CENTER FOR
DEMOCRACY
&
TECHNOLOGY
Working for Civil Liberties on the Internet

CDT Comments and Request to Participate:
FTC April 2004 Spyware Workshop

March 5, 2004

Office of the Secretary
Room 159-H
600 Pennsylvania Avenue N.W.
Washington, D.C. 20580

Re: Spyware Workshop – Request to Participate, P044509, and
Spyware Workshop – Comment, P044509

The Center for Democracy and Technology (CDT) submits these preliminary comments and requests the opportunity to participate in the Federal Trade Commission's Public Workshop, "Monitoring Software on Your PC: Spyware, Adware, and Other Software," on April 19, 2004.

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 a leader in the policy debate about the issues raised by so-called "spyware" applications. 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.[1] CDT hopes to bring the expertise gained through our ongoing efforts to our participation in the FTC's spyware workshop, and would provide a crucial public interest perspective.

---

[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). "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 and Technology have leapt into the front ranks of the Net's spyware-fighters.")

CDT is currently leading discussions among industry groups regarding definitions relating to consumer software and spyware, and is conducting technical and public opinion research on the spyware issue. We expect to be able to present early results from these efforts at the workshop.

CDT's report "Ghosts in Our Machines: Background and Policy Proposals on the 'Spyware' Problem,"[2] released in November 2003, covers CDT's response to many of the issues raised by the FTC in its current Request for Public Comments. The report describes the range of applications referred to as "spyware," and provides examples of the varieties of applications that have been placed in this category. It clarifies the privacy, transparency and user control issues raised by these applications. It also investigates the connection between spyware and peer-to-peer software; evaluates policy and other solutions to the spyware problem; and provides advice for Internet users about how to protect their personal information and their computers from these programs.

CDT is submitting the report as an attachment to these comments. We summarize below the findings of the report with regard to the specific questions posed by the Commission, and highlight some of CDT's ongoing efforts in these areas.

A. Defining and Understanding "Spyware" and "Adware"

CDT's report highlights the difficulty of precisely defining "spyware." 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.

In the specific case of advertising supported software, CDT has emphasized that there is nothing objectionable about ad-support as a business model. We highlight the Eudora email application as a successful and user-friendly example of ad-supported software. Ad-support can and should be implemented in a way that is transparent to users and respects their choices and privacy preferences.

As mentioned above, CDT is working with a number of companies and organizations to further explore public understanding of the spyware issue and to draft definitions relating to consumer software. We plan to release results from these efforts before April 19th.

B. Distribution of Spyware

"Spyware" programs can be distributed in a variety of ways. For example, they maybe 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

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

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.

C. The 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.

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.

Users must be able to control what programs are installed on their computers and how their Internet connections are used. They must be able to rely on a predictable web-browsing experience and they must have the ability to remove for any reason and at any point programs they don't want. A growing body of invasive applications takes away this control.

D. Possible Responses to Spyware Concerns

CDT believes that the practices of many spyware manufacturers are already illegal under the Electronic Communications Privacy Act, the Computer Fraud and Abuse Act, or Title 5 of the Federal Trade Commission Act. As mentioned above, CDT filed a complaint in February in a "browser hijacking" case that we believe warrants action by the FTC under its jurisdiction over unfair and deceptive trade practices. Increased enforcement of the

statutes that already apply to consumer software would be an important initial step in addressing the spyware problem.

Several companies have launched technologies to help users combat spyware. These efforts, combined with better consumer education, also promise to help mitigate the spyware problem. Best practices for consumer software and industry self-regulation also have important roles to play.

In addition, the growth of the spyware problem has prompted several proposals for targeted new legislation at both the federal and state levels. The challenge facing such efforts has been crafting language that effectively addresses the spyware issue without unnecessarily burdening the software industry.

CDT believes that combating the most invasive "spyware" technologies will require a combination of approaches. Legislation, increased enforcement, anti-spyware tools, better consumer education, and self-regulatory policies are all necessary elements of a spyware solution. These efforts will require cooperation among government, private sector, and public interest initiatives. CDT looks forward to a constructive discussion on these issues at the Commission's workshop, and to working with all parties towards solutions.

Respectfully submitted,

Ari Schwartz, Associate Director
Paula Bruening, Staff Counsel
Michael Steffen, Policy Analyst

Center for Democracy and Technology
1634 I St., NW
Washington, DC 20006
202-637-9800
http://www.cdt.org