

# Defining Abusive Software to Protect Computer Users from the Threat of Spyware

by  
*Chad A. Kirby\**

## ABSTRACT:

“Spyware” has become a major problem for computer users over the past few years. In response, quite a few states have enacted statutes intended to control the problem. But most of the existing legislation has taken the wrong approach to the problem of defining spyware. Generally speaking, most legislative definitions of spyware either have been too technology-specific to adapt to future developments, or have swept too broadly. Additionally, many legislative definitions of spyware have focused too little on protecting consumers. This article argues that any effective regulatory definition must have three characteristics: 1) it must protect the user’s control over his or her computer; 2) it must be technologically neutral; and 3) it must not be over-inclusive. The article then proposes a regulatory definition that has these three characteristics.

A couple weeks after one of my colleagues, J, got her new laptop in 2004, a certain infamous celebrity video was leaked onto the Internet and created quite a buzz. J’s husband, wishing to download the video but unwilling to do so using his work computer, borrowed J’s laptop and went searching for a website from which he could download the file. He never did find the video he was after, but while he was looking, a large number of programs somehow made their way onto the laptop without his knowledge. Dozens of these programs launched themselves each time the computer booted and slowed the computer down to the point that it was virtually useless. J had to wipe the drive and start fresh, as it would have been impossible to undo all of the changes made by those malicious programs. Most of these programs were designed to monitor J’s web browsing habits and send pop-up ads to her machine. In other words, J’s laptop had been infested with “spyware.”<sup>1</sup>

---

\* Chad A. Kirby is a December 2007 J.D. candidate at Seattle University School of Law. After receiving his bachelors degree from the University of Missouri at Kansas City, Mr. Kirby worked with computers and technology for fourteen years as an administrator, developer, and in various other capacities. During those years, he also earned graduate degrees in music from the University of Washington. Mr. Kirby wishes to extend many thanks to his wife, Karla Youngers.

1. Compare this example with a real life experience as related by Ray Everett-Church. FED. TRADE COMM’N WORKSHOP, MONITORING SOFTWARE ON YOUR PC: SPYWARE, ADWARE, AND OTHER SOFTWARE 123 (2004), <http://www.ftc.gov/bcp/workshops/spyware/transcript.pdf> .

---

## I. INTRODUCTION

We live in a world very different from that which existed only a decade ago. While the Internet may not have changed literally everything, it undeniably had a huge effect as computer literacy hit mainstream U.S. society and average citizens ventured out onto the information superhighway on a regular basis.<sup>2</sup> On today's Internet, you can buy a book,<sup>3</sup> rent a DVD,<sup>4</sup> apply for a mortgage,<sup>5</sup> balance your checkbook,<sup>6</sup> do legal research,<sup>7</sup> play games,<sup>8</sup> express your thoughts,<sup>9</sup> chat with others,<sup>10</sup> sell junk from your closet<sup>11</sup>. . . the list goes on and on. On the other hand, today's Internet also poses some risks to the unwary: you can catch a virus, be subjected to credit card fraud or identity theft, or your computer may download and install software without your consent. "Spyware" generally fits into this last category of bad things that can happen to your computer while you use the Internet.<sup>12</sup>

The anecdote about J's laptop is familiar to many computer users today.<sup>13</sup> Granted, J's husband was visiting some of the seedier sites on the Internet; if the Internet can be analogized to a modern city, he was doing the

---

2. See, e.g., NAT'L TELECOMM. & INFO. ADMIN., A NATION ONLINE: ENTERING THE BROADBAND AGE (2004), <http://www.ntia.doc.gov/reports/anol/NationOnlineBroadband04.pdf>.
3. See, e.g., Powells City of Books, <http://www.powells.com>.
4. See, e.g., Netflix, <http://www.netflix.com>.
5. See, e.g., E\*Trade Financial, <http://lending.etrade.com>.
6. See, e.g., Quicken, <http://quicken.intuit.com>.
7. See, e.g., FindLaw, <http://www.findlaw.com>.
8. See, e.g., SecondLife, <http://secondlife.com>.
9. See, e.g., Blogger, <http://www.blogger.com>.
10. See, e.g., Google Talk, <http://www.google.com/talk>.
11. See, e.g., Craigslist, <http://www.craigslist.org/>.
12. See SPYWARE, WIKIPEDIA, <http://en.wikipedia.org/wiki/spyware> (last visited Sept. 8, 2006).
13. In 2005, 61% of Americans had spyware infecting their home computers according to a study conducted by America Online and the National Cyber Security Alliance. CTR. FOR DEMOCRACY & TECH., STUDY FINDS DECREASE IN SPYWARE (Dec. 7, 2005), <http://www.cdt.org/headlines/840/>; see also AOL/NCSA ONLINE SAFETY STUDY, (Dec. 2005), [http://www.staysafeonline.info/pdf/safety\\_study\\_2005.pdf](http://www.staysafeonline.info/pdf/safety_study_2005.pdf); Brien Posey, *How Spyware and the Weapons Against It Are Evolving*, Oct. 26, 2004, <http://www.windowsecurity.com/articles/Spyware-Evolving.html> ("I have seen recent statistics indicating that approximately 95% of the world's PCs are infected with spyware."). In October, 2005, more than one in twenty executable files downloaded from the Internet were found to contain spyware. Alexander Moshchuk et al., *A Crawler-based Study of Spyware on the Web*, Feb. 2006, <http://www.cs.washington.edu/homes/gribble/papers/spycrawler.pdf> [hereinafter UW Study].

---

equivalent of wandering around the bad part of town at two a.m. looking for trouble. However, spyware can adversely affect even the most cautious and conservative computer user.<sup>14</sup> As a result, a sizable anti-spyware industry has sprung up in recent years<sup>15</sup> as more and more computer users feel the need to take affirmative steps to protect themselves so that they can use the Internet in relative safety.<sup>16</sup>

But what exactly is it that computer users need to protect themselves from? Put another way, how does one define “spyware”? In the case of an individual computer user, it is easy to definitively say, “that is spyware,” while pointing at a bunch of pop-up ad programs that have been installed without his or her knowledge, that transmit personal information to unknown third parties, and that have ruined the computer. But is it “spyware” because it displays pop-up ads? Because it was installed without permission? Because it is extremely difficult to remove from the computer? Because it transmits personal information? Because it renders the computer essentially useless? Or is it “spyware” for some combination of these reasons? This is a difficult question .

Any given anti-spyware software developer is free to define “spyware” as it sees fit, considering the needs and desires of its consumers.<sup>17</sup> If consumers disagree with that developer’s definition, they are free to select a compet-

---

14. See Comments by Eric L. Howes on the Problem of Spyware in Advance of the FTC April 2004 Spyware Workshop to the Fed. Trade Comm’n 7 (Mar. 29, 2004), <http://www.ftc.gov/os/comments/spyware/040329howes.pdf> (“When consumers visit web sites associated with pornography. . . or pirated software. . . they are certainly more prone to encounter unwanted, abusive spyware. Plenty of users, however, pick up spyware by visiting completely ‘legitimate,’ ‘mainstream’ web sites or by installing apparently innocuous software from seemingly reputable sources.”). Researchers at the University of Washington analyzed the spyware threat presented by various categories of web sites. That study showed that, in October 2005, the category of web sites presenting the highest risk of spyware was “games”, followed by “music”, “wallpaper”, “celebrity”, “adult”, and “pirate”. UW Study, *supra* note 13. R
15. See Konstantinos Karagiannis, *Antispyware*, PC MAGAZINE, Feb. 2, 2005, <http://www.pcmag.com/article2/0,1759,1758380,00.asp> (“The majority of PCs in America are infested with spyware. . . The explosion of dedicated antispyware apps in the past year began to address the growing problem. . .”); SPYWARE, *supra* note 12. R
16. CTR. FOR DEMOCRACY & TECH. *supra* note 13. R
17. See, e.g., Matt Tett, *To catch a spy: Anti-spyware tools reviewed*, ZDNET, Dec. 5, 2005, [http://www.zdnet.com.au/reviews/software/security/soa/To\\_catch\\_a\\_spy\\_Eight\\_anti\\_spyware\\_tools\\_reviewed/](http://www.zdnet.com.au/reviews/software/security/soa/To_catch_a_spy_Eight_anti_spyware_tools_reviewed/); Laura Hunter, *Choosing the Best Anti-Spyware Program*, Oct. 6, 2005, <http://www.informit.com/articles/article.asp?p=419257>. See generally Anti-Spyware Guide, <http://www.firewallguide.com/spyware.htm> (last visited Jan. 22, 2006) (a webpage devoted to informing consumers about the various methods to protect themselves against malicious programs).

---

ing anti-spyware product. But the stakes are a little different when it is the government creating definitions for regulatory purposes.<sup>18</sup> An anti-spyware developer's definition is flexible in that it can be modified as new pieces of software emerge, and it can be modified to correct errant miscategorizations.<sup>19</sup> On the other hand, a legislative definition is much more difficult to alter once it has been enacted, and most of the existing legislative definitions have taken the wrong approach to the problem. Generally speaking, most legislative definitions of spyware either have been too technology-specific to adapt to future developments or have swept too broadly.<sup>20</sup> Additionally, many legislative definitions of spyware have focused too little on protecting consumers.<sup>21</sup>

Simply put, a definition of spyware needs two characteristics to be effective. As a policy matter, the definition should be designed to protect the user's control over his or her computer. As a practical matter, the definition must walk a fine line between technological neutrality and over-inclusiveness.

Part II of this Comment explains the history of spyware and the confused nomenclature surrounding spyware and settles on the term "abusive software" to refer to software that behaves maliciously. To illustrate a real-world example of the issues surrounding spyware, Part III provides an overview of a recent, highly publicized spyware outbreak involving Sony BMG compact discs. Part IV examines the difficulties that have arisen as various private and public entities have unsuccessfully tried to separate permissible software behavior from impermissible software behavior and proposes a set of general principles that must underlie any successful definition of abusive software. Building upon that background, Part V applies those general principles in a proposed definition of abusive software. Finally, Part VI assesses what impact the adoption of the new definition might have on the modern internet user.

---

18. "Legislation is being considered in at least 28 states in 2005. Legislation has been enacted in twelve states." National Conference of State Legislatures, *2005 Legislation Relating to Internet Spyware or Adware* (Dec. 27, 2005), <http://www.ncsl.org/programs/lis/spyware05.htm> [hereinafter 2005 State Legislation]; *see also* Ben Edelman, *State Spyware Legislation*, <http://www.benedelman.org/spyware/legislation/> (Apr. 23, 2006) (16 states have enacted legislation). At the federal level, there were at least five bills proposed in Congress in 2005, but none have been enacted at the time of this writing. *See* Ben Edelman, "Spyware": Research, Testing, Legislation, and Suits, <http://www.benedelman.org/spyware/#legislation> (Sept. 7, 2006) [hereinafter Edelman2].

19. *See, e.g.*, Tett, *supra* note 17; Hunter, *supra* note 17.

20. *See infra* Part IV.

21. *See infra* Part IV.C.

## II. A BRIEF HISTORY OF SPYWARE

No single, clear definition of spyware has ever existed. First used in this context in 1999, the term referred to programs that literally “spied” on computer users by surreptitiously transmitting personal information back to a central server.<sup>22</sup> Such “spyware” either tricked computer users into installing it or installed itself via malicious web pages that exploited vulnerabilities in web browsers (a practice sometimes called a “drive-by download”).<sup>23</sup> When referencing software that “spies” on the user, the term “spyware” makes sense. But the term “spyware” rapidly became diluted as some people began to use it generically to refer to many types of software that were installed through trickery, regardless of whether the software actually spied on their computers.<sup>24</sup> Notably, great confusion exists as to the distinction (if any) between “adware”<sup>25</sup> and “spyware” (a distinction that is difficult to make, as the two concepts can overlap to a large degree).<sup>26</sup> Adding to the confusion, the term “spyware” has become closely associated with pop-up advertisements, which may or may not transmit any information from the user’s computer to a central server.<sup>27</sup> Much has been written about the difficulties of distinguishing “spyware” from “adware,” “malware,” and the many additional portmanteau words formed by affixing various epithets to the suffix “-ware.”<sup>28</sup>

22. See SPYWARE, *supra* note 12.

R

23. See SPYWARE, *supra* note 12; see also DRIVE-BY DOWNLOAD, WIKIPEDIA, [http://en.wikipedia.org/wiki/Drive-by\\_download](http://en.wikipedia.org/wiki/Drive-by_download) (last visited Nov. 10, 2006); Posey, *supra* note 13.

