an electronic communication that neither damages the recipient computer system nor impairs its functioning."[96]

The facts of the *Intel* case help to define the property, or chattel, in question in the tort of trespass to chattels in the internet age. In *Intel*, the e-mails themselves were not impairing the functioning of Intel's computer

90. PROSSER AND KEETON ON THE LAW OF TORTS *supra* note 86 (emphasis added).

91. *See* David E. Sorkin, *Unsolicited Commercial E-Mail and the Telephone Consumer Protection Act of 1991*, 45 BUFF. L. REV. 1001, 1018–19 (1997); *see also* 47 U.S.C. § 227 (2000). Restrictions on use of telephone equipment defines "unsolicited advertisement" as "any material advertising the commercial availability or quality of any property, goods or services which is transmitted to any person without that person's prior *express invitation* or permission." *Id.* § 227(a)(4) (emphasis added). *See generally* Kaufman v. ACS Systems, Inc., 2 Cal. Rptr. 3d 296 (2003); Chair King, Inc. v. GTE Mobilnet of Houston, Inc., No. 14-00-00711-CV, 2004 Tex. App. LEXIS 780 (14th Dist., Jan. 29, 2004) (comparing junk faxes to junk e-mail).

92. *See, e.g.*, Rowan v. United States Post Office Dep't, 397 U.S. 728, 737 (1970) (discussing trespass to chattels application to regular mail); Destination Ventures, Ltd. v. FCC, 844 F. Supp. 632 (1993) (discussing trespass to chattels application to junk faxes); CompuServe, Inc. v. Cyber Promotions, Inc. 962 F. Supp. 1015 (S.D. Ohio 1997) (discussing trespass to chattels application as a theory of email spammers' liability to Internet Service Providers).

93. *See* Loomis, *supra* note 82, at 5 (quoting attorney John Canoni).

94. *See CompuServe*, 962 F. Supp. 1015.

95. *See, e.g., Intel*, 71 P.3d 296.

96. *Id.* at 300.

system; in fact, the system was functioning perfectly.[97] Instead, the contents of the messages were found to cause an interference with the productivity of the company's workers, considered "chattel" by Intel, but not by the California Supreme Court.[98] The court reasoned that such communications were not actionable, stating that "[s]uch an electronic communication does not constitute an actionable trespass to personal property, i.e., the computer system, because it does not interfere with the possessor's use or possession of, or any other legally protected interest in, the personal property itself."[99] It is clear that many Internet pop-up ads do just what Hamidi's e-mails did not;[100] namely, they interfere with the Internet user's use of their personal property, i.e., their personal computers.[101]

One of the leading cases in Internet trespass to chattels is *eBay, Inc. v. Bidder's Edge, Inc.*[102] The case arose when Bidder's Edge, a company engaged in providing its customers with information regarding the prices of items in online auctions, began using Internet search "spiders"[103] to infiltrate eBay's website thousands of times per day.[104] Bidder's Edge "screen scraped"[105] the eBay website for pertinent auction information that they aggregated on their own site.[106] eBay demanded they stop and even blocked the Bidder's Edge IP address, but Bidder's Edge persisted.[107] Finally, eBay sued Bidder's Edge claiming trespass to chattels, citing eBay's degraded site performance due to the "spidering" of Bidder's Edge

97. *Id.* at 299.

98. *Id.* at 300.

99. *Id.*

100. *See generally* Register.com, Inc. v. Verio, Inc., No. 00-9596, 2004 U.S. App. LEXIS 1074 (2d Cir. 2004) [hereinafter *Register.com II*]. *See* discussion *infra* part IV. A. (showing situations where e-mail SPAM may be considered a trespass to chattels on different facts).

101. Internet user's use of their computers in a manner of their choosing, not subject to internet advertisers exercise of dominion over them, is a property right established in antiquity and reaffirmed in *Intel*. These pop-up ads interfere with the computer owners legally protected interest in the functioning of their personal computers which they have often spent considerable time and money purchasing and configuring to meet their personal and economic needs. *See* discussion *supra* note 63.

102. 100 F. Supp. 2d 1058 (N.D. Cal. 2000).

103. A spider is a program that automatically explores the web by retrieving some or all of the documents that are referenced in it. *See, e.g.,* DICTIONARY.COM, *at* http://dictionary.com/search?q=spider (last visited Mar. 3, 2004).

104. *eBay*, 100 F. Supp. 2d at 1062–63.

105. "A way of collecting data from a single mainframe screen." *See, e.g.,* NETLINGO.COM, *at* http://www.netlingo.com/lookupcfm?term=screen%20scraping (last visited Mar 28, 2004).

106. *eBay*, 100 F. Supp. 2d at 1062.

107. *Id.*

and the work that was required to block Bidder's Edge.[108] eBay eventually won an injunction against Bidder's Edge.[109]

The *eBay* case was crucial to promoting the theory that dispossession, or loss of use, of a section of computer space affecting the overall performance of the system is a trespass to chattel. The court rejected eBay's argument that the "spidering" and "screen scraping" techniques of Bidder's Edge were the equivalent of sending an army of hundreds of thousands of robots into a "brick-and-mortar"[110] establishment to check prices everyday.[111] Nevertheless, the court stated that the effects of multiple sites using the same techniques would be considered in its issuance of a temporary injunction.[112]

What occurred in *eBay* was revolutionary. Specifically, the court allowed the aggregation of damage, or degradation to system quality, to be established using not only specific data gathered as a result of eBay's actual experience with Bidder's Edge, but also *potential* damage that could occur if hundreds of other corporations and websites used similar tactics.[113] The court postulated that:

> Given that Bidder's Edge can be seen to have imposed a load of 1.53% on eBay's listing servers, simple arithmetic and economies reveal how only a few more such companies deploying rude robots [that do not respect the Robot Exclusion Standard] would be required before eBay would be brought to its knees by what would be then a debilitating load.[114]

In order for Hamidi's actions to fit under this interpretation, Intel would need to demonstrate that his messages slowed their servers and caused some loss of use of essential, measurable portions of their computer system, and, that in conjunction with other e-mail senders who were likely to be active, the messages would have affected the overall performance of their computer system.[115] That was not shown or argued in the *Intel* case, as Hamidi only sent six e-mail messages, to several thousand employees,

---

108. *Id.* at 1063.

109. *Id.* at 1073.

110. "Brick-and-mortar" is a name for a traditional business. *See e.g.*, NETLINGO.COM *at* http://www.netlingo.com/lookup.cfm?term=brick%2dand%2Dmortar (last visited Mar. 28, 2004).

