Before the
Federal Trade Commission
Washington, DC 20580

In the Matter of	)
	)
	)
Awarenesstech.com,	)
RemotePCSpy.com,	)
Covert-Spy.com,	)
RemoteSpy.com, and	)
Spy-guide.net.	)
----------	)

Complaint, Request for Investigation, Injunction, and Other Relief

I. Introduction

1. This complaint details practices within the amateur spyware industry which cause consumer harm and are unfair and deceptive trade practices. Amateur spyware technologies are surveillance products sold to individual consumers to spy on other individuals. Amateur spyware technologies are variously promoted as being capable of spying on email and instant message exchanges; recording websites visited; capturing passwords and logins; browsing of local filesystems; capturing screenshots; and capturing all keystrokes typed. Some of these features are available in real-time.

2. The Electronic Privacy Information Center (EPIC) has identified several practices that constitute unfair or deceptive trade practices in the marketing of amateur spyware. Several purveyors of amateur spyware technologies promote illegal surveillance practices. See 18 U.S.C. § 2510 *et seq.* Secondly, purveyors of spyware technology promote practices that violate computer crimes laws, such as the ability to "remotely deploy" the software using a form of a Trojan horse attack. See 18 U.S.C. § 1030. Finally, the several purveyors of amateur spyware technologies fail to warn users of the dangers of improper use of their services.

3. These practices harm the purchasers of the product, who are exposed to criminal and civil liability. They further harm the victims of this surveillance. The victims face privacy violations; are exposed to identity theft; are placed in physical danger; may not find help from law enforcement authorities; and may not find adequate compensation via the civil legal system.

4. In this complaint EPIC details the practices of a select few US-based operators in the market. Internet searches reveal many other participants in this market. EPIC believes many operators are tied together in affiliate relationships, as some of these

operators offer similarly named products and affiliate marketing opportunities.[1]

5. EPIC requests that the Commission investigate the companies named herein, determine the extent of threat to consumer privacy and safety, seek appropriate injunctive and compensatory relief, and further investigate other operators and practices in this market.

II. Parties

6. The Electronic Privacy Information Center (EPIC) is a not for profit research center based in Washington DC. Founded in 1994, EPIC focuses on the protection of privacy and the First Amendment. Among its other activities, EPIC first brought the Commission's attention to the privacy risks of online advertising.[2] EPIC also initiated the complaint to the FTC regarding Microsoft Passport.[3] The Commission subsequently required Microsoft to implement a comprehensive information security program for Passport and similar services.[4]

7. Awareness Technologies sells the "webwatcher" software via its website at http://www.awarenesstech.com. They list their address as 4640 Admiralty Way, Suite 1140, Los Angeles, CA 90292.[5] Their domain name is registered to a proxy DomainsByProxy.com, 15111 N. Hayden Rd., Ste 160, PMB 353, Scottsdale, AZ 85260. Their IP address is 72.32.135.176, and belongs to Rackspace.com, 9725 Datapoint Dr. Suite 100, San Antonio TX, 78229.

8. RemotePCSpy.com sells the "RealtimeSpy" software via its website at http://www.remotepcspy.com. The domain name is registered to Stephen Morrow, 438 32nd st, NW, Canton OH, 44709. The website is hosted at the IP address 216.246.48.197. That IP address is owned by Server Central Network, 209 W. Jackson Blvd, Suite 700, Chicago, IL 60606.

9. Covert-Spy.com sells the "RemoteSpy" software via its website at http://www.covert-spy.com. The domain name is registered to Total Innovations, Inc., PO Box 279, Jensen Beach, FL 34958-0279. The website is hosted at IP address

---

[1] *See e.g.,* Spytech Affiliate Program, http://www.spytechaffiliates.com/ (last visited Feb. 25, 2008).
[2] *In the Matter of DoubleClick*, Complaint and Request for Injunction, Request for Investigation and for Other relief, before the Federal Trade Commission (Feb. 10, 2000) *available at* http://epic.org/privacy/internet/ftc/DCLK_complaint.pdf.
[3] *In the Matter of Microsoft Corporation,* Complaint and Request for Injunction, Request for Investigation and for Other Relief (July 26,2001), http://epic.org/privacy/consumer/MS_complaint.pdf.
[4] *In the Matter of Microsoft Corporation*, File No. 012 3240, Docket No. C-4069 (Aug. 2002), available at http://www.ftc.gov/os/caselist/0123240/0123240.shtm. *See also*, Fed. Trade Comm'n, "Microsoft Settles FTC Charges Alleging False Security and Privacy Promises" (Aug. 2002) ("The proposed consent order prohibits any misrepresentation of information practices in connection with Passport and other similar services. It also requires Microsoft to implement and maintain a comprehensive information security program. In addition, Microsoft must have its security program certified as meeting or exceeding the standards in the consent order by an independent professional every two years."), *available at* http://www.ftc.gov/opa/2002/08/microsoft.shtm.
[5] Webwatcher Contact Us -- Computer Monitoring, http://www.awarenesstech.com/Consumer/ContactUs.html (last visited Feb. 25, 2008).

216.117.138.187, which is owned by Advanced Internet Technologies, Inc., 421 Mainden Ln, Fayetville, NC 28301.

10. RemoteSpy.com sells the "RemoteSpy" software via its website at http://www.remotespy.com. According to their website, remotespy.com is a division of CyberSpy Software LLC.[6] The domain name is registered to Cyberspy Software, LLC, 1512 E. Jefferson St, Orlando FL 32801. The website is hosted at IP address 69.20.16.139, which is owned by Rackspace.com 9725 Datapoint Dr., Suite 100, San Antonio, TX 78229.

11. Spy-guide.net sells several personal surveillance products from its website at http://www.spy-guide.net. The domain name is registered to Gifts for Geeks, 680 Spout Spring Rd., Lawrenceburg, TN 38464. The website is hosted at the IP address 209.51.155.186, which is owned by Global Net Access, LLC, 1100 White st, SW, Atlanta, GA 30310.

