

**Testimony of**  
**Ari Schwartz, Deputy Director**  
**Center for Democracy and Technology**  
**before**  
**The House Committee on Energy and Commerce**  
**Subcommittee on Commerce, Trade, and Consumer Protection**  
**on**  
**“Combating Spyware: H.R. 964, the Spy Act”**  
**March 15, 2007**

Chairman Rush and Ranking Member Stearns, thank you for holding this hearing on spyware, which continues to be a major problem for consumers and businesses alike. CDT is honored to have the opportunity to participate in the Committee’s hearing on this important topic.

CDT is a non-profit public interest organization dedicated to preserving and promoting privacy, civil liberties and other democratic values on the Internet. CDT has been a widely recognized leader in the policy debate about the issues raised by spyware.<sup>1</sup> Since CDT last testified before the Committee about spyware, in January 2005, the Federal Trade Commission has completed 11 spyware enforcement actions, three of which were based at least in part on petitions submitted by CDT. Over the past two years, CDT has also convened the Anti-Spyware Coalition (ASC), a group dedicated to building consensus about definitions and best practices in the debate surrounding spyware. The ASC’s work to create uniform language and guidelines that can be used across the software industry has been beneficial for both consumers and software makers.

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. We've worked with this

---

<sup>1</sup> For example, CDT leads the Anti-Spyware Coalition (ASC), a group of anti-spyware software companies, academics, and public interest groups dedicated to defeating spyware; In 2006, CDT Deputy Director Ari Schwartz won the RSA Award for Excellence in Public Policy for his work in building the ASC and other efforts against spyware. *See also* "Eye Spyware," *The Christian Science Monitor*, Apr. 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," *The New York Times*, Feb. 18, 2004 ["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 News.com*, Feb. 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."].

committee now for several years, and during that time we've been consistently impressed with its open, deliberative approach to this complex issue.

## **Summary**

Although we have seen advances in the fight against spyware, millions of consumers are still losing money, time and peace of mind to this online scourge. CDT believes that the necessary framework for combating spyware involves a combination of law enforcement, anti-spyware technology, industry self-regulation and consumer education, legislation, and increased responsibility on the part of advertisers.

On the law enforcement front, the number of spyware actions at the federal level has increased dramatically since this Committee reported spyware legislation during the 109<sup>th</sup> Congress. The FTC has had a successful run in pursuing spyware cases, but the Commission needs increased civil penalty authority in order to be comprehensively effective. H.R. 964 provides such authority.

Spyware enforcement has also been developing at the state level, with 10 cases across four states thus far. Although H.R. 964 safeguards state-level enforcement under consumer protection statutes, it does not explicitly preserve the ability for state attorneys general to bring civil actions under statutory provisions specific to spyware. With all of the enforcement work going on at the state level, we feel it is important to safeguard the role of state attorneys general by empowering them to help enforce federal law.

We remain firmly committed to the idea that a long-term solution to spyware and other similar issues requires baseline privacy legislation. General privacy legislation would provide businesses with guidance as they deploy new technologies and business models that involve the collection of information. At the same time, a baseline law would give consumers some measure of confidence that their privacy is protected as companies roll out new ventures.

There are now 13 major companies that have joined with consumer groups in support of baseline privacy legislation.<sup>2</sup> If we do not begin to address privacy issues more comprehensively, the same players will be back in front of this Committee in a few months to address the next emerging threat to online privacy. We hope that we can address these issues in a way that obviates the need to enact new legislation each time a new privacy threat arises.

## **I. Understanding and Combating the Spyware Problem**

When CDT last testified before this Committee about spyware, little data existed to quantify the size and impact of the spyware problem. Research conducted over the past two years, however, has produced some alarming results. Consumer Reports estimates

---

<sup>2</sup> See *Consumer Privacy Legislative Forum Statement of Support in Principle for Comprehensive Consumer Privacy Legislation*, June 2006, <http://www.cdt.org/privacy/20060620cplstatement.pdf>. General Electric announced its support after the statement was issued.

that spyware cost consumers \$2.6 billion last year and affected 1 in 8 Internet users.<sup>3</sup> An AOL/National Cyber Security Alliance study conducted in 354 homes found that 61% of users had spyware installed on their computers.<sup>4</sup> And the Pew Internet & American Life Project reported that nine out of ten Internet users say they have altered their behavior online due to fear of malicious software.<sup>5</sup> All of these figures indicate that while we have seen advances in the fight against spyware, it continues to be a problem for many consumers.