111. *eBay*, 100 F. Supp. 2d at 1065–1066. The court said that the analogy to a brick and mortar store with hundreds of thousands of robots checking prices would only be accurate if the customers of the store could not see the robots, and they did not interfere with the customers directly. *Id.* at 1066.

112. *Id.* at 1071–72.

113. *Id.*

114. *Id.* at 1066 n.14.

115. *See generally Intel*, 71 P.3d 296.

over a two-year period.[116] The logic however, has far reaching implications for future Internet cases.

A second seminal case in the evolution of Internet jurisprudence is *Ticketmaster Corp. v. Tickets.com, Inc.*[117] In *Ticketmaster*, Ticketmaster brought an action in Federal District Court in the Central District of California seeking injunctive relief to prevent Tickets.com from using information retrieved from Ticketmaster's website by an automated computer system on Tickets.com's website.[118] The case was originally a copyright case that involved the theories of copyright infringement, and trespass to chattels.[119] The court adopted the reasoning of Judge Whyte's *eBay* decision, which applied trespass to chattels to an electronic communication:

> The computer is a piece of tangible personal property. It is operated by mysterious electronic impulses which did not exist when the law of trespass to chattels was developed, but the principles should not be too different. If the electronic impulses can do *damage to the computer or to its function* in a comparable way to taking a hammer to a piece of machinery, then it is no stretch to recognize that damage as trespass to chattels and provide a legal remedy for it.[120]

Here the court acknowledged several essential elements of the tort of trespass to chattels in the Internet age, recognizing the importance of allowing claims for damage to a computer, or to *its function*, by electronic impulses. While the court in *eBay* did not recognize that the elements of trespass to chattels applied to this set of facts,[121] there was no significant impairment or use of system resources by Tickets.com and there were also no threats of other websites committing the same acts that Tickets.com had engaged in, the court's reasoning was that trespass to chattels was indeed applicable to the transmission of electronic communications over the Internet.[122]

Another landmark case, cited by the court in *Intel*, is *CompuServe Inc.*

---

116. *Id.* at 299.

117. No. CV 99-7654-HLH (BQRx), 2000 U.S. Dist. LEXIS 12987 (C.D. Cal., Aug. 10, 2000).

118. *Id.* at **4–5.

119. *Id.*

120. *Id.* at **15–16 (emphasis added).

121. *See eBay*, 100 F. Supp. 2d 1058.

122. No. CV 99-7654-HLH (BQRx), 2000 U.S. Dist. LEXIS 12987 (C.D. Cal., Aug. 10, 2000) at **16–17; *see also eBay*, 100 F. Supp. 2d at 1071.

v. Cyber Promotions, Inc.[123] In *CompuServe*, Cyber Promotions was in the business of sending bulk unsolicited e-mail advertisements ("spam")[124] to the subscribers of CompuServe.[125] These actions resulted in complaints from CompuServe's customers who demanded a stop to the spam.[126] The customers found the spam to be annoying, and this generated considerable ill will towards CompuServe.[127] Accordingly, CompuServe attempted to implement security measures which would block the addresses of Cyber Promotions.[128] However, Cyber Promotions responded by falsifying point of origin information in their mailings, thereby allowing them to bypass CompuServe's security measures, implemented specifically to keep them out.[129] The court, using a definition of trespass to chattels similar to California's, concluded that the element of damage to the system could be met given the simple fact that:

> [t]o the extent that defendants' multitudinous electronic mailings *demand the disk space and drain the processing power* of plaintiff's computer equipment, those resources are not available to serve CompuServe subscribers. Therefore, the value of that equipment to CompuServe is diminished even though it is not physically damaged by defendants' conduct.[130]

The court further concluded that in addition to diminishing system's performance, subscribers suffered harm to a legally protected interest. The court held:

> [D]efendants' messages are largely unwanted by its subscribers, who pay incrementally to access their e-mail, read it, and discard it. Also, the receipt of a bundle of unsolicited messages at once can require the subscriber to sift through, at his expense, all of the messages in order to find the ones he wanted or expected to receive. These inconveniences decrease the utility of CompuServe's e-mail service and are the foremost subject in recent complaints from CompuServe subscribers. . . . Many subscribers have terminated their accounts specifically because

123. 962 F. Supp. 1015 (S.D. Ohio 1997).

124. *Id.* at 1017. In the vernacular of the Internet, unsolicited e-mail advertising is sometimes referred to pejoratively as "spam." This term is derived from a skit performed on the British television show Monty Python's Flying Circus, in which the word "spam" is repeated to the point of absurdity in a restaurant menu. *Id.* at 1018 n.1.

125. *Id.* at 1017.

126. *CompuServe Inc.*, 962 F. Supp. 1015.

127. *See id.* at 1023.

128. *Id.* at 1019.

129. *Id.*

130. *CompuServe Inc.*, 962 F. Supp. at 1022 (emphasis added).

> of the unwanted receipt of bulk e-mail messages (citations omitted). Defendants' intrusions into CompuServe's computer systems, insofar as they harm plaintiff's business reputation and goodwill with its customers, are actionable under Restatement § 218(d).[131]

This case served as the basis for many lawsuits and spawned new legislation regarding the proper use of the Internet and the proprietary value of business websites and computer systems.[132] However, the California court is somewhat unsure of this court's interpretation of what constitutes interference with an interest in personal property.[133]

In fact, the court in *Intel* cites *CompuServe* and makes a point of differentiating the economic injuries identified in *CompuServe* from the definition of trespass to chattels that the California court wishes to establish. [134] The court queries whether the opinion in *CompuServe* "properly considered injuries to the ISP's[135] *possessory* interest in its personal property, the type of property interest the tort is primarily intended to protect. . . ."[136] However, "[t]he court broke the chain between the trespass and the harm [by] allowing the indirect harms to CompuServe's business interests—reputation, customer goodwill, and employee time—to count as harms to the chattel (the server)."[137] According to the court, this decision "cut trespass to chattels free from its moorings of dispossession or the equivalent, allowing the court free reign [sic] to hunt for 'impairment.'"[138] But even if the loss of goodwill identified in *CompuServe* were the type of injury that would give rise to a trespass to

---

131. *Id.* at 1023.

132. *See generally* America Online v. IMS., 24 F. Supp. 2d 548 (E.D. Va. 1998) (discussing how courts may recognize unsolicited bulk emails as trespass to chattels); *See* In re America Online, Inc., 168 F. Supp. 2d 1359, 1364–65 (S.D. Fla. 2001); Douglas H. Hancock, *To What Extent Should Computer Related Crimes be the Subject of Specific Legislative Attention?*, 12 ALB. L.J. SCI. & TECH. 97, 111 n.83 (2001).

