1-1-2010

Protecting Consumers From Spyware: A Proposed Consumer Digital Trespass Act

Richard G. Kunkel J.D.
University of St. Thomas, Minnesota, rgkunkel@stthomas.edu

Protecting Consumers From Spyware: A Proposed Consumer Digital Trespass Act

by
Richard G. Kunkel

We live in an online world. Nearly two billion people worldwide are Internet users.[1] There are an estimated 239 million Internet users in the United States, which means over seventy-seven percent of Americans are Internet users.[2] Internet use in the United States rose by 146 percent from 2000 to 2010.[3] Using the Internet is a common, and important, part of American life. We go online to work, to play, to shop or engage in commercial transactions, to obtain news, and for entertainment. We can engage in all of these activities only if we remain "wired" to the Internet. However, by obtaining access to the benefits of the Internet world, we also expose ourselves to a number of online risks such as identity theft, fraud, and other forms of cyber-crimes. Another risk is exposure to "spyware."

"Spyware" is a broad term used to describe software that resides on a user's computer and monitors the user's online behavior. Information about user behavior is then reported to others in order to enable responsive targeted interactions such as context sensitive advertising, enhanced search, or other legal or illegal activities.[4] Spyware may be helpful or benign (e.g. "cookies" that assist online shopping), or it can be very annoying (e.g. "adware" producing numerous pop-up ads covering the entire screen, interfering with use). More recently, much

---

1. *Internet Usage Statistics: World Internet Usage and Population Statistics*, INTERNETWORLDSTATS.COM (June 20, 2010), http://www.internetworldstats.com/stats.htm. (An estimated 1,966,514,816 people were Internet users as of June 20, 2010).

2. *Internet Usage Statistics: Internet Usage and Population Statistics for North America*, INTERNETWORLDSTATS.COM (June 30, 2010), http://www.internetworldstats.com/stats14.htm#north. (There were an estimated 239,232,863 Internet users in the U.S. as of December 31, 2009, for a penetration rate of 77.4 percent).

3. *Id.*

4. FED. TRADE COMM'N, STAFF REPORT: MONITORING SOFTWARE ON YOUR PC: SPYWARE, ADWARE, AND OTHER SOFTWARE 2-7 (2005), *available at* http://www.ftc.gov/os/2005/03/050307spywarerpt.pdf [hereinafter, "FTC Report"].

spyware is used for malicious purposes and also is classified as "malware". One type of malware includes programs that steal personal information and passwords that cyber-criminals use in identity theft, phishing scams. Other malware programs infect the user's computer and turn it into a "zombie" on a botnet[5] The botnet is then used to send unsolicited commercial email ("spam") and other malware. Legitimate business interests also use spyware to capture personal information enabling them to track the online behavior of their customers to assist with targeted advertising, selling goods, and other uses.

Consumers are especially vulnerable to online spyware threats because they (or the children in their family) often lack sophistication to avoid risky online practices or to recognize situations in which they download spyware.[6] Often spyware is installed without the computer user's knowledge, or without a *bona fide* consent of an adult, and will degrade computer usability and functionality and be extremely difficult to remove.[7] Spyware distributors target homes with child users or teenage users because such users are more easily induced to download "free" content that is bundled with software containing spyware. For example, social networking sites that are popular with teenagers and young adult computer users, such as MySpace and Facebook, have become significant sources for new spyware installations.[8] Peer-

---

5. A bot is a software robot that can be controlled remotely. It infects a computer without the knowledge of the computer use through a virus or worm that carries a Trojan program. Criminals who send out the bots typically use them to infest large numbers of computers, known as zombies, to create a network. These networks are referred to as botnets, and those who create them are known as botherders. *Bots, Botnets and Zombies*, MICROSOFT, http://www.microsoft.com/mscorp/safety/technologies/bots.mspx (last visited Jan. 5, 2010).

6. One study found spyware on personal computers in 69% of households with children under 18, but that only 8% were aware of the spyware on their computers. AMERICA ONLINE & NATIONAL CYBER SECURITY ALLIANCE, AOL/NCSA ONLINE SAFETY STUDY 6-7 (2004), *available at* ftp://rixstep.com/safety_study_v04.pdf.

7. *Id*. at 3.

8. Elinor Mills, *Microsoft Helps Keep Koobface Virus Off Facebook*, CNET NEWS (Apr. 2, 2009, 10:33 AM), http://news.cnet.com/8301-1009_3-10210376-83.html; Arik Hesseldahl, *Social-Networking Sites a "Hotbed" For Spyware,* BUSINESSWEEK ONLINE (Aug. 18, 2006, 6:10 PM), http://www.msnbc.msn.com/id/14413906/.

to-peer (P2P) sites such as BitTorrent, BearShare and Limeware also are vulnerable to spyware-infected content.[9]

Consequently by the mid-2000s, eighty-nine percent of consumer personal computers were infected with spyware despite a high degree of awareness about the spyware problem.[10] On average, a consumer PC had thirty different spyware programs installed.[11] Consumers often cannot afford to purchase and continually upgrade state-of-the-art anti-spyware software. They also lack the technical skills to repeatedly install security upgrades and to maintain their system software, Internet browsers, and other web-application software as spyware threats quickly evolve. Spyware plays an important role in facilitating spam, identity theft, phishing scams, and the spread of botnets used to distribute malware to consumer computers.[12]

Deleted: repeatedly

Consumers need new legal protection to prevent their own property -- their computers -- from being used against them as a spying device. Existing criminal laws have had minimal effect upon the prevalence of spyware used for cybercrime. Under tort law, consumers may be able to pursue a claim under a trespass to chattels. Such claims arise only *after* damage has occurred to their computers.[13] This is not sufficient legal protection to stop the proliferation of spyware on consumers' computers. In contrast, tort protection for real property interests allows legal recourse for trespass even though no damage has occurred. Applying a similar approach to spyware would provide the stronger legal protection that consumers need. Obviously it

---

9. Andrew J. Kalafut, et al., *A Study of Malware in Peer-to-Peer Networks*, IMC'06 (2006), *available at* http://www.cs.indiana.edu/~minaxi/pubs/imc06.pdf. (A month of data show that 68% of all downloadable responses in Limewire containing archives and executables contain malware).
10. WEBROOT SOFTWARE, INC., STATE OF SPYWARE, SECOND QUARTER 2006, 11 (2006), www.webroot.com/pdf/2006-q2-sos-US.pdf.

11. *Id.*

12. SYMANTEC INC., SYMANTEC GLOBAL INTERNET SECURITY REPORT: TRENDS FOR 2008, 5 (2009), http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf.

13. Intel Corp. v. Hamidi, 71 P.3d 296 (Cal. 2003).

would significantly distort common law tort theories to attempt to construe consumers' desktops as a form of "real estate." Thus, this article recommends the creation of a new statutory remedy to address spyware harms comparable to the tort remedies for trespass to real property.

This paper will first discuss the nature and scope of the spyware and malware problems affecting consumers. Second, the difficulty of applying the traditional tort theories of trespass and trespass to chattels to the problem of spyware will be explored. Next, the paper will argue that consumers' desktops are analogous to real property. Such "digital real estate" will best be protected by a private right of action that treats consumers' computers similarly to the tort protection provided for real estate interests. Finally, this paper will propose a new statute to address the widespread use of spyware methods by legitimate business interests engaged in behavioral advertising. These businesses include search sites, news and media websites financed by targeted advertising, Internet service providers (ISPs), advertising networks and online merchants. The proposed "Consumer Digital Trespass Act" (the "CDTA") would create a private cause of action based on concepts from real property and tort law. If enacted, the CDTA would effectively discourage legitimate business interests from using spyware to monitor consumer behavior and will provide consumers with the legal remedies to regain control over their desktops.

I. The Evolution of the Spyware Threat

Spyware began to emerge as a threat in the late 1990s and the first anti-spyware programs appeared in 2000.[14] Spyware frequently interferes with proper functioning of computers and causes them to crash, exposes private information to theft, drives up tech support costs for computer users, manufacturers and Internet service providers, and can cause a

14. FTC REPORT, *supra* note 4, at 2.

host of other harms.[15] By 2005, Webroot Software estimated that eighty percent of all computers it scanned contained spyware.[16] At that time, adware programs were the most common form of spyware. These programs tracked users' web browsing in order to repeatedly serve multiple online ads that covered the entire screen and obstructed further use of the computer. One anti-spyware software manufacturer detected nearly 40 million adware installations in use.[17] Adware merchants made easy money by creating extensive networks, often by using deceptive installation methods. The total adware market was estimated to be $2 billion in 2005.[18]

In April 2004, the Federal Trade Commission (FTC) convened a public workshop to discuss issues related to spyware, and in March 2005 FTC issued a staff report on spyware.[19] By 2005, widespread problems with spyware raised awareness such that 96% of computer users were familiar with the term "spyware."[20] Enforcement actions by the Federal Trade Commission and state attorneys general helped to discourage the most serious adware abuses.[21] Private litigation that named advertisers as co-defendants also chilled the market for adware.[22] Although adware prevalence dipped somewhat in 2005, it had risen again to 59% of surveyed

---

15. *Id.*

16. WEBROOT SOFTWARE, INC., STATE OF SPYWARE, SECOND QUARTER 2005, 43 (2005), http://www.webroot.com/pdf/2005-q2-sos.pdf.

