Testimony of

Ari Schwartz, Associate Director
Center for Democracy and Technology
before
The House Committee on Energy and Commerce
on
"Combating Spyware: H.R. 29, the SPY ACT"

January 26, 2005

Chairman Barton and Ranking Member Dingell, thank you for holding this hearing on spyware, an issue of growing concern for consumers and businesses alike. CDT is honored to have the opportunity to participate in the Committee's first hearing of this new Congress.

CDT is a non-profit, public interest organization devoted to promoting privacy, civil liberties, and democratic values online. CDT has been widely recognized as a leader in the policy debate surrounding so-called "spyware" applications.[1] We have been engaged in the 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.

As an organization dedicated both to protecting consumer privacy and to preserving openness and innovation online, CDT has sought to promote responses to the spyware epidemic that provide meaningful protection for users while avoiding unintended consequences that could harm the open, decentralized Internet. Last year we testified before the Subcommittee on Commerce, Trade, and Consumer Protection on the issue of spyware, attempting to define the problem and suggest the range of responses required to address it. Since that time, we have worked closely with the Committee toward legislation to target spyware. We have appreciated the Committee's open, deliberative approach to this complex and important issue.

---

[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 650 responses). Center for Democracy & Technology, *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 (hereafter *CDT Complaint Against MailWiper and Seismic).* "Eye Spyware," *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 and Technology have leapt into the front ranks of the Net's spyware-fighters.")

Summary

The alarming rate of growth of the spyware problem is a major threat to Internet users, as well as to the long-term health of the open and decentralized Internet. Of particular concern is the growing complexity of a marketplace that allows mainstream companies to unwittingly fund illegal activities through a maze of distributors and affiliates.

CDT sees three major areas where action is necessary to stem this disturbing trend toward a loss of control and transparency for Internet users: 1) enforcement of existing law; 2) better consumer education, industry self-regulation, and anti-spyware technologies; and 3) baseline Internet privacy legislation.

H.R. 29 marks a substantial step forward in addressing many of the concerns of consumer groups and companies. CDT is generally supportive of the current bill. In particular, we strongly endorse the idea of raising penalties on and calling specific attention to the worst types of deceptive software practices online. CDT is less enthusiastic about the specific notice and consent requirements on adware and information collection programs, because of the definitional difficulties in crafting such a regime narrowly targeted at certain classes of software. We look forward to continuing to work with the Committee to help improve these element of the bill.

On a broader note, we hope that work on the spyware issue will provide a jumping off point for efforts to craft baseline standards for online privacy, now that many companies have expressed their support for such a goal. Privacy legislation would provide businesses with guidance about their responsibilities as they deploy new technologies and business models that involve the collection of information. At the same time, privacy assurances in law would give consumers some measure of confidence that their privacy is protected as companies roll out new ventures.

If we do not begin to think about privacy issues more comprehensively, the same players will be back in front of this Committee in a matter of months to address the next threat to online privacy. We hope that we can address these issue up front, rather than waiting for each new privacy threat to present itself.

1. Understanding and Combating Spyware

What is "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. Much attention has been focused on the surveillance dimension of the spwyare issue, though it is in fact a much broader problem.

What the growing array of invasive programs known as "spyware" have in common is a lack of transparency and an absence of respect for users' ability to control over their own computers and Internet connections.

In this regard, these programs may be better thought of as *trespassware.*[2] Among the host of objectionable behaviors for which such nefarious applications can be responsible, are:

- "browser hijacking" and other covert manipulation of users' settings;
- surreptitious installation, including through security holes;
- actively avoiding uninstallation, automatic reinstallation, and otherwise frustrating users' attempts to remove the programs;
- substantially decreasing system performance and speed, in some cases sufficient to render systems unusable; and
- opening security backdoors on users' computers that could be used to compromise their computers or the wider network.

Each of these behaviors was specifically documented by CDT or reported to us by individual users frustrated by their inability to use their own systems. Although no single behavior of this kind defines "spyware," together they characterize the transparency and control problems common to such applications.

How can we respond to the problem? Combating spyware requires a multifaceted approach. Significant progress has already been made since the spyware issue first began to receive national attention over a year ago, but much ground still remains.

- *Law enforcement*—Under federal law, much spyware is currently covered by Section 5 of the FTC Act, banning unfair and deceptive trade practices, as well as by the Computer Fraud and Abuse Act or the Electronic Communications Privacy Act. Spyware programs may also violate a variety of state statutes.

- *Private efforts*, including continued consumer education, the continued improvement of anti-spyware technologies, and stepped up efforts to close the security holes exploited by spyware purveyors, are all necessary. In particular, sound best practices for downloadable software are sorely needed.