133. *Intel*, 71 P.3d at 307; *see also CompuServe*, 962 F. Supp. at 1023.

134. *Intel*, 71 P.3d at 307; *see also CompuServe*, 962 F. Supp. at 1023.

135. "An ISP [Internet Service Provider] is an entity that provides access to the Internet." some well known ISP's are: "America Online, UUNET and Juno." *Register.com II*, 2004 U.S. App. LEXIS 1074, *49 n.13 (2d. Cir 2004) (citations omitted). All people and entities that utilize Internet access subscribe to ISPs or are ISPs. Although the vast majority of ISP use is through some type of consumer ISP like AOL, primarily by individuals, "every Website, company, university, and government agency that utilizes Internet access also subscribes to an ISP or is one." In re DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 509 (S.D.N.Y. 2000).

136. *Intel*, 71 P.3d at 307 (emphasis added).

137. Laura Quilter, *The Continuing Expansion of Cyberspace Trespass to Chattels*, 17 BERKELEY TECH. L.J. 421, 429–30 (2002).

138. *Intel*, 71 P.3d at 307 (citing Dan L. Burk, *The Trouble with Trespass*, 4 J. SMALL & EMERGING BUS. L. 27, 35 (2000)).

chattels claim under California law, Intel's position would not follow for Intel's claimed injury has even less connection to its personal property than did CompuServe's.[139] In other words, CompuServe's customers were annoyed because the system was inundated with unsolicited commercial messages that made its use for personal communication more difficult and costly.[140] Their complaint, which allegedly led some to cancel their CompuServe service, was about the functioning of CompuServe's electronic mail service.[141] Thus there was a specific loss that could be accounted for, or revealed, in an investigation.[142]

In contrast, Intel's workers were distracted from their work because of the assertions and opinions the email messages conveyed, and not because of the *frequency* or *quantity* of Hamidi's messages.[143]

> Intel's complaint is thus about the *contents* of the messages rather than the *functioning* of the company's e-mail system. Even accepting CompuServe's economic injury rationale, therefore, Intel's position represents a further extension of the trespass to chattels tort, fictionally re-characterizing the allegedly injurious effect of a *communication's contents* on recipients as an *impairment to the device* which transmitted the message.[144]

The court reasoned that the *content* of the message could not affect the *functioning* of the computer system, which was the property at issue to which Hamidi allegedly trespassed.[145] Thus, it was established that the interference with the *functioning* of the system is the test, and not the *content* of the message.[146]

Thus, the modern requirement is that an electronic communication cause some sort of interference with dominion over the system in question.[147] Hamidi's actions fell short of this because it was not his use of the system to send e-mail, that is what the e-mail system was designed to do; but rather, the content of his message that caused the interference with the productivity of Intel's employees.[148] According to the California

139. *See Intel*, 71 P.3d at 307 n.6.
140. *CompuServe*, 962 F. Supp. at 1023.
141. *Id.*
142. *See id.*
143. *Intel*, 71 P.3d at 307.
144. *Id.* at 307–08.
145. *Id.*
146. *Id.* at 308.
147. *See id.* at 307–09.
148. *See Intel*, 71 P.3d at 308.

Supreme Court, the elements of trespass to chattels was not met, specifically, the loss of use, or dispossession elements of the tort.[149]

However, some would reason that "dispossession alone, without further damages, is actionable,"[150] but "other forms of interference require some additional harm to the personal property or the possessor's interests in it.[151] For example, while one may have no right temporarily to use another's personal property, such use is actionable as a trespass only if it 'has proximately caused injury.'"[152] Prosser explains this contingency by stating "[i]n the absence of any actual damage the action will not lie."[153] However, the Restatement, as cited by the California Supreme Court, goes on to say that *dispossession* in California is recognized as an injury.[154] "Short of dispossession, personal injury, or physical damage (not present here), intermeddling is actionable only if 'the chattel is impaired as to its condition, quality, or value, or . . . the possessor is deprived of the use of the chattel for a substantial time.'"[155] In particular, an actionable deprivation of use "must be for a time so substantial that it is possible to estimate the loss caused thereby. A mere momentary or theoretical deprivation of use is not sufficient unless there is a dispossession. . . ."[156] Therefore, it was not sufficient that Hamidi's messages temporarily used some portion of Intel's processors or storage. Rather, Intel should have demonstrated some measurable loss caused by Hamidi's use of its computer system, but it did not.[157]

This is where the revolutionary analysis of the California court is fully revealed. The court discussed prior case law where dispossession or loss of use was a significant issue.[158] These cases often resulted in a judgment for plaintiffs or in a finding of trespass to chattels.[159] The court enumerated several factors that they would consider crucial in determining if a certain action is considered a trespass to chattels.[160] Namely, that there

149. *See id.*

150. *See id.* at 306 (citing RESTATEMENT (SECOND) OF TORTS § 218 cmt. d (1965)).

151. *Id.* at 306.

152. *Thrifty-Tel*, 54 Cal. Rptr. 2d at 473.

153. *Intel*, 72 P.3d at 306 (citing W. PAGE KEETON et al., PROSSER AND KEETON ON THE LAW OF TORTS §14 (West Publishing Co. 1984)).

154. *Id.*

155. *Id.*

156. *Id.*

157. *See id.* at 306–07.

158. *See Intel*, 71 P.3d at 304–06.

159. *See id.* at 304–06 (citations omitted).

160. *See generally id.* 306–07.

must be some measurable loss or dispossession.[161] This conclusion by the California court made sense, as the court has chosen to focus on the proprietary nature of the tort, and has shown an inclination to recognize future claims which allege and prove dispossession or interference with the use of a computer system.[162]

Perhaps the case that most effectively reveals the application of this theory developed by the California court is the Second Circuit Court of Appeals decision in *Register.com, Inc. v. Verio, Inc.*.[163] Plaintiff, Register.com, is a company involved in the business of registering domain names and also provides web-site development services. The defendant, Verio, is engaged in the business of selling web site design, development, and operation services in competition with some elements of Register.com's website development business. Verio, in an effort to target Register.com's customer base, used Register.com's customer lists acquired through the use of an automated software search program, to target advertisements to Register.com's customers in a manner which led to confusion as to the source of the advertisements. In granting Register.com's motion for a preliminary injunction against Verio:

> The court's order enjoined Verio from (1) using Register's trademarks; (2) representing or otherwise suggesting to third parties that Verio's services have the sponsorship, endorsement, or approval of Register; *(3) accessing Register's computers by use of automated software programs performing multiple successive queries*; and (4) using data obtained from Register's database of contact information of registrants of Internet domain names to solicit the registrants for the sale of website development services by electronic mail, telephone calls, or direct mail. We affirm.[164]

While all four elements potentially impact future litigation involving Internet pop-ups, for the purpose of this section, the focus will remain on the third item of the injunction.