17. FTC REPORT, *supra* note 4, at 12; *see also infra* note 124.

18. Tom Zeller, *New Program Takes Aim at Purveyors of Malicious Software,* N.Y. TIMES, Jan. 25, 2006, *available at* http://www.nytimes.com/2006/01/25/technology/25spy.html?_r=1.

19. FTC REPORT, *supra* note 4, at 2-7.

20. AMERICA ONLINE & NATIONAL CYBER SECURITY ALLIANCE, *supra* note 6, at 6-7.

21. *See, e.g.,* Press Release, Fed. Trade Comm'n, Zango, Inc. Settles FTC Charges (Nov. 3, 2006), http://www.ftc.gov/opa/2006/11/zango.shtm; Press Release, N.Y. Office of the Att'y Gen., Groundbreaking Settlements Hold Online Advertisers Responsible For Displaying Ads Through Deceptively Installed "Adware" Programs, (Jan. 29, 2007), http://www.oag.state.ny.us/media_center/2007/jan/jan29b_07.html.

22. *See, e.g.,* Sotelo v. DirectRevenue, LLC, 384 F. Supp. 2d 1219 (N.D. Ill. 2005).

computers in 2006.[23] Consumers were the primary targets. Spyware attacks on home users accounted for 93% of all targeted attacks in 2006.[24] By 2009, Consumer Reports estimated that spyware infections caused 545,000 households to replace their computers, and caused total damages of $1.7 billion.[25]

Spyware often initially appeared in the form of viruses, worms, and other simple and visible attacks directed at disrupting the operations of computing *devices*. This continues in the form of sophisticated botnet networks today.[26] However, spyware has evolved to also include sophisticated web based attacks directed at the *end users*. Current attacks have the goal of obtaining personal information needed to commit financial fraud and other profitable illegal activity.[27] Criminals use spyware as part of their professional enterprise to make money by any means, legal or not. Cyber criminals now seek vulnerabilities in web browsers and other Internet applications to trick users into clicking on malware links that have been installed on legitimate, but compromised websites.[28] For example, one site spoofed President Obama's

---

23. WEBROOT SOFTWARE, INC., STATE OF SPYWARE, FIRST QUARTER 2006,9 (2006), http://www.webroot.com/pdf/2006-q1-sos.pdf.

24. SYMANTEC INC., "SYMANTEC INTERNET SECURITY THREAT REPORT: TRENDS FOR JULY-DECEMBER 06, 5 (2007), http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf.

25 *State of the Net 2009*, CONSUMER REPORTS, (June 2009), *available at* http://www.consumerreports.org/cro/magazine-archive/june-2009/electronicscomputers/state-of-the-net/state-of-the-net-2009/state-of-the-net-2009.htm.

26. MCAFEE, INC., 2009 THREAT PREDICTIONS 1 (2009) http://www.mcafee.com/us/local_content/reports/2009_threat_predictions_report.pdf.

27. SYMANTEC INC., SYMANTEC GLOBAL INTERNET SECURITY REPORT: TRENDS FOR 2008, 5 (2009), http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf.

28. SOPHOS, TOP FIVE STRATEGIES FOR COMBATING MODERN THREATS: IS ANTI-VIRUS DEAD? 1 (2008). https://secure.sophos.com/sophos/docs/eng/papers/sophos-combating-threats-wpna.pdf.

official inauguration site and duped visitors into downloading spyware.[29] In addition, seventy percent of the most frequently visited websites have either hosted malware or provided links to sites that hosted malware.[30] McAfee Security identified nearly 1.5 million items of malware in 2008 alone. Ninety percent of malware files are password-stealing Trojans designed to facilitate financial fraud and other criminal activity.[31]

One of today's most dangerous forms of spyware is the software used to convert desktop computers into "zombies" as part of "botnets" of networked computers controlled remotely by professional cyber criminals. Symantec reported an average of over 75,000 active botnets operating per day in 2008, an increase of thirty-one percent over 2007.[32] The eleven largest botnets control over one million computers and can distribute more than 100 billion spam messages per day, which distribute even more malware.[33] Spam now makes up more than ninety percent of all e-mail.[34] These botnets and the cybercrime activities that they support pose a substantial threat to U.S. businesses and financial systems. Use of botnets for distributed denial of service attacks against Internet service providers, domain name registries, and other

---

29. Thomas Claburn, *Fake Obama Web Site Reportedly Builds Botnet*, INFORMATION WEEK (Jan. 20, 2009, 3:05 PM), http://www.informationweek.com/news/security/government/showArticle.jhtml?articleID=212901473.

30. Thomas Claburn, *70 Of Top 100 Web Sites Spread Malware,* INFORMATION WEEK (Jan. 20, 2009, 4:45 PM), http://www.informationweek.com/news/internet/security/showArticle.jhtml?articleID=212901775.

31. MCAFEE, INC., *supra* note 26.

32. SYMANTEC INC., SYMANTEC GLOBAL INTERNET SECURITY REPORT: TRENDS FOR 2008, 5 (2009), http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf.

33. Gregg Keizer, *Top Botnets Control 1M Hijacked Computers*, COMPUTERWORLD (Apr. 9, 2008, 12:00 PM), http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9076278.

34. Lance Whitney, *Report: Spam Now 90 Percent of All E-Mail,* CNET NEWS, (May 26, 2009, 9:24 AM), http://news.cnet.com/8301-1009_3-10249172-83.html?tag=mncol;posts.

targets is increasing.[35] Economic losses due to cyber threats may be as much as $300 million per day.[36]

Government resources directed to combat spyware have been insufficient, and spyware defenses have been left to the private sector.[37] As a result, the security software industry had annual revenues of $14.5 billion dollars in 2009, and is expected to reach $16.3 billion by 2010.[38] Government regulators have only limited enforcement resources to take action against deceptive practices by enterprises using spyware to harm consumers. For example, even at the height of the adware craze, the FTC completed only eleven enforcement actions, and just ten enforcement cases by states.[39] The explosive growth in cybercrime triggered President Obama's 2009 Cyber-Security Plan -- a coordinated legal and technical response involving government, law enforcement, the security software industry, Internet companies, and business.[40] Consequently, this paper will not attempt to address this broad spectrum of online criminal activity.

This article instead will focus upon the ways in which legitimate businesses use spyware methods to surreptitiously monitor consumers' Internet activity for commercial gain, and will

---

35. Brian Krebs, *Experts Chart Spike in Cyber Sieges*, WASH. POST, May 1, 2009, http://www.washingtonpost.com/wp-dyn/content/article/2009/05/01/AR2009050101593_pf.html.

36. *Cybersecurity: Network Threats and Policy Challenges; Hearing Before the H. Energy and Commerce Subcomm. on Commc'ns, Tech., and the Internet,* 111th Cong. 1 (2009) (Testimony of Larry Clinton, President, Internet Security Alliance), *available at* http://energycommerce.house.gov/Press_111/20090501/testimony_clinton.pdf.

37. *Id.*

38. Press Release, Gartner, Inc., Gartner Says Worldwide Security Software Market on Pace to Grow 8 Per Cent in 2009 (Sept. 21, 2009), *available at* http://www.gartner.com/it/page.jsp?id=1184713.

39. *Combating Spyware: H.R. 964 (the Spy Act) Before The H. Comm. on Energy and Commerce Subcomm. on Commerce, Trade, and Consumer Prot.,* 110th Cong. 1-2 (2007) (testimony of Ari Schwartz, Deputy Director, Center for Democracy and Technology), *available at* http://www.cdt.org/files/pdfs/20070315schwartzspwyare_2.pdf.

40. David E. Sanger & John Markoff, *Obama Outlines Coordinated Cyber-Security Plan*, N.Y. TIMES, May 29, 2009, http://www.nytimes.com/2009/05/30/us/politics/30cyber.html.

propose a solution to protect consumers. Legitimate business websites use spyware on consumers' computers to capture private online behavior and personal information -- primarily for the purpose of facilitating sales of online advertising or for generating online sales. Internet advertising revenues increased 10.6% in 2008 to $23 billion,[41] and revenues have increased twelve-fold since 1998.[42] As more advertising dollars compete for the limited space on computer screens and mobile devices, advertisers are seeking increasingly targeted advertising that depends upon extensive monitoring of users' private browsing behavior and preferences. McAfee reports that most websites continue to use pop-up ad screens, despite blocking software.[43] Internet service providers (ISPs) also have considered spying upon consumers' online activity by conducting a "deep packet inspection" of each private Internet transmission made by their customers.[44] The Federal Trade Commission has issued self-regulatory guidelines for online advertising[45] but continues to lack serious enforcement capability. Consumers need legal protection to stop this intrusive use of their own computers by business interested in seeking to monitor their private information. Since government regulators lack

Comment [RK1]: Insert "have"

41. PRICEWATERHOUSECOOPERS & INTERACTIVE ADVERTISING BUREAU, LLP, 2008 INTERNET ADVERTISING REVENUE REPORT 3 (2009), http://www.iab.net/media/file/IAB_PwC_2008_full_year.pdf.

42. Press Release, Internet Advertising Bureau, First Quarter 1999 Internet Advertising Revenues Double Over First Quarter 1998 (Aug. 17, 1999), http://www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/58589. Internet advertising revenues for 1998 were $1.92 billion, compared to $23.4 billion in 2008.

