Prepared Statement of

Jerry Berman, President
The Center For Democracy & Technology
Before
The Senate Committee On Commerce, Science, And Transportation
Subcommittee on Communications
On
The SPY BLOCK Act

Tuesday, March 23, 2004

Mr. Chairman and members of the Committee, the Center for Democracy & Technology (CDT) is pleased to have this opportunity to speak to you about the growing threat to consumers and Internet users posed by spyware and other invasive or deceptive software applications.

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 deeply engaged in the policy debate about the issues raised by so-called "spyware." In November, 2003, CDT released a report "Ghosts in Our Machines: Background and Policy Proposals on the 'Spyware' Problem,"[1] providing background on the spyware issue, evaluating policy and other solutions, and presenting advice for Internet users about how to protect their personal information and their computers from these programs. At the same time, CDT launched our public "Campaign Against Spyware," calling for Internet users to send us descriptions of the problems they have encountered with these invasive applications.[2] CDT is also engaging in in-depth meetings with the wide range of stakeholders in the spyware issue, including ISPs, software companies, and consumer groups.

The proliferation of invasive software referred to as "spyware" is a large and rapidly growing concern. These deceptive applications compromise users' control over their own computers and Internet connections, and over the collection and sharing of their personal information. We praise the chairman and this Committee for holding this hearing on S. 2145—the SPY BLOCK Act—and thereby bringing public attention to this serious and complex issue.

In our testimony today, we hope to address three principal questions:

- *What is "spyware?"* The term spyware is extremely difficult to define precisely, and can itself be misleading. The term has been used to describe a wide and diverse range of software. 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.

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

[2] http://www.cdt.org/action/spyware

- *How bad is the problem?* It is difficult to precisely quantify the damage caused by these invasive applications—but it is clear that the problem is severe. Spyware is widespread and can threaten privacy, security, and computer performance. Even the less invasive forms of spyware can seriously inconvenience users and impose serious strains on the technical support resources of schools and legitimate businesses.

- *How can we respond to the problem?* Responding to the problem of spyware requires a multifacted approach.

    - Existing law 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 distributers. We encourage Congress to provide law enforcement with the necessary resources to understand the phenomenon of spyware and to bring to bear strong enforcement of these laws.

    - 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. We look to Congress to seize this important opportunity to address this larger issue. 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.

    - 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.

  Legislation directed at some of the specific issues raised by software—such as notice and consent for installation—may also have a role to play. While crafting such legislation will be difficult, the SPY BLOCK Act demonstrates the progress that has already been made in our understanding of the spyware problem. The bill plays a critical role in advancing the inquiry about spyware and developing approaches to addressing the issue.

We address each of these questions in more detail in turn below.

I. Understanding and Defining Spyware

No precise definition of spyware exists. The term has been applied to software ranging from "keystroke loggers" that capture every key typed on a particular computer; to advertising applications that track users' web browsing; to programs that hijack users' system settings. In

some cases, it has even been applied to web cookies or system update utilities designed to provide security patches directly to users. Spyware programs can be installed on users' computers in a variety of ways, and can have widely differing functionalities.

What the growing array of invasive 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. The debate over precisely how to define the term spyware (as well as other related terms such as "malware" or "adware") has been contentious, in some cases even leading to legal threats between companies.[3] But this semantic dispute diverts attention from the underlying question: Are consumers offered meaningful notice and choice about the programs installed on their computers and the ways in which their computers and Internet connections are used?

The most egregious forms of spyware (sometimes called "snoopware" to distinguish them from other categories) are typically stand-alone programs installed intentionally by one user onto a computer used by others. Some capture all keystrokes and record periodic screen shots, while others are more focused, collecting lists of websites visited or suspected passwords. These programs have legal uses (e.g. for certain narrow kinds of employee monitoring) as well as many clearly illegal ones.

The more widespread spyware problem is that of applications installed on Internet users' computers in the course of browsing online or downloading other unrelated software. Users are typically unaware that these programs are being installed on their computers. Many "piggyback" on other free applications, such as screen savers, system utilities, or peer-to-peer filesharing programs. In many cases, the only notice to the user about installation of such a secondary program is buried in a long and legalistic "end user licensing agreement." In some instances, no notice of the bundling is provided at all. Other programs trick users into authorizing installations through deceptive browser pop-ups, or exploit security holes to install themselves automatically when a user visits a particular website. In some instances, once a program is installed, it begins to download and install other software with no notice to the end user.

