COMMENTS

Oh, What a Tangled World Wide Web We Weave: An Analysis of Washington's Computer Spyware Act in a National Context

Laura L. Edwards†

I. INTRODUCTION

A spyware epidemic is compromising computer security in America.[1] Although the technology sector has not yet agreed on a formal definition,[2] spyware is commonly described as a type of software that can track the online activities and collect the personal information of Internet users.[3] Spyware is often installed without a user's knowledge[4]

---

† J.D. Candidate, 2008, Seattle University School of Law; B.A., Communication, Edward R. Murrow School of Communication, Washington State University, 2005. The author dedicates this Comment to her parents, Locky and Gin Edwards, for their steadfast encouragement and lifelong support. The author would also like to thank Lauren McLane, Justin Walsh, Erin Blinn, Katie Feero, and Andrew Hofeling for helping the author keep a level head during her law school years. Finally, the author would like to thank Professor Lori Bannai for imparting her legal writing wisdom, and Jon Minear and the *Seattle University Law Review* for their editing support.

1. *See* WEBROOT SOFTWARE, INC., STATE OF SPYWARE 30–32 (2005–2006), http://www.antyspyware.pl/state-of-spyware/2005-q4-sos.pdf (reporting that more than 400,000 websites hosted spyware in 2005 and 30.5% of the world's spyware originated in the United States). Spyware is "[s]oftware that self-installs on computers and tracks the user's Internet use, mainly for marketing purposes." THE NEW OXFORD AMERICAN DICTIONARY 1643 (2d ed. 2005).

2. *See* FED. TRADE COMM'N, MONITORING SOFTWARE ON YOUR PC: SPYWARE, ADWARE, AND OTHER SOFTWARE 1–5 (2005), http://www.ftc.gov/os/2005/03/050307spywarerpt.pdf (noting that a spyware definition is elusive because of the technical complexity and dynamic nature of software).

3. *See, e.g.*, *id.* at 4 (describing spyware as "software that aids in gathering information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge"); National Conference of State Legislatures, 2005 State Legislation Relating to Internet Spyware or Adware, http://www.ncsl.org/programs/lis/spyware05.htm (last visited Mar. 17, 2008) [hereinafter 2005 State Legislation].

4. *See* FED. TRADE COMM'N, *supra* note 2, at 3.

and can maliciously change settings on the user's computer[5] or cause advertising messages, commonly known as pop-ups, to appear on the user's
computer screen.[6] Difficult to detect and sometimes nearly impossible to remove, spyware has emerged as a significant security problem for Internet users.[7]

Spyware affects businesses as well as individuals.[8] Spyware can expose a company's confidential information, slow down computers and networks, and destroy data.[9] Employees lose efficiency while waiting for IT staff to fix the various problems caused by spyware, which increases costs.[10] Accordingly, spyware is not just a minor annoyance suffered by individual Internet users; rather, it harms American businesses and the economy as well.[11]

Washington and several other states have recently passed antispyware legislation.[12] This Comment will focus on the effectiveness of Washington's Computer Spyware Act (the Act),[13] while also surveying similar legislation from other states and approaches proposed at the federal level. Part II discusses the Act's content and briefly explains its definition of prohibited spyware and activities. Part III examines two early cases to invoke the Act and describes their procedural history, from filing to settlement. Part IV analyzes the Utah and California spyware statutes, which blazed the trail in this emerging area of law.[14] Moreover, at the time the first Washington lawsuits were filed, these statutes provided virtually the only state statutory guidance for Washington courts evaluating the Act.[15] Part V evaluates the current status of proposed federal spyware legislation and the role of the Federal Trade Commission

---

5. *Id.* at 9 (discussing browser hijacking).

6. *Id.* at 3–4; Chana R. Schoenberger, *Spy vs. Spy*, FORBES.COM, Jan. 17, 2005, http://www.forbes.com/personaltech/2005/01/17/cz_cs_0117spyvsspy.html.

7. FED. TRADE COMM'N, *supra* note 2, at 7–8.

8. *See* Arik Hesseldahl, *Fried by Spyware*, FORBES.COM, Jan. 17, 2005, http://www.forbes.com/enterprisetech/2005/01/17/cx_ah_0117spyfry.html.

9. *See* Microsoft.com, Microsoft's Spyware Strategy (Feb. 13, 2006), http://www.microsoft.com/athome/security/spyware/software/msft/strategy.mspx.

10. Silicon.com, Make No Mistake - Spyware Impacts Your Business (May 2005), http://whitepapers.silicon.com/0,39024759,60136305p,00.htm.

11. *See* Hesseldahl, *supra* note 8.

12. Benjamin Edelman, State Spyware Legislation, http://www.benedelman.org/spyware/legislation/ (last visited Mar. 17, 2008).

13. WASH. REV. CODE §§ 19.270.010–.900 (2008).

14. Andrew T. Braff, *Defining Spyware: Necessary or Dangerous*, 2 SHIDLER J.L. COM. & TECH. 1, 1 n.6 (2005), *available at* http://www.lctjournal.washington.edu/Vol2/a001Braff.html. Utah's Spyware Control Act is codified at UTAH CODE ANN. §§ 13-40-101 to -401 (2007), and California's Consumer Protection Against Computer Spyware Act is codified at CAL. BUS. & PROF. CODE §§ 22947–22947.6 (West 2007).

15. Braff, *supra* note 14.

(FTC) in adjudicating spyware disputes. Although no federal statutes on this subject have yet been enacted, the bills currently under consideration demonstrate the two leading approaches for penalizing spyware usage. Finally, Part VI proposes three changes to the Act that will more effectively deter prohibited conduct and compensate its victims. First, the Act's notice requirement must be more specific. Second, the plaintiff's burden of proving the defendant's intentional deceit should be eased; the Act should place the burden on the defendant by creating a rebuttable presumption of intentional deceit on the defendant's part. Finally, the legislature must increase the damages cap. These amendments will ensure that Washington remains a national leader in protecting its citizens from invasive spyware.

II. THE WASHINGTON COMPUTER SPYWARE ACT

The Act, which took effect in July 2005, makes it "unlawful for a person who is not an owner or operator to transmit computer software to the owner or operator's computer with actual knowledge or with conscious avoidance of actual knowledge," when that software is used in certain ways.[16] Such prohibited uses include: modifying security settings; collecting Internet browser histories or personally identifiable information; tracking keystrokes; preventing the blocking of software installation; and inducing the purchase of software by falsely identifying spyware or viruses on a user's computer.[17] The Act does not prohibit software that monitors a computer user's Internet connection if the monitoring is executed by a telecommunications carrier, software provider, or computer service providing authorized software updates,[18] because these activities aid in proper Internet functioning.[19]

Only the Attorney General of Washington or an adversely affected software provider, website owner, or trademark owner may bring suit for a violation of the Act.[20] A plaintiff who alleges that a defendant modified certain computer settings must prove that the defendant acted with an intent to deceive.[21] To prove that a defendant transmitted software to tamper with computer functions, a plaintiff must show that the defendant

16. § 19.270.020.