43. MCAFEE, INC. MCAFEE THREATS REPORT: FIRST QUARTER 2009, 12 (2009), http://img.en25.com/Web/McAfee/5395rpt_avert_quarterly-threat_0409_v3.pdf.

44. *See Communications Networks and Consumer Privacy: Recent Developments: Hearings Before the Subcomm. On Commc'ns, Tech., and the Internet*, 111th Cong. 2 (2009) (statement of Leslie Harris, President and Chief Executive Officer,Center for Democracy and Technology), *available at* http://energycommerce.house.gov/Press_111/20090423/testimony_harris.pdf. *See also*, Jeremy Kirk, *Adware Company Refines Opt-Out, Notification Technology*, NETWORK WORLD (Jul. 8, 2008, 11:30 AM), *available at* http://www.networkworld.com/news/2008/070808-adware-company-refines-opt-out-notification.html?ry=gs (describing the activities of targeted advertisers NebuAd and Phorm).

45. FED. TRADE COMM'N, STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING (2009), *available at* http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.

sufficient enforcement resources, the best solution is to empower consumers with a private right of action to protect their desktop "real estate."

II. Trespass to Land and Trespass to Chattels in Cyberspace.

The manner in which the torts of trespass to land and trespass to chattels would apply to the spyware context would, at first blush, seem obvious. Consumers own their computers. It is their personal property. Computers clearly are not real property, and thus, the tort of trespass to land would not apply. Consumers have legally protected rights in their computers, including the right to exclude others from making unauthorized use of the computer.[46] Thus, it seems apparent that those who install spyware on another's computer without consent would be liable for trespass to chattels.

The tort of trespass to chattels, unlike trespass to land, requires proof of actual damage to the chattel before an action can be brought.[47] The Restatement of Torts provides that a trespass to chattels arises only if the trespasser:

> (a) . . . dispossesses the other of the chattel, or
> (b) the chattel is impaired as to its condition, quality, or value, or
> (c) the possessor is deprived of the use of the chattel for a substantial time, or
> (d) bodily harm is caused to the possessor, or harm is caused to some person or thing in which the possessor has a legally protected interest.[48]

Early cases applying trespass to chattels to online interferences, or "cybertrespass," focused on whether unauthorized transmission of data to or from another's computer, and use of the computer's storage and processing capacity, was sufficient damage to trigger legal protection.

---

46. RESTATEMENT (SECOND) OF TORTS, §§ 217, 218 (1965). *See* Shyamkrishna Balganesh, *Common Law Property Metaphors On The Internet: The Real Problem With The Doctrine Of Cybertrespass,* 12 MICH. TELECOMM. & TECH. L. REV. 265, 294 (2006); Patricia L. Bellia, *Defending Cyberproperty,* 79 N.Y.U.L. REV. 2164, n.15 (2004).

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

48. RESTATEMENT (SECOND) OF TORTS, § 218 (1965).

In *CompuServe v. CyberPromotions*,[49] the defendant continued to transmit unsolicited commercial e-mail ("spam") through CompuServe's servers to CompuServe's subscribers after receiving a cease and desist letter. The court found sufficient harm existed because the defendant's use of CompuServe's computers to distribute the spam consumed CompuServe's server disk space and consumed processing power.[50] Several other spam-related cases have reached similar conclusions.[51]

EBay v. Bidder's Edge[52] involved data stored on eBay's servers and displayed on eBay's auction site. Bidder's Edge used automated web spiders to retrieve data from eBay and other auction sites, which it aggregated and displayed on the Bidder's Edge auction aggregation site.[53] At first, eBay permitted Bidder's Edge to do so.[54] Later, the parties began negotiations for a license for Bidder's Edge to continue its data retrieval practices.[55] When negotiations broke down, eBay ordered Bidder's Edge to stop, but it did not do so.[56] The court found that the minimal use of eBay's system by Bidder's Edge's spiders was sufficient damage to constitute a trespass to chattels.[57] The court noted that if eBay were unable to control access to its property by aggregators, others would likely engage in similar activities that could overwhelm the

---

49. CompuServe v. CyberPromotions, 925 F. Supp. 1015 (S.D. Ohio 1997).

50. *Id.* at 1022.

51. *See* Bellia, *supra* note 46, at 2176, at fn. 30.

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

53. *Id.* at 1060.

54. *Id.* at 1061.

55. *Id.*

56. *Id.* at 1062-63

57. *Id.* at 1070-1071

servers.[58] A similar result was reached in *Register.com Inc. v. Verio, Inc.*,[59] in which the court enjoined use of web robots to compile data from a domain name database available on the Internet.

The legal trend toward recognition of *de minimus* interferences as sufficient damage to trigger trespass to chattels claims continued in *Intel Corp. v. Hamidi.*[60] Hamidi was a former Intel employee who sent six mass email messages critical of Intel.[61] These messages were sent over a twenty month period to several thousand e-mail addresses of Intel employees.[62] Intel first attempted to block the emails from Hamidi, but Hamidi thwarted the blocking attempts by sending the messages from other computers.[63] Finally, Intel sent Hamidi a letter demanding that he stop sending the emails, but Hamidi continued.[64] There was no evidence that distribution of the six emails from Hamidi had damaged Intel's servers or impaired their functioning.[65] Yet, the trial court enjoined Hamidi from sending unsolicited e-mails to addresses on Intel's e-mail system.[66] The California Court of Appeals affirmed, ruling that the unauthorized use could trigger injunctive relief without proof of any actual damage to Intel's personal property under the theory of trespass to chattels.[67]

---

58. *eBay*, 100 F. Supp. 2d at 1066.

59. Register.com, Inc. v. Verio, Inc.,356 F.3d 393, 396 & 404 (2d Cir. 2004).

60. Intel Corp. v. Hamidi,114 Cal.Rptr. 2d 244 (Cal. Ct. App. 2001), *rev'd*, 71 P.3d 296 (Cal. 2003).

61. *Id.* at 246.

62. *Id.*

63. *Id.*

64. *Id.*

65. *Id.* at 261.

66. Intel Corp. v. Hamidi, 1999 WL 450944, at *1, *3 (Cal. Super. Ct. Apr. 28, 1999).

67. Intel Corp. v. Hamidi,114 Cal.Rptr. 2d 244 (Cal. Ct. App. 2001), *rev'd*, 71 P.3d 296 (Cal. 2003).

At this point in the evolution of the tort of "cybertrespass," courts had essentially eliminated the element of damage from the traditional trespass to chattels claim. In so doing, the cybertrespass became indistinguishable from trespass to land, for which damage is not an element.[68] These rulings emphasized the computer owner's right to exclude others from unauthorized uses, and extended to computer systems the same inviolability of proprietary rights that had existed for real estate for centuries. Computers connected to the Internet were, in effect, treated like real property.

These decisions triggered an avalanche of legal scholarship critical of the new doctrine of cybertrespass.[69] Critics argued that by extending property rule protections to computer systems that these claims would overly "propertize" the Internet.[70] A broad right to exclude would allow to each individual system owner to specify the desired and undesired uses of their site. Critics feared that such rules would restrict the free flow of informational resources on the Internet and create a default rule of closed access to websites. They also feared the right to exclude would block harmless but productive online interactions, stifle development and

Comment [CM2]: Should we insert an *Id.* cite here?

Comment [RK3]: I have added a new footnote 70, which lists two authorities that emphasize the propertization question. I will leave the citation/short citation format to you!

68. RESTATEMENT (SECOND) OF TORTS, § 158 (1965); PROSSER AND KEETON ON THE LAW OF TORTS § 1413 (W. Page Keeton et. al. eds., 5th ed. 1984).

69. *See, e.g.* James Boyle, *The Second Enclosure Movement and the Enclosure of the Public Domain*, 66 L. & CONTEMP. PROBS. 33 (2003); Dan L. Burk, *The Trouble with Trespass,* 4 J. SMALL & EMERGING BUS. L. 27, 53 (2000); Steve Fischer, *When Animals Attack: Spiders and Internet Trespass,* 2 MINN. INTELL. PROP. REV. 139 (2001); Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 CAL. L REV. 439 (2003); Steven Kam, Note, *Intel Corp. v. Hamidi: Trespass to Chattels and a Doctrine of Cyber-Nuisance,* 19 BERKELEY TECH. L.J. 427, 448-52 (2004); Niva Elkin-Koren, *Let the Crawlers Crawl: On Virtual Gatekeepers and the Right to Exclude Indexing,* 26 U. DAYTON L. REV. 179, 203-06 (2001); Mark A. Lemley, *Place and Cyberspace,* 91 CAL. L REV. 521 (2003); Lawrence Lessig, *The Architecture of Innovation,* 51 DUKE L.J. 1783 (2002); R. Clifton Merrell, *Note, Trespass to Chattels in the Age of the Internet,* 80 WASH. U. L.Q. 675, 687-97 (2002); Adam Mossoff, *Spam - Oy, What a Nuisance!,* 19 BERKELEY TECH. L.J. 625, 629 (2004); Maureen A. O'Rourke, *Property Rights and Competition on the Internet: In Search of an Appropriate Analogy,* 16 BERKELEY TECH. L.J. 561 (2001); Maureen A. O'Rourke, *Shaping Competition on the Internet: Who Owns Product and Pricing Information,* 53 VAND. L. REV. 1965 (2000); Laura Quilter, *The Continuing Expansion of Cyberspace Trespass to Chattels,* 17 BERKELEY TECH. L.J. 421 (2002).

