Testimony of
Ari Schwartz
Associate Director
Center for Democracy and Technology

Before

The House Committee on Energy and Commerce
Subcommittee on Commerce, Trade, and Consumer Protection

April 29, 2004

Hearing on
"Spyware"

Chairman Sterns and Ranking Member Schakowsky, thank you for holding this hearing on spyware, an issue of growing concern for consumers and businesses alike. CDT is pleased to have the opportunity to participate.

CDT is a non-profit, public interest organization dedicated to preserving and promoting privacy and other democratic values and civil liberties on the Internet. CDT has been widely–recognized as a leader in the policy debate about the issues raised by so-called "spyware" applications.[1] We have been engaged in the early legislative, regulatory, and self-regulatory efforts to deal with the spyware problem, and have been active in public education efforts through the press and our own grassroots network.

A. Summary

In our testimony today, we hope to address two questions: What is spyware? And how should we respond to it?

In Section B of our testimony below, we attempt to help define and understand the spyware problem. CDT's report "Ghosts in Our Machines: Background and Policy Proposals on the 'Spyware' Problem,"[2] released in November 2003, addresses this issue. The report describes the range of invasive software applications referred to as "spyware" and clarifies the privacy, transparency and user control issues raised by these rogue programs.

---

[1] See, e.g., CDT's "Campaign Against Spyware," http://www.cdt.org/action/spyware/action (calling on users to report their problems with spyware to CDT; since November 2003, CDT has received over 250 responses). CDT's Complaint and Request for Investigation, Injunction, and Other Relief, in the Matter of MailWiper, Inc., and Seismic Entertainment Productions, Inc., February 11,, 2004 (available at http://www.cdt.org/privacy/20040210cdt.pdf). "Eye Spyware," The Christian Science Monitor Editorial, April 21, 2004 ["Some computer-focused organizations, like the Center for Democracy and Technology, are working to increase public awareness of spyware and its risks. "The Spies in Your Computer," New York Times Editorial, February 18, 2004 (arguing that "Congress will miss the point (in spyware legislation) if it regulates specific varieties of spyware, only to watch the programs mutate into forms that evade narrowly tailored law. A better solution, as proposed recently by the Center for Democracy and Technology, is to develop privacy standards that protect computer users from all programs that covertly collect information that rightfully belongs to the user."). John Borland, "Spyware and its discontents," *CNET.com*, February 12, 2004. ("In the past few months, Ari Schwartz and the Washington, D.C.-based Center for Democracy andTechnology have leapt into the front ranks of the Net's spyware-fighters.")

[2] http://www.cdt.org/privacy/031100spyware.pdf

Additionally, over the last six months, CDT has led discussions of a Consumer Software Working Group that includes leading members of the Internet industry, advertising companies, public interest groups and academics in order to identify examples the worst practices that consumers are facing online. In our testimony today, we highlight some of the pertinent issues raised by the working group, summarize the findings of CDT's report, and describe some of CDT's subsequent research and ongoing efforts in these areas.

In Section C, we turn to potential responses to the spyware problem. CDT sees three major areas where action is necessary to stem the disturbing trend toward a loss of control and transparency for Internet users:

1) Enforcement of existing laws could go a long way toward reducing the problem of spyware. While longstanding fraud statutes already cover many of the issues raised by these applications, currently they are rarely enforced against spyware programmers and distributors.

2) Fundamental to the issue of spyware is the overarching concern about online Internet privacy. Legislation to address the collection and sharing of information on the Internet would resolve many of the privacy issues raised by spyware. If we do not deal with the broad Internet privacy concerns now, in the context of spyware, we will undoubtedly find ourselves confronted by them yet again when they are raised anew by some other, as yet unanticipated, technology.

3) To be effective, legislation and enforcement approaches will have to be carried out concurrently with better consumer education, industry self-regulation and the development of new anti-spyware technologies.

We address each of these avenues in turn.

B. Defining and Understanding "Spyware" and "Adware"

"Spyware" has no precise definition. The term has been applied to everything from keystroke loggers, to advertising applications that track users' web browsing, to web cookies, to programs designed to help provide security patches directly to users. "Spyware" programs can be installed on users' computers in a variety of ways, and they can have widely differing functionalities.

What these programs have in common is a lack of transparency and an absence of respect for users' ability to control their own computers and Internet connections.

While many programs that have been called "spyware" are advertising software, CDT has emphasized that there is nothing inherently objectionable about ad-support as a business model. We highlight email applications, such as Eudora, that are successful and user-friendly examples of ad-supported software.