17. *Id.*

18. § 19.270.050.

19. Free On-line Dictionary of Computing, http://foldoc.org/index.cgi?query=spyware (last visited Mar. 17, 2008).

20. § 19.270.060.

21. § 19.270.020; H.B. 1012, 59th Leg., Reg. Sess. (Wash. 2005); Legal Opinion Letter from Rob McKenna, Att'y Gen., State of Wash., Washington Spyware Law Addresses Serious Online Commercial Threat (Aug. 18, 2006), http://www.wlf.org/upload/081806mckennalol.pdf.

had actual knowledge or conscious avoidance of actual knowledge of his or her software transmission.[22]

Damages awarded under the Act are limited to either $100,000 per violation or actual damages, whichever is greater.[23] Total damages may not exceed $2 million.[24] Repeat offenders, however, may incur a three-fold increase in damages at the court's discretion, subject to the cap of $2 million.[25]

III. EARLY WASHINGTON CASES

Early in 2006, the Attorney General filed the first suit under the Act in *State v. Secure Computer, L.L.C.*, alleging that the defendants had performed false spyware scans in order to induce users to buy their products.[26] Then, in August 2006, the Attorney General brought a second suit against four Los Angeles companies in *State v. Digital Enterprises, Inc.*, alleging that the companies had distributed harmful spyware to users under the guise of promoting the companies' subscription-based entertainment services.[27] Because settlements with individual defendants have been reached in these two cases, neither case was decided in court.[28] Nevertheless, their procedural histories may provide guidance for other courts attempting to apply antispyware legislation, which currently have a limited body of case law to consult.[29]

---

22. § 19.270.030.

23. § 19.270.060(1).

24. § 19.270.060(3).

25. § 19.270.060(2).

26. Complaint for Injunctive and Additional Relief under the CAN-SPAM Act, the Unsolicited Commercial Email Act, the Computer Spyware Act, and the Unfair Bus. Practices–Consumer Prot. Act ¶¶ 8.10–.13, State v. Secure Computer, L.L.C., No. C06-0126RSL (W.D. Wash. Jan. 24, 2006), 2006 WL 317035 [hereinafter Complaint, State v. Secure Computer, L.L.C.]; *see also* Complaint for Damages and Injunctive Relief ¶¶ 70–74, Microsoft Corp. v. Secure Computer, L.L.C., No. CV06-0128 JCC (W.D. Wash. Jan. 25, 2006), 2006 WL 236341.

27. Complaint for Injunctive and Additional Relief under the Unfair Bus. Practices–Consumer Prot. Act and the Computer Spyware Act ¶¶ 6.1–6.8, 7.1–7.3, State v. Digital Enterprises, Inc., No. CV06-4923 CAS (W.D. Wash. Aug. 4, 2006) [hereinafter Complaint, State v. Digital Enterprises, Inc.] (on file with author).

28. McKenna, *supra* note 21.

29. Although several lawsuits based upon state spyware statutes have been filed, many have settled out of court. *See generally Sony BMG Settles CD Case*, N.Y. TIMES, May 23, 2006, at C4, *available at* 2006 WLNR 8813358; *Sony BMG Tentatively Settles Suits on Spyware*, N.Y. TIMES, Dec. 30, 2005, at C4, *available at* 2005 WLNR 22097854; Lisa Lerer, *Anti-Spyware Settlement*, FORBES.COM, Dec. 4, 2006, http://www.forbes.com/security/2006/12/04/spyware-settlement-washington-tech-security-cx_ll_1204spyware.html.

A. State v. Secure Computer, L.L.C.

State v. Secure Computer, L.L.C. was the first lawsuit filed under the Act.[30] The Attorney General filed the complaint against Secure Computer, a New York limited liability company, its president, and four individuals who allegedly advertised or otherwise aided the distribution of the company's products.[31] The complaint accused Secure Computer of violating two provisions of the Act.[32]

First, the complaint alleged that Secure Computer violated Revised Code of Washington (RCW) section 19.270.040(1) by intentionally marketing and selling products that purported to scan computers for spyware, alarming users, and enticing (or even forcing) them to purchase the products.[33] The complaint further alleged that Secure Computer persuaded users to get a free scan with pop-up advertisements that mimicked the Microsoft Windows security "dialog boxes."[34] These boxes advised users that their computers might be infected with spyware; when users clicked the box, they were guided through a process that downloaded Secure Computer spyware onto their computers.[35] Moreover, the complaint alleged that these scans failed to detect spyware on infected computers and purported to detect spyware on computers that had none.[36] Following the free scan, users received a false scan report that listed the types of spyware claimed to be found on their computers.[37] When users clicked the button to remove the spyware, the dialog box prompted users to purchase "Spyware Cleaner" for $49.95 by inputting credit card and other information.[38]

---

30. Complaint, State v. Secure Computer, L.L.C., *supra* note 26; *see also* Robert McMillan, *Antispyware Company Sued under Spyware Law*, PC WORLD, Jan. 26, 2006, http://www.pcworld.com/article/id,124508-page,1/article.html.

31. Press Release, Wash. State Office of the Att'y Gen., Attorney General McKenna Announces $1 Million Settlement in Washington's First Spyware Suit (Dec. 4, 2006), *available at* http://www.atg.wa.gov/pressrelease.aspx?id=5926 [hereinafter Press Release].

32. Complaint, State v. Secure Computer, L.L.C., *supra* note 26, ¶¶ 8.8, .13, .21 (alleging violations of WASH. REV. CODE §§ 19.270.030(2)(b), .040(1) (2008)); *see also* Press Release, *supra* note 31.

33. Complaint, State v. Secure Computer, L.L.C., *supra* note 26, ¶¶ 8.2, .8; *see* WASH. REV. CODE § 19.270.040(1) (2008) (providing that it is unlawful for a person who is not an owner or operator to "[i]nduce an owner or operator to install a computer software component onto the computer by intentionally misrepresenting the extent to which installing the software is necessary for security or privacy reasons").

34. Complaint, State v. Secure Computer, L.L.C., *supra* note 26, ¶ 8.3. A "dialog box" is a window utilized in user interfaces to display information to the user or to get a response. THE AMERICAN HERITAGE DICTIONARY OF THE ENGLISH LANGUAGE 500 (4th ed. 2000).