70 See, e.g. Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 CAL. L REV. 439 (2003) and Bellia, *supra* note 46.

growth of the Internet and even have the effect of producing an "anti-commons."[71] Supporters of the cybertrespass decisions argued that strong property rule protection of computer systems and resources would encourage development of Internet resources and maximize efficiencies of online networks.[72] The formerly obscure tort of trespass to chattels suddenly became the focal point in a policy debate regarding the most discussed topics in cyberlaw: 1) to what degree may computer owners using the Internet control or exclude unwanted uses of their systems; and 2) what degree of damage is sufficient to trigger legal protection?

The California Supreme Court found itself in the midst of this heated environment when it heard Hamidi's appeal. The court -- perhaps persuaded by the arguments made by cybertrespass critics that strong protection of the property rights of computer users would compromise the flow of network resources on the Internet -- restored the damage requirement for recovery in trespass to chattels cases. The court ruled that because Hamidi had caused no harm to Intel's computer hardware or software, nor interfered with its intended operation, nor dispossessed Intel, nor caused Intel's system to be slowed or impaired, nor imposed any marginal costs on Intel, that an action for trespass to chattels did not arise.[73] This decision, too, has been criticized for failing to strike the proper balance between the rights of computer

---

71. *See* Bellia, *supra* note 46, at 2170-71, 2180-81. If the right to exclude were too strong, Internet users would have to negotiate license terms with each web site owner. This would stifle normal Web activities such as indexing and web-linking. This would cause the common resource of the Internet to be under utilized because it has too many property owners unable to effectively agree or cooperate in its use, creating an anti-commons. *See also,* Dan L. Burk, *supra* note 69, at 53.

72. *See, e.g.* Richard A. Epstein, *Cybertrespass*, 70 U. CHI. L. REV. 73, 84 (2003) ("strong property rights for non-network elements function as well in cyberspace as they do anywhere else."); Richard A. Epstein, *Intellectual Property: Old Boundaries and New Frontiers,* 76 IND. L.J. 804, 818-21 (2001); Daniel Kearney, *Network Effects and the Emerging Doctrine of Cybertrespass,* 23 YALE L. & POL'Y REV. 313 (2005) (arguing that a clear rule of cybertrespass will maximize the efficiencies of online networks); David McGowan, *Website Access: The Case for Consent,* 35 LOY. U. CHI. L.J. 341, 375-83 (2003) (explaining benefits of property-rule approach over damages rule such as nuisance); Richard Warner, *Virtual Borders: Trespass to Chattels on the Internet,* 47 VILL. L. REV. 117 (2002).

73. Intel Corp. v. Hamidi, 71 P.3d 296 (Cal. 2003).

system owners to control use of their private resources and the free flow of networked information resources on the Internet.[74]

Applying the California Supreme Court's holding in *Hamidi* to spyware cases, it is likely that many consumers would be able to prove damage sufficient to bring a successful trespass to chattels claim. Spyware and malware programs cause harm to computers by causing them to freeze or crash, when the programs interfere with intended operations by covering the display screen with advertisements or sending spam,[75] or when users lose control of their computer because it has been taken over by a botnet. Because malware distributed by cyber-criminals uses or intermeddles with the personal property of computer users, and causes damage in a variety of ways, trespass to chattels may appear to provide an effective remedy for consumer spyware victims in such cases. However, behavioral targeting by legitimate businesses is less likely to cause serious harmful interference with consumer computers.

Yet consumers may encounter significant obstacles to recovery on their trespass to chattels claim. First is the issue of consent, a recognized defense to an intentional tort.[76] Frequently spyware is distributed by bundling it with other "free" software downloads and other content desired by consumers, such as YouTube videos, mp3 music files, peer-to-peer file sharing software, and other files.[77] Spyware vendors contend that each download is preceded by an ostensible consent given by the consumer when they click "Download" or "I agree" on a pop-up browser screen.

Consumers' right to use their computers as they wish should include the freedom to

---

74. Richard A. Epstein, *Intel v. Hamidi: The Role of Self-Help in Cyberspace?*, 1 J.L. ECON. & POL'Y 147 (2005).

75. FTC REPORT, *supra* note 4, at 2.

76. PROSSER AND KEETON ON THE LAW OF TORTS § 18 (W. Page Keeton et. al. eds., 5th ed. 1984).

77. WEBROOT SOFTWARE, INC., STATE OF SPYWARE, *supra* note 16, at 9.

agree to accept advertising or tracking software in exchange for software and other content that they find convenient or valuable, provided the consent is fully informed and knowingly given. However, the genuineness of the consent given to trigger a bundled download of "freeware" and spyware is open to a number of challenges. First, while the consumer may be consenting to installation of the desired free content, it is often highly dubious that they even know of, much less are consenting to, installation of a bundle that includes spyware.[78] Second, the FTC has chronicled several deceptive practices used to install spyware ranging from installations without notice, "pop-under exploits" (which make the installation appear to be related to a true site visited by the user), fake operating system messages, and "Cancel" buttons that actually continue the installation.[79] Spyware critic Ben Edelman has documented a variety of deceptive installation methods on his website.[80] Third, modern malware threats attempt to induce users to merely play a video clip, an mp3 file, or click a link to an interesting news story to trigger a malware download. In these cases, consumers have no idea that they have initiated a download, much less consented to one.[81]

When legitimate businesses seek permission to track consumers' online behavior, the purported consent may take the form of a "terms of use" link on the website of the business, or by a clickwrap license or a browsewrap license.[82] Commentators have questioned whether this

---

78. Ben Edelman, *Media Files that Spread Spyware,* (Jan. 2, 2005), http://www.benedelman.org/news/010205-1.html.

79 FTC REPORT, *supra* note 4, at 55-57.

80. Ben Edelman, *Spyware: Research, Testing, Legislation and Suits*, http://www.benedelman.org/spyware (last updated Feb. 2, 2010). These include sites targeted to children, bundling of spyware with peer-to-peer software at P2P sites, undisclosed licenses and other practices.

81. SYMANTEC INC., "SYMANTEC INTERNET SECURITY THREAT REPORT: TRENDS FOR JULY-DECEMBER 06, 5 (2007), http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf.

82. *See, e.g.,* Mark A. Lemley, *Terms of Use,* 91 MINN. L. REV. 459 (2006).

manifests an informed subjective assent to enter into a contractual agreement to authorize spyware installation, or rather, is merely an objective act to trigger the download of the free digital content.[83] Edelman has criticized the lengthy and complicated license agreements used by adware firms that can only be displayed on dozens of computer screens.[84] For example, if a consumer sought information on the monitoring policies of Google's Gmail email service, it would require approximately nine mouse clicks and the reading of terms equaling seventeen printed pages.[85] Thus consumers may be able to successfully argue that any purported consent to the spyware installation when creating such online accounts and relationships is invalid. In many instances consumers lack a true understanding of the extent to which they purportedly authorized others to use their computers as tracking devices.

Another challenge for consumers involves identification of the tortfeasor. The behavioral advertising business model includes a confusing array of advertisers, interactive agencies, advertising networks, third party advertising servers, software developers, and publishers.[86] Identifying the specific party responsible for installing the spyware causing the

---

83. Jordan M. Blanke, *"Robust Notice" and "Informed Consent:" the Keys to Successful Spyware Legislation,* 7 COLUM. SCI. & TECH. L. REV. 2 (2006); Ryan J. Casamiquela, *Contractual Assent and Enforceability in Cyberspace*, 17 BERKELEY TECH. L.J. 475, 477 (2002); Jennifer Femminella, Note, *Online Terms and Conditions Agreements: Bound by the Web,* 17 ST. JOHN'S J. LEGAL COMMENT. 87, 101 (2003); Richard G. Kunkel, *Recent Developments in Shrinkwrap, Clickwrap and Browsewrap Licenses in the United States,* 9 MURDOCH U. ELECTRONIC J.L. 3 (2002), *available at* http://www.murdoch.edu.au/elaw/issues/v9n3/kunkel93.html.
James J. Tracy, *Legal Update: Browsewrap Agreements: Register.Com, Inc. v. Verio, Inc.,* 11 B.U.J. SCI. & TECH.SCI. & TECH. L. 164 (2005);

84. For example, adware firms Claria and WhenU had license pages that were 56 and 45 screens long, respectively. Ben Edelman, *Hard-Coding Bias in Google "Algorithmic" Search Results* (Nov. 15, 2010), http://www.benedelman.org, (last visited March 25, 2007). *See also*, Ben Edelman, *Why I Can Never Agree With Adware And Spyware*, THE GUARDIAN, Jan. 25,2007, *available at* http://technology.guardian.co.uk/online/insideit/story/0,,1997629,00.html.

85. Based on a brief test by the author beginning from the Gmail Home Page on May 29, 2009. These pages do not include the privacy policy of Google generally (5 printed pages), or for its advertising subsidiary, DoubleClick (4 pages).

86. DESILVA & PHILLIPS, LLC, ONLINE AD NETWORKS: MONETIZING THE LONG TAIL 6, (2008), http://www.iab.net/media/file/AdNetworksWhitePaper.pdf; *see also,* CENTER FOR DEMOCRACY & TECHNOLOGY, FOLLOWING THE MONEY II: THE ROLE OF INTERMEDIARIES IN ADWARE ADVERTISING (2006),

damage may be difficult, even though all parties in the advertising distribution chain profit by tracking consumers' online behavior in order to sell interactive contextual advertising.