- *Legislative* approaches to fighting spyware fall into two broad categories—attempts to narrowly address the issues raised by spyware, and attempts to deal, in a coherent and long-term fashion, with the underlying privacy issues. H.R. 29, which we address in detail below, is an example of the first approach. CDT has appreciated the opportunity to work with the Committee on this bill and is supportive of this effort. However, we remain firmly committed to idea that a long-term solution to spyware and other similar issues requires baseline online privacy legislation. Many of the issues raised by spyware may be easier to deal with in this context.

This framework represented our starting point on the spyware issue a year ago, and remains largely unchanged today. There have, however, been important developments in the problem, and in our research on the issue, since we appeared before the House Subcommittee last year.

---

[2] Chairman Barton's statement at last year's Subcommittee hearing aptly expressed this idea: "[Spyware's] installation is often sneaky or deceptive and even when it runs, it often goes undetected…If I want someone to come into my home, I invite them into my home. If they come uninvited, it is a trespass." Doug Abrahms, "Anti-spyware bill drawing praise, support," *Gannett News Service*, Apr. 30, 2004.

We address these in the following sections.

2. Spyware Continues to Grow as a Threat to Internet Users

When CDT first became involved in the spyware issue, we launched a "Campaign Against Spyware," calling on Internet users to send us their experiences with these invasive applications.[3] We indicated that we would investigate the complaints received and, where we believed appropriate, file complaints with the FTC. In our appearance before the Consumer Protection Subcommittee, we testified regarding the dramatic response to our campaign. In the nine months since our last appearance, CDT has continued to receive complaints through our online submission form. Among what are now hundreds of complaints, a total which continues to grow daily, are regular reports of new spyware programs arising.

While it is exceptionally difficult to obtain precise data on the prevalence of the spyware problem, the best study done to date, conducted by AOL and the Nation CyberSecurity Alliance, found that 80% of broadband and dial-up users had adware or spyware programs running on their computers.[4] Our perception based on the complaints we have received and our own research is that the prevalence of egregious spyware violations, including many mentioned in Section 2 of H.R. 29 before this Committee, has increased dramatically. Of particular concern is the use of security holes in web browsers to silently force software onto users computers. We believe many Internet users may simply be turning off the Internet in response to these threats.[5]

CDT was very pleased to see the first public enforcement action brought in October by the FTC against Samford Wallace and Seismic Entertainment on the basis of a complaint filed earlier by CDT.[6] This case included many of the clearly unfair and deceptive activities mentioned above, including browser hijacking and covert installation through security holes. We applaud the Commission for its work on the case, which has led to an injunction against further exploitative practices by Seismic.

The Commission's initial action against Seismic must be only the first step, however. First, many other parties were involved in the unfair and deceptive activities which CDT highlighted in our complaint to the FTC. We believe that the FTC's discovery in the Seismic case will provide ample basis to pursue these connections, and we expect that the Commission will announce further actions as other bad actors come to light. We discuss this affiliate issue in more detail below.

In addition, both the FTC and other national and state level law enforcement agencies must actively pursue further cases. While the FTC's first spyware case was an important milestone, both the number and frequency of cases must be dramatically increased if law enforcement is to provide a significant deterrent to purveyors of spyware. Currently, we believe law

---

[3] *See* http://www.cdt.org/action/spyware

[4] http://www.staysafeonline.info/news/safety_study_v04.pdf

[5] *See, e.g.* Joseph Menn, "No More Internet for Them," *Los Angeles Times*, January 14, 2005, p. A1.

[6] There were instances of *private* enforcement against spyware purveyors that preceded the FTC's case. For example, in July of last year, 180solutions, a large adware vendor, sued a distributor that was using security holes to force 180solutions' software onto Internet user's computers in order to collect per-install commissions.

enforcement is still losing the battle against egregious spyware purveyors clearly guilty of violating existing law.

3. The Affiliate Problem is at the Center of the Spyware Issue

In CDT's complaint to the FTC regarding Seismic Entertainment and Mail Wiper, we asked the FTC to specifically investigate the affiliate relationships between the parties involved. We highlighted the problem of affiliate relationship being "exploited by companies to deflect responsibility and avoid accountability."[7]

Since CDT testified before the Consumer Protection Subcommittee last year, it has become increasingly clear to us that the affiliate issue is at the heart of several aspects of the spyware problem. We want to take the opportunity in our testimony today to highlight and explain this issue, which has not been given sufficient attention to date.

Adware companies have a superficially simple business model: they provide a means of support for free software programs in a similar way that commercials support free television. Advertisers pay adware companies a fee to have their advertisements included in the adware program's rotation. The adware company then passes on a portion of that fee to distributors in exchange for bundling the adware program with other free software—such as gaming programs, screen savers, or peer-to-peer applications. Finally, the consumer downloads the bundle, agreeing to receive the advertising served by the adware program in exchange for the free software.