35. Complaint, State v. Secure Computer, L.L.C., *supra* note 26, ¶ 8.4.

36. Press Release, *supra* note 31.

37. Complaint, State v. Secure Computer, L.L.C., *supra* note 26, ¶¶ 8.5–.6.

38. *Id.* ¶ 8.6.

Second, the complaint alleged that Secure Computer violated RCW section 19.270.030(2)(b) when Secure Computer transferred software to users' computers that altered the users' security settings.[39] Allegedly, the free scan software that produced the false scan reports also erased safeguards that users placed on their computers to protect themselves from viruses and spyware, rendering the computers more susceptible to these dangers.[40]

By June 2006, three individually named defendants settled for sums ranging from $2,000 to $84,000.[41] The case ended in December 2006 when Secure Computer president Paul Burke agreed to a $1 million settlement, of which only $75,000 was allocated to compensate the 1,145 Washington consumers who bought and were harmed by the software.[42] The State allocated the remaining $925,000 for penalties, attorney's fees, and costs.[43] Secure Computer is now out of business.[44] Although this case did not create any precedent to guide future courts deciding disputes under the Act, it put spyware companies on notice that violations of the Act will result in prosecution.

B. State v. Digital Enterprises, Inc.

In August 2006, the Attorney General brought suit against four Los Angeles companies and two individuals for allegedly promoting an online subscription-based entertainment service in violation of the Act.[45] The service provided movie clips, adult content, entertainment reviews, and Internet shopping information.[46] Yearly subscription fees ranged from $85 to $99, and monthly subscription fees ranged from $19.95 to $34.95.[47]

The companies allegedly utilized pop-up advertising to offer a free three-day trial but required computer users to download software in order to accept the offer.[48] Unfortunately, while this software did provide a free trial, it also allowed the defendants to deliver a relentless string of

---

39. *Id.* ¶ 8.20–.21; *see* WASH. REV. CODE § 19.270.030(2)(b) (2008) (providing that "[i]t is unlawful for a person who is not an owner or operator of a user's computer to transmit computer software with actual knowledge or with conscious avoidance of actual knowledge and to use the software to . . . modify any of the [computer's security] settings related to the computer's access to, or use of, the internet").

40. Complaint, State v. Secure Computer, L.L.C., *supra* note 26, ¶ 8.19.

41. McKenna, *supra* note 21.

42. Lerer, *supra* note 29.

43. *Id.*

44. *Id.*

45. Complaint, State v. Digital Enterprises, Inc., *supra* note 27.

46. *Id.* ¶ 5.1.

47. *Id.*

48. *Id.*

pop-up windows demanding payment.[49] These demands covered the computer screen and would not close.[50] Instead, the computer user's only option was to click "Continue," which launched a 40-second video that, again, the user was unable to close.[51] Finally, the user was confronted with a screen that provided only two options: pay the fee or be reminded again approximately one hour later to pay the fee, which would restart the entire process.[52] Eventually, many users tired of the reminders and paid either the monthly or yearly fee.[53] As such, the State alleged, the free three-day trial was nothing but a "smokescreen."[54]

In April 2007, the Attorney General announced a settlement in the case.[55] The defendants agreed to pay $50,000 and to cease offering anonymous free trials to Washington consumers for their movie download service.[56] In addition, they agreed to not install any billing software on a Washington user's computer without his or her express consent, to disclose whether the software will cause any pop-ups, and to clearly state all important contract terms in any advertisement.[57]

The Act specifically prohibits using an Internet service to take control of and damage a user's computer.[58] If no settlement had been reached in this case, the court could have found the defendants liable even though users initially consented to receive the software necessary for the free trial.[59] If, at trial, the State was able to demonstrate that the defendants intentionally misrepresented the software's purpose, actions, or effect, it likely would have prevailed on the issue of the defendants' liability under the Act.[60]

The *Digital Enterprises* defendants could have also been found liable for misrepresenting that their computer software could be uninstalled or disabled by the owner's actions.[61] When users attempted to remove the defendants' software by using the standard "Add/Remove Programs" function, the software allegedly provided a dialog box that either redirected the users to the payment screen or terminated the

49. *Id.* ¶ 5.2.
50. *Id.*
51. *Id.* ¶¶ 6.4–.6.
52. *Id.* ¶¶ 6.6–.7.
53. *Id.* ¶ 5.2.
54. *Id.*
55. Press Release, *supra* note 31.
56. *Id.*
57. *Id.*
58. WASH. REV. CODE § 19.270.040(1) (2008).
59. *See* Complaint, State v. Digital Enterprises, Inc., *supra* note 27, ¶ 6.3.
60. *See* § 19.270.020(3), .030.
61. § 19.270.020(4).

"Add/Remove Programs" function.[62] Therefore, if the case had not settled, it is quite possible that the court would have agreed with the State's argument that the software was intentionally designed to prevent Internet users from uninstalling the software through reasonable efforts, in violation of the Act.[63]

IV. COMPARISON TO SPYWARE LEGISLATION IN OTHER STATES

In addition to Washington, sixteen states passed antispyware legislation between 2004 and 2006, and a majority of states have considered similar legislation.[64] Utah broke ground in 2004 by passing the Spyware Control Act (SCA),[65] which was the first state statute to regulate spyware. California followed suit and passed the Consumer Protection Against Computer Spyware Act (CPACSA) later that year.[66]

Utah and California were the only states to pass antispyware legislation before Washington;[67] those statutes, therefore, provided virtually the only available guidance for the *Secure Computers* and *Digital Enterprises* courts. This Part begins by describing the SCA and discussing an important spyware case filed under it, *WhenU.com, Inc. v. State*.[68] Next, the Part describes the CPACSA and the class action suit against Sony BMG Music Entertainment that invoked it.[69]

A. Utah: The First State to Pass Antispyware Legislation

In 2004, Utah passed the first state antispyware legislation, which was broadly amended in 2005.[70] Like the Act, the SCA requires that providers of downloadable software give Internet users notice and obtain

62. Complaint, State v. Digital Enterprises, Inc., *supra* note 27, ¶ 7.2.

63. *See* § 19.270.020(4).

64. National Conference of State Legislatures, 2006 State Legislation Relating to Internet Spyware or Adware, http://www.ncsl.org/programs/lis/spyware06.htm (last visited Mar. 17, 2008); *see also* National Conference of State Legislatures, 2004 State Legislation Relating to Internet Spyware or Adware, http://www.ncsl.org/programs/lis/spyware04.htm (last visited Mar. 17, 2008); 2005 State Legislation, *supra* note 3.