III. Real Property Principles Applied to Spyware Trespasses.

Personal computers exchanging information over the Internet are not real property. The traditional tort of trespass to land is not applicable to computers infected with spyware. Yet early cybertrespass cases eviscerated the damage requirement and applied essentially the same rules as trespass to land. Both before and after the *Hamidi* case, commentators argued that real property-type rules were well suited to protect rights for computer owners and were an efficient means of allocating resources on the Internet. Moreover, when it is being used on the Internet a computer has characteristics that are analogous to real property in two vital respects: 1) its immovability, and 2) the effectiveness of using self-help to protect the owner's property interest.

Trespass to land allows legal recourse without proof of damage, even if the entry is in good faith or by mistake.[87] This rule protects the owner's right to exclude others and the inviolability of the real property interest.[88] When a continuing trespass or encroachment occurs, the land obviously cannot be moved out of the possession of the trespasser or encroacher. Since land is immovable, any unprivileged entry to real property is a challenge to the owner's right to exclude. Tort law permits legal action to vindicate the property right of the owner, to prevent acquisition of prescriptive rights, and to avoid breaches of the peace by physical ejection.[89]

---

http://www.cdt.org/privacy/20060809adware.pdf.

87. PROSSER AND KEETON ON THE LAW OF TORTS § 13 (W. Page Keeton et. al. eds., 5th ed. 1984).

88. *Id.*

88. *Id.*

89. *Id.*

In contrast, for movable property the tort of trespass to chattels requires actual damage. But because chattels are movable, when a trespasser interferes or meddles with a chattel, owners have the privilege of self-help. The owner can use self-help to pick up the chattel and remove it to a place beyond the trespasser's unwanted interference. For example, if you meddle with the music playlists on my iPod, I can use self-help to pick up the iPod, take it away from your control, and reset my music selections. I also can move it away form you, secure it in my possession, and prevent any further interferences by you. I have no legal remedy for such harmless intermeddling with the iPod because my privilege to use self-help to halt unauthorized use is adequate to protect my interests. The Restatement provides:

> The interest of a possessor of a chattel in its inviolability, unlike the similar interest of a possessor of land, is not given legal protection by an action for nominal damages for harmless intermeddling with the chattel . . . *Sufficient legal protection* of the possessor's interest in the mere inviolability of his chattel is afforded by his privilege to use reasonable force to protect his possession against even harmless interference.[90] (italics supplied.)

In 2010, a personal computer chattel has its highest and best use and functionality when used to access the network benefits of the Internet. There is only one Internet. The only way to receive the vast network benefits of the Internet is to be connected to it.[91] When online, the owner exposes herself to a myriad of potential unauthorized uses of her computer, including spyware, malware and the resulting loss of personal information and privacy; but under the *Hamidi* rule, the Internet user has no legal remedy to prevent such repeated invasions until sufficient damage to the computer occurs.

For example, suppose a computer was repeatedly subjected to malware installations of botnet software used to serve spam. Under *Hamidi*, the user's sole remedy is to attempt to exercise self-help by continually patching her system software and running anti-spyware

---

90. RESTATEMENT (SECOND) OF TORTS § 218 (Comment e) (1965).

91. Epstein, *Cybertrespass*, *supra* note 61, at 84.

applications to stay a close step behind the spyware merchants attacking her system. Until the botnet begins spamming and phishing to a sufficient degree to affect her computer's performance, or her personal data is hijacked, the consumer waits quietly for the inevitable harm to erupt.

Is it possible for the computer owner to remove her computer from harm's way? Could she avoid harm by simply disconnecting from the Internet? While this is technically possible, she suffers injury by being deprived of one of the primary uses of her computer chattel -- the ability to access the Internet. Could the computer owner choose to access another, different Internet (i.e. one that is not populated with spyware and malware sites?) No. In this sense the Internet-connected computer is immovable. It is impossible to both disconnect the computer from dangerous and unauthorized uses, while simultaneously being online using and enjoying the functionality of the Internet. Since the owner cannot move the computer and its Internet functionality out of harm's way without forfeiting a substantial portion of its value, a legal remedy is needed to protect the owner without the necessity of prior damage to the computer occurring.

Comment [RK4]: Need the closed parenthesis) here after question mark!

The use of self-help for computers on the Internet is also more analogous to real property than to personal property. Since real property is immovable, the only self-help possible would require physical ejection of the tortfeasor from the real property. Using self-help backed bywith force would likely result in breaches of the peace. Consequently, use of force and self-help is restricted. Self-help is replaced by the legal right to recover remedies in trespass without proving damage and to eject the trespasser. The legal right to recover remedies in trespass without proving damage and to eject the trespasser replaces self-help. In cyberspace, the only complete method of self-help to avoid unauthorized uses is to unplug from

the Internet and forfeit its benefits.[92] Perversely, this approach requires the innocent computer owner to eject herself from the useful benefits of the Internet, while the wrongdoers continue to benefit from it by causing harm.

One partial self-help remedy is to attempt to use anti-virus and anti-spyware programs to attempt to avoid or defeat (at least temporarily) unauthorized uses before damage occurs.[93] Consumers, in particular, are ill- equipped to exercise this privilege of self-help in cyberspace. Many cannot afford the costs of installing current anti-spyware software and keeping it up-to-date. The form of online threats and the sophistication of the techniques change too frequently. Self-help has become especially difficult for consumers because cyber-thieves manipulate their fears over spyware to distribute even more malware. Google's Security Team reports that fifteen percent of all malware is distributed via fake security and antivirus download scams, also known as "scareware."[94] The F.B.I. estimates that victims have lost up to $150 million from scareware scams.[95]

Business and corporate users may have technical support staff to update software, to install security patches, and to update anti-virus and anti-spyware software company-wide. However, few consumer users have the technical prowess to continuously install and maintain effective anti-spyware software. In addition, the threats are so sophisticated, numerous, and

---

92. A partial self-help remedy is to withdraw certain informational goods from the broader Internet and make them available only to subscribers via password protected accounts. If most computer owners restricted information goods in this way, the broad network effects would be lost and the anti-commons envisioned by property rule critics could result.

93. Self-help in the form of security software is now a $16 billion dollar industry. Press Release, Gartner, Inc., *supra* note 38.

94. Moheeb Abu Rajab, et al., *The Nocebo Effect on the Web: An Analysis of Fake Anti-Virus Distribution*, 3RD USENIX WORKSHOP ON LARGE SCALE EXPLOITS AND EMERGENT THREATS (2010), *available at* www.usenix.org/event/leet10/tech/www.usenix.org/event/leet10/tech/www.usenix.org/event/leet10/tech/tech.html#Rajab.

95. Press Release, Internet Crime Complaint Center, Pop-up Advertisements Offering Anti-virus Software Pose Threat to Internet Users (Dec. 11, 2009), *available at* http://www.ic3.gov/media/2009/091211.aspx.

rapidly evolving that even business enterprises are fighting a losing battle with spyware. In the physical world, self-help may provide "sufficient legal protection"[96] of an owner's inviolability interest in their chattel. However, in the context of cyberspace, there is no practical means for consumers to use self-help as a partial or temporary remedy to protect their computers from harm. In the absence of a legal remedy without damage occurring, they remain exposed to repeated violations of their computer assets, their personal information and their privacy.

Finally, for centuries the law has extended special protection to persons in their real property homesteads. The law recognizes the importance of protecting such places to provide persons with a sense of both privacy and security, including constitutional protection against unwarranted search and seizure.[97] Homes hold and secure consumers' most personal and treasured keepsakes and their most important records. Increasingly, consumers are storing their keepsakes and records on their personal computers. They store photos, correspondence, address books, work projects, financial information, and home videos on their computers.[98] Computers are the "digital homesteads" of many consumers and need additional legal protection from spyware invasions of these most personal items. Consumers deserve protection for their computers that is analogous to real property homesteads.

Tort law remedies for spyware trespasses leave consumers poorly protected. Remedies for trespass to real property are appropriate for consumers, but clearly inapplicable. Remedies for trespass to chattels are applicable, but inadequate. It is unrealistic to expect that ordinary consumers will be able to exercise their privilege of self-help so effectively as to defeat hordes of

---

96. RESTATEMENT (SECOND) OF TORTS § 218 (Comment e) (1965).

97. U.S. Const. amend. IV.

98. WEBROOT SOFTWARE, INC., PROTECTING YOUR DIGITAL LIFE 2 (2008), *available at* http://www.webroot.com/shared/pdf/2008_Consumer_SOIS-Protecting_Your_Digital_Life.pdf. In 2007, forty-six million people in the U.S. and U.K. lost personal files on their computers, in part because approximately forty-five percent of consumers backup their home data only once per year or less. *Id.*

professional programmers in a battle of wits over spyware installations. The other alternative is to await the level of computer damage necessary to pursue a trespass to chattels claim. Neither alternative is acceptable. Thus, a statutory remedy grounded in real property principles is a preferable solution.