Spyware programs perform a variety of functions once they have gained access to a computer. Many track users' web browsing and deliver pop-up advertisements. While there is nothing inherently objectionable about using advertising, including targeted advertising, as a means to support free software, advertising software must function in a way that is transparent to users, and users must have control over its installation and the ability to remove it.

Other spyware programs can change the appearance of websites, modify users' "start" and "search" pages in their browsers, or change low level system settings without notifying users or obtaining their consent. Some will even co-opt users' Internet connections to send out spam. Such software is often responsible for significant reductions in computer performance and system stability.

---

[3] *See, e.g.,* Paul Festa, "See you later, anti-Gators," *CNET.com*, October 22, 2003 (available at: http://news.com.com/2100-1032_3-5095051.html)

Although much of the discussion about the spyware problem to date has focused on the privacy dimension of the issue, clearly many of these behaviors raise concerns beyond privacy. The term spyware itself can be misleading in some of these cases; arguably, a better term would be "trespassware."

Many spyware applications resist uninstallation. For example, advertising programs that are originally installed as part of a "bundle" with other free software may not be removed when the main application is uninstalled. In some cases, spyware applications do not appear in the standard "Add/Remove" programs or other uninstallation feature of the system. In egregious instances, some programs reportedly even reinstall themselves after the user has made deliberate efforts to eliminate them.

No single behavior of this kind defines "spyware." However, together they characterize the transparency and control problems common to such applications. Disagreements will continue about whether particular applications do or not deserve this label. In the end, it may be best to think of spyware not as a discrete and well defined category, but as the bad end of a spectrum of software practices, ranging from industry best practices for transparency, notice, and control on one end, to clearly deceptive and fraudulent behaviors on the other. Unfortunately, the resistance of spyware to easy definition makes writing legislation to address the problem difficult, as we discuss in detail in Section III below.

II. Severity of the Spyware Threat

It is difficult to quantify the spyware problem because of the definitional questions mentioned above, and because the speed with which new spyware applications can appear and change makes reliable detection of the programs difficult. However, several indicators point toward the severity of the problem.

Since CDT launched our public "Campaign Against Spyware" in November 2003, we received over 300 accounts of problems encountered with various spyware applications. The sources of the responses demonstrate that the problem is pervasive—respondents included individuals dealing with the issue on corporate networks, on computers in schools, and on government networks. These users name a wide array of specific programs and identify several categories of concerns, including loss of privacy, decreased stability, and the inability to use their computer, either because of barrages of pop-ups, or as a result of severely diminished performance.

System administrators also responded to our "Campaign Against Spyware." One of the biggest concerns raised by network administrators relates to the security holes created by these applications. Some spyware programs open major vulnerabilities by including the

capability to automatically download and install additional pieces of code with minimal security safeguards. This capability is often part of an "auto-update" component.[4]

Network administrators report that spyware is as much or more of a problem than spam, viruses, or other security maintenance. One administrator told us that as many as 90% of the computers on the networks he manages have been infected with some variety of "spyware." Another technical support worker reported that the majority of the problems he encounters can be traced back to "spyware," and that his first recommendation to correct stability or performance problems is to run one of the free spyware search and removal utilities available on the Internet.

In our discussions with industry, CDT learned that invasive spyware applications also cause substantial harm to ISPs and distributors of legitimate software. In many cases, consumers are mistakenly led to believe that the problems resulting from spyware applications are a problem with another, more visible application or with their Internet provider. This confusion places a substantial burden on the support departments of providers of those legitimate applications and services. Not only are affected users required to pay for otherwise unnecessary technical support calls, but those calls impose significant costs on businesses offering the support. Some industry representatives we talked to estimated that the additional costs run in the millions or tens of millions of dollars.

III. Responses to Spyware

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 the SPY BLOCK act 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. We believe the current bill represents a major step forward, although several concerns still exist.