65. UTAH CODE ANN. §§ 13-40-101 to -401 (2007).

66. CAL. BUS. & PROF. CODE §§ 22947–22947.6 (West 2007).

67. *See* Braff, *supra* note 14.

68. Complaint, WhenU.com, Inc. v. State, No. 040907578 (Utah Dist. Ct. Apr. 12, 2004), *available at* http://www.benedelman.org/spyware/whenu-utah/complaint.pdf.

69. Class Action Complaint for Jury Trial Demand, Guevara v. Sony BMG Music Entertainment, No. BC342359 (Cal. Super. Ct. Nov. 1, 2005), 2005 WL 3143266 [hereinafter Class Action Complaint].

70. §§ 13-40-101 to -401; Anita Ramasastry, *Can Utah's New Anti-Spyware Law Work?*, FINDLAW, June 1, 2004, http://writ.news.findlaw.com/ramasastry/20040601.html.

their consent before installation occurs.[71] Damages under the SCA are limited to $500 per violation or actual damages, whichever is greater.[72]

Before the SCA was enacted, the bill's sponsors received criticism from industry giants such as Google, Microsoft, Yahoo!, eBay, and others for drafting an overly broad definition of spyware.[73] The critics asserted that the spyware definition included some beneficial and necessary software applications that provide basic Internet functions.[74] They warned that impeding access to these applications would actually decrease computer security by interfering with the data collection utilized by Internet companies to prevent hacker attacks.[75] These concerns ultimately failed to persuade the Utah legislature to vote down the bill, which was approved with the disputed spyware definition in March 2004.[76]

Immediately before the SCA was to become effective, however, adware[77] manufacturer WhenU.com, Inc. filed suit in the Third Judicial District Court in Salt Lake County, challenging the statute's constitutionality.[78] WhenU.com contended that sales of its adware products would be adversely affected by the SCA[79] because it proscribed the installation of software that tracked users' online actions, sent personal data to other companies, or generated pop-up advertisements.[80]

WhenU.com also alleged that the state of Utah had interfered with its rights under the Commerce Clause and the First and Fourteenth Amendments of the U.S. Constitution.[81] In support of its Commerce Clause claim, WhenU.com challenged the State's ability to regulate commerce outside of Utah's borders and impose excessive burdens on

---

71. § 13-40-201.

72. § 13-40-301(2)(b).

73. Letter from AOL et al. to John Valentine, Majority Leader, Utah State Senate, and Steve Urquhart, Representative, Utah State House of Representatives (Mar. 1, 2004), *available at* http://www.benedelman.org/spyware/utah-mar04/letter-01mar04.pdf.

74. *Id.*

75. *Id.*

76. § 13-40-102.

77. Adware is generally defined as any software application that displays advertising banners while the program is running. SearchCIO-Midmarket.com Definitions, http://searchcio-midmarket.techtarget.com/sDefinition/0,,sid183_gci521293,00.html (last visited Mar. 16, 2008). Adware is not necessarily banned under antispyware statutes. For an example of sanctionable adware conduct, however, consider the case of adware manufacturer Zango, Inc., based in Bellevue, Washington, which settled with the FTC in November 2006. *See* Lisa Lerer, *Adware Firm Settles With Feds,* FORBES.COM, Nov. 3, 2006, http://www.forbes.com/security/2006/11/03/adware-ftc-zango-tech-security-cx_ll_1103zango.html.

78. Complaint, *supra* note 68.

79. *See id.* ¶ 19.

80. § 13-40-201.

81. Complaint, *supra* note 68, ¶ 3.

interstate commerce in relation to the small local benefit.[82] WhenU.com also argued both that the statute violated its First and Fourteenth Amendment rights to commercial free speech and expressive activity and that the State could not show a tailored, compelling state interest to justify that infringement.[83]

WhenU.com won a partial victory when the court temporarily enjoined the law from going into effect.[84] Yet before the parties could litigate the constitutionality of the statute, the legislature amended the statute, narrowing the definition of spyware as well as the types of prohibited conduct.[85] Although WhenU.com subsequently abandoned its constitutional challenge, this case nevertheless drew nationwide attention to the emerging spyware problem and Utah's pioneering SCA.[86]

B. California Follows Utah's Lead

In September 2004, the California legislature passed the CPACSA[87] and became the second state to legislatively address the spyware problem. Like the Act and the SCA, the CPACSA outlaws the installation of software on someone else's computer without notice.[88] It also both prohibits the collection of personally identifiable information through intentionally deceptive means and bans software that cannot be uninstalled or disabled.[89]

Critics of the CPACSA argue that its notice provision is too lenient.[90] Like the Act, the CPACSA's notice provision only requires informing the computer user that software will be installed on their computer if the user consents (typically by clicking "OK" in a dialog box).[91] Critics argue that this general notice requirement is ineffective because many users manifest consent without comprehending the software's potential impact on their computers.[92]

In addition, critics contend that the CPACSA should not place on plaintiffs the onerous burden of proving that the defendants' actions were

---

82. *Id.* ¶¶ 66–67.

83. *Id.* ¶¶ 72–73.

84. Transcript of Record at 7, WhenU.com, Inc. v. State, No. 040907578 (Utah Dist. Ct. June 22, 2004), *available at* http://www.benedelman.org/spyware/whenu-utah/pi-ruling-transcript.pdf.

85. § 13-40-102.

86. Ramasastry, *supra* note 70.

87. CAL. BUS. & PROF. CODE §§ 22947–22947.6 (West 2007).

88. § 22947.2.

89. § 22947.2(b).

90. Jordan M. Blanke, *"Robust Notice" and "Informed Consent:" The Keys to Successful Spyware Legislation*, 7 COLUM. SCI. & TECH. L. REV. 2 (2006).

91. § 22947.1(h)(3).

92. Benjamin Edelman, California's Toothless Spyware Law (Sept. 29, 2004), http://www.benedelman.org/news/092904-1.html.

"intentionally deceptive."[93] This intentional deception element must also be proven by plaintiffs under the Act.[94]

One of the first lawsuits filed under this statute was a large class action against Sony BMG Music Entertainment.[95] In an attempt to prevent illegal copying, Sony BMG had embedded Extended Copy Protection technology (XCP2) in its copyrighted music CDs, which limited the capability of personal computers to copy the CDs.[96]

The complaint alleged that XCP2 contained a "rootkit" program, so named because the program attaches to the "root" of a computer and disguises itself to avoid detection.[97] Similar to spyware, the program allegedly made itself difficult to find, monitored computer usage, prevented removal without damage to the computer's operating system, and possessed misleading file names.[98] In addition, XCP2 increased a computer's vulnerability to worms and other viruses.[99]

Similar suits were soon filed against Sony BMG in New York and Texas.[100] Sony BMG eventually entered into settlements in which it agreed to stop manufacturing CDs containing XCP2.[101] Sony BMG also agreed to compensate consumers with free music downloads, small cash payments, and replacement CDs in exchange for the infected CDs.[102] Although this case did not result in a judicial opinion, it is nonetheless significant because the suit was brought by several class action plaintiffs.[103] This is unusual; spyware lawsuits have generally been initiated by state attorneys general or the FTC.[104] Sony BMG, however, appar-

---

93. H.B. 1012, 59th Leg., Reg. Sess. (Wash. 2005); Letter from Pam Dixon, Executive Dir., World Privacy Forum, and Beth Givens, Dir., Privacy Rights Clearinghouse, to Arnold Schwarzenegger, Governor, State of Cal. (Sept. 12, 2004), *available at* http://www.privacyrights.org/ar/SB1436Letter.htm.