R

24. See SPYWARE, *supra* note 12.

25. “Adware or advertising-supported software is any software package which automatically plays, displays, or downloads advertising material to a computer after the software is installed on it or while the application is being used.” ADWARE, WIKIPEDIA, <http://en.wikipedia.org/wiki/Adware> (last visited Nov. 10, 2006).

26. “It is not uncommon for people to confuse ‘adware’ with ‘spyware.’” *Id.*; see generally Mani Aliabadi, The Legal Implications of Adware and Targeted Advertising (unpublished whitepaper prepared for Widevine Technologies) (on file with author); Chris Gutzman et al., *Differences and Similarities of Spyware and Adware*, Fall 2003 (unpublished paper prepared for University of Minnesota, Morris, Computer Science Seminar) (on file with author).

27. ADWARE, WIKIPEDIA, <http://en.wikipedia.org/wiki/Adware> (last visited Sept. 8, 2006); see also POP-UP AD, WIKIPEDIA, [http://en.wikipedia.org/wiki/Pop-up\\_ad](http://en.wikipedia.org/wiki/Pop-up_ad) (last visited Sept. 8, 2006).

28. See, e.g., Anti-Spyware Coalition, Definitions and Supporting Documents (Oct. 27, 2005), <http://www.antispywarecoalition.org/documents/20051027definitions.pdf> [hereinafter ASC Definition]; Susan P. Crawford, *First do no Harm: The Problem of Spyware*, 20 BERKELEY TECH. L.J. 1433 n.2, (2005); CTR. FOR DEMOCRACY AND TECH., GHOSTS IN OUR MACHINES: BACKGROUND AND POL-

Part of the confusion results from the fact that there are two distinct interests that are both affected by this sort of software. First, there is an obvious privacy interest implicated. Most consumers presumably prefer to keep their personal information and web-browsing habits to themselves.<sup>29</sup> Second, the consumers' interest in retaining control over what software is installed on their computers may be less obvious, but is compelling nonetheless.<sup>30</sup> This latter interest could be called a "security" interest.<sup>31</sup> Typical spyware infestations will impact both of these interests.<sup>32</sup> A compromise of one's privacy interest can lead to harms as serious as identity theft.<sup>33</sup> Therefore, the great temptation is to focus on controlling spyware by protecting consumers' privacy interests.<sup>34</sup> However, at least with respect to spyware, protecting consumers' security interest would also protect their privacy interest—it is self-evident that if security measures prevent the installation of a piece of spyware, then that piece of spyware will have no opportunity to violate that computer user's privacy interest. Consequently, the most effective way of protecting consumers from all aspects of spyware is to control the abusive behavior that leads to spyware infestations in the first place.

Returning to the issue of nomenclature, the truth is that "spyware" is not very good as a general label for software that behaves improperly. Instead, this comment will use "abusive software" as a general term to refer to software that should be regulated because it interferes with the user's control over his or her computer. The term "spyware" will be used to refer specifically to abusive software that surreptitiously transmits personal information to a third party.

---

ICY PROPOSALS ON THE "SPYWARE" PROBLEM (2003), <http://www.cdt.org/privacy/031100spyware.pdf>.

29. See, e.g., Platform for Privacy Preferences (P3P) Project, <http://www.w3.org/P3P/> (last visited January 21, 2006) (an example of commercial software enabling users to ensure a higher degree of privacy); INTERNET PRIVACY, WIKIPEDIA, [http://en.wikipedia.org/w/index.php?title=Internet\\_privacy&oldid=35796176](http://en.wikipedia.org/w/index.php?title=Internet_privacy&oldid=35796176) (last visited Sept. 8, 2006).
30. See, e.g., COMPUTER INSECURITY, WIKIPEDIA, [http://en.wikipedia.org/w/index.php?title=Computer\\_insecurity&oldid=35755533](http://en.wikipedia.org/w/index.php?title=Computer_insecurity&oldid=35755533) (last visited Sept. 8, 2006).
31. *Id.*
32. See *infra* Part IV.C; see also BEN EDELMAN, DOCUMENTATION OF GATOR ADVERTISEMENTS AND TARGETING (June 7, 2003), <http://cyber.law.harvard.edu/people/edelman/ads/gator/>.
33. See Wall Street & Tech., *Identity Fraud is Finding Fewer U.S. Victims*, Apr. 14, 2006, <http://www.javelinstrategy.com/reports/2005IdentityFraudSurveyReport.html> (Noting that 9.3 million Americans were victims of Identity Theft in 2004.); see also IDENTITY THEFT, WIKIPEDIA, [http://en.wikipedia.org/w/index.php?title=Identity\\_theft&oldid=35958826](http://en.wikipedia.org/w/index.php?title=Identity_theft&oldid=35958826) (last visited Sept. 8, 2006).
34. See *infra* Part IV.C.4.

---

### III. A CASE STUDY IN ABUSIVE SOFTWARE: SONY BMG

In late October 2005, a computer security expert reported<sup>35</sup> that dozens of audio CD's<sup>36</sup> released by Sony BMG in 2005 installed "rootkit-based"<sup>37</sup> Digital Rights Management<sup>38</sup> ("DRM") software when consumers tried to play the CD in their computers running Microsoft Windows.<sup>39</sup> The story quickly made its way into the mainstream press.<sup>40</sup> Over two million such CD's were shipped, mostly to the United States.<sup>41</sup> Once installed, the DRM software cloaked<sup>42</sup> itself, making it extremely difficult for users to uninstall

---

35. Posting by Mark Russinovich to Sysinternals, <http://www.sysinternals.com/blog/2005/10/sony-rootkits-and-digital-rights.html> (Oct. 31, 2005, 11:04) [hereinafter DRM Gone Too Far].
36. Fred von Lohmann, *Are You Infected by Sony-BMG's Rootkit?*, Nov. 9, 2005, <http://www.eff.org/deeplinks/archives/004144.php>.
37. See ROOTKIT, WIKIPEDIA, <http://en.wikipedia.org/w/index.php?title=Rootkit&oldid=34929707> (last visited Sept. 8, 2006). ("A rootkit is a set of software tools frequently used by a third-party (usually an intruder) after gaining access to a computer system. These tools are intended to conceal running processes, files or system data, which helps an intruder maintain access to a system for purposes without the user's knowledge.").
38. See DIGITAL RIGHTS MANAGEMENT, WIKIPEDIA, [http://en.wikipedia.org/w/index.php?title=Digital\\_rights\\_management&oldid=28541874](http://en.wikipedia.org/w/index.php?title=Digital_rights_management&oldid=28541874) (last visited Sept. 8, 2006) ("Digital rights management (DRM) is an umbrella term referring to any of several technical methods used to control or restrict the use of digital media content on electronic devices with such technologies installed. The media most often restricted by DRM techniques include music, visual artwork, computer and video games, and movies."). The legal implications of DRM technologies are vast and are beyond the scope of this article.
39. "Microsoft Windows is a series of operating environments and operating systems created by Microsoft for use on personal computers and servers." MICROSOFT WINDOWS, WIKIPEDIA, [http://en.wikipedia.org/w/index.php?title=Microsoft\\_Windows&oldid=36128871](http://en.wikipedia.org/w/index.php?title=Microsoft_Windows&oldid=36128871) (last visited Sept. 8, 2006); see also Microsoft Windows Home Page, <http://www.microsoft.com/windows/default.mspx> (last visited Jan. 22, 2006).
40. See, e.g., Mark Ward, Sony slated over anti-piracy CD, Nov. 3, 2005, <http://news.bbc.co.uk/2/hi/technology/4400148.stm>; Matthew Fordahl, Sony to offer patch to reveal hidden copy-protection software, Nov. 2, 2005, [http://www.usatoday.com/tech/news/computersecurity/2005-11-02-sony-patch\\_x.htm](http://www.usatoday.com/tech/news/computersecurity/2005-11-02-sony-patch_x.htm); Neda Ulaby, Sony Music CDs Under Fire from Privacy Advocates, Nov. 4, 2005, <http://www.npr.org/templates/story/story.php?storyId=4989260>.
41. Sharon Gaudin, Trojan Exploits Sony's DRM Flaw, Nov. 11, 2005, <http://itmanagement.earthweb.com/secu/article.php/3563581>.
42. In this context, cloaking means that the software made itself invisible to the computer user without the use of specialized tools. Software generally cloaks itself in order to prevent the computer user from being able to remove it. Here,

or even to discover that the DRM software was installed on their computers.<sup>43</sup> The DRM software runs constantly in the background, always consuming a small quantity of system resources.<sup>44</sup> Even worse, within two weeks, virus writers released a Trojan horse<sup>45</sup> that exploited a flaw in the Sony BMG DRM software to take over computers running that software.<sup>46</sup> Shortly thereafter, Sony BMG announced that it would stop using the DRM software and recalled all CDs that used it.<sup>47</sup>

When consumers first insert a Sony BMG DRM-protected CD, they are presented with a 3000-word<sup>48</sup> “clickwrap”<sup>49</sup> End User License Agreement

---

the cloaking meant that the directory in which the software was installed did not show up in standard file browsers. Additionally, the name of the software did not show up in any of the lists of programs that were currently running on that machine. As a result, computer users would have no way of knowing that the DRM software had been installed. *See generally* EXTENDED COPY PROTECTION, WIKIPEDIA, [http://en.wikipedia.org/w/index.php?title=Extended\\_Copy\\_Protection&oldid=34233428](http://en.wikipedia.org/w/index.php?title=Extended_Copy_Protection&oldid=34233428) (last visited Sept. 8, 2006) (giving examples of cloaking); DRM Gone Too Far, *supra* note 35 (explaining that rootkits involve cloaking). R

43. *See* posting by Mark Russinovich to Sysinternals, [http://www.sysinternals.com/blog/2005/11/sony-you-dont-reeeeaaaally-want-to\\_09.html](http://www.sysinternals.com/blog/2005/11/sony-you-dont-reeeeaaaally-want-to_09.html) (Nov. 9, 2005, 11:31 a.m.) [hereinafter *You Don't Really Want to Uninstall*]; Posting by Mark Russinovich to Sysinternal, <http://www.sysinternals.com/blog/2005/11/sonys-rootkit-first-4-internet.html> (Nov. 6, 2005, 7:29 p.m.).

44. DRM Gone Too Far, *supra* note 35 (“I closed [Sony’s media] player and . . . was dismayed to see that it was still consuming between one and two percent [of my CPU]. It appears I was paying an unknown CPU penalty for just having the process active on my system.”). R

45. *See* TROJAN HORSE (COMPUTING), WIKIPEDIA, [http://en.wikipedia.org/w/index.php?title=Trojan\\_horse\\_%28computing%29&oldid=35214898](http://en.wikipedia.org/w/index.php?title=Trojan_horse_%28computing%29&oldid=35214898) (last visited Sept. 8, 2006) (“a Trojan horse is a malicious program that is disguised as legitimate software”).

46. *See* Sharon Gaudin, *Trojan Exploits Sony’s DRM Flaw*, Nov. 11, 2005, <http://itmanagement.earthweb.com/secu/article.php/3563581>; *see also* Troj/Stinx-E – Trojan – sophos Threat Analysis, <http://www.sophos.co.uk/virusinfo/analyses/trojstinx.html> (last visited Jan. 15, 2006).

47. Sony BMG Music Entertainment, <http://cp.sonybmg.com/xcp/> (last visited Sept. 8, 2006).

48. Fred von Lohmann, *Now the Legalese Rootkit: Sony-BMG’s EULA*, Nov. 9, 2005, <http://www.eff.org/deeplinks/archives/004145.php>.

49. *See* CLICKWRAP, WIKIPEDIA, <http://en.wikipedia.org/w/index.php?title=Clickwrap&oldid=34812307> (last visited Sept. 8, 2006) (“A clickwrap agreement. . . is a common type of software license found on the Internet. . . . In general, a clickwrap typically requires an end user to manifest his or her assent by clicking an “ok” button on a dialog box or pop-up window.”).

---

(EULA).<sup>50</sup> The EULA informs consumers that in order to listen to the CD on their computers, they must consent to the installation of a “small proprietary software program” that will reside on their computers “until removed or deleted.”<sup>51</sup> The EULA does not inform consumers that the DRM software

---

50. See SOFTWARE LICENSE, WIKIPEDIA, [http://en.wikipedia.org/w/index.php?title=Software\\_license&oldid=34838144](http://en.wikipedia.org/w/index.php?title=Software_license&oldid=34838144) (last visited Sept. 8, 2006) (“A software license is a type of proprietary or gratuitous license as well as a memorandum of contract between a producer and a user of computer software — sometimes called an End User License Agreement (EULA) — that specifies the perimeters of the permission granted by the owner to the user.”).