CDT has long endorsed a multi-faceted approach to the spyware problem. We believe that the appropriate framework incorporates the following components:

- *Anti-spyware technology* – Anti-spyware software is a consumer’s first defense against spyware infections. The collaboration fostered amongst technology vendors and public interest groups by the Anti-Spyware Coalition has helped to increase the usefulness of these technologies, which, in turn, creates a safer Internet experience for consumers.
- *Industry self-regulation and consumer education* – Helping industry and consumers understand the threat that spyware poses is an essential component of this framework. CDT has been active in the TRUSTe Trusted Download Program and the StopBadware campaign coordinated by Harvard’s Berkman Center. Both of these have helped consumers and companies better understand the spyware issue.
- *Responsible advertising* – Large, well-respected companies help to fund the spread of unwanted and harmful adware by paying for advertisements generated by those unwanted programs. The New York attorney general’s recent action against three high-profile advertisers,<sup>6</sup> along with public pressure from the FTC,<sup>7</sup> CDT,<sup>8</sup> and others has begun to increase advertiser awareness and accountability.

---

<sup>3</sup> “State of the net 2006,” *ConsumerReports.org*, Sept. 2006,

[http://www.consumerreports.org:80/cro/electronics-computers/online-protection-9-06/state-of-the-net/0609\\_online-prot\\_state.htm](http://www.consumerreports.org:80/cro/electronics-computers/online-protection-9-06/state-of-the-net/0609_online-prot_state.htm).

<sup>4</sup> *AOL/NCSA Online Safety Study*, America Online and the National Cyber Security Alliance, Dec. 2005, [http://www.staysafeonline.info/pdf/safety\\_study\\_2005.pdf](http://www.staysafeonline.info/pdf/safety_study_2005.pdf).

<sup>5</sup> Susannah Fox, *Spyware: The threat of unwanted software programs is changing the way people use the internet*, Pew Internet & American Life Project, July 6, 2005, [http://www.pewinternet.org/PPF/r/160/report\\_display.asp](http://www.pewinternet.org/PPF/r/160/report_display.asp).

<sup>6</sup> See *In the Matter of Priceline.com Incorporated* (filed Oct. 23, 2006); *In the Matter of Travelocity.com LP* (filed Dec. 18, 2006); and *In the Matter of Cingular Wireless LLC* (filed Jan. 29, 2007), all available at <http://www.oag.state.ny.us/press/2007/jan/adware-scannedAODs.pdf>.

<sup>7</sup> See, e.g., Cindy Skrzycki, “Stopping Spyware at the Source,” *The Washington Post*, Mar. 6, 2007 [“‘We need to stop the demand side of spyware,’ said Jon Leibowitz, one of the five [FTC] commission members and a Democrat. ‘We will send letters to major corporations and entities that place the majority of these ads. This is a wake-up call to put them on notice. That would be a good way to choke off the money.’”].

<sup>8</sup> See *Following the Money: How Advertising Dollars Encourage Nuisance or Harmful Adware and What Can be Done to Reverse the Trend*, Center for Democracy & Technology, May 2, 2006, <http://www.cdt.org/privacy/20060320adware.pdf>; and *Following the Money II: The Role of Intermediaries in Adware Advertising*, Center for Democracy & Technology, Aug. 2006, <http://www.cdt.org/privacy/20060809adware.pdf>.

- *Law enforcement* – The enforcement landscape has seen many changes over the past two years. The implications of these changes are discussed in section II below.
- *Legislation* – Legislative approaches to fighting spyware at the federal level fall into two broad categories – attempts to narrowly address the issues raised by spyware, and attempts to deal with the underlying privacy issues in a coherent, long-term fashion. H.R. 964, which we address in sections II and III below, is an example of the first approach. CDT has appreciated the opportunity to work with the Committee on this bill and is generally supportive of this effort, particularly because of the increased civil penalty authority it grants to the FTC for use in prosecuting spyware cases. At the same time, we remain firmly committed to the idea that a long-term solution to spyware and other similar issues requires baseline privacy legislation, as discussed in section IV below.

## **II. Spyware Enforcement and H.R. 964**

The spyware enforcement landscape looks vastly different than it did two years ago when CDT last expressed concern to the Committee about the lack of enforcement activity. When the Spy Act passed out of the House in 2005, the FTC had issued complaints against two spyware distributors and one state attorney general had sued one spyware company. As of this writing, the FTC has completed 11 spyware enforcement cases and four states have conducted a total of 10 spyware lawsuits.<sup>9</sup> The following sections explain the implications of FTC and state spyware enforcement for H.R. 964.