94. WASH. REV. CODE § 19.270.020 (2008).

95. Class Action Complaint, *supra* note 69.

96. Dan Mitchell, *What's Online; The Rootkit of All Evil*, N.Y. TIMES, Nov. 19, 2005, at C5, *available at* 2005 WLNR 18689390.

97. Class Action Complaint, *supra* note 69, ¶ 2.

98. *Id.*

99. Tom Zeller Jr., *The Ghost in the CD; Sony BMG Stirs a Debate over Software Used to Guard Content*, N.Y. TIMES, Nov. 14, 2005, at C1, *available at* 2005 WLNR 18365842.

100. Civil Complaint, Michaelson v. Sony BMG Music, Inc., No. 05 CV 9575 (S.D.N.Y. Nov. 14, 2005), *available at* http://www.sonysuit.com/classactions/michaelson/complaint.pdf; Plaintiff's Original Petition, State v. Sony BMG Music Entm't, L.L.C., (Tex. Dist. Ct. Nov. 21, 2005), *available at* http://www.sonysuit.com/classactions/texas/complaint.pdf.

101. *Sony BMG Settles CD Case*, *supra* note 29; *Sony BMG Tentatively Settles Suits On Spyware*, *supra* note 29.

102. *Sony BMG Tentatively Settles Suits on Spyware*, *supra* note 29.

103. *Sony BMG Settles CD Case*, *supra* note 29.

104. *See, e.g.*, Complaint, State v. Digital Enterprises, Inc., *supra* note 27; Complaint, State v. Secure Computer, L.L.C., *supra* note 26; Federal Trade Commission, Spyware Enforcement Actions, http://www.ftc.gov/bcp/edu/microsites/spyware/law_enfor.htm (last visited Mar. 17, 2008).

ently did not learn a lesson from the rootkit debacle. In August 2007, two security companies found that USB drives sold by Sony BMG installed hidden software on users' computers.[105]

V. NATIONAL LEGISLATION AND ENFORCEMENT

Although many states have enacted spyware statutes, spyware is also subject to federal regulations promulgated by the FTC and, potentially, congressional legislation. The FTC currently regulates spyware through its administrative adjudication of disputes.[106] In addition, Congress is currently considering four different spyware bills.[107] The Securely Protect Yourself Against Cyber Trespass Act (Spy Act) and the Internet Spyware Prevention Act of 2005 (I-SPY) represent two approaches lawmakers have taken to address the national spyware problem. The first approach discussed in this Part focuses on problems created by specific technology and is utilized in the Spy Act.[108] I-SPY exemplifies the second approach, which focuses instead on problems created by behaviors.[109] Finally, this Part discusses the basis for FTC spyware regulation and describes a milestone case successfully prosecuted by the FTC.

A. The Spy Act

The Spy Act would allow the FTC to seek civil penalties[110] against anyone that transmits spyware programs to a computer without notice and the user's consent.[111] The Spy Act was passed by the House of Representatives in May 2005 and has been referred to the Senate Committee on Commerce, Science, and Transportation, where it remains under consideration.[112]

The Spy Act is fairly specific in regulating certain technologies and their problems, as well as exempting other technologies.[113] For example, it prohibits software that logs keystrokes, fraudulently induces purchase

105. Andy Greenberg, *Sony's Spyware Strikes Back*, FORBES.COM, Aug. 29, 2007, *available at* http://www.forbes.com/technology/2007/08/29/sony-rootkit-security-tech-cx_ag_0829spyware.html.

106. Federal Trade Commission, A Guide to the Federal Trade Commission (Mar. 2004), http://www.ftc.gov/bcp/edu/pubs/consumer/general/gen03.shtm.

107. *See* SPY BLOCK Act, S. 687, 109th Cong. (2006); Internet Spyware (I-SPY) Prevention Act of 2005, H.R. 744, 109th Cong. (2005); Spy Act, H.R. 29, 109th Cong. (2005); Enhanced Consumer Protection Against Spyware Act of 2005, S. 1004, 109th Cong. (2005).

108. *See* H.R. 29.

109. *See* H.R. 744.

110. H.R. 29 § 4(a).

111. H.R. 29 § 3(c).

112. The Library of Congress, http://thomas.loc.gov/cgi-bin/bdquery/z?d109:h.r.00029: (last visited Mar. 17, 2008).

113. *See* H.R. 29.

of products, or displays advertisements that cannot be easily closed.[114] If the Senate passes the bill in its present form, it would exempt technologies that merely facilitate the appearance of Web pages without monitoring consumers' behavior or gathering personal information, such as "cookies."[115] Companies that monitor their own Web sites and advertise their products based upon that data would also be exempted by the Spy Act.[116]

B. I-SPY

The second piece of national legislation under consideration is I-SPY, which simply outlaws the installation of software that leaks personal information or threatens computer security without a user's consent.[117] In sharp contrast to the twelve lengthy sections of text that make up the Spy Act, I-SPY comprises four pithy sections and has an entirely different focus.[118] While the Spy Act regulates specific technologies, I-SPY regulates culpable behavior.[119] Because it focuses on behavior, the technology sector has applauded I-SPY for being less burdensome on Internet innovation.[120] By failing to identify any specific technologies, however, I-SPY may be too vague to enforce.[121] Notably, the approach taken by the Act is more similar to I-SPY than it is to the Spy Act, as the Act largely regulates culpable behaviors and actions rather than specific technologies.[122]

C. Criticism Directed at National Proposals

Opponents of the Spy Act and other spyware bills compare them to the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM),[123] which has been largely ineffective in eliminating junk email.[124] Indeed, CAN-SPAM convictions have been

114. H.R. 29 §§ 1(e), 2(a)(3).

115. *Id.*

116. H.R. 29 § 3(b)(2)(A)–(C).

117. Internet Spyware (I-SPY) Prevention Act of 2005, H.R. 744, 109th Cong. § 2(b) (2005).

118. *See* H.R. 744; H.R. 29.