51. In relevant part, the Sony BMG EULA reads as follows:

Before you can play the audio files on YOUR COMPUTER or create and/or transfer the DIGITAL CONTENT to YOUR COMPUTER, you will need to review and agree to be bound by an end user license agreement or “EULA”, the terms and conditions of which are set forth below. . . . [I]f you do not agree to be bound by these terms and conditions, you will not be able to utilize the audio files or the DIGITAL CONTENT on YOUR COMPUTER.

As soon as you have agreed to be bound by the terms and conditions of the EULA, this CD will automatically install a small proprietary software program (the “SOFTWARE”) onto YOUR COMPUTER. The SOFTWARE is intended to protect the audio files embodied on the CD, and it may also facilitate your use of the DIGITAL CONTENT. Once installed, the SOFTWARE will reside on YOUR COMPUTER until removed or deleted. However, the SOFTWARE will not be used at any time to collect any personal information from you, whether stored on YOUR COMPUTER or otherwise.

Once the SOFTWARE has been installed on YOUR COMPUTER, a menu will then appear on the screen of YOUR COMPUTER, giving you the option of playing the audio files on YOUR COMPUTER, creating a copy of the DIGITAL CONTENT directly onto the hard drive of YOUR COMPUTER, or making a limited number of backup copies of the CD onto other, recordable CDs. . . .

In order to access the DIGITAL CONTENT on YOUR COMPUTER, you will need to have a copy of an approved media player software program that is capable of playing the DIGITAL CONTENT in the file format you selected. . . This CD may also contain an APPROVED MEDIA PLAYER for the file format you selected. If it does, the menu that appears on the screen of YOUR COMPUTER will prompt you on how to transfer a copy of that APPROVED MEDIA PLAYER onto YOUR COMPUTER. To the extent you utilize an APPROVED MEDIA PLAYER contained on this CD, your use of such APPROVED MEDIA PLAYER may be subject, in each instance, to separate terms and conditions provided by the owner of the APPROVED MEDIA PLAYER concerned.

Sony EULA, <http://www.sysinternals.com/blog/sony-eula.htm> (last visited Jan. 15, 2006).

---

would “cloak” itself, making it extremely difficult to remove or delete.<sup>52</sup> Furthermore, the EULA does not inform consumers that attempting to manually remove the software could disable the computer’s CD drive.<sup>53</sup>

In response to public outcry, Sony BMG quickly issued a press release announcing that it would provide an uninstaller<sup>54</sup> to safely remove the DRM software.<sup>55</sup> But Sony BMG made little effort to inform affected computer users that an uninstaller existed, and those who discovered the uninstaller’s existence had to go through a complicated process to download it.<sup>56</sup> A commentator who tested the rootkit described the downloading process as follows:

First you have to go to Sony’s support site, guess that the uninstall information is in the FAQ, click on the uninstall link and then fill out a form with your email address and purchasing information, possibly adding yourself to Sony’s marketing lists in the process. Then, after you submit the information the site takes you to a page that notifies you that you’ll be receiving an email with a “Case ID”. A few minutes later you receive that email, which directs you to install the patch and then visit another page if you still really want to uninstall. That page requires you to install an ActiveX control. . . enter your case ID and fill in the reason for your request. Then you receive an email within a few minutes that informs you that a customer service representative will email you uninstall instructions within one business day.

When you eventually receive the uninstall email from Sony BMG support it comes with a cryptic link . . . to your personalized uninstall page. [The email] informs you that the uninstaller will expire in one week.<sup>57</sup>

The properly downloaded uninstaller will only work on a specific computer.<sup>58</sup> Therefore, a consumer who wishes to uninstall the DRM software on

---

52. Posting by Mark Russinovich on Sysinternal, <http://www.sysinternals.com/blog/2005/11/more-on-sony-dangerous-decloaking.html> (Nov. 4, 2005, 12:04 p.m.).

53. See Editorial, *Viruses Exploit Sony CD Anti-Piracy Scheme*, MSNBC, Nov. 10, 2005, <http://www.msnbc.msn.com/id/9991596/>.

54. See UNINSTALLER, WIKIPEDIA, <http://en.wikipedia.org/wiki/Uninstaller> (last visited Sept. 8, 2006) (“an uninstaller is a computer program which is designed to remove all or parts of a specific other program or application. It is the opposite of an installer. Most software vendors ship an uninstaller with their applications”).

55. See *You Don’t Really Want to Uninstall*, *supra* note 43.

56. See *You Don’t Really Want to Uninstall*, *supra* note 43.

57. *Id.*

58. *Id.*

---

multiple computers must go through this process for each computer affected.<sup>59</sup>

After some initial foot-dragging, the software industry reached a consensus to treat the Sony BMG DRM software as “spyware.”<sup>60</sup> In addition, the first class-action lawsuit over Sony BMG’s DRM software was filed in California on November 1, 2005, so that Sony BMG will now have to defend its DRM practices in court.<sup>61</sup>

The Sony BMG DRM case is interesting for a number of reasons. First, the case illustrates that, while most abusive software infestations result from some sort of internet activity, even offline users are not necessarily safe if they listen to music on their computers and have a live internet connection. Second, it illustrates that software need not literally “spy” on consumers in order to create a great public outcry. Even if Sony BMG’s music player reports back to Sony each time a consumer plays a protected CD,<sup>62</sup> this may not be the sort of transmission of personal information that needs to be regulated. Third, this case illustrates that the line between a EULA with an acceptable disclosure and one with an unacceptable disclosure is far from clear. Fourth, it illustrates that “harm” can be an increased vulnerability to attack by malicious software.<sup>63</sup> Finally, it illustrates the importance of giving con-

---

59. *Id.*

60. See Nate Mook, *Antivirus Firms Take On Sony DRM*, BETANEWS, Nov. 10, 2005, [http://www.betanews.com/article/Antivirus\\_Firms\\_Take\\_On\\_Sony\\_DRM/1131641594](http://www.betanews.com/article/Antivirus_Firms_Take_On_Sony_DRM/1131641594); Posting by Jason Garms to Blogmalware, <http://blogs.technet.com/antimalware/archive/2005/11/12/414299.aspx> (Nov. 12, 2005, 11:56 a.m.); see also Lorraine Woellert, *Sony BMG Ends a Legal Nightmare*, BUSINESSWEEK, Dec. 30, 2005, [http://www.businessweek.com/technology/content/dec2005/tc20051230\\_658336.htm](http://www.businessweek.com/technology/content/dec2005/tc20051230_658336.htm) (“On Dec. 28, Sony BMG settled a consolidated class-action lawsuit filed by consumers just six weeks earlier over particularly aggressive copy protections embedded in millions of the record label’s CDs.”).

61. See MSNBC, *supra* note 52 (The suit alleges that “Sony’s actions constituted fraud, false advertising, trespass and violated state and federal laws barring malware and computer tampering”). See also Posting by Brian Krebs to Washingtonpost.com, [http://blog.washingtonpost.com/securityfix/2005/11/calif\\_lawsuit\\_targets\\_sony\\_1.html](http://blog.washingtonpost.com/securityfix/2005/11/calif_lawsuit_targets_sony_1.html) (Nov. 8, 2005, 6:35 p.m. EST); Class Action Complaint at 2, *Guevara v. Sony BMG Music Entm’t*, No. BC342359 (Cal. filed Nov. 1, 2005), [http://www.washingtonpost.com/wp-srv/technology/daily/graphics/ca\\_complaint\\_110805.pdf](http://www.washingtonpost.com/wp-srv/technology/daily/graphics/ca_complaint_110805.pdf) (Alleging that the rootkit is surreptitiously installed, continuously depletes system resources, cannot be removed without damage to the system, and that “Sony does not advise consumers of the existence of true nature of the rootkit. . .and misleads consumers into believing that the program may be uninstalled.”).

62. See You Don’t Really Want to Uninstall, *supra* note 43; see also Neda Ulaby, *Sony Music CDs Under Fire from Privacy Advocates*, Nov. 4, 2005, <http://www.npr.org/templates/story/story.php?storyId=4989260>.

63. See MSNBC, *supra* note 52.

sumers control over what programs are installed on their computers. It seems certain that Sony BMG would not have encountered bad press and legal difficulties if it had originally empowered consumers to remove the DRM software simply and effectively.<sup>64</sup>

In the absence of a generally accepted definition of abusive software, Sony BMG had few guidelines to follow when creating procedures to install and uninstall its DRM software. If such an accepted definition existed in 2005, Sony BMG could have abided by that definition and remained legitimate. To provide such a definition, Part V will expand on the elements of abusive software. But before explaining those specific elements, we must examine the general characteristics that are essential to any meaningful definition of abusive software, beginning with a definition of spyware.

#### IV. GENERAL PRINCIPLES UNDERLYING A NEW DEFINITION OF ABUSIVE SOFTWARE

The Anti-Spyware Coalition (“ASC”) published a definition of spyware that serves as a good starting point for this comment’s development of a new definition of abusive software.<sup>65</sup> The ASC was convened in April 2005 by the Center for Democracy and Technology<sup>66</sup> and is “an organization made up of . . . prominent anti-spyware providers as well as key public interest groups committed to combating the rise of unwanted spyware clogging computers and endangering internet communications.”<sup>67</sup> The ASC defines spyware as follows:

Technologies deployed without appropriate user consent and/or implemented in ways that impair user control over:

- Material changes that affect their user experience, privacy, or system security;
- Use of their system resources, including what programs are installed on their computers; and/or
- Collection, use, and distribution of their personal or other sensitive information.<sup>68</sup>

---

64. See You Don’t Really Want to Uninstall, *supra* note 43 (“Without exaggeration I can say that I’ve analyzed virulent forms of spyware/adware that provide more straightforward means of uninstall.”).

65. See Alorie Gilbert, *Group pitches anti-spyware guidelines*, Oct. 27, 2005, [http://news.com.com/Group/pitches+anti-spyware+guidelines/2100-7348\\_3-5918113.html](http://news.com.com/Group/pitches+anti-spyware+guidelines/2100-7348_3-5918113.html); See ASC Definition, *supra* note 28.

66. Ctr. for Democracy & Tech., *Coalition Seeks to Define Spyware, Solicits Public Comment*, July 12, 2005, <http://www.cdt.org/headlines/headlines.php?hid=793>.

67. Anti-Spyware Coalition, *Frequently Asked Questions*, <http://www.antispywarecoalition.org/about/FAQ.html> (last visited January 15, 2006).

68. Anti-Spyware Coalition, *supra* note 28.

---

As an industry group comprised of vendors of anti-spyware software, the ASC understandably takes an industry-self-regulation approach to the definition problem.<sup>69</sup> It seems reasonable to infer that the ASC does not intend for its definition to be used primarily by the courts or regulatory agencies. Rather, the ASC's definition aims to establish a series of best practices within the software industry.<sup>70</sup> As a result, the ASC definition lacks the precision that would be desired in a more formalized legal definition of abusive software. Nonetheless, it is a good starting point for such a legal definition. Analysis of the ASC definition suggests that three related principles should guide the development of a general definition of abusive software: 1) the definition should protect the user's ability to control his or her computer; 2) the definition should be technology-neutral; and 3) the definition should not be over-inclusive.

#### **A. The Definition Should Protect the User's Control of the Computer**

Spyware and other types of abusive software affect different victims in different ways. The obvious victims are the individual users whose computers have become infested with abusive software. However, as will be discussed in the following pages, spyware and abusive software can affect almost any business that uses computers, including e-commerce<sup>71</sup> merchants. The first step in devising an effective definition of abusive software is to decide which class of users we are principally concerned with protecting.

##### **1. Protect Individual Users, Rather Than Business or Commercial Users**

Individual computer users are the most important class of users to protect against abusive software. They must bear the cost of paying for anti-spyware software to protect or disinfect their computers after a spyware infestation;<sup>72</sup> they must bear the cost of having their use of their computers

---

69. Anti-Spyware Coalition Homepage, <http://www.antispywarecoalition.org/> (last visited Jan. 22, 2006)

70. *Id.*

71. See ELECTRONIC COMMERCE, WIKIPEDIA, [http://en.wikipedia/wiki/Electronic\\_Commerce](http://en.wikipedia/wiki/Electronic_Commerce) (last visited Sept. 8, 2006) ("Electronic commerce, e-commerce or ecommerce consists primarily of the distributing, buying, selling, marketing, and servicing of products or services over electronic systems such as the Internet.")

