STATEMENT OF FTC COMMISSIONER MOZELLE W. THOMPSON
Before the United States House Committee on Energy and Commerce
for Testimony on Spyware
April 29, 2004

Good morning, Chairman Stearns, Ranking Member Schakowski and members of the Committee, I am Commissioner Mozelle Thompson of the FTC and I wish to thank the Committee holding this hearing on the important subject of spyware. I also appreciate the opportunity to appear before you today.[1]

As you know, the FTC has long been involved with Internet issues such as online privacy, identity theft, cross-border fraud, and spam. We were one of the first agencies in the world to bring consumer protection law enforcement actions in this context and to date, the Commission has brought over 300 Internet-related cases (*i.e.*, cases that involve an Internet product or service or where a company initially contacts or a consumer initially responds using the Internet). Along with technological advances, we have seen an increase in the sophistication of data gathering techniques. This technology can be used to benefit consumers, or to do them harm. Our experience has given us a unique vantage point to view important developments in the consumer marketplace and identify issues that warrant public attention.

---

[1] The views expressed here are my own and not necessarily those of the Commission or other Commissioners.

Last week, the Commission held a one-day public workshop on one of these topics - - the distribution and effects of software commonly referred to as "spyware." We held this workshop for three reasons: First, to learn more about what spyware is and what is does; second, to bring together experts and interested parties to share information and discuss solutions to problems associated with spyware; and third, to create opportunities for industry to develop consumer supportive, and effective self-regulatory responses that will deal with the problems spyware creates while, at the same time, preserving its benefits.

In my opinion, the workshop successfully achieved these goals. But the workshop's overall value as a starting point for addressing problems raised by spyware will rest upon future actions taken by industry, government and consumers together.

We began our workshop by asking participants to define what spyware is. The term "spyware" commonly refers to software that essentially monitors consumers' computing habits. As such, it necessarily raises privacy issues. This software can offer consumers and businesses various benefits, including a streamlined, interactive online experience, and can allow businesses to more

effectively communicate with their customers. However, spyware can also be used as "secret software" that surreptitiously gathers information and transmits it to a third party without the subject's knowledge or consent. Sometimes these uses can result in identity theft and other types of fraud and, in some cases, can interfere with a computer's operability. Such activities undermine consumer confidence in the online marketplace. They can also impose extra costs on good actors who are forced to compete against those willing to engage in deception, fraud or worse.

The FTC's workshop was a watershed event because it put a public face on what some see as a hidden issue. It gave government, industry and consumers the opportunity to talk about the good as well as the bad that can come from the use of spyware. The workshop also identified some steps that industry, government and individuals can take to ensure that consumers have a safe, secure and enjoyable online experience.

To that end, I used the workshop as an opportunity to issue a challenge to industry to promptly develop a set of "best practices" with respect to spyware. These best practices should contain several critical elements, including meaningful notice and choice so that consumers can make informed decisions about whether they wish to deal with an online business that uses monitoring software, or partners with companies that do. I also asked industry to develop a public campaign to

educate consumers and businesses about what spyware is and how it operates. This public campaign should also discuss the array of technological tools available for consumer use. Finally, I called upon industry to establish a mechanism that will allow businesses and consumers to maintain a continuing dialog concerning how government can take action against those who do wrong and undermine consumer confidence through misuse of spyware.

Some members of Congress, including Representative Bono, have called for spyware legislation. I understand the desire to take action before the problems associated with spyware grow worse and injure more consumers and businesses. But I do not believe that legislation is the answer at this time.

Instead, I respectfully submit that we should give industry an opportunity to respond to my challenge. My experience at the Commission working on issues like online privacy and spam tells me that, in approaching such problems, any solution must at the very least be based upon transparency, adequate notice and consumer choice.

So, I have used my challenge as a way to set out what I consider to be the critical elements that should form a baseline for any industry response. If the self-regulatory response is not timely or is inadequate, a legislative approach might be appropriate. In any event, any legislation in this area should work in conjunction

with existing laws like the Federal Trade Commission Act, which allows the Commission to stop deceptive or unfair practices. For example, the FTC's existing Section 5 authority allows us to pursue actions against those who use spyware, or other means, to engage in identity theft, or to collect personal information in violation of a company's privacy policy.

I make this suggestion with some circumspection, recognizing that some would like Congress to act right now. However, absent a comprehensive data privacy law in the United States, and recognizing the challenge posed by defining spyware, I believe that self-regulation combined with enforcement of existing laws, will help to address many of the issues raised in this area. I am also aware that some States might be anxious to legislate here. But, I ask them to be cautious as well. A patchwork of differing and inconsistent State approaches would be confusing to industry and consumers alike, and thus, might increase the need for federal legislation.

Finally, as I mentioned, spyware raises important privacy concerns. Several years ago, I appeared before Congress and suggested that a federal law incorporating well known, fair information practice principles of notice, choice, access, security and enforcement, might be an acceptable legislative response. I believe it may still be. For the time being, however, strong, responsible and

prompt industry self-regulation may help to provide an effective solution for the problems that spyware poses for both consumers and industry.