119. H.R. 744 § 2; H.R. 29.

120. Letter from Ari Schwartz, Assoc. Dir., Ctr. for Democracy & Tech., to James Sensenbrenner, Chairman, Comm. on the Judiciary, and John Conyers, Ranking Member, Comm. on the Judiciary (Sept. 24, 2004), *available at* http://www.cdt.org/privacy/spyware/20040924cdtjudiciary.pdf.

121. *See* H.R. 744. Identifying specific technologies allows a court to more easily determine whether an illegal act has taken place. In contrast, behaviors and characteristics of various types of software are sometimes difficult to determine and understand.

122. WASH. REV. CODE § 19.270.020 (2008); *see* H.R. 744 § 2.

123. 15 U.S.C. §§ 7701–7713 (2006).

124. Vivek Arora, *The CAN-SPAM Act: An Inadequate Attempt to Deal with a Growing Problem*, 39 COLUM. J.L. & SOC. PROBS. 299, 325 (2006).

few and far between.[125] Even more troubling for the spyware bills is the fact that CAN-SPAM already prohibits the transfer of software to another user's computer without that user's consent.[126] The failures of CAN-SPAM raise significant doubt as to whether the federal government is even capable of regulating these facets of the Internet.[127] Software and other computer technologies are constantly changing, and Congress is not renowned for its nimbleness; any attempt on its part to combat spyware faces the likelihood of being rendered obsolete soon after passage. One possible answer to this concern can be found in I-SPY, which does not name specific technologies, but focuses instead on culpable behaviors, such as accessing a computer without authorization, regardless of the means by which the resulting intrusion is accomplished.[128]

Another criticism of the spyware bills centers on the federal government's interference with state legislation. State legislatures are effectively responding to spyware dangers by passing laws,[129] but those laws will likely be preempted by any national legislation. The state legislative process may be in a better position to quickly adapt to rapid changes in technology.[130] If state spyware laws are working, the argument goes, national legislation would unnecessarily hinder state successes.

In addition, federal legislation might unintentionally affect legitimate businesses.[131] For example, the Spy Act is a massive document with numerous regulations and exceptions that are aimed at specific, current technology.[132] For the same reasons that Utah met significant resistance from technology sector giants, federal legislation (especially the Spy Act) is subject to criticism for providing overinclusive lists of prohibited technologies that inhibit basic Internet browser functionality.[133] Again, a possible answer to this criticism is I-SPY, which prohibits certain behaviors instead of banning specific technologies.[134]

---

125. Sharon Gaudin, *Two Men Convicted of Spamming Pornography*, INFORMATIONWEEK, June 26, 2007, http://www.informationweek.com/news/showArticle.jhtml?articleID=200000756; Edvard Pettersson, *California Man Guilty of Defrauding AOL Subscribers, U.S. Says*, BLOOMBERG, Jan. 16, 2007, http://www.bloomberg.com/apps/news?pid=newsarchive&sid=a3ukhOXubw3Y.

126. § 7701.

127. Arik Hesseldahl, *Spyware Wars*, FORBES.COM, May 13, 2005, http://www.forbes.com/personaltech/2005/05/13/cx_ah_0513diglife.html.

128. *See* Internet Spyware (I-SPY) Prevention Act of 2005, H.R. 744, 109th Cong. § 2 (2005).

129. *See supra* note 64.

130. *The States and Cyber Security*, NEWSL. (Cyber Sec. Indus. Alliance, Washington, D.C.), Nov. 2004, *available at* http://www.csialliance.org/news/newsletters/newsletter_nov-04.html#2.%20volume%201%20No.%203.

131. David McGuire, *States Speed Up Spyware Race*, WASHINGTONPOST.COM, May 13, 2004, http://www.washingtonpost.com/wp-dyn/articles/A24746-2004May13.html.

132. Spy Act, H.R. 29, 109th Cong. (2005).

133. AOL et al., *supra* note 73.

134. *See* Internet Spyware (I-SPY) Prevention Act of 2005, H.R. 744, 109th Cong. § 2 (2005).

D. The Role of the Federal Trade Commission

In addition to possible federal legislation, the FTC has authority to regulate spyware on a national level.[135] The FTC was created by President Wilson in 1914 for the purpose of preventing unfair competition practices in commerce.[136] Five commissioners—nominated by the President and approved by Congress—head the FTC for terms of seven years.[137]

Since the FTC's creation, Congress has passed several consumer protection laws empowering it to protect American consumers against unfair or deceptive practices.[138] For the good of the general public interest, the FTC can enforce regulations by conducting investigations and initiating actions against defendants engaging in such practices.[139] The FTC has already successfully pursued claims against several spyware companies and, like the state of Washington, has pursued an action against Digital Enterprises, Inc.[140] In order to facilitate reporting of fraudulent spyware practices, the FTC provides consumers with a toll-free number and online complaint forms.[141] With the assistance of these reports, the FTC filed eight actions against spyware perpetrators in 2005 and 2006.[142]

One such case that resulted in a landmark judgment was *FTC v. SmartBot.Net, Inc.*[143] This case bears many similarities to *Secure Computer*, and it will likely be considered by courts hearing spyware disputes nationwide since it is one of the only spyware cases to result in the entry of a judgment.[144] The FTC's complaint alleged that the defendants used a variety of methods to direct Internet users to their network of web sites.[145] When users arrived at the defendants' Web pages, spyware was

---

135. Federal Trade Commission, *supra* note 106.

136. *Id.*

137. *Id.*

138. *Id.*

139. *Id.*

140. Complaint for Permanent Injunction and Other Equitable Relief, FTC v. Digital Enterprises, Inc., No. CV06-4923CAS AJWx (C.D. Cal. Aug. 8, 2006), *available at* http://www.ftc.gov/os/caselist/0623008/060808movielandcmplt.pdf.

141. FTC Consumer Complaint Form, https://rn.ftc.gov/pls/dod/wsolcq$.startup?Z_ORG_CODE=PU01 (last visited Mar. 18, 2008); News Release, Federal Trade Commission, Court Halts Spyware Operations (May 4, 2006), *available at* http://ftc.gov/opa/2006/05/seismic.htm.

142. Federal Trade Commission, *supra* note 104.

143. FTC v. SmartBot.Net, Inc., No. 04-CV-377-JD (D.N.H. Mar. 16, 2006), 2006 WL 2058491.

144. The court ordered complete disgorgement of $4 million in profits gained through unfair business practices. *Id.* at *3.