In his discussion affirming the grant of temporary injunction by the District court, Judge Leval focused on the claim of trespass to chattels.[165] The court left undisturbed the district court's determination that allowed the aggregation of potential third party spammers as addressed in the *eBay*

161. *Id.* at 306.

162. *Id.*

163. 2004 U.S. App. LEXIS 1074 (2d. Cir. 2004).

164. *Id.* at *2 (emphasis added).

165. *See id.* at **30–31.

decision.[166] In addition, the court found that "Verio likely committed a trespass by using a search robot to access Register.com's computer systems without authorization to do so, consuming the computer systems' capacity. . . . [In doing so] Verio could interfere with Register.com's use of its own systems."[167] The court recognizes *Intel's* contribution to the jurisprudence of this emerging area of law and cites it as a case that "breathed new life into the common law cause of action for trespass to chattels by finding it viable online."[168] This court also found, using a definition of trespass to chattels similar to that used in *Intel*,[169] that "[a]lthough Register.com was unable to directly measure the amount by which its systems capacity was reduced, the record evidence [was] sufficient to establish the possessory interference necessary to establish a trespass to chattels claim."[170] In recognizing the possessory interest element of the tort, and at the same time stating that the interest did not have to be connected to an aggregation of other outside influences, the *Register.com* ruling went beyond the *eBay* decision, which it cites.[171]

166. *Id.* at **31–32. "Verio's use of search robots, consisting of software programs performing multiple automated successive queries, consumed a significant portion of the capacity of Register.com's ("Register") computer systems." *Id.* at *31. The court agreed that even though Verio's robots alone would not incapacitate Register's systems, if Verio continued to access Register's systems through such robots, it was "highly probable" that other ISP's would devise similar programs, access Register's data, and cause Register's system to be overtaxed and crash. *Id.*; *see also eBay*, 100 F. Supp. at 1066.

167. Register.com Inc. v. Verio, Inc., 2004 U.S. App. LEXIS 1074, **130–31 (2d Cir. 2004). The courts view of "chattel" in this instance, and in instances of similar computer related trespasses, is in their opinion at n55: "To be clear, the chattels in question are Register.com's computer systems, and the alleged trespass is Verio's intentional, unauthorized consumption of the capacity of those systems to handle, process and respond to queries." The court found that system capacity itself was not a chattel "possessed" by Register.com or those that used its systems. "Rather, 'capacity' describes the amount of use (or potential use) that a resource can sustain." Several examples given by the court were "the data processing potential of a computer system, the data storage potential of a computer system, and/or the information carrying potential of telecommunications facilities." *Id.* at *127 n.55 (citations omitted).

168. *Id.* at *125.

169. *Id* at *128 (quoting RESTATEMENT SECOND OF TORTS, § 256 (1965)). "One who uses a chattel with the consent of another is subject to liability in trespass for any harm to the chattel which is caused by or occurs in the course of any use exceeding the consent, even though such use is not a conversion." *Id.*

170. *Register.com Inc.*, 126 F. Supp. 2d 238, 250. "Although Register.com's evidence of any burden or harm to its computer system caused by the successive queries performed by search robots is imprecise, evidence of mere possessory interference is sufficient to demonstrate the quantum of harm necessary to establish a claim for trespass to chattels." It is sufficient that "the trespass diminishes the condition, quality, or value of personal property." *Id.* (citing *eBay*, 100 F. Supp. 2d at 1058, 1071. "The quality or value of personal property may be 'diminished even though it is not physically damaged by defendant's conduct.'" *Id.* "Verio does not dispute that its search robot occupies some of Register.com's systems capacity." *Id.*

171. *Register.com Inc.*, 126 F. Supp. 2d 238.

Moreover, this decision recognized the legitimacy of the application of trespass to chattels claims to non-aggregation scenarios.[172] Citing the *eBay* decision for the principle that any use of another's system is actionable as a trespass,[173] even if "negligible," the court continued to uphold the trespass to chattels theory for electronic trespasses, indicating that even if there is not the threat of others reproducing the harmful action, a trespass to chattels claim will still hold.[174]

After the Court's ruling in the *Intel* case and the upholding of the injunction in *Register.com*, courts may well recognize a cause of action for dispossession of a computer by pop-up ads. The ads, in effect, dispossess users of the use of their computers for a short time period and may impair the functioning of those computers.[175] This reasoning also follows the analysis developed in *eBay*, and adopted by *Intel* and *Register.com*, where the realities of thousands of Internet search "spiders" caused the dispossession of portions of the company's computer system for thousands of short, but measurable, periods of time.[176] In totality, the aggregate amount of lost computer time to the company resulted in trespass to chattels. Similarly, Internet pop-ups cause the dispossession of the computer for thousands of short, but measurable, periods of time. In totality, the aggregate amount of time lost to the user should, by this logic, also result in a trespass to chattels. However, even if there is no aggregation of undefined third parties the court in *eBay* as cited in *Register.com* allows for a claim for trespass to chattels without a showing of potential aggregation of trespassers.[177]

---

172. *See id.*

173. *See id.* at 250.

174. *Id.* (citations omitted). Bidders Edge ("BE") argued its searches presented "a negligible load on plaintiff's computer systems," and did not "rise to the level of impairment to the condition or value of eBay's computer system required to consitute [sic] a trespass." However, that ignored the fact that "eBay's server and its capacity are personal property, and that BE's searches use a portion of this property." So even if BE's searches used only use a small amount of eBay's computer capacity, BE "nonetheless deprived eBay of the ability to use that portion of its personal property for its own purposes. The law recognizes no such right to use another's personal property." *Id.* The court then held that BE's actions appeared to have caused injury and would likely continue to cause injury to eBay. *Id.* (citations omitted).

175. *See* MARKETINGTERMS.COM, *at* http://www.marketingterms.com/dictionary/pop_up_ad (last visited Mar. 3, 2004); McWilliams, *supra* note 40 (stating that users complain of system crashes and lock-ups caused by pop-ups).

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

177. *See Register.com I*, 126 F. Supp 2d at 250.