---

[4] *See, e.g.*, Saroiu, Stefan , Steven Gribble, and Henry Levy. "Measurement and Analysis of Spyware in a University Environment" *Proceedings of the First Symposium on Networked Systems Design and Implementation*, March 2004 (available at: http://www.cs.washington.edu/homes/gribble/papers/spyware.pdf).

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. We discuss each approach in turn below.

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.[5] 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.[6]

The FTC's plans for a workshop in April on "Monitoring Software on Your PC: Spyware, Adware, and Other Software," is an encouraging indication that the Commission is devoting greater attention to this issue. CDT hopes that the clear message emerges from this workshop that the FTC must take a more prominent role in addressing this issue.

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 of programs by exploiting security

---

[5] Examples of clearly deceptive or unfair practices include:

- installing unwanted applications without giving users notice in the end user license agreement or another form;
- providing notice only in a license agreement that is misleading or unclear, leading consumers to think they are downloading one program when in fact they are downloading and installing an application that does something completely different;
- utilizing consumer resources such as computer power or bandwidth or that capture personal information without consent; or
- distributing programs that evade uninstallation.

[6] *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).

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.

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.

At the same time, certain aspects of the spyware problem extend beyond the privacy issues. Privacy legislation would not, for example, apply to software that commandeers computing resources but does not collect or share user information. A comprehensive legislative solution to spyware should address the user-control aspects of the issue—piggybacking, avoiding uninstallation, and so on.

The SPY BLOCK Act currently before this Committee represents an important first step towards addressing some of these problems. We appreciate the desire to craft targeted legislation focusing on some of the specific problems raised by spyware, and CDT applauds Senators Burns, Wyden, and Boxer for bringing attention to these important questions. CDT strongly supports the goal of the SPY BLOCK Act—to assure that users are provided with meaningful notice and choice about the applications that run on their computers.

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.[7]

Recognizing that development of appropriate standards for consumer software notice is still in preliminary stages, we suggest two areas of the SPYBLOCK Act that warrant further consideration and may require revision.

- *Standards for Notice* – Providing consumers with informative, accurate notice is a challenging task. Ongoing efforts to craft "short notices" in the context of privacy

[7] *See, e.g.* Ross Fadner, "Leading Internet Providers Oppose Passage of Spyware Control Act," *MediaPost,* March 15, 2004 (available at: http://www.mediapost.com/dtls_dsp_news.cfm?newsID=242077)

statements under the Gramm-Leach-Bliley Act both demonstrate the complexity of this problem and may provide a valuable model for the kind of notices that are appropriate in the context of downloadable software. Many so-called "spyware" applications already provide minimal notice to consumers buried in legalistic licensing agreements that come with bundled software. (Programs that do not provide even this level of notice are probably already illegal, as described above.) However, such minimal notice does not provide consumers the opportunity to make meaningful and informed choices. To be effective, legislation will have to address the difficult issue of how best to ensure that the information that accompanies software is appropriately clear, distilled, and contextualized to allow users to make informed decisions. Simply requiring that programs list information prior to installation may not be enough. However, a bill that will burden users by prompting users for choice too often will not be effective either.

- *Scope* – As currently structured, the SPY BLOCK Act covers almost all software, but provides specific exemptions for certain kinds of "general purpose" software and certain specific uses of information. CDT is concerned that this approach creates difficulties for software developers while imposing unrealistic burdens on legislators. This tack requires that legislators develop a comprehensive list of functions for which the requirements of the bill are not appropriate. Creating such a list for existing technologies is challenging in itself. Moreover, such a list will likely become outdated as soon as new technologies are developed, or as the categories defined in the law shift. CDT has argued that privacy laws should be neutral with respect to technologies, and we believe the same principle applies here.

We believe that valuable insight into the questions of scope and appropriate notice for consumer software are likely to emerge from ongoing industry and public interest efforts to define best practices, discussed below, and from the FTC's April Workshop in spyware. We encourage the Committee to incorporate the results of these efforts into refinements of the current 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 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.[8]

CDT believes Congress can have an immediate positive impact by encouraging industry to continue to develop these efforts toward self regulation.

IV. 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 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.

---

[8] *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).