145. Complaint for Injunction and Other Equitable Relief ¶ 12, FTC v. SmartBot.Net, Inc., No. 04-CV-377-JD, (D.N.H. Oct. 6, 2004), 2004 WL 3958666.

installed on their computers without notice or authorization, causing pop-up advertising (including full-page ads) and other software to appear and eventually leading to computer malfunction.[146] The spyware also allegedly changed the users' home page to one of the defendants' Web pages; it also changed the users' search engines to one of the defendants' search engines.[147] This allegedly allowed the defendants to control the Web pages and search results to which users navigated, and they took advantage of this ability by continuously downloading spyware onto the users' computers.[148]

As in *Secure Computer*, some of the pop-ups in this case simulated Windows dialog boxes and urgently warned users to download antispyware programs.[149] If the user heeded this warning and clicked the link, he or she was prompted to purchase antispyware software for $30.[150] The defendants allegedly received a percentage of the profits made through sales of these software programs.[151]

The FTC brought suit in federal court in New Hampshire; that court eventually granted a default judgment against defendants and ordered them to disgorge their profits.[152] In addition, the court barred the defendants from transmitting spyware or other software onto computers or changing users' home pages or search engines without consent.[153] This case gained nationwide attention because of the large disgorgement order: $4 million in profits gained from engaging in unfair business activities.[154] This case is also significant because it resulted in a judgment, rather than a settlement; it thus created valuable case law for courts around the country.[155]

VI. A PROPOSAL FOR CHANGE

Although the Act effectively addresses many aspects of Washington's spyware problem, three improvements should be made. First, the goals of the Act would be better served if it provided better direction on what satisfies the notice requirement. Second, the requirement that plaintiffs prove defendants acted with intent to deceive is at odds with much consumer protection legislation and is too heavy of a burden for

146. *Id.* ¶ 13.
147. *Id.* ¶ 14–15.
148. *Id.*
149. *Id.* ¶ 18.
150. *Id.*
151. *Id.* ¶ 19.
152. Federal Trade Commission, *supra* note 141.
153. *Id.*
154. *Id.*
155. *Id.*

most spyware victims to carry.[156] Finally, a damages cap of $2 million neither adequately compensates victims for their economic loss nor effectively deters those who profit from the use of spyware.

A. The Notice Requirement Should Be More Specific

The Washington legislature should amend the Act to incorporate a more comprehensive notice provision. Currently, the Act does not describe how notice should be given to the user before software is installed. The only mention of notice is in the "Definitions" section of the statute, where notice is used to define intentional deception in terms of a company's behavior.[157]

The goals of the Act would be better effectuated if it included a descriptive notice provision. The notice provision is essentially the first line of defense for a user because he or she decides to accept or reject the software based upon the information given in the download dialog box.[158] If users cannot determine the impact particular software will have on their computer, they may unwittingly agree to download software that acts nothing like what they had anticipated.

The SCA has gone so far as to require that software companies write their notices in plain language and show full-sized examples of advertisements that users will see.[159] Although opponents of a broad notice provision argue that compliance will be unduly burdensome, make their products less attractive, and stifle Internet innovation,[160] Utah's notice provision is reasonable because it allows users to make informed decisions about the degree of control they will maintain over their computers. Because the Act's notice requirement does not provide specific guidelines for what constitutes adequate notice, users face increased danger that they will inadvertently consent to the transmittal of potentially dangerous spyware. Therefore, in order to afford greater protection to its constituents, the Washington legislature should amend the Act to incorporate the SCA's descriptive notice provision.

A second reason to expand the Act's notice provision is that spyware promoters will more clearly understand what is required under the statute, and noncompliance will be more easily discernable. Currently the Act fails to specify exactly what notice is required. In defending

---

156. H.B. 1012, 59th Leg., Reg. Sess. (Wash. 2005); McKenna, *supra* note 21.

157. *See* WASH. REV. CODE § 19.270.010(5)(c) (2008) (defining intentionally deceptive behavior as consisting of "[a]n intentional and material failure to provide any notice to an owner or operator regarding the installation or execution of computer software in order to deceive the owner or operator").

158. Schoenberger, *supra* note 6.

159. UTAH CODE ANN. § 13-40-102 (2007).

160. Complaint, *supra* note 68, ¶ 14.

claims brought under the Act, then, defendants will likely assert that they honestly or reasonably attempted to comply with this vague language and thus did not violate the statute. In fact, WhenU.com prospectively argued this very point in its challenge to the SCA.[161] This argument is a potential loophole for defendants that should be closed through the drafting of express language with specific definitions and notice requirements. In addition, this amendment would allow courts adjudicating these disputes to more easily determine whether defendants complied with the notice requirement. In sum, a more comprehensive notice provision is in the best interest of Washington citizens and would better serve the goals of the legislation.

B. Plaintiffs Should Not Be Required to Prove Intentional Deceit

Under the Act, a plaintiff is required to prove that a defendant was intentionally deceptive in modifying a computer's settings.[162] The CPACSA similarly imposes this burden on the plaintiff, and critics argue that this is an unreasonably difficult showing to make.[163] Admittedly, definitions of spyware vary.[164] The Act, however, lays out detailed lists of illegal activities that are typically carried out by most types of spyware.[165] The average computer user would not knowingly engage in this

---

161. *Id.* ¶ 15.

162. § 19.270.020.

163. H.B. 1012, 59th Leg., Reg. Sess. (Wash. 2005); Dixon & Givens, *supra* note 93.

164. Braff, *supra* note 14.

165. The Act states that

> [i]t is unlawful for a person who is not an owner or operator to transmit computer software to the owner or operator's computer with actual knowledge or with conscious avoidance of actual knowledge and to use such software to do any of the following: (1) Modify, through intentionally deceptive means, settings that control any of the following: (a) The page that appears when an owner or operator launches an internet browser or similar computer software used to access and navigate the internet; (b) The default provider or web proxy the owner or operator uses to access or search the internet; and (c) The owner or operator's list of bookmarks used to access web pages; (2) Collect, through intentionally deceptive means, personally identifiable information: (a) Through the use of a keystroke-logging function that records all keystrokes made by an owner or operator and transfers that information from the computer to another person; (b) In a manner that correlates such information with data respecting all or substantially all of the web sites visited by an owner or operator, other than web sites operated by the person collecting such information; and (c) Described in WASH. REV. CODE 19.270.010(9) (d), (e), or (f)(i) or (ii) by extracting the information from the owner or operator's hard drive; (3) Prevent, through intentionally deceptive means, an owner or operator's reasonable efforts to block the installation or execution of, or to disable, computer software by causing the software that the owner or operator has properly removed or disabled automatically to reinstall or reactivate on the computer;
>
> (4) Intentionally misrepresent that computer software will be uninstalled or disabled by an owner or operator's action; and

prohibited conduct. Moreover, the listed activities are unreasonably invasive to a computer user's privacy, with or without proof of intentional deception.