However, in many cases, the revenue that these applications provide has given software distributors the incentive to push them onto users' computers using deceptive or fraudulent means. Ad-support can and must be implemented in a way that is transparent to users and respects their choices and privacy preferences.

Distribution of Spyware

"Spyware" programs can be distributed in a variety of ways. For example, they may be bundled with other free applications, including peer-to-peer file sharing applications; they may be distributed through deceptive download practices; or they may be installed by exploiting security holes in the web browser or operating system on a user's computer. In some cases, once one "spyware" application has gained access to a user's computer, it will surreptitiously download and install other applications.

In each of these scenarios, users generally do not know that the software is being installed. And once these invasive applications are on a user's computer they can be difficult or impossible to find and remove.

Effects of Spyware

As mentioned above, the overarching concerns raised by spyware applications are *transparency* and *user control*. Within these broad categories, spyware programs can raise a host of specific concerns.

- These programs can change the appearance of websites, modify users' "start" and "search" pages in their browsers, or change low level system settings. In our complaint to the FTC against MailWiper and Seismic Entertainment Productions, filed in February, CDT asked the Commission to investigate one particularly egregious example of such "browser hijacking" behavior.

- Spyware programs are also often responsible for significant reductions in computer performance and system stability. In many cases, consumers mistakenly assume that the problem is with another application or with their Internet provider, placing a substantial burden on the support departments of providers of those legitimate applications and services.

- Spyware programs can track users' online activities. Some gather personally identifiable information. The most egregious forms of spyware can capture all keystrokes, or record periodic screenshots from a user's computer.

- Even in cases where spyware programs transmit no personally identifiable information, their hidden, unauthorized appropriation of users' computing resources and Internet connections threatens the security of computers and the integrity of online communications. The "auto-update" component of many of these applications can create major new security vulnerabilities by including capabilities to automatically download and install additional pieces of code without notifying users or asking for their consent, typically with minimal security safeguards.

CDT is currently conducting technical and public opinion research on the spyware issue. We hope to continue to report the results of this work to the Committee as we learn more.

C. Possible Responses to Spyware Concerns

Combating the most invasive spyware technologies will require a combination of approaches. First and foremost, vigorous enforcement of existing anti-fraud laws should result in a significant reduction of the spyware problem.

Addressing the problem of spyware also offers an important opportunity to establish in law baseline standards for privacy for online collection and sharing of data. Providing these protections would not only address the privacy concerns that current forms of spyware raise, but would put in place standards that would apply to future technologies that might challenge online privacy. Anti-spyware tools, better consumer education, and self-regulatory policies are also all necessary elements of a spyware solution.

Legislation to establish standards for privacy, notice, and consent specifically for software, such as H.R.2929, currently before this Committee, may play an important role as well. The challenge to such efforts is in crafting language that effectively addresses the spyware issue without unnecessarily burdening legitimate software developers or unintentionally hindering innovation.

So far the efforts to address the spyware issue are all in very preliminary stages. They will each require cooperation among government, private sector, and public interest initiatives.

Enforcement of Existing Law

CDT believes that three existing federal laws already prohibit many of the invasive or deceptive practices employed by malevolent software makers. Better enforcement of these statutes could have an immediate positive effect on the spyware problem.

Title 5 of the Federal Trade Commission Act is most directly applicable to the most common varieties of spyware. We believe that many of the more invasive forms of spyware discussed above clearly fall under the FTC's jurisdiction over unfair and deceptive trade practices. Some of these practices are highlighted in the Appendix – the Consumer Software Working Group's Examples of Unfair, Deceptive or Devious Practices Involving Software. To our knowledge, the FTC so far has not brought any major actions against spyware makers or spyware distributing companies. In February, CDT filed a complaint with the FTC against two companies for engaging in browser hijacking to display deceptive advertisements to consumers for software sold by one of the companies.[3]

We believe that one of the most immediate ways in which Congress could have a positive impact on the spyware problem is by directing the FTC to increase enforcement against unfair and deceptive practices in the use or distribution of downloadable software and by providing increased resources for such efforts.

Several laws besides the FTC Act may also have relevance. The Electronic Communications Privacy Act (ECPA), which makes illegal the interception of communications without a court order or permission of one of the parties, may cover programs that collect click-through data and other web browsing information without consent. The Computer Fraud and Abuse Act (CFAA) also applies to some uses of spyware. Distributing programs by exploiting security vulnerabilities in network software, co-opting control of users' computers, or exploiting their Internet connection can constitute violations of the CFAA, especially in cases where spyware programs are used to steal passwords and other information.