72. See Webroot Software, Spyware Education Center, <http://www.webroot.com/resources/spywareinfo> (last visited January 15, 2006) ("86% U.S. Adult Internet Users Believe that Spyware on Their Computers Has Caused Them to Suffer a Monetary Loss, 2005."); See also CIO Magazine, *The Cost of Spyware*, August 2, 2005, <http://www2.cio.com/metrics/2005/metric831.html> ("According to a recent survey of the 'best' anti-spyware products, not one can

impaired;<sup>73</sup> they must cope with the endless pop-up advertisements;<sup>74</sup> and they must bear the consequences of having their personal data exposed to identity thieves.<sup>75</sup> As this list shows, abusive software harms many of the individual computer user's interests. Of these, privacy and sovereign control are the most important.<sup>76</sup> In this context, privacy refers to the user's right to control the distribution of personal or sensitive data from his or her computer. Sovereign control refers to the user's right to have an appropriate level of control over the identity and behavior of programs that are installed and running on his or her computer.

The ASC definition reflects these dual factors when it recognizes spyware as programs that "impair user control over: Material changes that affect their user experience, privacy, or system security; Use of their system resources . . . ; and/or Collection, use, and distribution of . . . personal . . . information."<sup>77</sup> Similarly, most state laws recognize that abusive software

---

remove all spyware, forcing consumers to purchase more than one."); Jim Moore, *Spyware*, Jan. 2005, <http://www.naspa.com/PDF/2005/0105/T0501010.pdf> ("And here's another real cost of spyware: Time—both your own and others as you attempt to hunt down and remove this stubborn, deeply buried gunk from your machine.").

73. See Jerry Honeycutt, *How to Protect Your Computer from Spyware and Adware*, Apr. 20, 2004, [http://www.microsoft.com/windowsxp/using/security/expert/honeycutt\\_spyware.msp](http://www.microsoft.com/windowsxp/using/security/expert/honeycutt_spyware.msp) ("The main problem that most people notice with [spyware programs] is that they cause performance issues with their computers. For example, Internet Explorer might not work properly any more, your computer might hang more frequently, or your computer might slow down significantly."); Microsoft, *What is Spyware*, Oct. 23, 2006, <http://www.microsoft.com/athome/security/spyware/spywarewhat.msp> (explaining that spyware hurts a computer's efficiency).
74. See Honeycutt, *supra* note 73 (explaining that computer users might have spyware or other unwanted software on their computers if they see pop-up advertisements even when they are not online).
75. See SPYWARE, *supra*, note 12 ("spyware has been closely associated with identity theft"); Clint Ecker, *Massive spyware-based identity theft ring uncovered*, Aug. 5, 2005, <http://arstechnica.com/news.ars/post/20050805-5175.html> ("The list of [information stolen by the spyware application] includes not only bank accounts but website passwords, eBay accounts. . ."); Wayne Porter, *Identity Theft and Spyware-The New Threat*, <http://www.spywareguide.com/articles/identity-theft.html> (last visited Jan. 29, 2006) ("Spyware can be used to surreptitiously gather all types of confidential information and in most cases the user has no idea the information is being taken.").
76. The other interests affected by abusive software—time, money, loss of use of the computer—would all be protected by ensuring that the user is able to maintain *control* over his or her computer because abusive software cannot impair those interests if the user's control prevents the abusive software from being installed. Privacy is addressed in Part IV.A.2.
77. ASC Definition, *supra* note 28.

R

R

---

implicates concerns beyond control of personal data (i.e., privacy).<sup>78</sup> At a minimum, most of this legislation reflects the notion that computer users should have the right to control the software running on their computers. This sovereign control includes the right to be free from unwanted pop-up advertising.<sup>79</sup>

But individual computer users are not the only victims of spyware and abusive software; abusive software inflicts comparable harms also on businesses that use personal computers.<sup>80</sup> The scale of the intrusion is different (a business may have hundreds or thousands of computer desktops to protect from abusive software),<sup>81</sup> but the interests implicated are substantially similar.<sup>82</sup> Consequently, business interests should be adequately guarded by protections granted to individuals.

Finally, e-commerce merchants and other entities that make money from drawing traffic to their websites have interests that are affected by certain kinds of abusive software, notably targeted pop-up advertising

---

78. See Edelman, *supra* note 18.

R

79. See *id.*

80. See, Blue Coat, White Paper: Spyware Prevention for the Enterprise, (2006), [http://www.bluecoat.com/downloads/whitepapers/BCS\\_spyware\\_wp.pdf](http://www.bluecoat.com/downloads/whitepapers/BCS_spyware_wp.pdf).

81. 92% of enterprises acknowledge a serious spyware problem, and an estimated 30% of enterprise computer desktops are infected with some form of spyware. See *id.* at 3.

82. Cf. *id.* at 4 (noting that the business entity is left out of the loop if commercial abusive software vendors seek to comply with potential new legislation by making license agreements clearer and getting more explicit consent because neither of those measures goes beyond the computer user). Business computer users do differ from individual computer users insofar as in the business context, the costs of an abusive software infestation will be mostly borne by the business entity, rather than the individual user. Moreover, in many cases, only the employee—not the business entity—would be asked for consent to a specific software installation initiated by that employee. *Id.* This “authorization gap” is a legitimate concern and echoes the perils of over-reliance on consent to control abusive software. See *infra*, note 129. Admittedly, the definition of abusive software set out in Part V of this comment may not protect business users as completely as it does individual computer users. Still, the “authorization gap” is a necessary consequence of requiring adequate authorization as set out in Part V.B., From the software publisher’s perspective, the person sitting in front of the computer must have the apparent authority to authorize the installation, even if the computer in question is actually managed by another. In other words, the software publisher has no way to determine the relationship between the person clicking the mouse (the end user) and the entity that manages the computer, so it would be manifestly unfair to require the software publisher to attempt to discern whether the end user has the actual authority to proceed with the installation. See *infra*, Part V.B.

R

software,<sup>83</sup> which has been the source of a large amount of spyware litigation so far.<sup>84</sup> Even though this type of spyware does affect the interests of e-commerce merchants, anti-abusive software regulation should not focus solely on e-commerce concerns. Rather, the interests of e-commerce merchants will be indirectly protected by ensuring that each computer user retains control over the software running on his or her machine. The focus of this comment, and the proper focus for abusive software regulation, is the relationship between the abusive software publisher and the computer user, not the relationship between the “spyware” publisher and the businesses whose websites trigger an ad. Such targeted pop-up advertising may be an unfair trade practice, or it may constitute infringement under trademark doctrine. But whether it is an unfair trade practice is a question distinct from whether or not the installation of the software in question was unfair or deceptive with respect to the computer user.<sup>85</sup>

## 2. Protect Users’ Control Rather Than Their Privacy

Having decided that this proposed definition of abusive software should primarily protect individual computer users, the next question is whether the definition should focus primarily on protecting their privacy or their control interests. Many forms of abusive software “merely” interfere with users’ control over their computers, but some of the more malicious variants have been linked to serious privacy-related crimes such as identity theft.<sup>86</sup> Even if

---

83. The interest in question can best be described by an example. Consider the impact of a piece of targeted pop-up abusive software on the hypothetical retailer WidgetWorld, which sells widgets through its website widgetworld.com. In this scenario, the pop-up software monitors which website the computer user is currently visiting in order to display ads from competitors. WidgetWorld’s competitor, Widgets-R-Us, has paid the pop-up software publisher to send pop-up ads directing the user to widgetsrus.com whenever the user visits widgetworld.com. So, the user goes to WidgetWorld with the intention of ordering a widget, but then the pop-up software kicks in, affecting two of WidgetWorld’s interests. First, the pop-up software sends a window that partially obscures the website of widgetworld.com, thus inserting itself in between WidgetWorld and one of its customers. Second, WidgetWorld might lose a sale if the user clicks on the pop-up ad and ends up purchasing the widget from the Widgets-R-Us website.

84. See Edelman2, *supra* note 18.

R

85. The recently passed Alaska spyware legislation is somewhat unusual in that it virtually ignores the computer user, instead treating spyware exclusively as a business competition matter. See ALASKA STAT. § 45.45.792 (2006); see also Edelman, *supra* note 18 (The Alaska statute “Prohibits certain pop-up ads displayed by spyware, including popups displayed in response to a specific web address or trademark, unless with consent of the site or mark owner.”).

R

86. See, e.g., Mark Ward, *ID Theft Spyware Scam Uncovered*, Aug. 23, 2005, <http://news.bbc.co.uk/1/hi/technology/4173218.stm> (describing the discovery of a

---

most forms of abusive software collect personal information without any criminal intent, they still collect personal information in ways that trouble consumers.<sup>87</sup> Thus, there is some overlap between consumer privacy doctrine and abusive software doctrine.

However, even though these doctrines overlap to some degree, they should not be conflated. Identity theft and other such consequences of breached privacy must be controlled regardless of how the offending party acquired the personal information at issue—consumers need privacy protection regardless of whether abusive software was used to gather personal information. Likewise, software that interferes with consumers' control over their machines is harmful regardless of whether that software also steals personal information. This is not to suggest that the theft of personal information should not be regulated and punished—far from it. However, protection of privacy is too important to be left to anti-abusive software regulation. Trying to mix the protection of consumer privacy and control interests in the same doctrine will benefit neither cause as it will only muddy the waters.

Therefore, this comment's proposed definition of abusive software will focus on protecting consumers' interests in maintaining appropriate control over their computers without addressing their sometimes parallel interests in protecting their personal privacy. While U.S. privacy laws may need updating for the Internet Era,<sup>88</sup> such updating belongs outside abusive software doctrine and is beyond the scope of this comment. In sum, the first general principle underlying this abusive software definition is that of all the interests affected by abusive software, the individual computer user's sovereign control interests are paramount and should be the primary interests that anti-abusive software regulations seek to protect.

## B. The Definition Should Be Technology-Neutral

A law that targets web browser bookmarks and start pages says nothing about instant messenger traffic. And what about the portable device that connects to the Internet but offers no way to accept or reject the terms of a useful new feature? New tech-specific laws

---

trojan that transmitted names, credit card numbers, bank account numbers, and other sensitive data to a central repository).

87. See, e.g., Benjamin Edelman, *Methods and Effects of Spyware*, Public Comment for Fed. Trade Comm'n Spyware Workshop at 4-6 (March 19, 2004), <http://www.ftc.gov/os/comments/spyware/040319edelman.pdf> (describing how 'Gator' software tracks the address of every website the user of an infected computer visits, allowing companies to maintain huge databases that can identify and classify specific consumers based on their web-browsing habits).
88. See Jane K. Winn, *Contracting Spyware by Contract*, 20 BERKELEY TECH. L.J. 1345, 1358 (2005) ("U.S. information privacy law is now in shambles after decades of narrowly focused, piecemeal legislation.").

---

will look outdated in five years (if not sooner) as the technology changes.<sup>89</sup>

Because much of abusive software's bad behavior is specific and easily identifiable by computer users (including legislators),<sup>90</sup> most, if not all, of state anti-spyware legislation tries to regulate abusive software by prohibiting a list of technology-specific actions.<sup>91</sup> For example, the anti-spyware statute in Washington State makes it unlawful for an unwanted piece of software to (among other things) modify the user's web browser home page, web proxy settings, or bookmarks,<sup>92</sup> or to "[open] multiple, sequential, stand-alone advertisements in the [user's] internet browser."<sup>93</sup>

This last provision provides a good example of the dangers of technology-specific definitions. First, the provision is under-inclusive in that it would not make it unlawful to open multiple pop-up ads in the user's new-reader or mail program (if those were special purpose programs that the user did not use as an internet browser).<sup>94</sup> Second, as a technology-specific prohibition, it is subject to technological avoidance. For example, a spyware vendor might open just one advertisement that periodically updates itself and is difficult or impossible for the user to close. Such an advertisement would certainly be as vexatious to the user as "multiple, sequential, stand-alone advertisements,"<sup>95</sup> yet such an advertisement would avoid the dictates of the statute. Finally, such technology-specific provisions are not "future-proof." While the pop-up ad provision seems to adequately address the immediate pop-up ad problem, it will likely have no effect on the next annoying practice the spyware vendors will invent—perhaps, for example, spyware vendors will start causing computers to play jingles or other types of audio-advertising, thus circumventing the statute by not opening any windows in the user's browser.