IV. A Proposed Consumer Digital Trespass Act.

Consumers are both the most highly targeted victims of spyware and the least able to exercise self-help to defeat the onslaught of spyware activity they face. Consumers need stronger legal protection to control their desktops and return to productive and enjoyable computer uses. Legislation that recognizes a right to exclude spyware and that creates a private right of action to recover damages for spyware installed without proper notice and express consent will be a significant consumer protection achievement.

This article proposes the enactment of a Consumer Digital Trespass Act (hereinafter, the "CDTA")[99] that protects the inviolability interest of consumer computer owners in a manner similar to real estate interests under tort law.[100] The CDTA allows consumers to self-identify their computers as "consumer digital property" by installing a "digital boundary" on their computing devices, such as computers, cable or DSL modems,[101] wireless transmitters or even mobile phones accessing the Internet.[102] The digital boundary is simply a standard form digital file that any incoming or outgoing transmission could readily detect. The function of the digital boundary file is to provide notice in all communications to or from the computing device that the device is protected under the CDTA. Anyone seeking to install spyware on a device or to

---

99. The proposed Consumer Digital Trespass Act (hereinafter "CDTA") is attached as Appendix 1.

100. *See* Appendix 1.

101. *See* Thomas Claburn, *DSL Modems Becoming Botnet Zombies*, INFORMATION WEEK (Mar. 25, 2009, 4:58 PM), *available at*, http://www.informationweek.com/news/security/vulnerabilities/showArticle.jhtml?articleID=216300399.

102. CDTA, *infra* App. 1, at Section 1(b).

transmit protected data from the device would be required to design their software to detect the digital boundary and comply with the CDTA in order to avoid digital trespass liability.

Under the CDTA, "digital trespasses" can occur either by unauthorized transmissions *into* the computing devices, or by unauthorized transmissions *out of* the device.[103] The types of digital trespass are based upon threats identified in the SPY-ACT passed by the U.S. House of Representatives in 2007[104] and the threats identified by the Anti-Spyware Coalition.[105] The CDTA enumerates nine forms of *incoming* digital transmissions that constitute a digital trespass if installed on the device. Examples of the most serious incoming trespasses are installation of monitoring software used for keylogging, for disabling of the digital boundary file, or other security or anti-spyware software, for collection of personally identifiable information,[106] or for using the device to send spam, deliver ads or as part of a botnet to spread malware or cause damage to other computers.[107] Incoming transmissions that are not prohibited by the CDTA may be received into the computer without legal consequence, unless they cause harm to or interfere with the computer.[108]

Comment [RK5]: Please note new footnote.

Consumers may consent to incoming installations, provided that a "robust notice" as defined in the CDTA precedes such consent.[109] Robust notice requires explicit disclosure of the

---

103. CDTA, *infra* App. 1, at Section 2.

104. Securely Protect Yourself Against Cyber Trespass Act (SPY-ACT), H.R. 964, 110th Cong. (2007).

105. ANTI-SPYWARE COALITION, BEST PRACTICES: GUIDELINES TO CONSIDER IN THE EVALUATION OF POTENTIALLY UNWANTED TECHNOLOGIES (2007), http://www.antispywarecoalition.org/documents/documents/best_practices_final_working_report.pdf.

106. CDTA, *infra* App.1, at Section 1 (g). The definition of personally identifiable information also is taken from the SPY-ACT, *supra* note 103.

107. CDTA, *infra* App. 1, Section 2 (a).

[108] Causing harm or interference with the computer would trigger trespass to chattels liability under existing tort law as discussed in Section II, *supra.*

Formatted: Font: Italic

109. CDTA, *infra* App. 1, at Section 1 (h). The concepts of robust notice and informed consent were developed in an article by Jordan M. Blanke. *See* Blanke, *supra* note 82.

potentially harmful features of the software to be installed. It also requires an affirmative consent by the user to each offending installation, along with an option to abandon the installation and remove the item completely at any time. Providing consent by means of a browsewrap agreement or by terms of use on a website would not be sufficient. A digital trespass occurs if the software is installed on the device without robust notice.

The CDTA also enumerates seven forms of *outgoing* transmissions that constitute a digital trespass.[110] Examples of outgoing digital trespasses are transmissions for spam, botnets, distributed denial of service attacks, or for disclosure of web browsing history or personally identifiable information. Consumers may provide an "informed consent" to these transmissions that complies with the CDTA.[111] Informed consent requires 1) a clear and conspicuous warning that the protected information is about to be transmitted, 2) an affirmative consent, and 3) the option to completely remove, or "uninstall" the software being used to transmit the information.[112] Transmissions of prohibited information without satisfying all three features of informed consent are a digital trespass.

Digital trespasses under the CDTA trigger a statutory damage remedy without the need for the consumer to show damage to the computing device or any other harm. This right of recovery is substantially limited so as to avoid unduly burdening the network benefits of the Internet. First, the CDTA only protects designated consumer computers. Corporate and business interests make greater use of the network benefits of the Internet but business computers will be unaffected. Businesses are capable of understanding the risks and rewards of their online presence and can calculate the costs and benefits for their business accordingly.

---

110. CDTA, *infra* App. 1, at Section 2 (b).

111. CDTA, *infra* App. 1, at Section 1 (f). *See* Blanke, *supra* note 82.

112. CDTA, *infra* App. 1, at Section 1 (f).

They have the money and expertise to use self-help to limit their exposure to spyware and to protect their valuable information from Internet risks. Business interests also are able to spread the risks and costs of security measures through insurance and through pricing of their goods and services.

Second, not every unwelcome incoming or outgoing transmission to consumers' computers causes a digital trespass. The CDTA identifies only the most harmful and disruptive spyware operations[113] as digital trespasses. Unwelcome messages such as those that Ken Hamidi sent to Intel Corporation would not trigger CDTA liability even if sent to consumer computers. The CDTA will have no effect on freedom of speech and will preserve the network benefits of free information flow on the Internet. In addition, the consumer can authorize even those transmissions restricted by the CDTA if the muscular "robust notice" and "informed consent" requirements are met. Consumers can decide for themselves in real time whether the so-called "free" content they receive is valuable enough to earn their informed consent. The CDTA merely provides them with full knowledge that in the future they may experience interferences with their computing power, bandwidth and privacy interests in exchange for that content. This approach protects the beneficial network effects of the Internet by continuing the widespread sharing of information among Internet participants, while imposing liability only on the most harmful spyware transmissions.

Consumers can recover nominal statutory damages for digital trespass without proof of actual damage to their computing devices.[114] In essence, the CDTA makes the consumer computer partially inviolable. While this may seem oxymoronic, it protects consumers from most harmful spyware activities in their dealings with otherwise legitimate business and

---

113. *See* SPY-ACT, *supra* note 103; ANTI-SPYWARE COALITION, *supra* note 104.

114. CDTA, *infra* App. 1, at Section 3 & Section 5(c).

commercial interests. Yet, it does not trigger a flood of liability for *de minimus* interferences with consumer computers that have been heavily criticized by opponents of the early cybertrespass cases. Actual damages also are recoverable for harm to the computer and its operations and for consequential damages that result.[115] Because the statutory damages are small with respect to each transmission and each individual consumer, class actions are specifically authorized[116] as are recovery of attorney fees and costs.[117] Losses to offenders will be substantial if the spyware users commit digital trespasses on a large scale, and thus will act as a strong deterrent.

Perhaps the most important remedy is the joint and several liability of all parties who either participate in installing or using spyware to track consumers' behavior while they use their own computers or those who distribute the information gathered by spyware monitoring.[118] The behavioral marketing "ecosystem" includes advertisers, advertising agencies, web publishers, Internet access services providers, desktop application software providers and online advertising networks.[119] With the growing market for online advertising exceeding $20 billion dollars, the participants in this ecosystem all profit from being able to compile sophisticated profiles of consumer Internet users using the most advanced tracking tools. This allows the advertisements to be targeted, relevant, and most cost-effective. These detailed consumer profiles are valuable and very profitable for those who compile, sell and use

Deleted: in using

Deleted: and the

Deleted:

Deleted: ion

Deleted: of the content transmitted

Comment [RK6]: The content of the footnote 118 appears to be incorrect. I think it should be "CDTA, *infra* App. 1, at Section 5 (e). Do your agree?

115. CDTA, *infra* App. 1, at Section 5 (b).

116. CDTA, *infra* App. 1, Section 5 (f).

117. CDTA, *infra* App. 1, at Section 5 (d).

118. The proposed Consumer Digital Trespass Act ("CDTA") is attached as Appendix 1,118 §5(e).

Formatted: Highlight

119. FED. TRADE COMM'N, STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING, *supra* note 45, at 19. These Principles were jointly developed by the American Association of Advertising Agencies, the Association of National Advertisers, the Council of Better Business Bureaus, the Direct Marketing Association, and the Interactive Advertising Bureau. *Self-Regulatory Principles for Online Behavioral Advertising*, IAB (July 2009), http://www.iab.net/media/file/ven-principles-07-01-09.pdf.

them. Perhaps the most extreme proposal was for ad networks, such as NebuAd, to partner with ISPs to analyze all consumer communications using a "deep packet inspection" technique.[120]

The CDTA seeks to "follow the money" as it moves through the behavioral advertising ecosystem by holding all participants jointly responsible for legal compliance with the CDTA. This will ensure that advertisers and other industry participants will not turn a blind eye to deceptive methods for installing monitoring software or to be willfully ignorant of improper consent when creating the ad distribution networks. Reputable advertisers would insist on fully compliant advertising agencies, partners and networks to avoid liability and damage to their brands. Any new information transmitted from existing spyware installations would have to comply with the informed consent requirements of the CDTA. This would, in most cases, require that already installed monitoring software be disabled or removed, or to be modified and replaced with new CDTA-compliant installations. These new installations would have to comply with the CDTA's robust notice provisions.