In addition to federal laws, many states have long-standing fraud statutes that would allow state attorneys general to take action against invasive or deceptive software. Like their federal counterparts, these laws have not been strongly enforced to date.

---

[3] Complaint and Request for Investigation, Injunction, and Other Relief, in the Matter of MailWiper, Inc., and Seismic Entertainment Productions, Inc., February 11, 2004 (available at

New Legislation

CDT has argued that the most effective way to address the spyware problem through legislation is in the context of online privacy generally. Specifically, we believe that the privacy dimension of spyware would best be addressed through baseline Internet privacy legislation that is applicable to online information collection and sharing irrespective of the technology or application. CDT has advocated such legislation before the Senate Commerce Committee and in other fora. Until we address the online privacy concern, new privacy issues will arise as we encounter new online technologies and applications.

Still, software may pose some unique problems. A comprehensive legislative solution to spyware may need to address the user-control aspects of the issue such as piggybacking, and avoiding uninstallation. H.R. 2929 before this Committee represents an important acknowledgement of several of these problems. We appreciate the desire to craft targeted legislation focusing on some of the specific problems raised by spyware, and CDT commends Representatives Bono and Towns for bringing attention to this important issue.

At the same time, we wish to emphasize the complexity of such efforts. The broad industry opposition to an anti-spyware bill recently passed in the Utah legislature, based on potential unintended consequences of the bill for legitimate software companies, demonstrates the difficulties that can be introduced by such legislation if it is not carefully drafted. We know Representatives Bono and Towns have been looking hard at some of the specific definitional concerns raised by CDT and others, and we look forward to continuing to work with the Committee on this bill.

Non-Regulatory Approaches

Technology measures, self-regulation and user education must work in concert, and will be critical components of any spyware solution. Companies must do a better job of helping users understand and control how their computers and Internet connections are

---

http://www.cdt.org/privacy/20040210cdt.pdf).

used, and users must become better educated about how to protect themselves from spyware.

The first step is development of industry best practices for downloadable software. Although not all software manufacturers will abide by best practices, certification programs will allow consumers to quickly identify those that do and to avoid those that do not. In the current environment consumers cannot easily determine which programs post a threat, especially as doing so can involve wading through long and unwieldy licensing agreements.

Technologies to deal with invasive applications and related privacy issues are in various stages of development. Several programs exist that will search a hard-drive for these applications and attempt to delete them. Some companies are experimenting with ways to prevent installation of the programs in the first place. However, even these technologies encounter difficulties in determining which applications to block or remove. Clear industry best practices are crucial in this regard as well.

Standards such as the Platform for Privacy Preferences (P3P) may also play an important role in technical efforts to increase transparency and provide users with greater control over their computers and their personal information. P3P is a specification developed by the World Wide Web Consortium (W3C) to allow websites to publish standard, machine-readable statements of their privacy policies for easy access by a user's browser. If developed further, standards like P3P could help facilitate privacy best practices to allow users and anti-spyware technologies distinguish legitimate software from unwanted or invasive applications.

The IT industry has initially been slow to undertake such efforts. However, increasing public concern about spyware and the growing burden placed on the providers of legitimate software by these invasive applications has led to more industry attention on

this front.[4] The Consumer Software Working Group, including major Internet service providers, software companies, and hardware manufacturers, has expressed its view that this area is ripe for industry self-regulation and best practices.

CDT believes Congress can have an immediate positive impact by encouraging industry to continue to follow through on these efforts.

D. Conclusion

Users should have control over what programs are installed on their computers and over how their Internet connections are used. They should be able to rely on a predictable web-browsing experience and to remove for any reason and at any time programs they don't want. The widespread proliferation of invasive software applications takes away this control.

Better consumer education, industry self-regulation, and new anti-spyware tools are all key to addressing this problem. New laws, if carefully crafted, may also have a role to play. Many spyware practices, however, are already illegal. Even before passing new legislation, existing fraud statutes should be robustly enforced against the distributors of these programs.

The potential of the Internet will be substantially harmed if users come to believe that they cannot use the Internet without being at risk of infection from spyware applications. We must find creative ways to address this problem through law, technology, public education and industry initiatives if the Internet is to continue to flourish.

---

[4] See, e.g. , Earthlink press release: Earthlink Offers Free Spyware Analysis Tool to All Internet Users, January 14, 2004 (available at: http://www.earthlink.net/about/press/pr_analysis/); America Online press release: America Online Announces Spyware Protection for Members, January 6, 2004 (available at: http://media.aoltimewarner.com/media/newmedia/cb_press_view.cfm?release_num=55253697); Microsoft press release: Battling 'Spyware': Debate Intensifies on Controlling Deceptive Programs, April 20, 2004 (available at: http://www.microsoft.com/presspass/features/2004/apr04/04-20Spyware.asp)

Appendix: Examples of Unfair, Deceptive or Devious Practices Involving Software

Consumer Software Working Group

The Consumer Software Working Group is a diverse community of public interest groups, software companies, Internet service providers, hardware manufacturers, and others that are seeking consensus responses to the concerns raised by practices that harm consumers.