In fact, this simple description of how distribution of adware and other bundled software takes place is often a radical oversimplification. In fact, many adware companies and other software bundlers operate through much more complex networks of affiliate arrangements, which dilute

[7] *CDT Complaint Against MailWiper and Seismic* at 2.

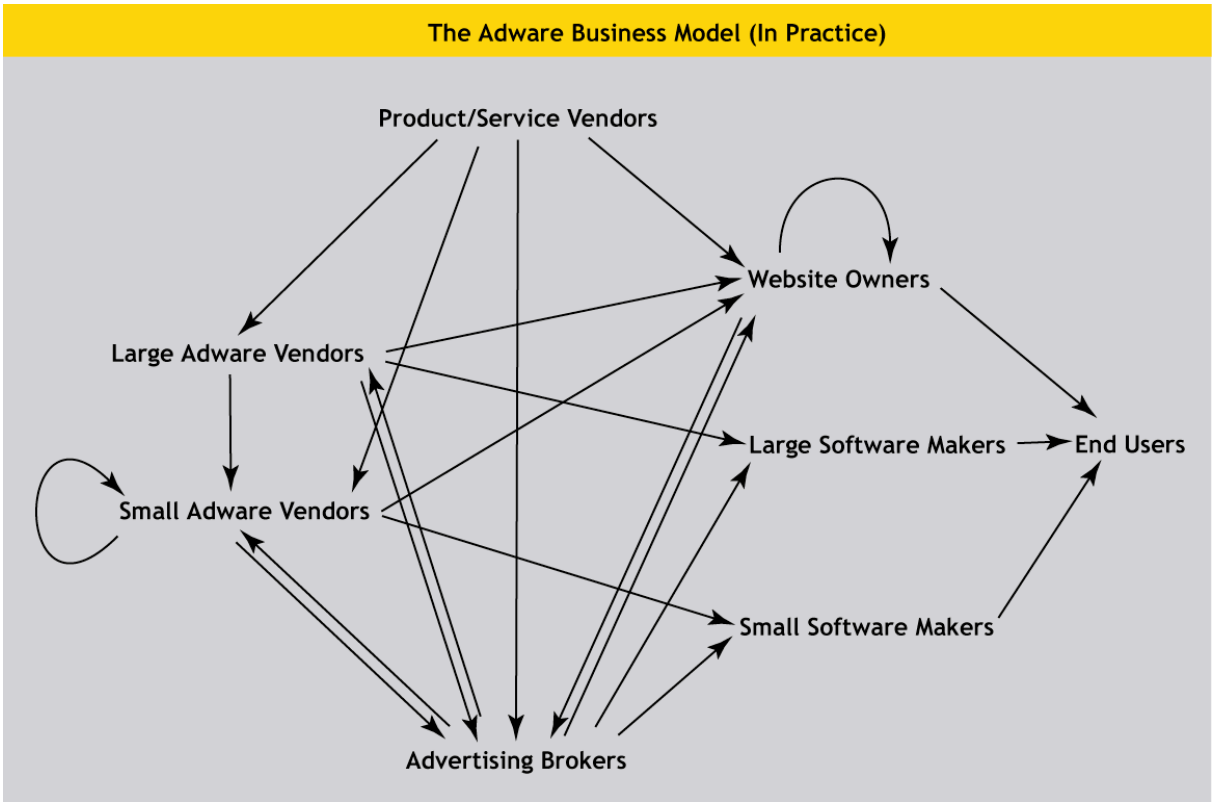
accountability, make it difficult for consumers to understand what is going on, and frustrate law enforcement efforts.

The diagram below presents some of the actors and relationships in the online advertising world as we currently understand it. These include:

- *product and service vendors*, who have contracts with adware vendors and advertising brokers to distribute ads for their offerings;
- *adware companies,* who have multi-tier affiliate arrangements with other adware companies, software producers, website owners, and advertising brokers;
- *software makers and website owners,* who enter into bundling and distribution agreements with adware companies and advertising brokers, as well as with other software makers and website owners; and
- *advertising brokers*, who serve as middlemen in the full array of affiliate arrangements.