B. The Failure of Modern Statutory Law

In the search for ways to protect their online properties, large Internet corporations have favored wielding the common law to protect their online business interests. "[T]he common law concept of *Trespass to Chattels* . . . is now being used by companies to protect themselves from aggressive screen scrapers and users who use web services not in accordance with use policies."[178] Many of the modern cases discussed by the court in *Intel* were connected by the fact that the parties involved were large Internet companies that were being exploited by other large Internet companies.[179] The question that arises is whether or not the present state of Internet law will allow for private individuals to use these causes of action or class actions in order to defeat pop-ups.

Since its inception, the Internet has not easily been classified, and the bodies of law used to regulate access to computer systems have varied tremendously.[180] Legislation such as the Digital Millennium Copyright Act (DCMA) has been introduced to bring law to what was once lawless cyberspace.[181]

The DMCA provides two sections relating to online devices designed to prevent pop-ups and other forms of spamming. First, the DMCA provides that "[i]t is illegal for a person/campany [sic] to circumvent technical protection measures," such as those designed to prevent spammers from practicing their trade on a given system.[182] Second, it provides that "[i]t is illegal to traffic in devices/tools that circumvent protection measures."[183]

The case of *Lexmark Int'l, Inc. v. Static Control Components, Inc.*,[184] exemplifies a scenario in which the DMCA affected unconventional areas of technology. In that case, Lexmark, a computer printer manufacturer, brought an action against Static Control Components (SCC) for copyright infringement.[185] Apparently, Lexmark embeds a *depleted* flag[186] into each

178. Robert Kaye, *ETech: Laws and Emerging Technology*, *at* http://www.oreillynet.com/pub/wlg/3083 (last posted Apr. 22, 2003).

179. *See generally CompuServe*, 962 F. Supp. 2d at 1015; Hotmail Corp. v. Van$ Money Pie Inc., 1998 U.S. Dist. LEXIS 10729, at *7; *America Online, Inc.*, 24 F. Supp. 2d at 548. (Both plaintiff and defendants in these cases were well established Internet corporations.).

180. *See generally* Kaye, *supra* note 178 (discussing copyright, DCMA, and Trespass to Chattels, as different approaches to the regulation of the Internet).

181. *See* Kaye, *supra* note 178.

182. *See* Kaye, *supra* note 178.

183. *See* Kaye, *supra* note 178.

184. 253 F. Supp. 2d 943 (E.D. Ky. 2003).

185. *Id.* at 946–47.

printer cartridge, and when the printer cartridge runs low on ink, the depleted flag in the cartridge is triggered.[187] When such cartridge is refilled, and reinserted into the printer, by a company such as SCC, rather than replaced by a new cartridge, "the printer will refuse to print since the cartridge is marked as depleted.[188] Author Robert Kaye describes the steps SCC took to circumvent the code:

> To get around this, [S]CC started replacing the chips with fresh new chips that didn't have their depleted flag set. And by doing this they committed a copyright violation. Huh? Copyright violation? It turns out that the Lexmark folks had the lawyers involved from day one and they in turn got the engineers to design the print heads so that the print head would actually download required firmware in order to start printing. By inserting a [S]CC cartridge, proprietary code from the printer was copied onto a non-Lexmark component, thus creating a copyright violation. Lexmark was granted an injunction against [S]CC creating printer cartridges for Lexmark printers.[189]

Website owners facing unauthorized system use and online systems exploitation have turned to alternative legal theories and remedies—including copyright and contract law—in order to protect their intellectual property.[190] However, neither copyright law nor other forms of common law (other than property) provide adequate protections for website owners and operators.[191] For example, I. Trotter Hardy notes:

> Copyright law might seem the more obvious way to establish "rights" over one's own Website, since copyrightable information is often at issue. But copyright law suffers from several disadvantages. First, it seems a stretch of reasoning to make copyright apply to a "visit" to a Website. Copyright, after all, is most at home with multiple reproductions or performances of individual works of authorship—not with Web reading and

186. A "depleted flag" is a device in used in printing software that informs the user if their ink is low by reading a "flag" embedded in a computer chip on the physical ink cartridge that indicates that the cartridge is depleted of ink. "If the user has a depleted cartridge refilled and reinserted into the printer, the printer will refuse to print since the cartridge is marked (flagged) as depleted." *See generally* Kaye, *supra* note 178.

187. Kaye, *supra* note 178.

188. *Id.*

189. *Id.*

190. *See generally* I. Trotter Hardy, *The Ancient Doctrine of Trespass to Web Sites*, 1996 J. ONLINE L. ART. 7 *at* http://warthog.cc.wm.edu/law/publications/jol/95_96/hardy.html (last visited Mar. 3, 2004) (discussing various property theories applied to websites).

191. *See id.* ¶ 6.

> browsing. Viewed afresh, without knowledge of current case law, a trespass action is actually a more straightforward and intuitively sensible means of controlling access to "sites" than is a copyright one. [192]

As a result, as more threats have emerged to computer systems, companies and individuals have come up with creative ways to manage their websites, and lawyers have honed cunning legal tools to deal with new and previously unimaginable threats.[193]

Several lawsuits have been filed in relation to Internet advertising, mainly in the arena of e-mail spam.[194] However, two recent cases have addressed Internet pop-up advertisements in particular.[195] Uhaul and Wells Fargo have both recently been denied injunctive relief against WhenU.com, the makers of SaveNow software, for alleged copyright and trademark infringement.[196] The companies sought injunctive relief to prevent SaveNow from downloading protected information from their respective sites in order to display advertising to Internet users.[197] These cases, in which the courts denied relief, demonstrate that pop-up ads create such a negative impact that large corporations are compelled to take action.[198]

In addition to the aforementioned lawsuits, many corporations and Internet users have looked to government agencies for some relief.[199] In fact, Google.com, one of the most visited Internet websites[200], provides a link to the Federal Trade Commission's (FTC) website. The Google site suggests that users report web advertisers who abuse the "back doors" contained in some software programs in order to create unstoppable pop-ups.[201] While the FTC has recently begun to enforce the "do not call list,"[202] current legal challenges could delay full enforcement of the do not

---

192. *Id.* ¶ 54.

193. *See generally id.* (discussing evolving trends regarding trespass to websites).

194. *See, e.g., CompuServe*, 962 F. Supp. 1015; Hotmail Corp. v. Van$ Money Pie Inc., 1998 U.S. Dist. LEXIS 10729; *America Online*, 24 F. Supp. 2d 548.

195. Wells Fargo & Co. v. WhenU.com, Inc., 293 F. Supp. 2d 734 (E.D. Mich. 2003); U-Haul Int'l, Inc. v. WhenU.com, Inc., 279 F. Supp. 2d 723 (E.D. Va. 2003).

196. *Wells Fargo & Co.*, 293 F. Supp. 2d 734; *U-Haul Int'l, Inc.*, 279 F. Supp. 2d 723; *see also* discussion *supra* Part II.A.

197. *See Wells Fargo & Co.*, 293 F. Supp. 2d at 736; *U-Haul Int'l Inc.*, 279 F. Supp. at 725.

198. *See Wells Fargo & Co.*, 293 F. Supp. 2d at 736; *U-Haul Int'l Inc.*, 279 F. Supp. at 725.

199. *See Wells Fargo & Co.*, 293 F. Supp. 2d 734; *see also U-Haul Int'l, Inc.*, 279 F. Supp. 2d 723.

200. *See About the Pop-up Blocker*, GOOGLE.COM, *at* http://toolbar.google.com/popup_help.html (last visited Mar. 3, 2004).

201. *Id.* "To file a complaint, visit: http://www.ftc.gov and click on 'File a Complaint Online.' http://ftc.gov." *Id.*

202. *See* FTC v. Mainstream Mktg. Servs., Inc., 345 F.3d 850, 851 (10th Cir. 2003).

call measure for some time.[203] Therefore, it seems unlikely that the FTC will be able to effectively combat Internet spammers anytime soon. Moreover, it is only as recently as this year that the Senate has begun to recognize and deploy the CAN-Spam Act, to address the e-mail spam problems that have existed for years, providing further evidence that full enforcement of existing measures may be delayed.[204] The CAN-Spam act is described as:

> [A] bill . . . which recently passed the Senate 97-0, and is awaiting a vote in the House. It would enforce certain etiquette (e-mailers must be truthful in subject lines and honor remove requests) and lay the groundwork for the creation of a Do Not Spam list similar to the Do Not Call list. It would also allow ISPs, states and the Federal Trade Commission (but not individuals) to sue spammers.[205]

Given the delays discussed above, is it realistic for Internet users to rely on Congress to act on the issue of pop-up advertising? It seems particularly important to explore alternative solutions, such as tort law, since federal spam legislation, which offers only corporate, not private, actions, may preempt state legislation.[206]

IV. FINALLY, THE CAUSE OF ACTION I'VE BEEN LOOKING FOR

Many Internet users have been looking for the silver bullet in the fight against intrusive and system performance degrading forms of Internet advertising. Whether it is spam, junk faxes, or telemarketing; companies and individuals have been searching for years for a cause of action to invoke against unruly and unscrupulous advertisers.[207] In the case of an Internet pop-up, the user arguably indeed suffers a dispossession or loss of use similar to those recognized by the courts in *Intel*, *CompuServe*, *eBay*, and *Register.com*. Under the reasoning of the *Intel* court, such

---

203. *See, e.g., id.* 860–61 (staying enforcement of an order from the District Court permanently enjoining it from implementing the national do not call list).

204. Brad Stone, *Soaking in Spam*, NEWSWEEK, Nov. 24, 2003 *available at* http://msnbc.msn.com/*id*/3474984/ (last visited Mar. 3, 2004).

205. *Id.*

206. *See id.*

207. *See, e.g.*, Rowan v. United States Post Office Dep't, 397 U.S. 728, 737 (1970) (discussing trespass to chattels application to regular mail); Destination Ventures, Ltd. v. FCC, 844 F. Supp. 632 (1993) (discussing trespass to chattels application to junk faxes); CompuServe, Inc. v. Cyber Promotions, Inc. 962 F. Supp. 1015 (S.D. Ohio 1997) (discussing trespass to chattels application as a theory of email spammers' liability to Internet Service Providers); Chair King, Inc. v. GTE Mobilnet of Houston, Inc., No. 14-00-00711-CV, 2004 Tex. App. LEXIS 780 (14th Dist., Jan. 29, 2004) (comparing junk e-mail to junk faxes).

dispossession or loss of use would constitute an actionable trespass to chattels.[208]

Internet pop-ups present a plausible trespass to chattel claim under the *Intel* standard, as the advertiser "hijacks" the user's system, causing momentary dispossession which results in slower system performance. On its face, Internet pop-up software may appear to fall into the content-oriented approach of Plaintiff Intel, in that, the content of the e-mail messages was the central issue.[209] However, with Internet pop-ups, the functioning of the ad itself creates the problem for many users.[210] These background programs run in conjunction with the programs that the user is intentionally using, and leads to both slowing of Internet access and, in some circumstances, causes the system to crash.[211]

It seems that the present state of the law, as stated in *Intel*, will provide Internet users with a cause of action against such insidious acts. The *Intel* court indicated that to obtain relief, Internet users must prove that their computer systems were either "damaged", or, more importantly, that "functioning was impaired."[212] Even WhenU.com, the makers of SaveNow software, admits that some "sustained CPU usage"[213] occurs during the functioning of the program.[214] If that program were accidentally downloaded or hidden in a package of "free" software, this sustained CPU usage could cause extensive impairment of the computer's functioning.[215] According to the court in *Register.com*, proof of damage to the computer system is not altogether necessary.[216] However, for the purposes of this section, assume that damages would be greater not only if the user is dispossessed of the system for a period of time, but also if the functioning

208. *See generally* Intel Corp. v. Hamidi, 71 P.3d 296 (Cal. 2003); eBay Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058 (N.D. Cal. 2000); CompuServe v. Cyber Promotions, Inc., 962 F. Supp. 1015 (S.D. Ohio 1997); Register.com, Inc. v. Verio, Inc., 2004 U.S. App. LEXIS 1074 (2d Cir. 2004); *see also* discussion of properties of pop-up ads *supra* Part II. (Revealing pop-up ads meet all of the criteria of trespass to chattels discussed in these cases).

209. *See* Intel Corp. v. Hamidi, 71 P.3d 296 (Cal. 2003).

210. *See id.* at 300–01.

211. *See generally* WHENU.COM, *supra* note 42 (discussing the principle that pop-ups created by certain programs cause sustained CPU usage by the pop-up program).

212. *Intel*, 71 P.3d at 296.

213. *See* WHENU.COM, *supra* note 42 ("Users have noted that the program contacts our servers every once in a while, it does so in order to retrieve content from us and store that content on your computer and make it available to you at the right moment. There is one daily communication sent just to let us know that the software is functioning—nothing more (i.e. no collection of browsing history, etc). The desktop application checks for the presence of new browser windows every 3 seconds, which results in sustained (but very low) CPU usage.").