The three problems just enumerated are not limited to this particular technology-specific provision. Most technology-specific legislation will fall victim to one or more of these problems. Notably, specific definitions are often under-inclusive because they create loopholes and tend to be suscepti-

---

89. Electronic Frontier Foundation, *Spitzer Suit Shows the Right Way to Fight Spyware*, Apr. 28, 2005, [http://www.eff.org/deeplinks/archives/2005\\_04.php](http://www.eff.org/deeplinks/archives/2005_04.php).

90. For example, the software alters the user's home page, displays endless pop-up ads, alters the user's bookmarks, or prevents its removal from the system.

91. See Crawford, *supra* note 28 at 1445-50; see also Edelman, *supra* note 18.

92. WASH. REV. CODE § 19.270.020 (2006).

93. See *id.* § 19.270.030.

94. Certainly it is conceivable that a court might interpret "Internet browser" broadly enough to encompass mail and news reader programs, but a court would not have to resort to such statutory interpretation trickery if the statute were more broadly drafted.

95. WASH. REV. CODE § 19.270.030.

---

ble to changing practices.<sup>96</sup> Therefore, any abusive software definition should be as technology-neutral as is reasonably possible.<sup>97</sup>

### C. The Definition Should Not Be Over-Inclusive

The final general principle that must underlie a definition of abusive software is that the definition should not be over-inclusive. While a technology-specific definition may be too narrow, technology-neutral definitions, which necessarily use broad, general language, have the potential to include too much conduct within their ambit.<sup>98</sup>

---

96. Perhaps the best example of the failure of technology-specific definitions to adapt involves the Audio Home Recording Act of 1992 (AHRA), 17 U.S.C. §§ 1001-1010 (2000). The AHRA requires “digital audio recording devices” to have a particular Copyright Management System in order to prevent copyrighted songs from being copied. Andrew C. Humes, *The Day the Music Died: The RIAA Sues Its Consumers*, 38 IND. L. REV. 239, 252-55 (2005). However, due to its technical specificity, courts only a decade after its passage refused to hold the AHRA applicable to computers or MP3 players, even though those two classes of devices were arguably the greatest sources of music copyright infringement at the time. *See id.* Accordingly, the AHRA, which was intended to prevent digital music sharing, proved to be almost completely ineffective at that task. *See id.*; *see also, e.g.*, Craig A. Grossman, *From Sony to Grokster, The Failure of the Copyright Doctrines of Contributory Infringement and Vicarious Liability to Resolve the War Between Content and Destructive Technologies*, 53 BUFF. L. REV. 141, 233 (2005) (“In the case that presented the closest analogy to the VCR challenged to date, the digital MP3 player, the Ninth Circuit eschewed any direct discussion of Sony, choosing instead to base its finding that the MP3 player was a legal device on the arcane peculiarities of the definitions of various devices found in the Audio Home Recording Act.”); June M. Besek, *Anti-Circumvention Laws and Copyright: A Report from the Kernochan Center for Law, Media and the Arts*, 27 COLUM. J.L. & ARTS 385, 472 (2004) (“due to [the AHRA’s] narrow definitions, works copied by means of computers do not qualify.”).

97. *See Crawford, supra* note 28 at 1450-54.

R

98. For example, consider the recently passed measure that amended 47 U.S.C. 223 to expand the types of technology that are regulated as telephone harassment, thus making it a crime to “[send] annoying e-mail messages without disclosing your true identity.” Declan McCullagh, *Perspective: Create an e-annoyance, Go to Jail*, Jan. 9, 2006, [http://news.com.com/Create+an+e-annoyance,+go+to+jail/2010-1028\\_3-6022491.html](http://news.com.com/Create+an+e-annoyance,+go+to+jail/2010-1028_3-6022491.html). At least one commentator has noted that the resulting law is so broad that it “would likely imperil much of Usenet.” *Id.*; *see also* Declan McCullagh, *FAQ: The New ‘Annoy’ Law Explained*, Jan. 11, 2006, [http://news.com.com/FAQ+The-ew+annoy+law+explained/2100-1028\\_3-6025396.html](http://news.com.com/FAQ+The-ew+annoy+law+explained/2100-1028_3-6025396.html). Usenet is an Internet discussion system, similar to bulletin board systems. Users read and post messages to a number of distributed newsgroups on widely varying topics. USENET, WIKIPEDIA, <http://en.wikipedia.org/w/index.php?title=Usenet&oldid=36782362> (last visited Sept. 8, 2006).

In particular, the definition of abusive software could easily stifle innovation on the Internet if it were so broad as to include any piece of software that inadvertently caused some harm to the user. By way of illustration, consider the following hypothetical, technology-neutral definition of abusive software: any software that interferes with the user's experience on a computer without the user's consent or that causes loss of data. Next, apply that very broad definition to a useful software widget that is given away freely by a hobbyist software developer. If that widget has a bug that causes a few users' machines to lock up when they run the widget, resulting in the loss of unsaved work, then this otherwise useful piece of software would be marked as abusive under the hypothetical definition.

Computers are useful only to the extent that they have useful software programs to run.<sup>99</sup> Given the extent to which computers have pervaded modern society,<sup>100</sup> there is social utility in maximizing the number of useful software programs that are available. Therefore, the definition of abusive software should exclude as many useful pieces of software as possible; it should minimize "false-positives." But it is not immediately clear how to best accomplish this goal.

One way to avoid over-inclusiveness might be to introduce a consent element: so long as software publishers did not surreptitiously install their programs on a user's computers, but rather installed them only at the request of the user, their programs would not fall within the definition. Yet exclusive reliance on a consent element to avoid over-inclusiveness too is potentially problematic in certain scenarios.<sup>101</sup> For example, relying exclusively on consent would lead to false-positives on web applications<sup>102</sup> and automatic updates to a special-purpose computing device like TiVo®.<sup>103</sup> The

---

99. See COMPUTER, WIKIPEDIA, <http://en.wikipedia.org/w/index.php?title=Computer&oldid=37147916> (last visited Sept. 8, 2006).

100. "With computers now almost as common in American homes as cable television service, the Internet continues to expand in importance as a communication, information, entertainment, and transaction tool." NAT'L TELECOMM. & INFO. ADMIN., *supra* note 2, at 3.

101. See FED. TRADE COMM'S, *supra* note 1, at 36-38 (comments of Mark Bohannon, General Counsel and Senior Vice President for Public Policy, Software and Information Industry Association).

102. See WEB APPLICATION, WIKIPEDIA, [http://en.wikipedia.org/w/index.php?title=Web\\_application&oldid=35207331](http://en.wikipedia.org/w/index.php?title=Web_application&oldid=35207331) (last visited Sept. 8, 2006) ("A web application is an application delivered to users from a web server over [the] internet [sic]. . . . [W]eb applications are used to implement webmail, online retail sales, online auctions, wikis, discussion boards, weblogs, MMORPGs, and perform many other functions.").

103. See generally TiVo, <http://www.tivo.com/> (last visited Sept. 8, 2006). A TiVo is a computer-based device that records television programs for later viewing. *Id.* As part of the service, the user's TiVo connects to a central server and automatically downloads software updates that could materially affect the

---

commonality between these two seemingly disparate examples is the lack of explicit user consent and the potential to cause some sort of harm to the user. When users visit Google's Gmail™ web page in order to read their email, they expect the necessary software to run so that the Gmail web application will run correctly, enabling them to read their mail.<sup>104</sup> Users do not expect to explicitly consent to running the Gmail software each time they visit the site. Similarly, TiVo updates typically happen in the dead of night, and users do not expect to have to consent to each update. Because an overly consent-focused definition of abusive software would sweep in such desirable behavior, a workable definition must not focus exclusively on consent.

Considering whether the software publisher *intended* to cause harm suggests a possible solution to the problem of false-positives arising from an over-reliance on consent. Under this approach, the software in question would only be designated as abusive if it was installed without consent and intentionally caused harm. Web applications and automatic updates, for example, would be immunized even if they inadvertently led to some harm.

This kind of mental state element must be rejected, however, not only because it would be difficult to assess the intent of any given software publisher, but also because it could lead to false-negatives in some cases. For example, such a mental state element would probably lead to a false negative in the case of the Sony BMG DRM software.<sup>105</sup> While Sony BMG intended to install “cloaked” software without specific disclosure of that fact, it certainly did not intend to severely compromise the security of affected systems.<sup>106</sup> Ultimately, the proper approach is to abandon the subjective mental state element. The definition proposed in this comment avoids false positives

---

user's use of the device. For example, a software update could potentially remove the user's ability to skip commercials when watching previously recorded material.

104. See generally Gmail, <http://www.gmail.com/>. Gmail is an email service operated by Google.

105. See *supra* Part III.

106. The Sony-BMG software created a vulnerability that opened up affected systems to being compromised by the Troj/Stinx-E Trojan. See *supra* Part III. To address this particular false negative, perhaps the concept of “single-intent” could be borrowed from Tort doctrine. See 6 AM. JUR. 2D *Assault and Battery* § 8 (1999) (“In modern practice, the requirement of intent has been relaxed to a certain extent, with some courts holding that a battery need not be committed out of malice or an intent to cause harm, to injure, or to inflict actual damage.”). This would make the harm caused by Sony-BMG's software intentional because Sony BMG intended to install the software even though it did not intend to cause security vulnerabilities. But that approach would increase the subjectivity and complexity of the analysis, which would make the definition inherently less clear and less useful to software publishers trying to publish legitimate software.

---

by excluding software that does not interfere with a user's *reasonable* control over his or her system or which secures *adequate* consent.<sup>107</sup>

Having established the three general principles that will underlie the proposed definition of abusive software, we are ready to move on to Part V, the actual definition of abusive software.

## V. ELEMENTS OF A NEW DEFINITION OF ABUSIVE SOFTWARE

Based on the general principles outlined above, the proposed definition of abusive software is as follows:

Software that is executed without adequate authorization and that intentionally causes reasonably unavoidable ongoing harm or reasonably irreversible harm.

While this definition appears simple on its face, as with most legal definitions, the devil is in the details. The definition can be broken down into three elements: software, adequate authorization, and harm. While "software" is relatively straightforward and requires little discussion, statements from the Federal Trade Commission illustrate that "adequate authorization" and "harm" will both be difficult elements to nail down.<sup>108</sup>

At the FTC [spyware] workshop [April 2004], there was "broad agreement that spyware should be defined to include software installed without adequate consent from the user," yet there remained "*substantial differences of opinion as to what distributors must do to obtain such consent.*" In addition, there was agreement that "to avoid inadvertently including software that is benign or beneficial, the term spyware should be limited to software that causes some harm to consumers," although there were "*substantial differences of opinion as to when software has caused the type and magnitude of harm to warrant being treated as spyware.*" The FTC staff therefore concluded that "*these fundamental issues of consent and harm need to be resolved before any common definition of spyware can be developed.*"<sup>109</sup>

---

107. The "reasonable" and "adequate" modifiers call for a fact-dependent analysis and will be further discussed in Parts V.B and V.C.

108. FED. TRADE COMM'S, PREPARED STATEMENT OF THE FEDERAL TRADE COMMISSION BEFORE THE COMMITTEE ON COMMERCE, SCIENCE AND TRANSPORTATION 2-3 (2005), <http://ftc.gov/os/testimony/051005spywaretest.pdf> (statement of Deborah Platt Majoras, Chairman, Federal Trade Commission) [hereinafter Prepared Statement of the FTC].

109. *Id.* at 2 n.4 (emphasis added, internal citations omitted).

---

## A. Software

The “software” element should be construed broadly in order to encompass any set of instructions executed on a computer.<sup>110</sup> This definition includes many sets of instructions that do not fit the common mold of a software “program” or “application” such as web pages, web applications, and shell scripts.<sup>111</sup> Some pieces of state legislation, such as the Washington state spyware act,<sup>112</sup> make specific exceptions for web pages. To avoid the problem of under-inclusiveness, such technology-specific determinations should not form part of this definition. Almost all websites fall outside of the proposed abusive software definition without resorting to a technology-specific exception because they would fail to meet one of the harm elements.<sup>113</sup>

## B. Adequate Authorization

In contrast to the relatively straightforward definition of “software,” the question of what sort of user consent will constitute “adequate authorization” is difficult to answer. Clearly, users do not authorize the execution of a piece of software if they are tricked or misled into its execution.<sup>114</sup> Similarly, any piece of software that is installed by exploiting a security hole<sup>115</sup> would not be authorized. But it is unclear if software would be authorized when the

---

110. Compare WASH. REV. CODE § 19.270.010 (2006), with 17 U.S.C. § 101 (Supp. 2004) (“A ‘computer program’ is a set of statements or instructions to be used directly or indirectly in a computer in order to bring about a certain result.”), and CAL. BUS. & PROF. CODE § 22947.1 (Deering 2006) (“‘Computer software’ means a sequence of instructions written in any programming language that is executed on a computer.”).

