The Federal Trade Commission

Remarks of Deborah Platt Majoras[1]
Chairman, Federal Trade Commission
Anti-Spyware Coalition
February 9, 2006

"Finding the Solutions to Fight Spyware: The FTC's Three Enforcement Principles"

Thank you. I am pleased to be here today for the Anti-Spyware Coalition's first public meeting, and I thank the Center for Democracy and Technology, which convened the Anti-Spyware Coalition, for inviting me. CDT has been an important advocate for consumers on technology issues in general and on spyware issues in particular. In another "first," my remarks this morning will be available on the first-ever FTC podcast and downloadable video file.

The FTC's mission is to protect consumers from unfair or deceptive practices whether they occur through old or new technologies. However, making predictions about the nature, timing, and effect of new technologies can be humbling. In 1943, for example, Thomas Watson, then-Chairman of IBM, offered his insight that "there is a world market for maybe five computers." Of course, Mr. Watson's prediction seems a bit more reasonable when one recalls that six years later, *Popular Mechanics* magazine reported the hope that "computers in the future

[1] The views expressed herein are my own and do not necessarily represent the views of the Federal Trade Commission or of any other individual Commissioner.

may have only 1,000 vacuum tubes and weigh only 1.5 tons."

If Mr. Watson were here today, I am certain that he would agree that technological advances and uses – whether beneficial or harmful – are difficult to predict. The development and widespread deployment of spyware is no exception. In 1995, the Commission held hearings for government policymakers to consider the risks presented by rapidly evolving technologies such as the Internet and to formulate policies to address these risks.[2] We gathered more than 70 experts from the fields of law, business, technology, economics, and consumer protection to help us evaluate the consumer protection challenges of the future. Time has shown that these experts showed great foresight. But interestingly, at those hearings, no one even mentioned spyware or similar intrusive software. Today, however, spyware is fast overtaking spam as consumers' top online concern.

It is understandable that the hearing participants did not predict the emergence of this digital menace called spyware.[3] Ten years now is an eternity for technology, and the technological underpinnings for spyware were just being developed at about the time of the FTC's hearings.

Today, while the problem of spyware is more clearly understood, finding the best

---

[2] The staff report entitled "Anticipating the 21st Century: Consumer Protection Policy in the New High-Tech, Global Marketplace: A Report by Federal Trade Commission Staff," can be found at http://www.ftc.gov/opp/global/report/gc_v2.pdf.

[3] Consider these quotes from the Report: "Consumer transactions online soon may become routine." Report at Page 2. "Telephone technologies soon may give consumers the ability to block calls they do not want to receive, specify calls they will receive, and identify businesses that are calling." Report at Page 3. "While it seems certain that the Internet will grow dramatically in the next 10 years, few are willing to predict exactly how the new marketplace will develop." Report at Page 25.

solution remains a challenge. Here, the four principal lessons of the 1995 hearings are still germane. First, we must study and evaluate new technologies so that we are as prepared as possible to deal with harmful, collateral developments. Second, we need to bring appropriate law enforcement actions to reaffirm that fundamental principles of FTC law apply in the context of new technologies. Third, we must look to industry to implement self-regulatory regimes and, more importantly, to develop new technologies. Finally, we need to educate consumers so that they can take steps to protect themselves.

Policy Development

At our 1995 hearings, CDT's co-founder Jerry Berman urged us to build the "intellectual capital" we need to do our jobs before wading into technology issues. Consistent with this advice, and the Commission's longstanding approach to technology issues, one of our first steps in responding to spyware and other problems arising from new technology has been to educate ourselves in order to develop, implement, and advocate effective policies. Thus, in 2004, the FTC sponsored a public workshop entitled "Monitoring Software on Your PC: Spyware, Adware, and Other Software," and in March 2005, we released a staff report based on the information received in connection with the workshop.[4] We have also discussed spyware as a

[4] The agency received almost 800 comments in connection with the workshop, and 34 representatives from the computer and software industries, trade associations, consumer advocacy groups and various governmental entities participated as panelists. The workshop agenda, transcript, panelist presentations, and public comments received by the Commission are available at http://www.ftc.gov/bcp/workshops/spyware/index.htm. The FTC Staff Report, Monitoring Software on Your PC: Spyware, Adware, and Other Software, released Mar. 2005, is available at http://www.ftc.gov/os/2005/03/050307spywarerpt.pdf.

significant consumer protection issue in various public fora.[5]

The Report recommended that the private sector and government act separately and in concert to combat the scourge of spyware. The Report included three specific recommendations for private entities: (1) assistance with law enforcement efforts, (2) expansion of consumer education efforts, and (3) the development both of new technologies to protect consumers and of standards for defining spyware and disclosing information about it. The Report also included three specific recommendations for the government: (1) increased law enforcement, (2) expanded consumer education efforts, and (3) encouragement of technological solutions. The agenda for today's conference – which includes discussions about corporate responsibilities, technology, education, industry self-regulation, and enforcement – suggests that the Report's recommendations were well-developed, and we are eager to hear your thoughts on these important issues.

Law Enforcement

One of the principal conclusions of the FTC's spyware report was that spyware presents consumer protection issues similar to those posed by more traditional technologies, and that active enforcement of consumer protection laws is an important step to prevent the spread of spyware. Our report also found that many of the most troubling aspects of the spyware problem raised issues under existing consumer protection laws.