214. *Id.*

215. *See id.*

216. *See Register.com*, 126 F. Supp. 2d at 250.

of the chattel is impaired.

Take for example a hypothetical situation: working from home or telecommuting. One of the great advances that allowed many tech employees to work from home was the rise of a functioning Internet and email system. Today some employees do not need to go to an office on a regular basis, and many offices are only able to be productive when they have Internet access. Perhaps the cause of action for trespass to chattels is most clearly applied to someone who uses the Internet and a personal computer as their source of income, such as a three dimensional (3D) graphic designer or animator.[217] 3D designers often use high-speed computers with massive computing power to build 3D models on their computers.[218] These models can then be made into print advertisements, television commercials, web based commercials, or to create special effects using techniques such as "green screening."[219]

At any given time, a 3D graphic designer or animator is online and using a great deal of their computing power in one way or another.[220] Often ideas for their projects are garnered from trips to various websites, and it is likely that they will submit story-boards, first drafts, and even their final projects online over a high speed connection.[221]

After a 3D designer takes a break to surf the web, and returns to their work, often the tedious process of "rendering"[222] their final products, every last megahertz of processing power, memory, and hard drive space is utilized, in fact desperately needed, to complete their projects.[223] After working for weeks designing and building models, the render is often the

217. Also consider an Internet day trader who makes trades of stock and securities over the internet. It takes very little imagination to see how one Internet pop-up at the crucial moment of stock trade execution could lead to dire financial consequences. Missing an opportunity to buy or sell a stock at a particular price and a particular moment is irreplaceable. This could be especially damaging if the pop-up also contains spyware and downloads the confidential financial information of the trader.

218. Interview with Blake Robertson, graphics producer, Zoic Studios in Los Angeles, CA (Nov. 17, 2003).

219. Green Screening is a process used to combine together two or more images. Perhaps best known originally as "blue screen" used in weather broadcasts, and now for special effects in film and television, green screening and "blue screening [work] by placing an actor or image in front of a blue screen, applying a mask to identify the picture's blue elements, and replacing them with another image... [G]reen and red [screening] are used also." WEBOPEDIA, *at* http://www.webopedia.com/TERM/B/blue_screen.html (last visited April 2, 2004).

220. Interview with Blake Robertson, *supra* note 218.

221. *Id.*

222. Rendering is defined as "convert[ing] (graphics) from a file into a visual form, as on video display." DICTIONARY.COM, *at* http://dictionary.reference.com/search?q=rendering (last visited Mar. 5, 2004).

223. Interview with Blake Robertson, *supra* note 218.

final element required to complete a project that may have taken weeks, months, or years to finish.[224] The strain on an individual computer system is such that often machines are linked to each other to help the artist finish their project in the most efficient manner possible.[225] The Internet connection is used to download and upload the projects onto their destination servers.[226] A pop-up delivered during this time could have an utterly devastating effect. As the adware program contacts its server using valuable computer resources, the resulting system crash could lead to massive amounts of data, and time spent working on the project, often billed in excess of $300 per hour, to vanish. When a system crashes during one of these renders, hours of time are lost, and the data which the artist was working on becomes corrupted,[227] damaging the primary function of the computer (to process visual images for the artist's livelihood). At the very least, these usages of computer system resources fall directly into the "system performance" element of the test developed by the court in *Intel*.[228] Damages in a case like this would not be speculative, as the amount of hours of lost use, degraded performance, and damaged disk-space could be related to the hours it takes to fix the project, or the full value of the thing with which the tortfeasor has interfered; either the computer or the data itself.[229] If the charge is for lost hours, then the tortfeasor would surely be liable for damages.[230] However, paying the full value of the entire computer system or an entire design product could reach into tens, if not hundreds, of thousands of dollars.[231]

If you are a pop-up advertiser, hopefully that got your attention. The work that is taking place on these machines is often time-sensitive (such as an opening graphic for the Super Bowl) and would result in horrendous damages to any design company who had "computer problems" that led to the destruction of their company's product. In theory, the California Supreme Court, under their analysis in *Intel*, could legally recognize the aforementioned scenario as interference by an electronic communication that *damages* the recipient computer system and *impairs its functioning*. Such an electronic communication seems to fit the definition of an

224. *Id.*

225. *Id.*

226. *Id.*

227. *Id.*

228. *See Intel*, 71 P.3d at 305.

229. *See eBay*, 100 F. Supp. 2d 1058; *see also* PROSSER AND KEETON ON THE LAW OF TORTS § 14 (W. Page Keeton et. al. 5th ed. 1984).

230. *See eBay*, 100 F. Supp. 2d 1058; *see also* PROSSER AND KEETON ON THE LAW OF TORTS § 14 (W. Page Keeton et. al., 5th ed. 1984).

231. Interview with Blake Robertson, *supra* note 218.

actionable trespass to personal property, i.e., the computer system, because it *interferes with the possessor's use*, a legally protected interest in, *the personal property itself*, in this case the computer system.[232]

Calculating damages in such a situation could be a point of contention, as the *Intel* case does not fully address how damages should be assessed.[233] However, the above reasoning was adopted from the reasoning espoused by Prosser and the court in *eBay*,[234] where the court allowed injunctive relief based on the fact that some measurable interference had occurred.[235] Even if Internet pop-up advertisers would not be liable for the damages that occur as the result of the above scenario, they would perhaps be subject to injunctions prohibiting them from sending advertisements to computer systems that would be damaged as a result. The court in *eBay* granted injunctive relief based on the fact that system performance would be affected drastically if others took action similar to Bidder's Edge.[236] However, it is not known if the California Supreme Court would also issue an injunction for a similar set of facts relating to Internet pop-ups.

Another possible difficulty in collecting damages in an action such as this would be tracking down the company that sent a user the actual pop-up that damaged his or her computer system. As many companies send out software that produces pop-ups, it could be relatively difficult to show which program or which ad was the true cause of the system problem. In addition, another question arises as to whether or not the California court will recognize a cause of action for trespass to chattels involving repeated minor effects to general system performance. Under the analysis of *eBay*, these small disruptions to complete control over a computer system, when multiplied by the hundreds or thousands of possible advertisers, would aggregate into a recognizable effect on system performance and result in the issuance of a protective injunction.[237] A question also arises if the court would allow a private non-commercial user to sue an advertiser for the hundreds of seconds each day spent closing pop-ups, slower download times, and the sheer annoyance of the entire process, or if the court would instead conclude that these were the result of a properly functioning

232. *See id.*; *see also* Zaslow v. Kroenert, 29 Cal. 2d 541, 551 (1946); Ticketmaster Corp. v. Tickets.com, Inc., No. CV99-7654-HLH (BQRx), 2000 U.S. Dist. LEXIS 12987, at **14–16 (C.D. Cal. Aug. 10, 2000); RESTATEMENT (SECOND) OF TORTS § 218 (1965).