### *FTC Spyware Enforcement*

The FTC filed the nation’s first spyware lawsuit in 2004 against a network of deceptive adware distributors and their affiliates.<sup>10</sup> The scammers involved were secretly installing software that left consumers’ computers vulnerable to hackers, and then duping those same users into purchasing fake security software to help repair their systems. Not only did the FTC succeed in the case – obtaining a \$4 million order against the primary defendant and over \$300,000 in disgorgement from the other defendants – but the investigations in the case opened up several additional leads that contributed to the FTC’s pursuit of other malicious software distributors. In the more than two years since launching this first suit, the FTC has used its broad authority under Title 5 of the FTC Act to pursue cases that cover a wide range of malicious software behaviors, all of which have ended with settlements or court orders that benefit consumers.

The FTC’s enforcement efforts have also played an integral role in establishing standards for the software industry as a whole. In two of its most recent enforcement efforts, the

---

<sup>9</sup> See Appendix A for a summary of all FTC, state, and Department of Justice spyware enforcement actions.

<sup>10</sup> *FTC v. Seismic Entertainment, Inc., et al.*, No. 04-377-JD, 2004 U.S. Dist. LEXIS 22788 (D.N.H. Oct. 21, 2004).

FTC reached settlement agreements with major adware distributors Zango Inc. and DirectRevenue LLC that required the distributors to clearly and conspicuously disclose material terms about their adware programs *outside of any End User License Agreement (EULA)*.<sup>11</sup> With these requirements the FTC has set a disclosure guideline that can be applied across the software industry, for the benefit of consumers. Not only were the adware distributors themselves forced to abandon the practice of offering deceptive or nonexistent disclosures, but software vendors throughout the industry were also put on notice about what constitutes legitimate behavior. The FTC's leadership in this respect has helped to curb uncertainty in the software industry while creating a better online experience for consumers.

While these settlements set important precedents, the monetary relief obtained by the Commission was not commensurate with the harms perpetrated on consumers. Zango, a company that used deceptive tactics to earn over \$50 million in revenue in 2004 alone,<sup>12</sup> settled for a mere \$3 million with the FTC.<sup>13</sup> The founders of DirectRevenue have pocketed a combined \$23 million,<sup>14</sup> yet the FTC's proposed settlement requires only a \$1.5 million payment.<sup>15</sup> As FTC Commissioner Jon Leibowitz noted in his dissenting statement in the DirectRevenue case, these numbers are disappointing because they leave the owners of the adware companies "lining their pockets . . . from a business model based on deceit."<sup>16</sup>

The increased civil penalty authority granted by H.R. 964 provides the FTC with the means to obtain more appropriate monetary relief. By giving the FTC explicit authority to seek large civil penalties for spyware infractions, the Commission will be much less encumbered and much more willing to obtain monetary relief commensurate with the harms committed. Both CDT and officials at the FTC have long been supportive of increased penalties, and we are pleased to see them included in H.R. 964.

### *State Spyware Enforcement*

Several state attorneys general have become active in challenging spyware purveyors under state consumer protection, trespass, business practices, and spyware laws. In some of these cases the state attorneys general have taken the lead in nabbing high-profile offenders. For example, Texas took swift action against Sony BMG after it was

---

<sup>11</sup> See *In the Matter of Zango, Inc., formerly known as 180solutions, Inc., Keith Smith, and Daniel Todd*, FTC File No. 052 3130 (filed Nov. 3, 2006), available at <http://www.ftc.gov/os/caselist/0523130/index.htm>; *In the Matter of DirectRevenue LLC, DirectRevenue Holdings LLC, Joshua Abram, Daniel Kaufman, Alan Murray, and Rodney Hook*, FTC File No. 052 3131 (filed Feb. 16, 2007), available at <http://ftc.gov/os/caselist/0523131/index.htm>.

<sup>12</sup> "Inc. Magazine Reveals America's 500 Fastest Growing Private Companies," Zango Inc., Nov. 1, 2005, <http://www.zango.com/Destination/Corporate/ReadArticle.aspx?id=36>.

<sup>13</sup> See *supra* note 11.

<sup>14</sup> Ben Elgin and Brian Grow, "The Plot to Hijack Your Computer," *BusinessWeek*, July 17, 2006, [http://www.businessweek.com/magazine/content/06\\_29/b3993001.htm](http://www.businessweek.com/magazine/content/06_29/b3993001.htm).

<sup>15</sup> See *supra* note 11.