111. SHELL SCRIPT, WIKIPEDIA, [http://en.wikipedia.org/w/index.php?title=Shell\\_script&oldid=35069488](http://en.wikipedia.org/w/index.php?title=Shell_script&oldid=35069488) (last visited Sept. 8, 2006) (“A shell script is a script written for the shell, or command interpreter, of an operating system. . . . Typical operations performed by shell scripts include file manipulation, program execution, and printing text. Usually, shell script refers to scripts written for a Unix shell, while DOS and Windows command-line scripts are called batch files.”).

112. *E.g.*, WASH. REV. CODE § 19.270.010.

113. See discussion *infra* Parts V.C.3-4. Specifically, almost all websites would be excluded from being labeled as abusive software because they would fail to meet both the “ongoing” and “reasonably irreversible” sub-elements of harm.

114. *Cf.* Ben Edelman, Spyware Installation Methods, <http://www.benedelman.org/spyware/installations/> (last visited Sept. 1, 2006) (giving examples of specific spyware installation techniques involving trickery or deception).

115. See, *e.g.*, *id.*; see also Microsoft, Microsoft Security Advisories, <http://www.microsoft.com/technet/security/advisory/default.mspx> (last visited Sept. 8, 2006) (noting security holes in Microsoft programs).

software is executed after the user has ostensibly agreed to the terms of a click-wrap agreement<sup>116</sup> or a complex EULA.<sup>117</sup>

All too many of the EULAs that consumers encounter with unwanted software are presented in confusing, pressured circumstances—in the midst of several pop-ups from a web site that refuses to work unless the user installs the correct plug-in, for example. Moreover, these EULAs often couch complex, even outrageous, terms of agreement in long, dense blocks of legalese that few consumers have any hope of understanding. Many of these EULAs point to still more EULAs from other associated parties, requiring users to track down and plow through a pile of prose so daunting that few would ever venture to attempt it.<sup>118</sup>

Modern internet contracts doctrine tends to allow valid contracts to be formed using novel, ambiguous, or even confusing means<sup>119</sup> despite the fact that many spyware EULAs are intended to bewilder rather than enlighten the computer user.<sup>120</sup> This deference favors the interests of abusive software distributors over the interests of computer users and suggests that an effective authorization scheme to protect consumers from abusive software will almost certainly have to be found outside contracts doctrine.<sup>121</sup>

The Securely Protect Yourself Against Cyber Trespass Act (Spy Act),<sup>122</sup> introduced to Congress in 2005, approaches the authorization issue from

- 
116. See *CLICKWRAP*, *supra* note 49. See also Kevin W. Grierson, Annotation, *Enforceability Of "Clickwrap" Or "Shrinkwrap" Agreements Common In Computer Software, Hardware, And Internet Transactions*, 106 A.L.R.5th 309 (2004). R
117. See *SOFTWARE LICENSE*, *supra* note 50. R
118. Howes, *supra* note 14, at 5. See also Winn, *supra* note 88, at 1348-49. R
119. Winn, *supra* note 88, at 1346-53. See generally Christina L. Kunz et al., *Browse-Wrap Agreements: Validity of Implied Assent in Electronic Form Agreements*, 59 BUS. LAW. 279 (2003) (comparing standard electronic and paper contracts). R
120. See Lohmann, *supra* note 48, at 1-2 (describing Sony-BMG's 3000-word EULA); Ben Edelman, *Gator's EULA Gone Bad*, Nov. 29, 2004, <http://www.benedelman.org/news/112904-1.html> ("At 5,936 words, the license stretches to 63 on-screen pages as presented by the current Kazaa installer (bundling Gator)."); Ben Edelman, *Claria License Agreement Is Fifty Six Pages Long*, Dec. 1, 2004, <http://www.benedelman.org/spyware/claria-license/> ("Among the various characteristics of spyware are license agreements and disclosures that are absent, confusing, unintelligible, or otherwise such that users do not provide meaningful consent to software being installed on their PCs."). R
121. Winn, *supra* note 88, at 1346-53. R
122. Spy Act, H.R. 29, 109th Cong. (2005).

---

more of a tort law perspective than from a contract law perspective.<sup>123</sup> Section 3(c)(1) of the Spy Act requires a spyware “program [to provide] clear and conspicuous notice in plain language” about its collection of information and its use of that information.<sup>124</sup> The Spy Act describes a two-stage notification regime. First, the installer must clearly and noticeably inform users that installation of the software will generally impact the privacy of their personal

---

123. Winn, *supra* note 88, at 1358.

124. H.R. 29, 109th Cong. § 3 provides:

(c) Notice and Consent.

(1) In general. Notice in accordance with this subsection with respect to an information collection program is clear and conspicuous notice in plain language, set forth as the Commission shall provide, that meets all of the following requirements:

(A) The notice clearly distinguishes such notice from any other information visually presented contemporaneously on the computer.

(B) The notice contains one of the following statements, as applicable, or a substantially similar statement:

(i) . . . “This program will collect and transmit information about you. Do you accept?”.

(ii) . . . “This program will collect information about Web pages you access and will use that information to display advertising on your computer. Do you accept?”.

(iii) . . . “This program will collect and transmit information about you and will collect information about Web pages you access and use that information to display advertising on your computer. Do you accept?”.

(C) The notice provides for the user—

(i) to grant or deny consent referred to in subsection (a) by selecting an option to grant or deny such consent; and

(ii) to abandon or cancel the transmission or execution referred to in subsection (a) without granting or denying such consent.

(D) The notice provides an option for the user to select to display on the computer, before granting or denying consent using the option required under subparagraph (C), a clear description of—

(i) the types of information to be collected and sent (if any) by the information collection program;

(ii) the purpose for which such information is to be collected and sent; and

(iii) in the case of an information collection program that first executes any of the information collection functions of the program together with the first execution of other computer software, the identity of any such software that is an information collection program.

*Id.* § 3.

---

information and will possibly trigger targeted advertising.<sup>125</sup> Second, the installer must provide a link to a specific description of the information that would be collected and how it would be used.<sup>126</sup> In essence, the Spy Act's notice and consent requirements attempt to ensure that reasonable computer users will be informed of certain facts that materially affect their decision to install the program.

While the Spy Act only applies to a relatively narrow cross-section of abusive software, its authorization requirements provide good guidance for the development of a more general standard. Most importantly, any meaningful authorization scheme must ensure that distributors of spyware and other abusive software cannot rely on "implied assent" to legitimize the installation of such software on computers.<sup>127</sup>

Consequently, to meet the "adequate authorization" element of this proposed definition of abusive software,<sup>128</sup> the distributor should have to provide clear and prominent notice that installation of the software would have a material negative impact on the users' privacy or use of their computers. Furthermore, the distributor should have to provide a link to the details of the material effects.<sup>129</sup>

---

125. *See id.*

126. *Compare id., with Kunz, supra* note 118, at 291 (stating the first two elements of the proposed test to determine whether a user validly assented to a "browse-wrap" agreement are the following: "(i) The user is provided with adequate notice of the existence of the proposed terms. (ii) The user has a meaningful opportunity to review the terms.").

127. *See Kuntz, supra* note 118.

128. Note that meeting this element would legitimize the installation of otherwise abusive software.

129. Before continuing, it should be noted that some commentators have expressed skepticism about the efficacy of notice and consent requirements as a tool to control spyware. *See, e.g., Crawford, supra* note 28, at 1456-57. Certainly there is a danger that computer users could become so inundated with requests for authorizations that they would blindly click "YES" without reading any of the notices so that they could continue working on their computers. *See id.* at 1456 ("Users who set their browsers to 'not accept cookies without permission' end up having terrible usage experiences, because they have to click to agree over and over again in order to sustain a single session on a single website."). But this dire prediction will not come to pass if the authorization scheme would only be required for software that would cause *ongoing* harm. Thus, any transient software—JavaScript™, html, or otherwise—would not need to seek authorization from the computer user. Furthermore, it is important to bear in mind that the requirement to seek authorization would be triggered only at the time a piece of software is installed or materially altered.

### C. Harm

This comment has defined spyware and other abusive software as software that is executed without adequate authorization and that causes reasonably unavoidable ongoing harm or reasonably irreversible harm.<sup>130</sup> The nature of the behavior that will be classified as “harm” will serve to mark the boundary between software that needs to seek authorization under this abusive software definition and software that does not. A broad definition of harm would be preferable since harm alone is by no means dispositive of the question of whether a piece of software is abusive.<sup>131</sup> But, unsurprisingly, commentators disagree as to what constitutes harm.<sup>132</sup>

The ASC definition again provides a good place to start. The ASC implicitly categorized harm into three (overlapping) categories: loss of control over user experience, privacy, or system security; loss of control over what programs are installed and running on a computer; and loss of control over the use and distribution of personal or other sensitive information.<sup>133</sup> This definition of harm has the advantage of being relatively technology-neutral.<sup>134</sup> As a result, it is difficult to conceive of potentially objectionable software conduct that would not fall into one of these categories. This definition coincides with the view that one of the primary reasons that spyware is objectionable is that it wrests away users’ control over their computers, even if it does not steal personal information or engage in other particularly egregious behavior.<sup>135</sup>

130. *See supra* Part V.

131. Viewed in this manner, meeting the *harm* element triggers the requirement that a piece of software seek adequate authorization. It is not the harm alone that makes a program abusive; it is the combination of harm and inadequate authorization.

132. *See* Prepared Statement of the FTC, *supra* note 109, at n.4.

R

133. *See* ASC Definition, *supra* note 28.

R

134. *Cf.* Spy Act, H.R. 29, 109th Cong. (2005) (prohibiting a list of specific actions such as modifying the user’s home page, altering bookmarks, diverting the web browser away from the user’s intended destination, delivering advertisements that the user cannot stop without quitting the web browser or restarting, etc.); WASH. REV. CODE § 19.270.020 (2005) (prohibits using intentionally deceptive means to modify the user’s home page or bookmarks, collect personally identifiable information, prevent the user from uninstalling the software, etc.). *See also* Howes, *supra* note 14, at 5. (would prohibit making unwelcome modifications to users’ systems and web browsers, installing unwanted toolbars and other widgets, displaying unsolicited pop-up ads, and preventing users from reversing changes made to their systems or browsers).

R

135. *See* FED. TRADE COMM’N, *supra* note 1, at 56, 58 (comments of Avi Nader, President and CEO, WhenU.com, Inc.) (“We absolutely believe that in order for something to be legitimate, the consumer has to have ultimate control over it. . . . And so, basically, we do think that the ability to uninstall, the ability to control your experience, is a fundamentally important part of this debate.”); *see*

A definition of harm can be inferred and adapted from the ASC definition of spyware. Harm is loss of reasonable control over user experience, privacy, or security of a computer; over what programs are installed and running on a computer; over the use and distribution of personal or other sensitive information;<sup>136</sup> or over user data files (including documents, spreadsheets, bookmarks, photos, etc.).

Before moving on to the remaining sub-elements of harm from this definition of abusive software (reasonably unavoidable, ongoing, reasonably irreversible), some discussion is warranted on the meaning of the key phrase in the definition of harm just set out. Harm is loss of *reasonable control*, not loss of absolute control.

This definition of abusive software is intended to protect the user's control over his or her computer. But the reality of computer ownership is that many, if not most, of the actions that a computer takes are to some degree outside the user's direct control.<sup>137</sup> In fact, it would be unreasonable to expect users to be in absolute control over every aspect of their computers' functioning.<sup>138</sup> Therefore, a definition of abusive software that attempted to preserve absolute user control over every aspect of the computer's functioning would be so over-inclusive as to be meaningless (hence the use of the term "reasonable control").

The "reasonable control" clause creates an area where software distributors can freely interfere with aspects of a computer's function that are not deemed reasonably within users' control. To limit the scope of this area where consent is not required, "reasonable control" must be interpreted broadly. Thus, users' asserted control must be presumptively reasonable unless the software at issue falls within one of a few narrow categories. The most obvious category involves automatic security updates.<sup>139</sup>

---

*also* Joris Evers, *Homeland Security Official Suggests Outlawing Rootkits*, Feb. 16, 2006, [http://news.zdnet.com/2100-1009\\_22-6040726.html](http://news.zdnet.com/2100-1009_22-6040726.html) (quoting Jonathan Frenkel, director of law enforcement policy at the U.S. Department of Homeland Security) ("[W]e need to be thinking about how we ensure that consumers are not surprised by what their software programs do.").

