Remarks by Commissioner Orson Swindle
Federal Trade Commission

Monitoring Software on Your PC: Spyware, Adware, and Other Software

Washington, D.C.
April 19, 2004

Good morning and welcome to the FTC's spyware workshop. Unfortunately, I am not able to be at the workshop today; but I nevertheless want to share some thoughts with you concerning the workshop, with particular emphasis on the questions that spyware raises concerning online security and privacy.

As it has in the past, the FTC finds itself gathering information about another new Internet development and its impact on consumers, to determine the appropriate course of action.

- Over the past decade, the FTC has used workshops and hearings as the first step in dealing with novel and evolving online technologies and practices.

- Once we have learned more about an online technology or practice, we have encouraged industry self-regulation; pursued targeted law enforcement actions; and used consumer education to address the problems that exist or may be on the horizon.

- We have followed this model for many online technologies and practices, such as online privacy, the online privacy of children, and spam.

- This workshop is a similar first step to confront spyware.

We have ample experience on which to draw in looking at the privacy and security risks that spyware may pose for businesses and consumers.

- The FTC has been in the forefront of privacy and security issues, working with industry to develop best practices and bringing legal actions where companies violated their privacy policies or failed to adopt reasonable security measures.

- The FTC has an aggressive track record of working with industry and consumer groups to understand and explore potential online security issues, such as workshops last summer relating to the protection on personal information and convening an online security advisory committee in early 2000.

We have undertaken a variety of consumer and business education efforts to promote online security. These include:

- The "Dewie the Turtle" comprehensive awareness campaign to make businesses and consumers aware of and protect themselves from online security vulnerabilities.

- "Operation Secure Your Server" — an international effort to contact and educate operators of servers left open to unauthorized use by spammers.

Our effort today is to assess the privacy and security risks of spyware.

A survey of broadband users released last summer by the National CyberSecurity Alliance found that over 90% of consumers had some form of adware or spyware on their computers, and most consumers were not aware of it.

The next two panels will focus on the extent to which the increasing prevalence of spyware poses privacy and security risks for consumers.

The security panel will address some very important questions.

- What is the impact of spyware on computer resources? And what effect does this have on a consumer's ability to use his or her computer?

- To what extent do spyware programs hijack the browsers of computers?

- Do spyware programs pose security hazards, and if so, what are they?

- Can spyware capture a computer and use it for its purposes — for example, to send out spam?

- Do spyware programs when bundled with file sharing software, pose any unique security concerns?

- Does spyware raise similar or different security risks for consumers as it does for businesses?

The privacy panel will discuss questions such as:

- What type of information about users does spyware collect?

- Is the information collected on an aggregated or an individual basis?

- Is the information collected used primarily to display targeted ads?

- Is keystroke information being captured and has it been or could it be used in identity theft?

The debate that has ensued about spyware reminds me of the early dialogue we had about privacy policies, that was filled with a lot of emotion and calls for regulation.

As a result of a continuing and energetic dialogue between industry, government, and consumer groups, industry responded to the public's demand for greater disclosure and better privacy notices — without legislation. Today, almost 100% of the most frequently visited websites offer some form of privacy notice.

I believe we have made greater progress in finding solutions to privacy concerns than if there was simply static legislation attempting to address the problem.

As we go forward, we must keep in mind the unintended consequences of regulation. The challenge with spyware is to seek effective solutions that address consumer concerns without unnecessarily burdening legitimate software developers or hindering innovation.

This workshop is asking the right questions at the right time. I regret that I am not able to attend and hear the discussion. However, I am confident that we will have a lively and informative discussion that will help government, industry, and consumers to find focused and effective ways to address spyware.