The behavioral advertising model is based on the questionable assumption that consumers make fully informed and knowledgeable choices about the costs and benefits of their online behavior. Consumers readily perceive the benefits they receive from the use of purportedly "free" software or website access, but they do not truly understand their costs. Consumers bear the costs of behavioral advertising in the form of lost privacy, diminished computer performance and a poor user experience. Often the "consent" consumers provide in license agreements, privacy policies or in the terms of use of a browsewrap agreement is of

---

120. *See* CENTER FOR DEMOCRACY & TECHNOLOGY, AN OVERVIEW OF THE FEDERAL WIRETAP ACT, ELECTRONIC COMMUNICATIONS PRIVACY ACT, AND STATE TWO-PARTY CONSENT LAWS OF RELEVANCE TO THE NEBUAD SYSTEM AND OTHER USES OF INTERNET TRAFFIC CONTENT FROM ISPS FOR BEHAVIORAL ADVERTISING 2 (2008), http://www.cdt.org/privacy/20080708ISPtraffic.pdf.

questionable integrity.[121] Many consumers, if not most, would be unaware of the full nature, extent and frequency of the online surveillance to which they are subjected and of the degree to which their information is sold and aggregated to support behavioral advertising.[122] Consumers have little, if any, control over their data once it has been captured from their computers. The CDTA enables consumer choices by making the cost-benefit calculation more transparent and explicit for the consumer by requiring affirmative opt-in provisions both for incoming and outgoing transmissions. They are able to affirm or change these choices with each transmission. If the value of the "free" content is sufficient to justify the costs - once fully understood - then the behavioral advertising industry will remain essentially unchanged by the CDTA.

A more likely scenario is that consumers will insist on greater value in the content they access, or will demand lower costs in terms of their lost privacy and their computer's performance. The CDTA shifts the costs of using spyware for behavioral advertising back to the parties who both benefit most from it and have the greatest ability and opportunity to reduce or prevent the costs to consumers. Not every incoming or outgoing transmission triggers CDTA liability. Only the most harmful practices listed in the CDTA will make behavioral advertisers liable. Advertisers can tailor their activities either to avoid prohibited activities or to obtain the required informed consent. Consumers will likely avoid sites that frequently ask

Comment [7]:
Rick Kunkel 11/18/10 11:36 AM
See new footnote 121 below

Comment [8]:
Rick Kunkel 11/18/10 11:36 AM
See new footnote 122 below

---

[121] See, e.g Wayne R. Barnes, Rethinking Spyware: Questioning the Propriety of Contractual Consent to Online Surveillance, 39 U.C. Davis L. Rev. 1545 (20060, and Nancy S. Kim, Clicking and Cringing, 80 Or.L.Rev 797, 822 (2007).

122. *See,* Aleecia M. McDonald and Lorrie Faith Cranor. Americans' Attitudes About Internet Behavioral Advertising Practices; In WPES '10: Proceedings of the 9th Annual ACM Workshop on Privacy in the Electronic Society, (October 4, 2010) available at http://www.aleecia.com/authors-drafts/wpes-behav-AV.pdf. This may be especially true for consumers who share a computer among several family members. For example, a child might be induced to visit several web sites whose terms of use give broad consent to install monitoring software that could copy address books, or download web browsing histories, or obtain other private information that can be sold on to data aggregators, behavioral advertising firms or other third parties. Adult users of the same computer would be unlikely to know that the computer was surreptitiously running monitoring software that reported their every online movement.

Formatted: Normal, Don't adjust right indent when grid is defined, No widow/orphan control, Don't adjust space between Latin and Asian text, Don't adjust space

Deleted:

Deleted: would

Deleted: not

Formatted: Font: (Default) , English (U.S.)

them to consent to outgoing transmissions, either because of the privacy implications or the inconvenience of multiple interruptions. They also may, at any time, exercise the option to uninstall the monitoring software that transmits the protected information. They will gravitate to sites that offer the highest quality content with minimal privacy risk or intrusion on their user experience. This will create a strong incentive for advertisers to limit outgoing transmissions to the bare minimum necessary to support the free site content.

Governmental response to the problem of spyware use in behavioral advertising has been tepid. The Federal Trade Commission (FTC) has not promulgated any enforceable regulations to limit this use of spyware. Instead, the FTC has focused on a program of industry self-regulation first proposed in December 2007.[123] Public comments encouraged the FTC to revise and strengthen the self-regulatory guidelines. In February 2009, the FTC released the new voluntary guidelines.[124] In July 2009, a coalition of industry groups, led by the Interactive Advertising Bureau (IAB), responded with proposed self-regulation principles for industry participants.[125] The IAB proposal carefully defined "behavioral advertising" to exclude coverage of several industry practices that affect consumer privacy. Privacy advocacy groups criticized both the FTC and IAB schemes as inadequate. These groups instead recommended federal legislation to deal more comprehensively with online privacy interests based on Fair Information Principles.[126]

---

123. FED. TRADE COMM'N, ONLINE BEHAVIORAL ADVERTISING: SELF-REGULATORY PRINCIPLES 1 (2007), *available at* http://www.ftc.gov/os/2007/12/P859900stmt.pdf.

124. FED. TRADE COMM'N, STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING, *supra* note 45.

125. *Id.*

126. CENTER FOR DIGITAL DEMOCRACY ET AL., ONLINE BEHAVIORAL TRACKING AND TARGETING, LEGISLATIVE PRIMER SEPTEMBER 2009 4 (2009), http://www.democraticmedia.org/files/privacy-legislative-primer.pdf.

The FTC, industry and privacy group proposals are helpful because they address a broad spectrum of behavioral advertising industry practices that are harmful to consumer privacy. However, industry self-regulatory programs are unlikely to be successful because they are not likely to cover or be enforced against all entities, and are unlikely to be fully implemented.[127] The FTC admits that its self-regulatory guidelines are heavily dependent upon industry members' own willingness to "actively monitor compliance and ensure that violations have consequences."[128] Because industry members are not legally required to follow the FTC principles, any FTC investigation and enforcement will likely be based on the FTC's general principles governing unfair or deceptive practices.[129] Proposals for comprehensive federal privacy legislation are necessary and highly desirable, but may take several years to enact. In addition, these proposals would rely on the FTC for investigation and enforcement. The FTC has a broad consumer protection mandate and limited enforcement resources. Enforcement of any new privacy legislation will likely be as limited as its response to spyware - an infrequent handful of enforcement actions.[130]

Comment [RK9]: See footnote - remove the hyperlinking feature?

The CDTA approach to the issue of behavioral advertising is more focused, clear, and empowering for consumers. It does not attempt to solve the full range of privacy concerns that arise once spyware has collected private consumer data. The CDTA addresses the problem of behavioral advertising by focusing on the consumer's desktop, which is the primary source of the surreptitious data collection that is used to build consumers' advertising profiles. Instead of

---

127. CENTER FOR DEMOCRACY AND TECHNOLOGY, ONLINE BEHAVIORAL ADVERTISING: INDUSTRY'S CURRENT SELF-REGULATORY FRAMEWORK IS NECESSARY, BUT STILL INSUFFICIENT ON ITS OWN TO PROTECT CONSUMERS 3, 35 (2009), http://www.cdt.org/files/pdfs/CDT%20Online%20Behavioral%20Advertising%20Report.pdf.

128. FED. TRADE COMM'N, STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 47 (2009), *available at* http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.

129. CENTER FOR DEMOCRACY AND TECHNOLOGY, ONLINE BEHAVIORAL ADVERTISING: INDUSTRY'S CURRENT SELF-REGULATORY FRAMEWORK IS NECESSARY, BUT STILL INSUFFICIENT ON ITS OWN TO PROTECT CONSUMERS, *supra* note 124.

130. *See* discussion *supra* at footnote 39 and accompanying text.

broad privacy principles, it clearly defines specific forms of prohibited conduct and the actions required for behavioral advertisers to obtain robust notice and informed consent from consumers. This clarity provides a safe harbor for the behavioral advertising industry to seek information from consumers in a transparent way that respects consumers' informed choices about their privacy.

The CDTA empowers consumers in a number of ways. It protects the computer owner's inviolability interest in the use and control of their own property by correcting the flaws in the trespass to chattels rules under the *Hamidi* case. It gives consumers power to make a truly informed choice in real time about the costs and benefits of the "free" content and access they receive on the Internet as they are accessing the content. Finally, the CDTA's private right of action places both the control of the computer and control of the legal remedy in the same hands - the consumer computer owner. When faced with the possibility of class action lawsuits, statutory damages and attorneys' fees and costs, behavioral advertisers will have strong incentives to limit the data they collect from consumer computers. They also will be motivated to develop and enforce stringent advertising placement practices and will partner only with behavioral advertising partners capable of rigorous compliance with the CDTA.