233. *See generally*, 71 P.3d 296. (In this case no damages were awarded as the defendant did not commit trespass to chattels.).

234. *See eBay*, 100 F. Supp. 2d at 1070.

235. *Id.* at 1072.

236. *See id.* at 1072–73.

237. *Id.*

machine that was just displaying things that were annoying only because the user happened to object to their content.

The court in *Intel* focused on the fact that it was the content of the messages that Intel truly objected to and not the effect of the e-mail on their chattel (computer system).[238] Pop-ups are different because not only do they sometimes contain ads for things such as bestiality or pornographic materials (objectionable content which is not a trespass to chattels), they also slow and impair system performance, cause the user to perform actions to regain control of their machine (exercise dominion over the chattel), and may cause user's systems to crash (damage to the system). There are likely to be hundreds more advertisers in the future performing similar acts of unwanted and unrequested advertising, using the user's own computer against their wishes.

Even if one only uses his or her computer for entertainment, or non-business e-mail, this tort could still function as a form of relief under this standard, as it is not related to a monetary loss but instead a loss of control over, damage to, impairment of, or the loss of the functioning of a computer system.[239] While the use of this tort speaks to the positive elements of attempting to use the common law as a form of relief from Internet pop-up ad attacks, there are many questions that remain unanswered and will likely remain unanswered until tested in the real world.[240]

---

238. *See Intel*, 71 P.3d at 307.

239. *See supra* Part III.A.

240. *See* Michelle Delio, *Students Toil as Spyware Hunters*, WIRED NEWS, Oct. 6, 2003 *at* http://www.wired.com/news/infostructure/0,1377,60694,00.html (for example of future litigation).

> Outraged by the damage inflicted by a fast-spreading spyware application, a pair of high school students team up to fight back. Jay Cross Jr. and Christopher Carlino, two high school seniors from Stamford, Connecticut, are determined to track down the creators of Xupiter spyware software and take them to court. Carlino and Cross recently signed on as participants in a pending class action suit against Xupiter, joining thousands of other disgruntled users whose machines were vandalized by the spyware. . . . 'In the greater scheme of things Xupiter may not seem like a big deal, but we believe that people should care about the little everyday injustices,' said Cross. 'Little problems can quickly turn into big issues.' Not that anyone who has had the misfortune of meeting Xupiter would classify it as a little problem. Xupiter attaches itself to Internet Explorer's toolbar. Once active in a system, it periodically changes users' designated homepages to Xupiter.com, redirects all searches to Xupiter's site, and blocks any attempts to restore the original browser settings. Xupiter also attempts to download updates each time an affected computer boots up, and has been blamed for causing system crashes. Several versions of Xupiter appear to download other programs, such as gambling games, which later appear in pop-up windows. Xupiter arrives in some peer-to-peer programs, and is also offered for download from an ever-changing array of websites. But a significant number of users claim they never gave permission before the application was installed on their machines. And the program doesn't allow itself to be easily

Recent legislative activity regarding the regulation of the Internet has been the cause of some concern. There is the threat of legislation that would prohibit a private cause of action in cases involving some electronic communications. The FCC and FTC have recently been involved in creating such legislation in the US Congress for SPAM e-mail.[241] If this important tort is subjugated to rule of the United States Congress it is unlikely that future discoveries of loopholes in the law by unscrupulous advertisers could be closed as easily as they will be discovered. The fluidity of the common law, reflected in its resilience and persistent relevance over hundreds of years, could be the perfect weapon against threats that have evolved so quickly over the last few years and presented a threat to the timeless values that tort law embodies and protects.

V. CONCLUSION

An action for trespass to chattels could be the solution to the pop-up problem. Lawsuits by individual Internet users and class actions brought by graphic designers, day-traders or disgruntled Internet users tired of paying fifty dollars a month for a high speed Internet connection that only sends pop-ups faster, could bring the pop-up industry to its knees. Those that have simply had enough of pop-ups' intrusive and destructive nature could find a remedy in this ancient tort as redefined for the Internet age by the California Supreme Court and adopted by the Second Circuit.[242]

> uninstalled. As of late last month Xupiter.com, the spyware's mother ship, appeared to be inactive. But various mutations of Xupiter, lurking on sites such as xjupiter.com and orbitexplorer.com, continue to infest the computers of unwary users, as does Xupiter itself. 'Both of us became infected with Xupiter about a year or so ago,' said Carlino. 'We neither agreed to nor authorized an installation of this software; we just found it on our PCs. We were furious and frustrated. After trying for hours to manually delete Xupiter—a difficult task for even PC experts—we turned to Web forums for advice.' At one forum they found out how to pluck Xupiter from their computers and heard about the pending class action suit. They quickly signed on as participants and volunteered to do research in order to reduce legal costs. 'Judging by the 25,000-some odd posts on SpywareInfo alone, I'd say quite a few people are pretty ticked off about Xupiter,' said Cross. 'And we've been told that hundreds of people every week want to get in on the lawsuit.' The suit participants are now looking for a legal firm to represent them, and expect to file the suit within a week.

Id.

241. *See generally* Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, 15 U.S.C. § 7701 (2003) (regulating interstate commerce by enacting penalties and liabilities on unsolicited commercial e-mail delivered via the Internet).

242. *See generally* Intel Corp. v. Hamidi, 71 P.3d 296 (Cal. 2003); Register.com, Inc. v. Verio, Inc., 2004 U.S. App. LEXIS 1074 (2d Cir. 2004) (applying the tort of trespass to chattels to computer systems).

* This comment is dedicated to my family: Mom, Ali, Sean, Dad, Diane, and Kristi. Thank you all for your love and support over the years. Dad, thank you especially for your suggestions

Adware proponents, Spyware smugglers, and pop-up advertisers beware: the law is coming, and pop-up advertising could soon become much more expensive.

*Geoffrey D. Wilson**

and perspective on this work. Ali thank you especially for your editorial contributions to this piece and others. Thank you also to Emily Ayers, and the editors and staff writers of the Loyola of Los Angeles Entertainment Law Review that sacrificed their Saturdays and more. Special thanks to Lenore Schreiber, Esq. of Fresno, California for your mentorship and for encouraging me to read the California Supreme Court case from which my topic originated.