Instead of requiring plaintiffs to meet such a high burden, the Act should be amended to create a rebuttable presumption that defendants acted with an intent to deceive. Making intentional deceit a rebuttable presumption is reasonable because defendants are in a better position to offer evidence of their own intent in distributing and managing the software in issue. If a defendant engaged in activities prohibited by the Act without any ulterior motive or an intent to deceive the user, the defendant should be required to bring forth evidence showing the legitimate reasons for his or her actions. Requiring a plaintiff to prove the defendant's intentional deceit is overly burdensome and is simply unnecessary to prove that the plaintiff was harmed by the defendant's actions.[166]

Notably, requiring plaintiffs to show that defendants possessed actual knowledge or conscious avoidance of actual knowledge in *transmitting* software should remain unchanged.[167] Many kinds of software, including spyware and viruses, are inadvertently transmitted to and from computers connected to the Internet. Prosecuting individuals who had no actual knowledge or conscious avoidance of actual knowledge in transmitting software would not serve the goals of this legislation. If such prosecution were allowed, a victim of spyware infiltration would likely unknowingly later become a perpetrator under the law.

C. The Damages Cap Must Be Increased

The Act currently imposes a damages cap of $2 million.[168] In comparison to the actual damage spyware causes Americans each year,[169] this sum does not begin to adequately compensate for the harm. One expert estimated that in 2007, Americans would spend an estimated $259 million in antispyware programs.[170] This figure does not account for indirect economic effects, such as productivity losses, that occur when spyware slows or shuts down a business's entire network.[171] Nor does this figure factor in the many cases of identity theft that result from keystroke

---

(5) Through intentionally deceptive means, remove, disable, or render inoperative security, antispyware, or antivirus computer software installed on the computer.

§ 19.270.020.

166. *See* H.B. 1012, 59th Leg., Reg. Sess. (Wash. 2005); Dixon & Givens, *supra* note 93.

167. *See* § 19.270.030.

168. § 19.270.060(3).

169. Arik Hesseldahl, *Spyware by the Numbers*, FORBES.COM, Jan. 17, 2005, http://www.forbes.com/technology/2005/01/17/cx_ah_0117spynumbers.html.

170. *Id.*

171. Hesseldahl, *supra* note 8.

logging each year.[172] Researchers at Webroot Software, an antispyware software company, recently found a collection of thousands of stolen identities from 125 countries that were believed to have been collected by a spyware program.[173]

The current cap on damages neither adequately compensates victims of spyware nor sufficiently deters current and would-be spyware distributors. A substantial increase in the damages cap is necessary to effectively deter these distributors, in light of the potentially large profits possible. Although opponents of a high damages cap assert that higher penalties will have a cooling effect on Internet innovation and encourage many private plaintiffs to sue,[174] failing to increase the damages cap encourages large spyware distributors to continue their operations because they can receive substantially greater sums from engaging in illegal practices than they face to lose for violating the Act. For example, in *SmartBot.Net*, the defendants made a profit of more than $4 million from their spyware operations.[175] If spyware distributors who are found liable under the Act can escape with a relatively nominal penalty, instead of complete repayment of profits, they have a powerful incentive to relocate and resume the same operations, despite the possibility of more fines. Damages incurred under the Act could potentially be viewed as merely a cost of continuing business.

Additionally, because many spyware schemes are self-sustaining, unscrupulous companies can earn large profits. These programs build upon themselves by reinstalling software and increasing pop-ups until the computer user capitulates by buying the marketed product that is purported to "cure" the problem. For example, the spyware employed in *SmartBot.Net* was designed to perpetuate its own installation every time the computer user accessed the Internet.[176] Profits from this self-sustaining enterprise would have been much larger had the court merely ordered fines or nominal damages instead of the complete disgorgement of profits. Although damages of $2 million would have cut the profits in half, the company still would have escaped with a substantial profit.

The Act's maximum allowable damages award is simply not large enough to deter actual and potential violators from engaging in the moneymaking opportunity that spyware distribution provides. Therefore, the

---

172. Nick Booth, *Surge in ID Theft Using Spyware*, FORBES.COM, Sept. 19, 2005, http://www.forbes.com/intelligentinfrastructure/2005/09/19/spyware-id-theft-cx-vnu_0919spyware.html.

173. Paul F. Roberts, *Webroot Uncovers Thousands of Stolen Identities*, INFOWORLD, May 9, 2006, http://www.infoworld.com/article/06/05/09/78139_HNTrojanrebery_1.html.

174. Complaint, *supra* note 68, ¶¶ 19–20.

175. Federal Trade Commission, *supra* note 141.

176. Complaint for Injunction and Other Equitable Relief, *supra* note 145, ¶¶ 14–15.

legislature should amend the Act to allow the result reached in *Smart-Bot.Net*: The damages limit should be increased to allow the complete disgorgement of a liable defendant's profits obtained through violations of the Act. Washington legislators must send a clear message to the sultans of spyware: Those who profit from violating the Act will not be permitted to retain their illegally gotten gains.

VII. CONCLUSION

Damage from spyware is steadily increasing because attacks are more frequent, and their delivery is more sophisticated.[177] The Act is a timely response to this threat and has already resulted in multiple settlements; it has plainly begun to have a positive impact. Moreover, because Congress continues to delay the passage of federal legislation that would provide a viable alternative, Washingtonians must continue to rely on the Act. Although the Act successfully addresses many of the problems created by spyware, the legislature should make three changes that will more effectively deter proscribed conduct and compensate victims. First, a more comprehensive notice requirement will not only allow Internet users to fully understand proposed software transactions, but will also enable spyware companies to better comply with the law. Second, rather than forcing plaintiffs to prove the element of intentional deception on the part of defendants, the Act should create a presumption of intentional deception that defendants would have the burden of rebutting. The burden of proof currently imposed on plaintiffs is too heavy for most spyware victims to meet; in any event, defendants are better positioned to prove what their true intent was when they distributed their software. Finally, increasing the Act's damages cap and adding the possibility of complete disgorgement of profits will increase the deterrent effect of the Act and more adequately compensate victims. By amending the Act in this fashion, the Washington legislature can both effectively protect its citizens and remain a national leader in reducing the proliferation and harmful effects of spyware.

177. Webroot Software, Inc., Webroot State of Spyware Report Finds 2005 Biggest Year Yet for Spyware, Feb. 7, 2006, http://www.webroot.com/En_US/about-press-room-press-releases-pr-biggest-year-for-spyware.html.