CONCLUSION

This article proposes that a Consumer Digital Trespass Act be enacted to give consumers the power to take action to protect themselves against the spyware used to monitor their behavior online. The CDTA fills the gap between the tort remedies of trespass to land and trespass to chattels that leave consumers without a meaningful remedy to spyware risks. The CDTA's narrow focus preserves the network benefits of the Internet. The CDTA's clear requirements for robust notice and informed consent give consumers a transparent and effective choice to control and protect the private data on their computers. The CDTA's remedies create the proper

incentives for behavioral advertisers limit the amount of information they collect and to collect information responsibly. The CDTA strikes a proper balance between the benefits of the "free" content supported by behavioral advertising and the right of consumers to control the operations of their own computers and access to the private information stored on them.

Appendix 1

The Consumer Digital Trespass Act

Section 1. DEFINITIONS.

For the purposes of this Act-

(a) Authorized User means the owner or lessee of consumer digital property or any person in the owner or lessee's household authorized by the owner or lessee to use the consumer digital property.

(b) Computer means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. This term includes a modem, router or other transmission device connected to the computer and a mobile phone used to connect to the Internet.

(c) Consumer means a natural person.

(d) Consumer Digital Property means a computer owned or leased by a consumer that is used by authorized users primarily for personal, family, or household purposes, and on which a digital boundary has been installed.

(e) Digital Boundary means a digital data file or document in a form prescribed by the United States Federal Trade Commission and stored on consumer digital property. The digital boundary shall

be 1) in a form detectable by other computers which attempt to access or transmit information to or from consumer digital property by means of the Internet or any computer network; 2) shall provide notice that the computer on which the digital boundary is installed is consumer digital property; 3) provide notice of the state in which the consumer is a resident; and 4) provide a reference to this Act.

(f) Informed Consent means a clear and conspicuous notice in a form specified by the United States Federal Trade Commission, which shall contain all of the following elements:

(1) For each digital trespass activity described in Section 2 (b), (1) to (6), a separate Warning Statement shall be displayed on successive computer screens: "Warning - software installed or executed on your computer is being used to transmit information to {insert description from applicable section of Section 2 (b), (1) to (6)}. Would you like to: 1) Stop the transmission of the information, or 2) Consent to the transmission, or 3) Remove the software from your computer?" A clearly labeled clickable button shall be provided for each option.

(2) The default option shall be to stop the transmission.

(3) If affirmative consent is given, for successive outgoing transmission described in Section 2 (b), (1) to (6), a separate warning, as applicable, shall be displayed, and the notices specified in (a) and (b) above shall be completed with regard to each successive digital trespass activity described in Section 2 (b), (1) to (6) that is applicable.

(4) The requirement of informed consent may not be waived, limited or modified.

(g) Personally Identifiable Information means the following information, to the extent only that such information allows a living individual to be identified or re-identified from that information:

(1) First and last name of an individual.

(2) A home or other physical address of an individual, including street name, name of a city or town, and zip code.

(3) An electronic mail address.

(4) A telephone number.

(5) A social security number, tax identification number, passport number, driver's license number, or any other government-issued identification number.

(6) A credit card number.

(7) Any access code, password, or account number, other than an access code or password transmitted by an owner or authorized user of a protected computer to the intended recipient to register for, or log onto, a web page or other Internet service or a network connection or service of a subscriber that is protected by an access code or password.

(8) Date of birth, birth certificate number, or place of birth of an individual, except in the case of a date of birth transmitted or collected for the purpose of compliance with the law.

(h) Robust Notice means a clear and conspicuous notice in a form specified by the United States Federal Trade Commission, which shall be contain all of the following elements:

(1) For each digital trespass activity described in Section 2 (a), (1) to (9), a separate Warning Statement shall be displayed on successive computer screens: "Warning - if installed, this software will {insert description from applicable section of Section 2 (a), (1) to (9)}. Do you consent to continue the installation of this software?"

(2) The default option shall be to deny consent and to abandon or cancel the installation.

(3) Upon affirmative consent, the user shall be presented with the option to obtain a clear description of the software to be installed and its functions and the type of information to be collected, if any, and the manner in which it may be used, before proceeding with the installation. The default option shall be to view the information. After viewing the description, or upon declining the option to view, the user shall be presented with another screen stating: "Do you consent to continue the installation of this software?" The default option shall be to deny consent and to abandon or cancel the installation.

(4) If affirmative consent is given, the next successive applicable warning regarding a digital trespass activity described in Section 2 (a), (1) to (9), if any, shall be displayed, and the notices specified in (h)(1) through (h)(3) above shall be provided with regard to each successive form of digital trespass activity described in Section 2 (a), (1) to (9) that is applicable.

(5) Only after all warnings have been displayed, and affirmative consent is given to each warning displayed, shall robust notice be considered completed and the software of information may be permitted to download.

(6) The requirement of robust notice may not be waived, limited or modified.

Section 2. DIGITAL TRESPASS. The following acts shall constitute a digital trespass:

(a) transmitting to consumer digital property any computer software, information collection program or other digital code or instructions that is installed, stored or executed on consumer digital property without robust notice to the authorized user, by any person who is not an authorized user, that is used or may be used to exercise control over the computer's functions, processes, or settings to:

(1) divert the Internet browser of the computer, or similar program of the computer used to access and navigate the Internet, away from the site the user intended to view, to one or more other web pages, such that the user is prevented from viewing the content at the intended web page;

(2) utilize such computer to send unsolicited information or material from the computer to others, including unsolicited email or transmissions used as part of a distributed denial of service attack;

(3) access, hijack, or otherwise use the modem, or Internet connection or service, for the computer for a service not authorized by the owner or authorized user;

(4) use the computer as part of an activity performed by a group of computers that causes damage to another computer or a violation of this Act on other consumer digital property, including sending of unsolicited email or transmissions used as part of a distributed denial of service attack;

(5) deliver advertisements or a series of advertisements that a user of the computer cannot close without undue effort or knowledge by the user or without turning off the computer or closing all sessions of the Internet browser for the computer;

(6) modify settings related to use of the computer or to the computer's access to or use of the Internet by altering--

(i) the web page that appears when the owner or authorized user launches an Internet browser or similar program used to access and navigate the Internet;

(ii) the default provider used to access or search the Internet, or other existing Internet connections settings;

(iii) a list of bookmarks used by the computer to access web pages; or

(iv) security or other settings of the computer that protect information about the owner or authorized user;

(7) collect personally identifiable information through the use of a keystroke logging function or any other information collection program;

(8) collect information regarding web pages accessed using the computer through the use of a keystroke logging function or any other information collection program; or

(9) remove, disable, or render inoperative a digital boundary file, or any security, anti-spyware, or anti-virus technology installed on the computer;

or,

(b) transmitting from consumer digital property by means of computer software or hardware, an information collection program or any other digital code or instructions, whether or not installed or stored on consumer digital property, by any person who is not an authorized user, without the informed consent of an authorized user, any computer software, information collection program,

any other digital code or instructions or any information or data that is or may be executed or otherwise controlled or used to:

(1) send unsolicited information or material from the computer to others;

(2) access, hijack, or otherwise use the modem, or Internet connection or service, for the computer;

(3) use the computer as part of an activity performed by a group of computers that causes damage to another computer;

(4) disclose any personally identifiable information of any authorized user of the computer;

(5) disclose any information regarding web pages accessed using the computer that is used to deliver advertising to, or display advertising on, the computer; or

(6) remove, disable, or render inoperative a digital boundary, or a security, anti-spyware, or anti-virus technology installed on the computer.

(c) Limitation on Information Retention. Retention of any personally identifiable information or any web page access information that is disclosed or collected pursuant to informed consent under this Act may not be retained for more than 90 days after the date of informed consent unless the information is modified so as to no longer be identifiable to any specific person or computing device or any IP address.

Section 3. DAMAGE NOT REQUIRED.

It is unnecessary to prove any damage to the computer hardware, computer devices or systems or processing power, software, and any contents stored on the computer in order to recover in a civil action the remedies set forth in Section 5.

Section 4. INTENTION UNNECESSARY.

It is unnecessary to prove any intention to commit a digital trespass or intention to cause damage or harm in order to recover under this Act. The only intention required is the intention to cause the transmission of the computer software, information collection program or other digital code or instructions that result in the digital trespass.

Section 5. REMEDIES

(a) Private Right of Action. Any owner of consumer digital property who suffers a digital trespass may commence a civil action for injunctive relief and the other remedies specified in this section.

(b) Damages. Any person who commits digital trespass shall be liable for any damage caused to the consumer digital property including the computer hardware, computer systems or processing power, software, and any contents stored on the computer, and for any consequential damages resulting therefrom.

(c) Statutory Damages: For digital trespasses under Section 2 (a), statutory damages of $.10 per trespass shall be awarded. For digital trespasses under Section 2 (b), statutory damages of $.25 per trespass shall be awarded.

(d) Attorney Fees and Costs. Costs shall be allowed to the owner of the consumer digital property unless the court otherwise directs. The court in its discretion may award attorneys' fees to the owner of the consumer digital property if the party causing a digital trespass has willfully engaged in digital trespass.

(e) Joint and Several Liability. If a digital trespass occurs in connection with the delivery of advertising to, or display advertising on the computer, then all parties who received any consideration in connection with causing the delivery or display in violation of this act shall be jointly and severally liable for all damages, costs, attorney fees and other remedies awarded under this Act.

(f) Class Actions Authorized. Class actions to recover remedies under this Act are specifically authorized.