Using the FTC Act's grant of broad authority to challenge unfair or deceptive acts and

---

[5] *See, e.g.*, "Protecting Markets and Consumers in a High-Tech World," Remarks of Deborah Platt Majoras before the Software Information Industry Alliance, February 1, 2005, *available at* http://www.ftc.gov/speeches/majoras/050201protectingmarkets.pdf.

practices,[6] the Commission launched an aggressive law enforcement program to fight spyware. To be sure, spyware presents serious new challenges in detection, apprehension, and enforcement. But through litigation, the FTC has successfully challenged the distribution of spyware that causes injury to consumers in the online marketplace.[7]

These law enforcement actions reaffirm three key principles about spyware. First, a consumer's computer belongs to him or her, not to the software distributor. Second, buried disclosures do not work, just as they have never worked in more traditional areas of commerce. And third, if a distributor puts a program on a consumer's computer that the consumer does not want, the consumer must be able to uninstall or disable it.

The first principle reflects the basic common-sense notion that Internet businesses are not free to help themselves to the resources of a consumer's computer. The principle is reflected in the FTC's first spyware case, *FTC v. Seismic Entertainment.*[8] In that case, the Commission alleged that the defendants exploited a known vulnerability in Internet Explorer to download spyware to users' computers without their knowledge. Specifically, the complaint alleged that the defendants used "drive-by" tactics[9] to install their software, which, among other things,

---

[6] 15 U.S.C. § 45.

[7] The FTC has also successfully challenged the bogus claims of purported anti-spyware companies that they remove "any and all" spyware from consumers' computers. *See FTC v. MaxTheater, Inc. et al*, No.: 05-CV-0069 (E.D. Wash. March 8, 2005); *FTC v. Trustsoft, Inc., et al.*, Civ. No. H 05 1905 (S.D. Tex May 31, 2005).

[8] *FTC v. Seismic Entertainment, Inc., et al.,* No. 04-377-JD, 2004 U.S. Dist. LEXIS 22788 (D.N.H. Oct. 21, 2004).

[9] "Drive-by" tactics typically involve exploiting security vulnerabilities to install software automatically onto users' computers without generating any notice to the computer users.

[11] *FTC v. Odysseus Marketing, Inc.*, No. 05-CV-330 (D.N.H. filed Sept. 21, 2005).

advertising. The Commission recently issued a final consent order to resolve administrative complaint allegations that this failure to disclose adequately was deceptive in violation of Section 5 of the FTC Act. The settlement requires the respondents to disclose clearly and prominently any adware bundled with software advertised to enhance security or privacy.

The third principle, that if a distributor puts a program on a computer that the consumer does not want, the consumer should be able to uninstall or disable it, is underscored in the *Odysseus* case. The *Odysseus* complaint alleged that consumers could not uninstall the harmful software that Odysseus downloaded (and which

can play.

There is some good news here. Technology is already moving forward. For example, some operating systems and browsers are including tools that help protect consumers' computers from unauthorized software downloads. Companies offering anti-spyware software, including many of those who are here today, have made significant efforts to improve their products' scanning capabilities, and are working to detect and prevent unauthorized software downloads. And Internet Service Providers are offering anti-spyware services to their members. In recognition of the importance consumers now are placing on the security of their computers, we are seeing companies compete on the basis of security packages. I applaud the efforts that industry has made to develop and deploy new technologies to combat spyware, and I hope that these efforts are just the beginning.

Industry Self-Regulation

Industry self-regulation has the potential to become an important complement to technological development and government action in this area. Not surprisingly, the challenge for self-regulation has been defining with sufficient precision what is considered to be "spyware" and should be, therefore, subject to prohibitions and limitations. Recently, there have been some promising initial developments in industry self-regulation, and these developments may ultimately benefit consumers as well as businesses.

The efforts of the Anti-Spyware Coalition are one example. As everyone here appreciates, there are currently substantial disputes between anti-spyware companies and other software developers about how to define spyware. The FTC's Report from the 2004 Spyware Workshop recognized the difficulty in reaching a definition. The stated goal of the Anti-

Spyware Coalition is to make clear what anti-spyware companies consider to be spyware. Other initiatives are also seeking to help define spyware. For example, Trust-E's Trusted Download Program plans to create a "whitelist" of programs that meet the organization's standards, while the Stopbadware.org initiative intends to create a "blacklist" of programs that do not meet that group's standards. Such efforts, and in particular the efforts to be inclusive, may be useful first steps towards meaningful industry self-regulation.

In the adware context, the question of disclosure – whether the consumer has been notified adequately of, and consented to, the installation of a particular adware program – has been a key issue. Trust-E's Trusted Download Program is intended to create a notice regime to address the issue. Also, the Interactive Travel Services Association and the Board of the Direct Marketing Association recently adopted guidelines that address how to disclose that adware will be installed.

Without endorsing any particular approach or definition, I can state that these initial anti-spyware self-regulatory developments are promising. Self-regulation can be prompt, flexible, and responsive – characteristics that are very important where the market changes as rapidly as this one does. Self-regulation can also be based on the judgment and experience of industry members who are likely able to devise workable rules. Industry support and participation are key to any self-regulatory regime, and the level of participation and support in these new anti-spyware efforts will ultimately determine their effectiveness.

Consumer Education

Consumers also have a critical role in combating spyware and other technology problems. But if they are to play that role, it is essential for them to be informed. In October

2004, the FTC issued a publication that detailed what consumers can do to reduce their risk of having spyware downloaded to their computers. It also lists clues that may notify consumers that they have spyware and explains what consumers can do to get rid of spyware.

But spyware is simply one part of a larger picture of computer security risks. Rather than

States Senate. We are pushing for its enactment, so that we will not be hampered in our cross-border investigations; certainly spyware purveyors are not so hampered. This afternoon Maneesha Mithal, Acting Associate Director of the FTC's Division of International Consumer Protection, will provide a more detailed discussion of this legislative proposal.

2006 Hearings on Global Marketing and Technology

As I stated earlier, a decade has passed since the FTC held hearings to identify significant consumer protection issues associated with ne