Over the past several years, a subset of computer software referred to as "spyware" has become the subject of growing public concern. Computer users increasingly find programs on their computers that they did not know were installed, that create risks to privacy, that open security holes, that impair the performance and stability of their systems, that frustrate their attempts to uninstall or disable the programs, or that lead them to mistakenly believe that these problems are the fault of another application or their Internet service provider.

There is agreement that these practices can raise serious concerns. At the same time, the wide range of and lack of clarity in attempted definitions for the types of software practices that most concern consumers hamper attempts at self-regulatory, technological and legislative responses. Many definitions of spyware in circulation today are either under-inclusive in important respects or, more commonly, overbroad so that they include practices that clearly benefit consumers, or both.[5]

The Center for Democracy and Technology convened the Consumer Software Working Group. Companies, public interest groups or academics interested in joining the Working Group should contact Ari Schwartz <ari@cdt.org>, Michael Steffen <msteffen@cdt.org>, or John Morris <jmorris@cdt.org> at the Center for Democracy and Technology.

Examples of Unfair, Deceptive or Devious Practices Involving Software
Version 1.0

The Consumer Software Working Group is concerned about a specific set of devious, deceptive or unfair practices that adversely affect consumers online. While the following list of examples is not nearly complete, it describes a series of activities and behaviors that the Group considers to be clearly objectionable.

Specifically, the Group identifies three broad types of practices where abuses occur today. Most of these practices may be illegal under current law, depending on the specific facts of the particular case. Within each area, we offer illustrative examples, based on real cases. We note that each of the objectionable behaviors we identify has constructive consumer-friendly counterparts when carried out with proper notice and consent and in ways that give consumers control. Automatic installation, personalization

[5] For example, the Working Group observes that the current Utah law addresses practices involving software that most informed consumers would not consider unfair, deceptive or devious and fails to cover some practices that most informed consumers would consider unfair, deceptive or devious.

and tracking, and in some cases resistance to uninstallation can provide important benefits to consumers.

We hope that this list of objectionable practices will help to focus technical, self-regulatory, regulatory and law enforcement efforts to protect consumers from inappropriate activities in a more targeted and effective manner, while avoiding unintended negative consequences for good actors and consumers alike. The Working Group believes that this is an area that could be ripe for self-regulatory efforts to craft industry principles to protect consumers and the marketplace.

1) **Hijacking** — The practices described in this section are objectionable to the extent that they enable an unaffiliated person to use the user's computer in a way that ordinarily would not be expected. This may occur through an unnoticed program consuming the user's computing resources or resetting a user's existing configurations without the user's knowledge, or through coercion or deception.

> Example: A computer user sees an Internet advertisement for Program A. The user clicks on the ad and is sent to a page that pops up a window asking if the user wants to download Program A. The user clicks “no,” but Program A is eventually downloaded and installed anyway.
>
> Example: A computer user sees an Internet advertisement for Product B. The user clicks on the advertisement, and is sent to a page that informs the user that “Program C is needed to view this Web page.” This leads the user to believe that Program C is necessary to view the site about Product B, so the user clicks “yes” and the program is downloaded and installed. In fact, Program C is not necessary to view the website for Product B and the user is never informed of the actual reason why Program C was installed.
>
> Example: A computer user sees an Internet advertisement for Program D. The user clicks on the ad, and she is sent to a page that immediately pops up a window asking if she wants to download Program D. The user clicks “no.” This happens repeatedly until the user gets frustrated and clicks “yes.”
>
> Example: A computer user receives an Internet advertisement for Product E as part of a webpage he is looking at. Simply as a result of loading the ad, Software Program F wholly unrelated to Product E is downloaded onto the user’s computer. No notice or opportunity to consent to download Software Program F was provided.
>
> Example: While browsing the Internet, a computer user is offered the opportunity to download and install Software Program G. Using a fraudulently obtained digital certificate, the download request falsely identifies Software Program G as being from the user’s trusted Internet Service Provider, H. In fact, the Program is not from Internet Service Provider H, and has no relation to the ISP. However, based on its claimed affiliation with H, the user agrees to let the program be downloaded and installed.
>
> Example: A computer user loads Company I’s Web page. The Web page opens another page running a java script. When the user closes Company I’s Web page, the java script page covertly resets the user's homepage without obtaining consent.