III. Statement of Facts

12. The following facts are the result of EPIC investigation of the complained companies. We describe the companies' representation of their products, including suggested uses and technical abilities. We note three main practices: the promotion of illegal surveillance targets; the promotion of Trojan horse email attacks; and the failure to adequately warn consumers of the dangers of using these products.

Awareness Technologies

13. Awareness Technologies markets the "Webwatcher" software via their website at awarenesstech.com. The marketing promotes illegal surveillance and fails to adequately warn consumers of the dangers of misusing the product.

14. The webwatcher software is, in headline form, touted as being able to "Record everything that happens on any computer and see it online from anywhere."[7] This company repeats the statement on several of its webpages.[8] We include below a screenshot from their homepage:[9]

[6] Remote Spy -- About Remote Spy Software, LLC, http://www.remotespy.com/aboutus.php (last visited Feb. 25, 2008).
[7] http://www.awarenesstech.com/ (last visited Feb. 25, 2008).
[8] http://www.awarenesstech.com/Parental/, http://www.awarenesstech.com/Cheating/, http://www.awarenesstech.com/Consumer (last visited Feb. 25, 2008).
[9] http://www.awarenesstech.com/ (last visited Feb. 25, 2008).

15. The ability of the software to "steal passwords," as well as its characterization as "spy software," is described under the headline "CONSUMER." Awareness Technologies states that:

> WebWatcher's computer monitoring software redefines computer spy software. Read emails, monitor IMs, take screenshots, monitor or block web sites, and even steal passwords: WebWatcher is spy software that can help you do it all.[10]

A screenshot is reproduced below:[11]

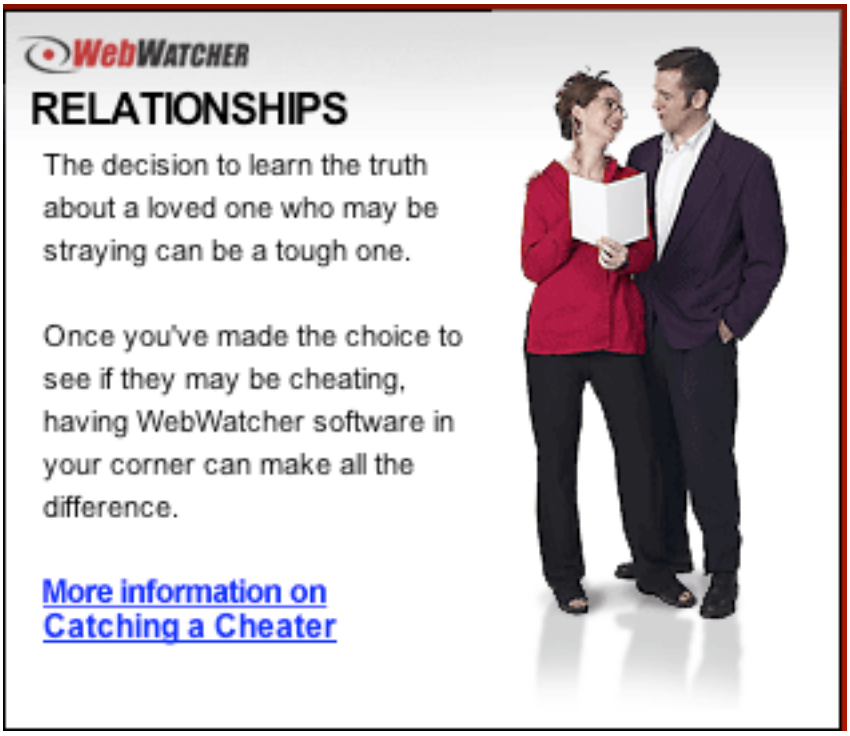
[10] http://www.awarenesstech.com/ (last visited Feb. 25, 2008).
[11] *Id.*

16. Under "RELATIONSHIPS," Awareness Technologies states that its product is capable of secretly obtaining information on "loved ones":

> The decision to learn the truth about a loved one who may be straying can be a tough one. Once you've made the choice to see if they may be cheating, having WebWatcher in your corner can make all the difference.[12]

A screenshot is reproduced below:[13]

[12] *Id.*
[13] *Id.*



17. Awareness Technologies describes several other functions of the product on its website. In the section devoted to "consumers," Awareness Technologies claims it can "get the truth about **anyone**" [emphasis added]. [14] A screenshot demonstrates the other abilities:[15]

[14] http://www.awarenesstech.com/Consumer (last visited Feb. 25, 2008).
[15] *Id.*

18. Nowhere on the awarenesstech.com website did EPIC find a disclaimer that warned users of the legal consequences of illegal surveillance.

RemotePCSpy.com

19. RemotePCSpy markets the "industry leading remote spy software" known as RealtimeSpy.[16] RemotePCSpy promotes illegal surveillance targets; advertises Trojan horse attacks as a legitimate means of installation; and fails to adequately warn users of the dangers of illegally using the product.

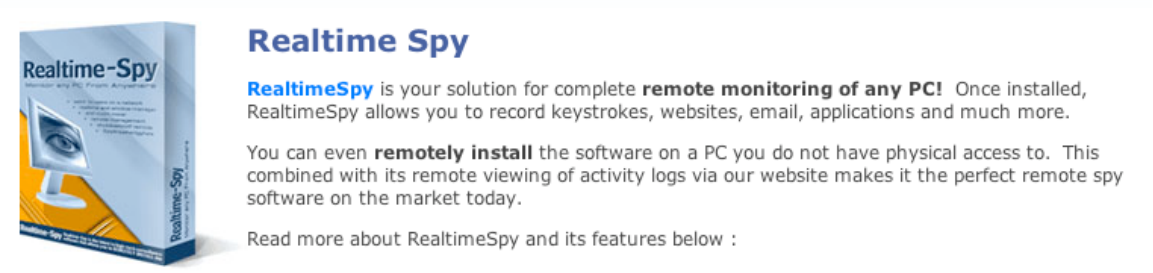
20. RemotePCSpy states that Realtime Spy is suitable for accessing any personal computer:

> Combined with remote install and remote viewing of activity logs right from our website, you now have the power to monitor ANY PC from ANYWHERE in the world![17]

21. Clicking on a link entitled "Learn More" takes the user to a further description of the product. RemotePCSpy claims that the product can be remotely installed, that this feature makes it the "perfect remote spy software.":

> You can even **remotely install** the software on a PC you do not have physical access to. This combined with its remote viewing of activity logs via our website makes it the perfect remote spy software on the market today.[18]

A screenshot is provided below, scaled to fit this paper:[19]



22. The spying victim is not made aware of this surveillance, and is fooled by the "remote install" Trojan horse feature into installing the surveillance. The "remote install" Trojan, and the experience of the surveillance victim, are described by the RemotePCSpy website: [20]

> Advanced Stealth and Cloaking

[16] http://www.remotepcspy.com/ (last visited Feb. 25, 2008).
[17] *Id.*
[18] http://www.remotepcspy.com/remotespy.htm (last visited Feb. 25, 2008).
[19] *Id.*
[20] *Id.*

> Realtime-Spy runs in **COMPLETE STEALTH** and **cloaks itself** to hide from the remote user! The file you send to the remote user is able to be discarded and deleted - without affecting Realtime-Spy's monitoring process! Realtime-Spy is also invisible in the Windows task manager on all Windows platforms!
>
> . . . .
>
> Email Deployment
> simply send your configured Realtime-Spy module to the remote PC. The user only has to run the attached file - they do not have to respond or send you any response to start monitoring - and they will not know they are being monitored! (optional splash notice available for non-stealth remote installs)

23. At the bottom of the RemotePCSpy homepage, there is a link to a "User Agreement." Leaving the homepage, one arrives at the User Agreement. The User Agreement includes text that contradicts and limits the more prominent claims of the software's ability to spy on any remote PC without the user's knowledge:[21]

> 1. Before choosing RealtimeSpy you must first acknowledge and agree to the fact that you are the owner of the remote PC you wish to install the software on. It is a federal and state offense to install monitoring/surveillance software on a PC of which you do not own. (emphasis added)
>
> 2. If you are NOT the owner of the computer you want to monitor you must have the expressed consent of the owner of that computer to install RealtimeSpy on it.

Covert-Spy

24. Covert-Spy sells the "RemoteSpy" software via its website at http://www.covert-spy.com. Covert-Spy engages in all three of the practices EPIC has identified: The promotion of illegal surveillance targets; the promotion of "remote install" via a Trojan horse attack; and the failure to adequately warn consumers of the risks of using this software illegally.

25. The RemoteSpy software is touted, via a banner, as being "100% undetectable."[22] Just below that is promoted the ability to "SPY ON ANYONE. FROM ANYWHERE"[23] A screenshot is provided:[24]

[21] http://www.remotepcspy.com/agreement.htm (last visited Feb. 25, 2008).
[22] http://covert-spy.com/ (last visited Feb. 25, 2008).
[23] *Id.*
[24] *Id.*

26. Covert-spy follows up this ability to "spy on anyone" with further statements describing possible targets for surveillance, including a "spouse" or a "friend."

> Do you need to find out what someone is doing online? Is your spouse, child, or friend hiding secrets from you? If so Remote-Spy is the perfect solution for anyone that needs this information quickly and secretly. Now you can use the same software professionals use to find out the information you need in total privacy.[25]

Covert-Spy provides a list of potential targets to "secretly record," including "husband", "wife", "friend", "lover" and "anyone else."[26] A screenshot is provided:

27. The "remote deployment" is achieved by creating an email Trojan horse which secretly installs on the victim's machine:

> Remotely Deployable - The most notable feature about Remote-Spy - it can be sent remotely via email secretly. Once the Remote-Spy file (you create) is executed on a computer, it will continuously record log data on the computer you are monitoring.[27]

The remote Trojan is created by the following a "wizard" provided by the RemoteSpy software:

---

[25] *Id.*
[26] *Id.*
[27] http://covert-spy.com/ (last visited Feb. 25, 2008).

> .EXE Module Creation - Configure your deployable Remote-Spy module easily by using the quick module configuration wizard given to you upon ordering.[28]

The experience of the victim of the Trojan horse is described in the "Frequently Asked Questions" portion of the website:

> [Question]: What happens when a user clicks on the monitoring .exe?
> Remote-Spy is completely stealth and designed to install without warning. Once the executable is clicked the monitoring application will be started instantly. There are no signs or warnings whatsoever.[29]

28. No statements were found on Covert-spy.com's website that served to limit, qualify, or warn about the surveillance of other individuals or the use of the "remote deploy" Trojan horse attack.

Remotespy.com

29. RemoteSpy.com sells the "Remote Spy" software.[30] Remotespy.com promotes illegal surveillance targets; promotes the use of a Trojan horse email attack; and fails to adequately warn users of the dangers of using this software.

30. Remotespy.com advertises that it is capable of spying on "anyone," "secretly and covertly" and "without the need of physical access."[31] A screenshot is provided:[32]

31. Clicking on "features" sends one to a page with more information concerning the features and ability of the software. RemoteSpy describes the ability to "remotely install", to "deploy with one click via email" and to monitor "ANY PC."[33] A screenshot is provided:

---

[28] *Id.*
[29] *Id.*
[30] http://www.remotespy.com/ (last visited Feb. 25, 2008).
[31] *Id.*
[32] *Id.*
[33] http://www.remotespy.com/features.php (last visited Feb. 25, 2008).

32. The "remote install" is accomplished by facilitating the purchaser's creation of a Trojan horse email. This is then sent to the victim who unknowingly executes it. The process is described on the remotespy.com page:[34]

> * Remotely Deployable - The most notable feature about RemoteSpy - it can be sent remotely via email secretly. Once the RemoteSpy file (you create) is executed on a computer, it will continuously record log data on the computer you are monitoring secretly. You can login anytime to your RemoteSpy account to view the recorded data in real-time!

The victim of the spyware is not made aware of the surveillance. Their experience is described in an FAQ:[35]

> [Question]: What happens when a user clicks on the monitoring .exe?
>
> RemoteSpy is completely stealth and designed to install without warning. Once the executable is clicked the monitoring application will be started instantly. There are no signs or warnings whatsoever.

33. Navigating several clicks to the end of the tutorial provides a legal disclaimer. From the homepage, clicking "support,"[36] then "Online User Tutorial,"[37] past the first page of the tutorial,[38] RemoteSpy presents a "final end user notice" at the bottom of the second page of the tutorial.[39] This notice begins by warning that the recipient of the Trojan horse email must execute the attachment for monitoring to work. [40] The notice further mentions that some users may block executables from their emails, and advises

[34] http://www.remotespy.com/features2.php (last visited Feb. 25, 2008).
[35] http://www.remotespy.com/faq.php (last visited Feb. 25, 2008).
[36] http://www.remotespy.com/ (last visited Feb. 25, 2008).
[37] http://www.remotespy.com/helpdesk/ (last visited Feb. 25, 2008).
[38] http://www.remotespy.com/tutorial.php (last visited Feb. 25, 2008).
[39] http://www.remotespy.com/tutorial-2.php (last visited Feb. 25, 2008).
[40] *Id.*

that this be avoided by placing the file in an MS-WORD document or zip compression.[41] After these technical work-arounds to the victim's filtering are presented, remotespy.com delivers its legal disclaimer:

> Legal Notice: The execution of RemoteSpy on a computer you do not have rights of ownership too is illegal. Sending the application to a PC to maliciously record data without the owners consent is illegal. RemoteSpy will not take responsibility for actions taken after your purchase. You must abide by all state and federal laws while using the RemoteSpy monitoring software.[42] (emphasis added)

Spy-Guide.net

34. Spy-guide.net advertises several amateur spyware products on its website.[43] The home page touts the "iSpyNow Remote Computer Monitoring Software." The software includes a "remote install" Trojan horse, and no messages disclaim or warn consumers of the dangers of illegal uses.

35. Spy-Guide promotes the ability of iSpyNow to record the activity of other users besides the installer on a given machine:

> Always Running! - iSpyNOW will startup with EVERY Windows user in active mode, so you will never have blackout monitoring sessions![44]

Those who are not otherwise aware of the installation on the machine are not made aware by the program's operation:

> Undetectable! - iSpyNOW keylogger software uses the latest in stealth recording technology - no one will know it is running![45]

However, given the "remote install" feature, it may be the case that none of the actual users of the machine are aware of its presence.

36. iSpyNow includes a "remote deployment" feature. The Spy-Guide website explains:[46]

> E-Mail Deployment - Simply send iSpyNOW keylogger software as an email attachment to the workstation or PC you wish to monitor remotely in real time, and the program will install immediately! iSpyNOW keylogger software is the only program capable of doing this!

This description implies that the iSpyNow software installs without *any* activity from the users of the target computer.

---

[41] *Id.*
[42] *Id.*
[43] http://www.spy-guide.net/ (last visited Feb. 25, 2008).
[44] http://www.spy-guide.net/ispynow-spy-software.htm (last visited Feb. 25, 2008).
[45] *Id.*
[46] *Id.*

37. Nowhere in the spy-guide.net website are users warned of laws or regulations protecting the privacy of computer users, or the legal risks one faces when monitoring others without their knowledge or consent.

IV. Legal Analysis

38. These providers of amateur spyware are engaging in unfair and deceptive trade practices. Several amateur spyware providers promote illegitimate surveillance activity. This harms the purchaser who is exposed to civil and criminal liability. This also harms the target of the surveillance because their privacy is violated. Secondly, several providers of amateur spyware also promote Trojan horse email attacks that facilitate the spyer's ability to target another individual, and thus increases the likelihood of harm to the victim. Finally, several amateur spyware providers fail to adequately warn the public of the risks of using their products.

The FTC's Unfairness and Deception Authority

39. The FTC Act declares unlawful unfair or deceptive acts or practices, and empowers the FTC to enforce this prohibition.[47] These powers are described in FTC Policy Statements on Deception and Unfairness, respectively.

40. A trade practice is unfair if it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[48]

41. The injury must be "substantial."[49] Typically, this involves monetary harm, but may also include "unwarranted health and safety risks."[50] Emotional harm and other "more subjective types of harm" generally do not make a practice unfair.[51] Secondly, the injury "must not be outweighed by any offsetting consumer or competitive benefits that the sales practice also produces."[52] Thus the FTC will not find a practice unfair "unless it is injurious in its net effects."[53] Finally, "the injury must be one which consumers could not reasonably have avoided."[54] This factor is an effort to ensure that consumer-decision making still governs the market by limiting the FTC to act in situations where seller behavior "unreasonably creates or takes advantage of an obstacle to the free exercise of consumer decisionmaking."[55] Sellers may not withhold from consumers important price or performance information, engage in coercion, or unduly influence

[47] 15 U.S.C. § 45.
[48] *Id.* at § 45(n).
[49] Fed. Trade Comm'n, FTC Policy Statement on Unfairness, (Dec. 17, 1980), *available at* http://www.ftc.gov/bcp/policystmt/ad-unfair.htm [*hereinafter* FTC Unfairness Policy].
[50] *Id.*
[51] *Id.*
[52] *Id.*
[53] *Id.*
[54] *Id.*
[55] *Id.*

highly susceptible classes of consumers.[56]

42. The FTC will also look at "whether the conduct violates public policy as it has been established by statute, common law, industry practice, or otherwise." [57] Public policy is used to "test the validity and strength of the evidence of consumer injury, or, less often, it may be cited for a dispositive legislative or judicial determination that such injury is present." [58]

43. The FTC will make a finding of deception if there has been a "representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment."[59]

44. First, there must be a representation, omission, or practice that is likely to mislead the consumer.[60] The relevant inquiry for this factor is not whether the act or practice actually mislead the consumer, but rather whether it is *likely* to mislead.[61] Second, the act or practice must be considered from the perspective of the reasonable consumer.[62] "The test is whether the consumer's interpretation or reaction is reasonable."[63] The FTC will look at the totality of the act or practice and ask questions such as: "how clear is the representation? how conspicuous is any qualifying information? how important is the omitted information? do other sources for the omitted information exist? how familiar is the public with the product or service?"[64]

45. Finally, the representation, omission, or practice must be material.[65] Essentially, the information must be important to consumers. The relevant question is whether consumers would have chosen another product if the deception had not occurred.[66] Express claims will be presumed material. Materiality is presumed for claims and omissions involving "health, safety, or other areas with which the reasonable consumer would be concerned."[67]

46. The FTC has used its unfairness and deception authority to prosecute spyware purveyors. A recent report outlined 11 different cases brought by the FTC as of October 2007.[68] None of the FTC prosecutions have addressed amateur spyware and the specific harms it causes. The Department of Justice has instituted criminal prosecutions for

---

[56] *Id.*
[57] *Id.*
[58] *Id.*
[59] Fed. Trade Comm'n, FTC Policy Statement on Deception, (Oct. 14, 1983), *available at* http://www.ftc.gov/bcp/policystmt/addecept.htm [hereinafter FTC Deception Policy].
[60] *Id.*
[61] *Id.*
[62] *Id.*
[63] *Id.*
[64] *Id.*
[65] *Id.*
[66] *Id.*
[67] *Id.*
[68] Center for Democracy and Technology, SPYWARE ENFORCEMENT (2007) *available at* http://www.cdt.org/privacy/spyware/20071015SpywareEnforcement.pdf.

amateur spyware.[69] The harms of amateur spyware are within the scope of the unfairness and deception authority, and its purveyors should face FTC action for their unfair and deceptive trade practices.

The Harm of Amateur Spyware

47. The harm from amateur spyware is experienced first by the deployer of the spyware, who is exposed to legal risks by using the software as advertised. The harm is further experienced by the victim of the surveillance. Their privacy is invaded, and this harm is sometimes quantified by statutory remedies. These invasions are often the advertised purpose of amateur spyware. Further, amateur spyware is used in domestic violence and stalking in keeping with representations that the software can "spy on your spouse." Amateur spyware is also used for identity theft.

48. Several federal laws regulate the use and marketing of electronic surveillance software. Federal law prohibits the interception of, and disclosure of illegally intercepted electronic communications.[70] Federal law also prohibits the unauthorized access to stored communications.[71] The Computer Fraud and Abuse Act prohibits the unauthorized access to a protected computer in a way that obtains information.[72] The manufacture, distribution, possession, and advertising of electronic interception devices is also prohibited.[73]

49. The existence of civil remedies may not rectify the damages experienced by surveillance victims. Both users and victims may face high litigation costs. Technology experts begin in the $5,000 to $10,000 range, and it is hard to know the full cost at the onset.[74] Victims may not be able to satisfy judgments and be made whole if these judgments exceed the ability of the intruder to pay.

50. Users and distributors of amateur spyware have been criminally prosecuted. While the purchaser faces the risk of criminal prosecution, the victims may not see final justice because law enforcement may not have the resources to pursue criminal charges. In either situation, there has been a harm. The creator and several customers of the "LoverSpy" software were indicted for federal crimes in 2005.[75] The Loverspy operation had many elements in common with current amateur surveillance software:

> Loverspy was a computer program designed and marketed by Mr. Perez for people to use to spy on others. Prospective purchasers, after paying $89 through a web site in Texas, were electronically redirected to Perez's computers in San

[69] Department of Justice, Creator and Four Users of Loverspy Spyware Program Indicted, Aug. 26, 2005, *available at* http://www.usdoj.gov/criminal/cybercrime/perezIndict.htm. *See also, infra* ¶ 50.
[70] 18 U.S.C. § 2511.
[71] 18 U.S.C. § 2701.
[72] 18 U.S.C. § 1030.
[73] 18 U.S.C. § 2512.
[74] Sharon Nelson & John Simek, *Ghostbusters: "Who You Gonna Call"*, FAMILY ADVOCATE, Winter 2006, at 40.
[75] Department of Justice, *Creator and Four Users of Loverspy Software Indicted* (Aug. 26 2005), http://www.usdoj.gov/criminal/cybercrime/perezIndict.htm.

> Diego, where the "members" area of Loverspy was located. Purchasers would then select from a menu an electronic greeting card to send to up to five different victims or email addresses. The purchaser would draft an email sending the card and use a true or fake email address for the sender. Unbeknownst to the victims, once the email greeting card was opened, Loverspy secretly installed itself on their computer. From that point on, all activities on the computer, including emails sent and received, web sites visited, and passwords entered were intercepted, collected and sent to the purchaser directly or through Mr. Perez's computers in San Diego. Loverspy also gave the purchaser the ability remotely to control the victim's computer, including accessing, changing and deleting files, and turning on web-enabled cameras connected to the victim computers.[76]

51. Two men in Austin were charged under Texas law for installing spyware on the computers of their victims.[77] One was sentenced to four years for spying on his estranged wife with the "SpyRecon" software.[78] Another case is pending against a man that installed the "Eblaster" software on his ex-girlfriend's computer, and used the information gained to access her online dating and other accounts.[79] SpectorSoft, the makers of "Eblaster" have stopped advertising its software for spying on a spouse.[80]

52. Several of the advertisements tout behaviors which rank as medium and high risk factors identified by the Anti-Spyware Coalition.[81] The factors are "behaviors that have potential for user harm and disruption."[82] Factors present in amateur spyware include:

- Installation without user's explicit permission or knowledge.
- Incomplete or inaccurate identifying information.
- Obfuscation with tools that make it difficult to identify.
- Sending communications including email without user permission or knowledge.
- Transmission of personally identifiable data.
- Collection and local storage personal information.
- Intercepts communications, such as email and IM conversations.
- Hiding files, processes, program windows or other information from the user.
- Allowing remote users to alter or access the system.
- Allowing for remote control of the application, beyond self-update.
- Self healing behavior that defends against removal or changes to its

---

[76] *Id.*
[77] Tony Plohetski, *Spying on Lovers Email? Monitoring May Be Illegal*, AUSTIN AMERICAN-STATESMAN, Nov. 13 2007, *available at* http://www.statesman.com/news/content/news/stories/local/11/13/1113spy.html.
[78] *Id.*
[79] *Id.*
[80] Ellen Messmer, *Spouse vs. Spouse,Cyberspying Dangerous, Possibly Illegal,* NETWORK WORLD, Aug. 16, 2007.
[81] Anti-Spyware Coalition, *Anti-Spyware Coalition Risk Model Description*, Nov. 12, 2007, *available at* http://www.antispywarecoalition.org/documents/documents/2007riskmodel.pdf [hereinafter ASC Risk Model].
[82] ASC Risk Model, *supra* note 81, at 3.

components.

Under the Anti-Spyware Coalition Risk Model, these risk factors are mitigated by consent factors.[83] High levels of consent mitigate high risk behavior. Amateur spyware advertising often promotes that the surveilled person will experience a *lack* of these features. A few of these missing consent factors are shown:

- High level of consent before installation, such as registration, activation, or purchase.
- Clear explicit setup experience that users can cancel.
- User opt-out and opt-in of potentially unwanted behaviors.
- Indications of activity, including minor ones such as tray icons and major ones such as an application window or dialog box.

53. Amateur spyware is used in domestic violence and stalking. The harm perpetrated via consumer spyware is not limited to the privacy invasions protected by electronic communications laws. News accounts tell of abusers easily finding and using amateur spyware as part of their abuse:

> It's not hard to figure out. Do-it-yourself manuals are widely available online. Some sites advertise otherwise legitimate programs for stalking uses. For instance, spyware was developed commercially to help parents keep tabs on their children's Web use and to provide information for advertisers. Now it is commonly advertised on Web sites as a way to snoop on a spouse. "Monitor any PC from anywhere!" one ad promises. "Spy stealthily so that the user won't know such monitoring exists," another says.[84]

The article quotes a lawyer describing the pervasiveness of the problem:

> "This happens more frequently than people realize. . . . It's like a virus," said Mehagen McRae, a Fairfax lawyer who said she worked on a spate of such cases in 2005 and 2006. "I tell my clients to act as if the entire world is reading their e-mails and that if they feel as if they are being watched, they are probably right."[85]

Domestic violence experts have noticed that amateur spyware is taking on an increasing role in abuse:

> "We are seeing an increase of GPS devices and installing spyware on victims' computers," [Cindy] Southworth, [director of technology for the National Network to End Domestic Violence] said. "Our recommendation to victims is for them to trust their instincts. Don't use a computer at home if you think your

[83] ASC Risk Model, *supra* note 81, at 8.
[84] Chris L. Jenkins, *Stalkers Go High Tech to Intimidate Victims*, WASHINGTON POST, Apr. 14, 2007, at A1, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2007/04/13/AR2007041302392_pf.html.
[85] *Id.*

> abusive partner is monitoring your actions."[86]

Victims are forced to take precautions, and are limited in the sources of safety they can find:

> The group [National Network to End Domestic Violence] gets many calls from women who say their abusers "know too much. We advise women, if you're researching an escape plan or trying to find a new job, don't do it on your home PC."[87]

The danger comes not only from the presence of the amateur spyware, but also from user's efforts to rid themselves of it:

> Even making seemingly common sense moves such as searching for spyware and erasing it from a home computer can trigger an escalation in violence, advocates say. Such a move could also destroy evidence necessary to bring a criminal prosecution or to obtain a civil protection order.[88]

The Commission has recognized the consumer harm from such a loss of control. Assistant Director of the Bureau of Consumer Protection Tara Flynn states that "[c]onsumers must have control of the software installed on their computers."[89]

54. Amateur spyware is used by identity thieves to capture personal information used in accessing online accounts. A Philadelphia couple used the amateur spyware Spector to access account information on their neighbors.[90] Their fraud was estimated to have cost $100,000 in the year 2007 alone.[91]

55. Though prosecutions have occurred, it can be difficult to get law enforcement help in the case of amateur spyware:

> "When a victim presents herself to law enforcement, it doesn't necessarily look that dangerous," says Sandy Bromley, an attorney with the Stalking Resource Center at the National Center for Victims of Crime in Washington, D.C.

---

[86] Lisa Osburn, *Spyware GPS Become Tools for Domestic Violence*, ST. PAUL PIONEER PRESS, Oct. 25, 2007.
[87] Ellen Messmer, *Spouse vs. Spouse,Cyberspying Dangerous, Possibly Illegal,* NETWORK WORLD, Aug. 16, 2007.
[88] Marie Tessier, *Hi-Tech Stalking Devices Extend Abuser's Reach*, WOMEN'S E-NEWS, Oct. 1, 2006, http://www.womensenews.org/article.cfm/dyn/aid/2905/.
[89] *Spy Tools Raise Child Development, Illegal Use Concerns*, WASHINGTON INTERNET DAILY, Mar. 19, 2007.
[90] David Silverber, *Arrest of Identity Theft's Bonnie and Clyde Opens Debate on Spyware Programs*, DIGITAL JOURNAL, Dec. 5 2007, http://www.digitaljournal.com/article/246998/Arrest_of_Identity_Theft_s_Bonnie_and_Clyde_Opens_Debate_on_Spyware_Programs.
[91] MaryClaire Dale, *Jet-Setters Charged With Identity Theft*, ASSOCIATED PRESS, Dec. 4, 2007, http://ap.google.com/article/ALeqM5gIGiwX_6-n_B-u1ipXyNzVBg1EGQD8TB0DO01.

"Individual incidents alone usually would not be criminal, but when you add them together in a pattern of following, calling and using technology to track a victim, it becomes a type of behavior that is designed to induce fear. And it works."[92]

56. Previous FTC findings on the harms of spyware are applicable to the amateur spyware industry. In its staff report on an FTC Spyware workshop, the staff concludes:

- Spyware, especially keystroke loggers, can create substantial privacy risks.
- Spyware can assert control over computers, and use that control to create security risks and cause other harms.
- Spyware often is more difficult to uninstall than other types of software.[93]

57. Participants in the workshop also pointed to other harms of spyware which are potentially applicable to the amateur spyware market. Removal of spyware can impose a substantial cost on consumers and business, including even the formatting of hard drives, subsequent data loss, and reinstallation of operating systems.[94] Spyware imposes costs on computer manufacturers and ISPs who must respond to technical support calls.[95] Spyware programs can interfere with security tools.[96] Spyware programs can increase security risks -- allowing remote access to the machine in a poor manner may make it easy for hackers to access the machine.[97] Participants also discussed the difficulties that law enforcement has in prosecuting spyware.[98]

58. These harms are clearly against public policy. As described above, Federal and State criminal laws regulate the interception of electronic communications and unauthorized access to computers.[99] Federal and state laws are also concerned with identity theft. The President has created a national identity theft task force.[100] The task force has issued strategic plan for combating identity theft.[101] Stalking, domestic violence and intimate partner abuse are also the targets of evolving state and federal policy.[102] Over the years this policy has increasingly included the protection of the privacy of stalking and domestic violence survivors.[103]

---

[92] Marie Tessier, *Hi-Tech Stalking Devices Extend Abuser's Reach*, WOMEN'S E-NEWS, Oct. 1, 2006, http://www.womensenews.org/article.cfm/dyn/aid/2905/.
[93] Federal Trade Comm'n, Monitoring Software on Your PC: Spyware, Adware. and Other Software, 2 (March 2005), *available at* http://www.ftc.gov/os/2005/03/050307spywarerpt.pdf [hereinafter *FTC Spyware Report*].
[94] *Id*. at 8-9.
[95] *Id*. at 11-12.
[96] *Id*. at 10.
[97] *Id*. at 10-11.
[98] *Id*. at 19.
[99] *Supra*, ¶ 48.
[100] Exec. Order No. 13,402, 3 C.F.R 225 (2006), *available at* http://edocket.access.gpo.gov/cfr_2007/janqtr/3CFR13402.htm.
[101] The President's Identity Theft Task Force, COMBATING IDENTITY THEFT: A STRATEGIC PLAN (2007).
[102] See eg., Violence Against Women and Department of Justice Reauthorization Act of 2005, Pub. L. No. 109-162, 119 Stat. 2960 (2005).
[103] EPIC, *Violence Against Women Act and Privacy*, http://epic.org/privacy/dv/vawa.html.

59. FTC Chair Deborah Platt Majoras has summarized the FTC's view of the consumer harms of spyware:

> Spyware also is a major focus of FTC law enforcement activities to protect consumer privacy in an online environment. Spyware may cause a full range of consumer injury, from keystroke logger software that tracks all of a consumer's online activity, causing a significant risk of identity theft, to adware that forces a consumer to receive a substantial number of unwanted pop-up ads. The FTC has focused significant resources addressing spyware, bringing ten law enforcement actions during the past two years against spyware distributors. These actions have reaffirmed three key principles. First, a consumer's computer belongs to him or her, not the software distributor. Second, buried disclosures about software and its effects are not adequate, just as they have never been adequate in traditional areas of commerce. And third, if a distributor puts an unwanted program on a consumer's computer, he or she must be able to uninstall or disable it.[104]

In the context of pretexting, the Commission has recognized the danger of abusive spouses having access to the personal information of their victims:

> The dangers from pretexting are grave; in one of our cases, Commission staff obtained evidence that in some circumstances, defendants sold such records to abusive spouses who were subject to court orders of protection and who had threatened consumers with physical harm.[105]

Purveyors' Unfair and Deceptive Practices

60. The practice of promoting illegal surveillance targets is unfair because these claims cause a substantial harm, not outweighed by any countervailing benefits, which consumers cannot reasonably avoid. Several of the websites make claims about spying on "anyone" or "any computer." These claims clearly include illegal surveillance targets. Other websites tell of surveillance of a "spouse" or "loved one." These claims also include illegal surveillance targets, as shown by the legal actions for intrafamily surveillance. These advertisements are likely to cause illegal surveillance, and thus likely to cause the harms described above in ¶¶ 47 et seq. The promotion of illegal surveillance practices has few if any countervailing benefits. Consumers may benefit from the fact that the simple advertising promoting spying on "anyone" is easy to understand. This benefit can easily be achieved by simple marketing that does not include illegitimate surveillance targets. The victims of surveillance cannot reasonably avoid this harm, as they are not made aware of the surveillance by the operation of the product.

61. The promotion of illegal surveillance practices is also deceptive. Purchasers are

[104] Deborah Platt Majoras, Chairman, Fed. Trade Comm'n, Building a Culture of privacy and Security, 6 (March 7, 2007) *available at* http://www.ftc.gov/speeches/majoras/070307iapp.pdf.
[105] *Id.* at 8-9.

likely to believe they are purchasing software that can be legitimately used for the purposes advertised. The advertised purposes include spying on "anyone" and a "spouse." These representations are material. Express claims are presumed to be material.[106] Claims are material if they concern safety or the concerns of a reasonable consumer.[107] The exposure to potential criminal and civil liability is of concern to reasonable consumers like health and safety concerns. The purchasers are harmed when they are exposed to civil and criminal liability as detailed above in ¶¶ 47 et seq.