136. See ASC Definition, *supra* note 28.

R

137. For example, most modern computers regularly synchronize their clocks to one of the Network Time Servers on the Internet. While all operating systems provide the user with some way to turn this feature on or off, most users do not need or want to exercise control over this function. Most users just want their clocks to be accurate. Similarly, many media player applications automatically search the Internet for cover art to display when the user is listening to a CD. There are countless examples of automatic features such as these that contribute to make the user experience conform to the user's expectations.

138. See Crawford, *supra* note 28, at 1456 ("Users may not actually want to know everything that their machines are doing.").

R

139. As bugs and potential security holes are discovered in computer operating systems (OS), the OS maker typically releases "patches" that are designed to fix

---

The modern internet-connected desktop computer lives in a very hostile environment, and most are constantly probed for security vulnerabilities.<sup>140</sup> Once a computer has been infected with a virus, worm or other form of malicious software, it is extremely common for that computer to be used as a base from which to attack thousands of other computers on the Internet.<sup>141</sup> Thus, while computer security might seem like a matter of individual interest, the public at large also has a great interest in keeping each and every computer on the Internet secure.<sup>142</sup> Because malicious software spreads via unsecured computers and inflicts high costs on internet society,<sup>143</sup> an abusive software doctrine must take steps to ensure that it does not hinder the distribution of security updates. Therefore, a software distributor does not interfere with users' reasonable control over their computers when it disseminates

---

the bugs or plug-up the security holes. See *COMPUTER INSECURITY*, WIKIPEDIA, [http://en.wikipedia.org/w/index.php?title=Computer\\_insecurity&oldid=35755533](http://en.wikipedia.org/w/index.php?title=Computer_insecurity&oldid=35755533) (last visited Sept. 8, 2006). Promptly patching bugs in OSs is an important step in protecting individual computers and controlling the spread of viruses and other forms of malicious software. *Id.* In recent years, OS makers have started building programs that automatically apply patches as they are released. See *WINDOWS UPDATE*, WIKIPEDIA, [http://en.wikipedia.org/w/index.php?title=Windows\\_Update&oldid=35991912](http://en.wikipedia.org/w/index.php?title=Windows_Update&oldid=35991912) (last visited Sept. 8, 2006). The most common example of this automatic security update service is Windows Update. *Id.* ("Windows Update is a web-based software update service for Microsoft Windows operating systems. It offers a location for downloading critical system component updates, service packs, security fixes, patches and free upgrades to selected Windows components."); see also *SOFTWARE UPDATE*, WIKIPEDIA, [http://en.wikipedia.org/w/index.php?title=Software\\_Update&oldid=34558660](http://en.wikipedia.org/w/index.php?title=Software_Update&oldid=34558660) (last visited Sept. 8, 2006).

140. See Larry Rogers, *The Goal of Computer Security or What's Yours is Yours Until You Say Otherwise!*, [http://www.cert.org/archive/pdf/homeusers/goal\\_of\\_computersecurity.pdf](http://www.cert.org/archive/pdf/homeusers/goal_of_computersecurity.pdf) (last visited Jan. 15, 2006); see also *COMPUTER INSECURITY*, *supra* note 137; U.S. Computer Emergency Readiness Team, *Technical Cyber Security Alerts*, <http://www.us-cert.gov/cas/techalerts/> (last visited Jan. 15, 2006). The author has inspected log files on countless computers, and in his experience, virtually all machines that are not secured behind a firewall are being constantly probed for vulnerabilities.
141. See *MALWARE*, WIKIPEDIA, <http://en.wikipedia.org/w/index.php?title=Malware&oldid=35226112> (last visited Sept. 8, 2006).
142. Researchers at the University of Washington measured a decline in "spyware" on the Internet between May and October 2005 and attributed this decline in part to the increased availability of automatic patch installation tools such as Windows Update. UW Study, *supra* note 13, at 13. R
143. See *COMPUTER INSECURITY*, *supra* note 140 ("Severe financial damage has been caused by computer security breaches, but estimating reliable costs is quite difficult. Figures in the billions of dollars have been quoted in relation to the damage caused by malware such as computer worms like the Code Red worm, but such estimates may be exaggerated."). R

---

security updates or patches to software that was legitimately installed on those computers.<sup>144</sup>

Another category of unconsented-to software installations that does not interfere with a user's reasonable control might be called the "TiVo Exception" and again involves automatic updates. The need for this exception was pointed out at the FTC Spyware Workshop: "So for example, you know, I'll give you my personal experience. I have Tevo [sic]. I get regular updates from Tevo [sic]. I don't consent to those every time they happen, but they're very important to me."<sup>145</sup> In this case, the underlying rationale is not security but a recognition that users have a limited expectation of control over certain types of special-purpose, subscription-based computing services like TiVo.<sup>146</sup> This exception might also apply to updates sent out to such special-purpose, subscription-based computing devices as cell phones, music players, set-top boxes,<sup>147</sup> gaming consoles, or other types of internet appliances.<sup>148</sup>

At this point, we have defined "software," "adequate authorization," and have set out the basic definition of "harm." Limited to the pieces discussed thus far, however, the definition is still too overreaching. For example, a

---

144. Many software distributors currently solicit explicit consent before installing security updates, and it is expected that that general practice will continue. However, it is also generally possible to adjust one's preferences so that updates are installed automatically, without explicit and specific consent. The latter practice shields software distributors.

145. FED. TRADE COMM'S, *supra* note 1, at 37 (comments of Mark Bohannon, General Counsel and Senior Vice President for Public Policy at the Software and Information Industry Association).

146. It is also the case that the use of such subscription-based computing services will almost invariably involve the formation of some kind of contractual relationship between the user and the entity sending the software updates. Why not rely on that contractual relationship to legitimize software updates to TiVos? That is a good question. The answer can be found in the brief discussion of internet contracts doctrine. *See supra* Part V.B. My belief is that contracts doctrine is too permissive to provide an effective means of controlling abusive software, so we should not rely on that doctrine to create exceptions to the definition being discussed here. *See id.*

147. The term set-top box describes a device that connects to a television and some external source of signal, and turns the signal into content that is displayed on the screen. The signal source might be a satellite dish, a coaxial cable, a telephone line, or even an ordinary VHF or UHF antenna. SET-TOP BOX, WIKIPEDIA, [http://en.wikipedia.org/w/index.php?title=Set-top\\_box&oldid=38850364](http://en.wikipedia.org/w/index.php?title=Set-top_box&oldid=38850364) (last visited Sept. 8, 2006).

148. *See generally* MSN TV, WIKIPEDIA, [http://en.wikipedia.org/w/index.php?title=MSN\\_TV&oldid=35211624](http://en.wikipedia.org/w/index.php?title=MSN_TV&oldid=35211624) (last visited Sept. 8, 2006); WEB TV, WIKIPEDIA, [http://en.wikipedia.org/w/index.php?title=Web\\_tv&oldid=16070760](http://en.wikipedia.org/w/index.php?title=Web_tv&oldid=16070760) (last visited Sept. 8, 2006); INFORMATION APPLIANCE, WIKIPEDIA, [http://en.wikipedia.org/w/index.php?title=Information\\_appliance&oldid=34873631](http://en.wikipedia.org/w/index.php?title=Information_appliance&oldid=34873631) (last visited Sept. 8, 2006).

---

legitimate web page that runs a JavaScript<sup>TM149</sup> program could fall within the definition as explained so far if it sends pop-up ads to the user while he or she is reading the page. Fortunately, there are several additional qualifications on the harm element built into the definition of abusive software: either the harm must be reasonably unavoidable and ongoing, or it must be reasonably irreversible.

### 1. Reasonably Unavoidable

The “reasonably unavoidable” qualification is intended to function as a safe harbor provision that will encourage developers of spyware-like software to provide an easy way for computer users to put an end to software conduct that they find objectionable. In other words, a program that otherwise causes harm would escape the “abusive software” label as long as it provided an obvious, simple, and effective way for the computer user to return the computer to the state it was in before the unwanted software was installed (or to otherwise regain reasonable control over his or her computer). Note that this qualification does not require software vendors to provide an uninstaller in order to avoid being labeled “abusive”; rather, it provides an incentive to software publishers to provide the consumer with an effective means of control once a program is installed. The means of control will vary from program to program, and providing an uninstaller is only one possible way to ensure that consumers retain control over the software running on their machines. In effect, this provision also creates a duty in computer users to take reasonable steps to mitigate the harm caused by an unwanted program.

One other thing to note is that the “reasonably unavoidable” qualification functions prospectively, not retrospectively. This qualification is not intended to create a loophole that software distributors can use to escape the “spyware” label by asserting that computer users could have avoided installation of the program if the user had not visited Site X, or had not clicked on a particular link, or had not run a particular browser. On the contrary, this qualification merely means that a program is presumptively legitimate if it provides an obvious and effective uninstaller, or provides some other simple method for reasonable computer users to regain control of their systems.

---

149. JavaScript is an embedded scripting language developed by Netscape that has been licensed for use and registered as a trademark by Sun Microsystems, Inc. The syntax of JavaScript is intentionally similar to that of the Java programming language (developed by Sun Microsystems). But aside from that similarity, the two languages are unrelated. Although other uses of JavaScript are becoming common, it is most often used to create dynamic web applications as JavaScript is embedded in virtually all modern web browsers. See JavaScript, <http://www.mozilla.org/js/> (last visited Jan. 15, 2006); JAVASCRIPT, WIKIPEDIA, <http://en.wikipedia.org/w/index.php?title=JavaScript&oldid=35256765> (last visited Sept. 8, 2006). See also Sun Trademarks, <http://www.sun.com/sun-trademarks/#J> (last visited Jan. 15, 2006); WEB APPLICATION, *supra* note 102.

---

## 2. Ongoing

In conjunction with “reasonably unavoidable,” the “ongoing” qualification would act, among other ways, to exempt all client-side software, such as JavaScript, that is executed when you visit a website. In other words, software is presumptively legitimate if users can permanently eradicate the problematic behavior simply by closing a window, easily quitting a program, easily uninstalling a program, or rebooting.<sup>150</sup> As a result, software that only has a transient effect on users’ computers is generally not abusive. However, a program that runs only one time might still be abusive if it causes reasonably irreversible harm.

## 3. Reasonably Irreversible

The “reasonably irreversible” qualification overlaps to a large degree with the “reasonably unavoidable and ongoing” qualification: if a program’s objectionable actions are reversible, then those actions are ongoing merely to the extent that the user chooses not to reverse them. However, this qualification is needed to ensure that a program would be labeled “abusive” even if its objectionable action consisted of a one-time (not ongoing) deletion of a user’s bookmarks or other data files.<sup>151</sup> The argument could be made that the “reasonably irreversible” qualification is not needed in this scenario because the permanent deletion of an important file *does* constitute “ongoing” harm even though the program itself has ceased its objectionable actions. However, this qualification also serves another purpose.

The “reasonably irreversible” qualification also eliminates a potential loophole in the “reasonably unavoidable ongoing” qualification. A software distributor might try to avoid that qualification by arguing that its program was too complicated to be removable, that the changes made to the user’s system were so pervasive that the program’s installation was a one-way street.<sup>152</sup> As a result, the distributor would argue that there was no reasonable way to avoid the ongoing harm. If such an argument prevailed, it would

---

150. Cf. H.R. 29, 109th Cong. § 1(a)(1)(E) (2005) (making it unlawful to “[deliver] advertisements that a user of the computer cannot close without . . . *without turning off the computer or closing all sessions of the Internet browser* for the computer.”) (emphasis added).

151. Arguably, software that serves only malicious purposes, such as destroying data, does not belong in spyware doctrine. Spyware doctrine will almost certainly be of little use against malicious software that is not distributed by a known entity that would respond to legal sanctions. And while it is clear why a company might have a business model that involved sending advertising to computer users, it is much less clear how a business could monetize malicious data destruction. Nonetheless, such malicious software certainly impairs users’ control over their computers and is installed without authorization, and it causes few problems to include such software within spyware doctrine.