Example: A computer user loads Company J's Web page. The Web page opens another page running a java script. When the user closes Company J's Web page, the java script page covertly resets the user's homepage. The java script is written such that any time the user attempts to reset his homepage, the program automatically resets it again so the user cannot reset his homepage to what it was before the hijacking took place.

Example: A computer user downloads Software Package K. Among the programs in Software Package K is a dialer application that was not mentioned in any advertisements, software licenses, or consumer notices associated with the package or in information provided in conjunction with the ongoing operations of the package. The dialer application is not an integral part of Software Package K. When the user opens her Web browser after installation of Software Package K, the dialer opens in a hidden window, turns off the sound of the user's computer, and calls a phone number without the user's permission.

Example: A computer user is sent Software Package L as an attachment to an unsolicited commercial email message. There is no documentation for Software Package L. Included in Software Package L is Program M that sends a message to Computer N. Computer N then uses Program M on the user's computer as a means to send out unsolicited commercial emails.

2) **Surreptitious surveillance** — The practices described in this section are objectionable to the extent that they involve intrusive and surreptitious collection and use of personally identifiable information about users that is wholly unrelated to the purpose of the software as described to the consumer.

Example: A computer user downloads Software Package P. Software Package P contains a keystroke logger unrelated to any functions described to the user. The keystroke logger records all information input on the user's computer and sends this information on to another computer user. The first user is not informed about the operation of the keystroke logger.

Example: Program Q advertises itself as a search tool bar. A user downloads Program Q to gain the search functionalities. Program Q installs a tool bar, but — once installed — also mines the user's registry and other programs for personally identifiable information about the user unrelated to the search functionality and without informing the user or obtaining consent. When the user connects to the Internet, Program Q sends this information back to the company that makes Program Q.

3) **Inhibiting termination** — The practices described in this section are objectionable to the extent that they frustrate consumers' efforts to remove a program, deactivate it or otherwise render it inoperative. Generally, these practices are intended to prevent the user from severing or terminating a relationship with the provider of the program.

Example: A computer user downloads Software Package S. Software Package S contains Advertising Program T. Advertising Program T sends the user pop-up ads while the user is surfing the Web even if no other programs in Software Package S are running. The pop-up ads are not labeled as related to Advertising Program T or Software Package S in any way and there is no other way to find the ads' origin. The user is concerned about the increase in pop-up ads, but does not know whether they

are caused by Program T or are from the Web sites that he is visiting. The user has no means to find out the origin of the ads in order to make a decision about uninstalling Program T.

Example: A computer user downloads Software Package U. As initially disclosed to the user, Software Package U contains a mandatory program, Advertising Program V, which is bundled as a way to generate revenue and pay for the development of Software Package U only. When the user uninstalls Software Package U, the user is not given a clear opportunity to uninstall Program V at that time, and Advertising Program V stays on the user's computer.

Example: A computer user downloads Gaming Program W. The user wants to remove Gaming Program W from the computer. Gaming Program W does not have an uninstall program or instructions and does not show up in the standard feature in the user's operating system that removes unwanted programs (assuming this feature exists in the operating system). The user's attempts to otherwise delete Program W are met by confusing prompts from Program W with misrepresentative statements that deleting the program will make all future operations unstable.

Example: A computer user downloads Program X. The user wants to remove Program X from the computer. Program X appears in the standard feature in the user's operating system that removes unwanted programs. However, when the user utilizes the "remove" option in the operating system, a component of Program X remains behind. The next time the user connects to the Internet, this component re-downloads the remainder of Program X and reinstalls it.

The following companies, organizations and individuals have worked to describe Examples of Unfair, Deceptive and Devious Practices Involving Software. These descriptions can be used to help focus technical, self-regulatory, regulatory and law enforcement efforts to protect consumers from inappropriate activities.

America Online
Business Software Alliance
Center for Democracy and Technology
Claria Corporation
Consortium of Anti-Spyware Technology Vendors
Consumer Action
CryptoRights Foundation
Dell, Inc.
Distributed Computing Industry Association
EarthLink
eBay
Electronic Frontier Foundation
Google
HP
Information Technology Industry Council
Internet Commerce Coalition
Lavasoft
Microsoft
Network Advertising Initiative
Privacilla.org
Sharman Networks
Peter Swire, Moritz College of Law of the Ohio State University[6]
TRUSTe
Webroot Software
WhenU
Yahoo!

[6] Individuals are listed with their affiliation for identification purposes only.