<sup>16</sup> *Dissenting Statement of Commissioner Jon Leibowitz In Re DirectRevenue LLC, et al., File No. 052 3131*, Feb. 16, 2007, <http://www.ftc.gov/os/caselist/0523131/0523131directrevenueleibowitzstmnt.pdf>.

discovered that the company had distributed millions of audio CDs containing spyware, and New York launched the nation's first investigation into DirectRevenue, nearly a year before the FTC announced its settlement with the company. That litigation is still pending.

This growth in spyware enforcement at the state level in particular has several implications for H.R. 964. All of the state spyware cases have invoked state consumer protection laws, and thus we are pleased that Section 6(a)(2)(B) safeguards the authority of state attorneys general to challenge spyware practices under consumer protection statutes. What H.R. 964 does not safeguard, however, is the ability for state attorneys general to bring civil actions under statutory provisions specific to spyware. H.R. 964 preempts state spyware statutes without giving state attorneys general explicit authority to bring civil actions under the new federal law.

Six out of the 10 state spyware cases have invoked state spyware laws. If these state-level laws were to be replaced with a single federal standard, we feel it would be important to preserve the role of state attorneys general by empowering them to help enforce federal law. We understand that adding authority for state attorneys general raises jurisdictional issues, but we feel that this vital component of spyware enforcement must be addressed.

### **III. Comments on Specific H.R. 964 Language**

CDT has minor suggestions on two specific parts of the bill.

First, CDT believes that Section 4(b) of H.R. 964, which gives the FTC explicit authority to seek civil penalties for pattern or practice violations of the Spy Act, will effectively increase the deterrent effect of spyware enforcement. However, it is important for the statute to be clear about what constitutes a "single action or conduct" in violation of the Act, because each single action or conduct carries either the \$3 million or \$1 million penalty as described in Section 4(b)(1). For example, DirectRevenue is a company that distributed similar software under a handful of different names and through dozens of different distribution channels and schemes. Had the FTC been able to bring its case against DirectRevenue under the Spy Act, we would hope that each of the different software distributions would be considered a "single action or conduct," and thus the civil penalty sought by the FTC could be commensurate with the harm caused. We believe this clarification – that software provided by a single entity using multiple versions, configurations, or distributions can cause multiple violations – may be appropriately addressed in the Committee Report for H.R. 964.

Second, the definition of "personally identifiable information" provided in Section 11(13)(A) includes a list of different types of information that may be used to identify a living individual. An email address is one piece of information in this list, but in some cases email addresses cannot be used to determine the "real world" identity of particular individuals. Thus, some interpretations of this language could exempt email addresses from the definition of personally identifiable information. We believe that this would be a mistake, and we suggest that in Section 11(13)(A) the phrase "allows a living individual

to be identified” should be replaced with “allows a living individual to be identified *or contacted*.” This will ensure that email addresses are considered as part of PII, since a person can generally be contacted via email even if the email address does not identify the person.

#### **IV. General Privacy Legislation and H.R. 964**

Since our first testimony on this issue, we have urged the Committee to consider how some provisions of the Spy Act may be better addressed in baseline consumer privacy legislation. In light of the growing momentum behind this effort and the numerous other consumer and government privacy issues facing this Congress, we hope that the Committee will revisit these issues. For example, Section 3(c)(1)(B) of H.R. 964 prescribes specific notice language for software. Given the influence that H.R. 964 may have on the broader privacy debate, we have misgivings about a notice approach that specifies disclosure language in statute. Addressing notice at this level of detail in this bill could risk conflicting with or establishing difficult precedents for more general notice provisions in a broader privacy law.

A comprehensive privacy law may also address behaviors that have been omitted by the specificity of H.R. 964. For example, Section 3(b)(1)(B) includes in the definition of “information collection program” computer software that collects information about Web pages accessed on the computer and uses such information to display advertising on the computer. The statute does not, however, cover computer software which is used to collect information about Web pages accessed where that information is later disclosed to a third party but not directly used for advertising purposes. A broader privacy bill could help plug such gaps in H.R. 964.

#### **V. Conclusion**

CDT would like to thank the Committee for its hard work and openness throughout the spyware legislation process. While we believe H.R. 964 provides valuable increases to FTC civil penalty authority, we have several concerns with the bill. These include the bill’s pre-emption of state-level enforcement in an area where states are proving effective and interstate commerce has not been negatively affected, and the bill’s potential impact on the process of crafting and implementing general privacy legislation. We look forward to continuing to work with the Committee in addressing these issues and developing the strongest possible framework to protect consumer privacy in the digital age.