152. For example, a software installer on a machine running a version of the Windows operating system might make thousands of changes to the Registry, or it

create a perverse incentive for spyware publishers to create software that avoided the “reasonably unavoidable and ongoing” qualification because it was intentionally too complicated to uninstall. Hence, the “reasonably irreversible” qualification would explicitly eliminate such an argument. A software publisher is still free to create software that is too complex to remove, but the burden of such “uninstallable” software should fall on the publisher, not the consumer. Still, a publisher of “uninstallable” software can avoid being labeled as “abusive” on “reasonably irreversible harm” grounds either by taking care not to cause harm or by taking steps to ensure that the program is only installed with adequate authorization.

## VI. CONCLUSION

How would Sony BMG have fared under the definition of abusive software just proposed?<sup>153</sup> Its software would clearly have fallen within this definition.

First, the DRM software caused harm because it interfered with the computer user’s control not only over the security of the computer,<sup>154</sup> but also over what programs were running.<sup>155</sup> This harm was certainly ongoing,<sup>156</sup> but whether it was reasonably unavoidable is a more difficult question. Sony BMG did eventually provide a means for an affected computer user to uninstall the DRM software.<sup>157</sup> But Sony BMG obfuscated the existence of the uninstaller,<sup>158</sup> rather than providing an “obvious, simple, and effective”

---

might replace numerous critical system files such that it would be extremely difficult to restore the system to the state that it was in before the installation.

153. *Supra* Part III.

154. *See supra* note 46.

155. *See supra* note 43.

156. *See supra* note 44.

157. *See supra* note 57.

158. *See id.* The uninstaller was not included on the CD that installed the DRM software, which would have been the simplest place to put the uninstaller if Sony BMG had been serious about giving users an easy way to undo the harm. Rather, users must “go to Sony’s support [web] site [and] guess that the uninstall information is in the FAQ.” You don’t really want to uninstall, *supra* note 43. Furthermore, Sony made the uninstaller available via this route only after a great public outcry and after considerable damage had already been done. *See id.* Now, the mere fact that the uninstaller was on Sony’s web site does not make the DRM software *reasonably unavoidable*. Much abusive software is downloaded from the web in the first place, and the natural spot to put an easily accessible uninstaller would be “near” where the installer was. Therefore, in most cases, putting an uninstaller on the web would be a good thing to do, so long as the existence of the uninstaller was reasonably apparent to the computer user. However in this case, a computer would not necessarily even be connected to the Internet when it got infected with the Sony BMG software and

R  
R  
R  
R

R

means to remove the DRM software.<sup>159</sup> Therefore, the DRM software fails to meet the reasonably unavoidable element. As a result, Sony BMG was required to seek adequate authorization for the installation, and it failed to do so. The standard for adequate authorization is “clear . . . notice that installation of the software would have a material negative impact on the . . . use of [the] computer.”<sup>160</sup> Instead of providing such notice, Sony BMG presented the user with a 3000-word license that mislead users in at least two ways: it implied that the software was more easily removable than was really the case, and it failed to disclose that the software had any negative security implications.<sup>161</sup> For these reasons, the Sony BMG DRM software is “abusive” under the definition proposed in this comment. Without claiming that the mere existence of this definition would have averted the Sony BMG fiasco, this definition does have the potential to be a useful tool in the fight against abusive software.

Given the recent spate of state spyware legislation<sup>162</sup> and the several bills currently pending in Congress,<sup>163</sup> it seems inevitable that Congress will enact the first specific federal “spyware” statute in the next few years. Even if the statute adopted the definition set out in this comment, it is unlikely the problem of unwanted, harmful software would be magically eradicated. But given the vast room for improvement in the current abusive software landscape, intelligent government regulation could be of great benefit. Yet this outcome is not a foregone conclusion.<sup>164</sup> Only one outcome is certain; no matter how the regulation of abusive software is implemented, there will always be unscrupulous individuals and corporations willing to flirt with the

---

nothing about the existence of an uninstaller was made readily apparent to the user at the time of installation.

159. See discussion *supra* Part V.C. 1.

160. *Supra* Part V.B.

161. See discussion *supra* Part III, notes 51–53.

R

162. See Edelman, *supra* note 18.

R

163. See Edelman2, *supra* note 18 (Safeguard Against Privacy Invasions Act, H.R. 29, 109th Cong. (passed House, May 23, 2005); Internet Spyware (I-SPY) Prevention Act, H.R. 744, 109th Cong. (passed House, May 23, 2005); Software Principles Yielding Better Levels of Consumer Knowledge (SPYBLOCK), S. 687, 109th Cong. (passed committee, November 2005); Computer Software Privacy and Control Act, H.R. 4255, 109th Cong. (introduced, April 2004); Enhanced Consumer Protection Against Spyware Act, S. 1004, 109th Cong. (introduced, May 2005)).

R

164. See Evers, *supra* note 135 (quoting Jonathan Frenkel, director of law enforcement policy at the U.S Department of Homeland Security) (“Legislation or regulation may not be a solution in all cases, but it may be warranted in appropriate circumstances.”).

R

---

edge of legitimacy, or flout the regulations altogether.<sup>165</sup> Therefore, some commentators have argued that just as the CAN-SPAM Act of 2003<sup>166</sup> has had little, if any, effect on the prevalence of unsolicited commercial email (i.e., spam),<sup>167</sup> regulation of abusive software would be similarly ineffective and, in fact, might make the problem worse.<sup>168</sup> They argue that a technical solution is the only effective approach to controlling the technical problem of abusive software.<sup>169</sup> Although this argument certainly has merit, government regulation could play an important role.

Well-crafted legislation using the principles set out in this comment would have a definite positive effect on abusive practices by several targeted-advertising vendors. At the time of this writing, the reality of abusive software is that many major corporations view spyware-driven pop-up advertising as “just a marketing tool.”<sup>170</sup> Several major players in the online marketing industry are responsible for the installation of millions of copies of unwanted software on consumers’ computers<sup>171</sup> and have been targets of nu-

- 
165. See Crawford, *supra* note 28, at 1462 (“Real spyware—the truly harmful kind, not the broadly defined kind—comes from people who are completely dedicated to breaking the law.”). R
166. Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act), 15 U.S.C. §§ 7701-7703 (2003).
167. See Crawford, *supra* note 28, at 1461 (“Unsolicited e-mail on the Internet has actually increased since the passage of CAN-SPAM, and now amounts to 80 percent or more of all e-mail sent, up from 60 percent during the period before the law went into effect.”). R
168. See *generally id.* (discussing Ms. Crawford’s concern that sloppily-crafted legislation would not only create loopholes that would effectively legitimize certain forms of spyware, but would also stifle innovation on the Internet by mandating or prohibiting certain technical practices).
169. See *id.* at 1468-74 (advocating technical “immunity networks” as a method to control spyware).
170. See MSNBC, *Major Advertisers Caught in Spyware Net*, <http://www.msnbc.msn.com/id/8349690/> (last visited Jan. 15, 2006).
171. See, e.g., PC Pitstop, *WhenU Awareness, One Year Later*, <http://www.pcpitstop.com/spycheck/whenu2.asp> (last visited Jan. 15, 2006) (“[P]eople are uninstalling [WhenU software] at a faster rate than WhenU or its partners can convince, trick, or deceive people into installing it.”); PC Pitstop, *Gator Information Center*, <http://www.pcpitstop.com/gator/> (last visited Jan. 15, 2006) (“Gator’s marketing power lets them put ad-delivery software onto systems with high efficiency, using techniques such as drive-by downloads. Gator claims more than 35 million people currently have GAIN on their systems. If our survey results hold for the general population of Gator users, only a small minority of them consciously agreed to installing Gator’s software and accepted its terms.”); Ben Edelman, *Advertisers Using WhenU*, <http://www.benedelman.org/spyware/whenu-advertisers/> (last visited Sept. 7, 2006) (noting that WhenU’s largest advertisers include Priceline, J.P Morgan Chase, and Ver-

merous lawsuits stemming from their questionable software installation methods.<sup>172</sup> In other words, the current abusive software problem has been fueled in part by the advertising budgets of scores of otherwise reputable, legitimate businesses.<sup>173</sup> And in response to anti-abusive software legislation, mainstream U.S. companies that disseminate much of the problematic spyware at the time of this writing (such as Claria, WhenU, 180solutions, et al.) would most likely change their more abusive practices rather than face repeated civil sanctions.<sup>174</sup> Yet, it may come to pass that after the current major U.S. spyware vendors change their practices, small, underground, virtually judgment-proof organizations will step into the gap, as has happened with spam vendors after the CAN-SPAM Act of 2003.<sup>175</sup> Still, deceptive software installation methods deserve to be driven underground, where they would no longer be viewed as legitimate marketing tools.

Furthermore, well-crafted, effective anti-abusive software legislation would clarify that legitimate businesses have no right sneaking software onto consumers' computers.<sup>176</sup> The Sony BMG DRM fiasco in late 2005 is a good case-in-point. It illustrates the cavalier attitude even large, mainstream corporations can have about the importance of ensuring that consumers retain control over their computers.<sup>177</sup> As this comment explained,<sup>178</sup> the surreptitious installation of cloaked software presents an unacceptable potential security

---

izon); Ben Edelman, *How Yahoo Funds Spyware*, Aug. 31, 2005, <http://www.benedelman.org/news/083105-1.html> (showing "Yahoo ads [support] Claria, eXact Advertising, Direct Revenue, 180solutions, and various others").

172. See Edelman2, *supra* note 18.

173. See, e.g., MSNBC, *supra* note 170 (noting that many mainstream companies have purchased ads to be delivered via spyware including J.C. Penney, Capital One Financial, Sprint, Sony, Mercedes-Benz, Expedia, Orbitz, et al.). R

174. Researchers at the University of Washington measured a decline in "spyware" on the Internet between May and October 2005 and attributed this decline in part to civil lawsuits against spyware distributors. UW Study, *supra* note 13, at 13. R

175. See Dan Ilett, *U.S. Leads the Dirty Dozen Spammers*, Dec. 24, 2004, [http://news.com.com/U.S.+leads+the+dirty+dozen+spammers/2100-7349\\_3-5503344.html](http://news.com.com/U.S.+leads+the+dirty+dozen+spammers/2100-7349_3-5503344.html) ("...many spammers are using hacked PCs with broadband connections to send out their spam.").

176. See Evers, *supra* note 135 (quoting Jonathan Frenkel, director of law enforcement policy at the U.S Department of Homeland Security) ("Companies now know that they should not surreptitiously install a rootkit on computers."). R

177. See Posted by Robert Mungo on Malbela.com, <http://www.malbela.com/blog/archives/000375.html> (Nov. 20, 2005, 2:57 a.m.) (quoting RIAA President Cary Sherman, approving of Sony-BMG's use of technology to protect its Intellectual Property, and noting that the only problem with the Sony-BMG DRM software was that it happened to contain a security vulnerability).

178. *Supra* Part III.

---

risk whether that risk is realized or not. Effective legislation would codify the notion that consumers' interests in retaining control over their computers and in remaining free from unwanted or hidden software are interests that corporations cannot trample on, even to protect intellectual property rights.<sup>179</sup>

As is the case with anti-spam measures, spyware controls will probably end up being a combination of desktop technical protections (anti-spyware software), industry self-regulation (published best-practices such as the ASC definition, or some sort of privately-run "Spyware-free" certification program<sup>180</sup>), government regulation (by the FTC), and litigation (under existing consumer-protection laws and a likely federal statute). But as all of these measures develop in the coming years, it will be important to bear in mind the principles outlined in this comment in order to assure adequate consumer protection from abusive software without hindering true innovation or the development of legitimate business models.

---

179. See Posted by Brian Krebs on washingtonpost.com, [http://blog.washingtonpost.com/securityfix/2005/11/dhs\\_official\\_weighs\\_in\\_on\\_sony.html](http://blog.washingtonpost.com/securityfix/2005/11/dhs_official_weighs_in_on_sony.html) (Nov. 11, 2005, 1:30 p.m. EST) (quoting Stewart Baker, the Department of Homeland Security assistant secretary for policy) ("It's very important to remember that it's your intellectual property—it's not your computer. And in the pursuit of protection of intellectual property, it's important not to defeat or undermine the security measures that people need to adopt in these days.").

180. For example, something along the lines of the TRUSTe® independent privacy certification program used by many Internet retailers. See TRUSTe, <http://www.truste.org/> (last visited January 29, 2006) ("TRUSTe® is an independent, nonprofit enabling trust based on privacy for personal information on the internet. We certify and monitor web site privacy and email policies, monitor practices, and resolve thousands of consumer privacy problems every year.").