62. The practice of promoting a "remote install" Trojan horse attack is unfair. The described operation of the "remote install" features bears a striking resemblance to descriptions of the Trojan horse computer attacks issued by the Department of Homeland Security's United States Computer Emergency Response Team (US-CERT). According to a US-CERT advisory:

> A trojan horse is an attack method by which malicious or harmful code is contained inside apparently harmless files. Once opened, the malicious code can collect unauthorized information that can be exploited for various purposes, or permit computers to be used surreptitiously for other malicious activity.[108]

This definition captures, for example, the Remotespy.com "remote install" feature. As Remotespy.com promotes it:

> Once the RemoteSpy file (you create) is executed on a computer, it will continuously record log data on the computer you are monitoring secretly. You can login anytime to your RemoteSpy account to view the recorded data in real-time!
> …
> RemoteSpy is completely stealth and designed to install without warning. Once the executable is clicked the monitoring application will be started instantly. There are no signs or warnings whatsoever.[109]

Promoting "remote install" Trojan horse attacks is unfair because this technique causes a substantial harm, not outweighed by countervailing benefits, which consumers cannot reasonably avoid. In the example above, the "remote install" involves promoting the secret nature of the delivery of the software, and the fact that the target is a computer which one does not have physical proximity or access to. This promotion is likely to cause harmful surveillance of the form of a Trojan horse attack. The likelihood of harmful surveillance is increased by two factors present in the promotion of the "remote install": the promotion of the secret nature of the surveillance, and the fact that it is installed by sending a surreptitious email to a computer that one does not have physical control of, or the ability to remotely log in via pre-existing administrative accounts. The

[106] FTC Deception Policy, *supra* note 59.
[107] *Id.*
[108] US-CERT, *Targeted Trojan Email Attacks*, TA05-189 (July 8, 2005), http://www.us-cert.gov/cas/techalerts/TA05-189Apr.html.
[109] *supra,* ¶ 32.

harm from such surveillance is described above in ¶¶ 47 *et seq.*

Little to no countervailing benefit comes from the promotion of "remote install" Trojan horse attacks. Consumers may benefit from easily finding software to install in remote computers for legitimate monitoring. Such promotion may be achieved by other methods which do not teach users to create Trojan horse attacks, such as teaching the remote users to download the surveillance software directly, or by having the purchaser log into the remote machine and install the software via an administrative account.

Finally, consumers cannot reasonably avoid this harm because they are not aware of the installation of the surveillance software via the "remote install" Trojan horse attack. Consumers also do not receive adequate warnings of the dangers of using the software in a Trojan horse attack.

63. Promoting "remote install" Trojan horse attacks is deceptive because purchasers are likely to believe they are purchasing software that can be legitimately used for the purposes advertised, thus causing harm. The injury of illegitimate surveillance is likely because of two main factors: the promotion of the secret nature of the surveillance; and the fact that it is installed by sending a surreptitious email to a computer that one does not have physical or administrative control of. The promotion of "remote install" Trojans is material. Express claims are presumed to be material.[110] Claims are material if they concern safety or the concerns of a reasonable consumer.[111] The exposure to potential criminal and civil liability is of concern to reasonable consumers like health and safety concerns. Using the software to conduct Trojan horse attacks exposes the purchaser to legal liabilities and harms the victims of the attacks, as described above in ¶¶ 47 *et seq.*

64. Several of the companies above fail to adequately warn users of the risks of illegitimate uses of the surveillance products. The failure to warn is unfair because substantial harms are likely, there is a low cost to remedy the lack of warnings, and users cannot reasonably avoid these harms. The substantial harm is likely because purchasers are likely to believe they can use the software for its advertised purposes in any setting. There is little countervailing benefit from a lack an adequate warning -- consumers may appreciate the simpler advertisements, but warnings can be simply delivered as well. Remedying this belief is the low cost alternative of prominent disclaimers warning users that they require authorization in order to monitor another's computer. Victims cannot reasonably avoid these harms because they are not made aware of the surveillance of their computers. Purchasers also cannot reasonably avoid the harm because they are not made aware of the dangers of the product.

65. The failure to adequately warn users is deceptive because it is likely to materially mislead consumers, causing injury. An omission can be misleading if a seller does not adequately correct a false impression.[112] Consumers are likely to use these products for

[110] FTC Deception Policy, *supra* note 59.
[111] *Id.*
[112] FTC Deception Policy, *supra* note 59; See *id* at n. 9, quoting "The nature, appearance, or intended use of a product may create the impression on the mind of the consumer . . . and if the impression is false, and if the seller does not take adequate steps to correct it, he is responsible for an unlawful deception."

the advertised purposes: monitoring others' computers. Specifically, consumers are likely to believe that they are permitted to spy on their spouses. Private investigators consider the ability to install spyware on a spouse's computer to be part of a misconception that many have -- that "[i]f its my spouse. I can do what I want."[113] Thus harmful use is more likely if the promotion does not include adequate warnings. The omission is material because reasonable users are concerned that they not violate the law. The injury caused is described above in ¶¶ 47 *et seq.*

V. Prayer for Investigation and Relief

66. EPIC requests that the Commission investigate the above named parties, enjoin their unfair and deceptive practices, and seek damages for aggrieved individuals.

67. EPIC requests that future Commission spyware enforcement include the amateur spyware industry.

68. EPIC requests that the FTC investigate other potential harms of the amateur spyware industry beyond the named parties, including:

a. Amateur spyware disabling or avoiding of user installed anti-virus and anti-spyware technology.

b. Amateur spyware opening security holes in the systems of users.

c. Amateur spyware companies' securing of data collected.

d. Amateur spyware companies' response to non-customer victims of surveillance who contact them for legal and technical support.

69. EPIC requests that the FTC promulgate a set of best practices, enforced via its Section 5 authority, to provide guidelines to the amateur spyware industry about what constitutes an adequate level of consumer protection.

Respectfully submitted,

Marc Rotenberg
Executive Director

Guilherme Roschke
Skadden Fellow

Electronic Privacy
Information Center
1718 Connecticut Ave NW

[113] Pam Dawkins, *So You Want to Be a Private Eye,* CONNECTICUT POST ONLINE, Oct 12, 2007.

#200
Washington DC 20009
202-483-1140
http://epic.org

March 6, 2008