Prepared Statement of
The Federal Trade Commission

Before the

Committee on Energy and Commerce
Subcommittee on Commerce, Trade, and Consumer Protection
United States House of Representatives

To encourage broad-based participation, the FTC issued a Federal Register Notice announcing the workshop and requesting public comment.(4) The Commission received approximately 200 comments, and the record will remain open until May 21, 2004, for submission of additional comments. At the workshop, a wide range of panelists engaged in a spirited debate concerning spyware, including what government, industry, and consumers ought to do to respond to the risks associated with spyware.

Although the agency is continuing to receive information on this important issue, the record at the workshop leads to some preliminary conclusions. First, perhaps the most challenging task is to carefully and clearly define the issue. "Spyware" is an elastic and vague term that has been used to describe a wide range of software.(5) Some definitions of spyware could be so broad that they cover software that is beneficial or benign; software that is beneficial but misused; or software that is just poorly written or has inefficient code. Indeed, there continues to be considerable debate regarding whether "adware" should be considered spyware. Given the risks of defining spyware too broadly, some panelists at our workshop argued that the more prudent course is to focus on the harms caused by misuse or abuse of software rather than on the definition of spyware.

Panelists described a number of harms caused by spyware. These include invasions of privacy, security risks, and functionality problems for consumers. For example, spyware may harvest personally identifiable information from consumers through monitoring computer use without consent. Spyware also may facilitate identity theft by surreptitiously planting a keystroke logger on a consumer's personal computer. It may create security risks if it exposes communication channels to hackers. Spyware also may adversely affect the operation of personal computers, including slowing processing time and causing crashes, browser hijacking, home page resetting, installing dialers, and the like. These harms are problems in themselves, and could lead to a loss in consumer confidence in the Internet as a medium of communication and commerce.

Many of the panelists discussed how spyware may cause problems for businesses. Companies may incur costs as they seek to block and remove spyware from the computers of their employees. Employees will be less productive if spyware causes their computers to crash or they are distracted from their tasks by a barrage of pop-up ads. Spyware that captures the keystrokes of employees could be used to obtain trade secrets and other confidential information from businesses. In addition, representatives from companies such as ISPs, PC manufacturers, anti-virus providers, and an operating system manufacturer indicated that they spend substantial resources responding to customer inquiries when PCs or Internet browsers do not work as expected due to the presence of spyware. As such, these companies also may suffer injury to their reputations and lose good will.

Because of the relatively recent emergence of spyware, there has been little empirical data regarding the prevalence and magnitude of these problems for consumers and businesses. Given how broadly spyware can be distributed and the severity of some of its potential risks, government, industry, and consumers should treat the threats to privacy, security, and functionality posed by spyware as real and significant problems.

At the workshop, we heard that substantial efforts are currently underway to address spyware.

6. Panelists at the workshop noted that consumers need to be very careful to obtain anti-spyware programs from legitimate providers because some purported anti-spyware programs in fact disseminate spyware.

7. The Commission will find deception if there is a material representation, omission, or practice that is likely to mislead consumers acting reasonably in the circumstances, to their detriment. *See* Federal Trade Commission, Deception Policy Statement, *appended to Cliffdale Assocs., Inc.*, 103 F.T.C. 110, 174 (1984) ("Deception Statement"). An act or practice is "unfair" if it causes or is likely to cause substantial injury to consumers, that injury is not outweighed by any countervailing benefits to consumers and competition, and consumers could not have reasonably avoided the injury. 15 U.S.C. § 45(n).

8. Identifying the source of spyware is especially difficult ou4