The consequence of these ubiquitous affiliate arrangements is that when an adware program ends up on a user's computer, it may be many steps removed from the maker of the software itself. The existence of this complex network of intermediaries exacerbates the spyware problem in several ways. For example:

- *Industry Responsibility* – Adware companies, advertising brokers, and others all may disclaim responsibility for attacks on users' computers, while encouraging these behaviors through their affiliate schemes and doing little to police the networks of affiliates acting on their behalf. Advertisers, too, should be pushed to take greater



responsibility for the companies they advertise with.[8]

- *Enforcement* – Complex webs of affiliate relationships obstruct law enforcement efforts to track back parties responsible for attacks. The complexity of these cases puts an extreme strain on enforcement agencies, which struggle to tackle the problem with limited resources.
- *Consumer Notice* – Adware companies and their affiliates have been reluctant to clearly disclose their relationships in a way that is transparent to consumers. Appendix A excerpts a recent CDT submission to the FTC on this issue, demonstrating ways that adware companies could begin to improve transparency in bundling and ad-support arrangements. Companies have resisted these changes. Efforts to bring transparency to the full chain of affiliate and distribution arrangements have met with even greater opposition.

For these reasons, the affiliate issue has become a central aspect of the spyware epidemic. Finding ways to effectively reform affiliate relationships will remove a lynchpin of spyware purveyors' operations.

4. Comments on H.R. 29, the "SPY ACT"

H.R. 29, before this Committee, represents the outcome of an extended drafting effort to target bad practices and bring responsibility back to the distribution of downloadable software.

The overwhelming support for this bill in the last Congress demonstrates the desire to craft targeted legislation focusing on some of the specific problems raised by spyware. CDT commends Representatives Bono and the Committee for your work raising the profile of this formerly silent plague on our computers. The focus of this Committee has allowed consumer groups and companies to bring the attention of the public and law enforcement agencies to this issue.

The current bill marks a substantial step forward in addressing many of the concerns of consumer groups and companies and CDT is generally supportive of the current bill. In particular, CDT believes that Section 2's focus on bad practices and its increase of the penalties for violators will serve as a valuable deterrent. H.R. 29 will give the Federal Trade Commission the clear authority and explicit mandate to pursue spyware purveyors. To this end, CDT also strongly supports the reporting requirement under Section 7.

CDT has been more hesitant to embrace Section 3 of this bill. The notice and other requirements on adware and information collection programs raise extremely difficult definitional issues which, if handled wrong, could have unintended consequences in the regulatory process that could ultimately harm consumers.

For this reason, the bill may be well served by another round of input from a wide range of parties in order to limit unintended consequences—especially in Section 3, where H.R. 29

[8] Examples of steps in this direction include public policies by Major League Baseball and Verizon setting standards for what software companies they will advertise with. Similarly, Google has drafted a specific public policy on what other applications it will bundle its utilities with.

deviates from the effort to focus on bad practices. CDT still believes that it would be most effective to address notice and consent issues in a general online privacy bill rather than a software specific bill, but we understand the desire to attempt to address this acute concern first, despite the complexities involved. We look forward to working with the Committee on this process.

CDT main concern is actually not with the bill itself, but the political process to move the bill forward. We do not want to see the passage of this bill be used to diminish efforts by this Committee or others in Congress to address online privacy in a long-term and coherent way. Rather we hope that the current effort on spyware can provide a jumping off point for efforts to craft baseline standards for online privacy now that many companies have expressed their support for such a goal. Otherwise, we will simply be back in this same place when we confront the next privacy-invasive technology.

We have very much appreciated the Committee's hard work and openness to comment in the anti-spyware legislation process, and we look forward to continuing to work with you on this and other digital privacy issues.

Appendix A

Adware companies face a particular hurdle in making their operations and value proposition transparent to users because adware programs typically do not run at the same time as the applications they support. In general, adware programs display advertisements while the user is surfing the web, regardless of whether the bundled game or file-sharing program is even running. This behavior can obscure the connection between the adware program and its bundled affiliate.

As one way to help address this issue, CDT has pushed adware companies—and the software companies they bundle with—to implement co-branding, putting the names and logos of supported applications on all advertisements. Although advertisements would still appear to users out-of-context, separated from the applications they support, co-branding would at least provide an immediately visible indication of the connection between the advertisements users see and the applications those ads support.

The mock-ups below show some ways that co-branding might be implemented. CDT submitted these same examples to the FTC's workshop on peer-to-peer file sharing applications. Some of these examples demonstrate more consumer-friendly labeling than others, but they all illustrate the fundamental principle of creating a visible link between adware and their co-bundled partners. Co-branding is needed because notice and consent at the time of installation is not enough. The ongoing operations of adware programs must also be made transparent.

To date, no adware company of which we are aware co-brands its advertisements.

Without Co-branding
(Adware Supporting a Single Application):

With Co-branding:

Without Co-branding
(Adware Supporting a Single Application):

With Co-branding:

Without Co-branding
(Adware Supporting Multiple Applications):

With Co-branding: