FEDERAL TRADE COMMISSION

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

AGENCY: Federal Trade Commission (FTC).

ACTION: Notice Announcing Public Workshop and Requesting Public Comment

SUMMARY: The FTC is planning to host a public workshop, "Monitoring Software on Your PC: Spyware, Adware, and Other Software," to explore the issues associated with the distribution and effects of software that aids in gathering information about a person or organization without their knowledge and which may send such information to another entity without the consumer's consent, or asserts control over a computer without the consumer's knowledge.

DATES: The workshop will be held on April 19, 2004, from 8:30 a.m. to 5:30 p.m. at the Federal Trade Commission's Satellite Building located at 601 New Jersey Avenue, N.W., Washington, D.C. The event is open to the public and there is no fee for attendance. Pre-registration is not required.

REQUESTS TO PARTICIPATE AS A PANELIST: As discussed below, written requests to participate as a panelist in the workshop must be filed on or before Friday, March 5, 2004. Persons filing requests to participate as a panelist will be notified on or before Friday, March 19, 2004, if they have been selected.

WRITTEN AND ELECTRONIC COMMENTS: Whether or not selected to participate, persons may submit written or electronic comments on the topics to be discussed by the panelists. Such comments must be filed on or before Friday, March 19, 2004. For further instructions on submitting comments, please see the "ADDRESSES" and the "Form and Availability of Comments" sections below. To read our policy on how we handle the information you submit, please visit www.ftc.gov/ftc/privacy.htm.

ADDRESSES: Comments and requests to participate as a panelist in the workshop filed in paper form should be mailed or delivered, as prescribed in the "Form and Availability of Comments" sections below, to the following address: Federal Trade Commission/Office of the Secretary, Room 159-H (Annex B), 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580. Because paper mail in the Washington area and at the Agency is subject to delay, please consider submitting your comments via electronic mail. Comments and requests to participate filed in electronic form (except comments and requests containing any confidential material) should be sent, as prescribed in the "Form and Availability of Comments" section below, to the following email box: spywareworkshop2004@ftc.gov. All federal government agency rulemaking initiatives are also available online at http://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: Beverly Thomas, 202-326-2938, Dean Forbes, 202-326-2831, or David Koehler, 202-326-3627, Division of Advertising Practices, Federal Trade Commission. The above staff can be reached by mail at: Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington, DC 20580. A detailed agenda and additional information on the workshop will be posted on the FTC's website, at www.ftc.gov/bcp/workshops/spyware/index.htm, by Friday, March 19, 2004.

SUPPLEMENTARY INFORMATION:

Background and Workshop Goals

The FTC has addressed online privacy and security issues affecting consumers for nearly a decade. Through a series of workshops and hearings, the Commission has sought to understand the online marketplace and its information practices, to assess the impact of these practices on consumers, and to encourage and facilitate effective self-regulation. The Commission's efforts include bringing industry and consumer and privacy advocates together to address online privacy and security issues and challenging industry leaders to develop and implement meaningful self-regulatory programs. The Commission has also undertaken a wide variety of education and civil enforcement initiatives to reduce the harms caused by the disclosure of personal information, such as identity theft, violations of privacy promises, and breaches of customer databases.

As part of these ongoing efforts, the Commission is announcing a workshop designed to explore the issues surrounding the distribution and effects of software, sometimes identified as "spyware," that aids in gathering information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge. The Commission is especially interested in the issue of spyware disseminated through peer-to-peer software because of the widespread use of peer-to-peer file-sharing software among young people who may download it to their families' computers without their parents' knowledge.

Questions to be addressed at the workshops may include:

A. Defining and Understanding Spyware

- What types of software (particularly downloaded software) should be considered "spyware"?

- How is adware different from spyware?

B. Distribution of Spyware

- How is spyware distributed?
- What role does peer-to-peer file-sharing play in the distribution of spyware?
- To what extent is spyware bundled with other software, especially freeware?
- Do consumers know that spyware is being placed on their personal computers?
- How does spyware operate once it has been placed on a personal computer?

C. The Effects of Spyware

- Does spyware affect the functioning of personal computers? Does spyware interfere with use of the Internet or programs on personal computers? If so, how?
- Does spyware raise privacy concerns for consumers?
    - Does spyware collect personal information about consumers?
    - How is the personal information spyware collects used? Is it combined with data from other sources? Is it transferred or disclosed to third-parties?
    - Does spyware capture the key strokes of consumers? Is key stroke information combined with data from other sources? Is it transferred or disclosed to third-parties?
    - To what extent is spyware used for identity theft?
- Does spyware raise security concerns for consumers? Does spyware expose personal computers to increased risk from hackers? If so, how?
- Are there special or unique consumer privacy or security risks associated with spyware disseminated through peer-to-peer file-sharing software? If so, what are these risks?
- To what extent are the privacy, security, and other concerns spyware raises for consumers different from those associated with other types of software?
- Does spyware create security risks for or cause harm to businesses, including harm to the reputation of software companies and others in the high-technology industries?
- Does spyware benefit consumers or competition? If so, what are the nature and extent of these benefits?

D. Possible Responses to Spyware Concerns

- What can consumers do to prevent the harms related to spyware?
    - What can consumers do to avoid downloading unwanted spyware?
    - What can parents do to minimize the risk that their children will download spyware, especially spyware disseminated via peer-to-peer file-sharing software?
    - Can consumers detect and remove installed spyware? If so, how difficult is it to do so?
    - Can consumers detect and remove peer-to-peer file-sharing software? If so, how difficult is it to do?
- What can government do to prevent the harms related to spyware?
    - Can law enforcement action reduce the harms related to spyware? If so, how, to what extent, and by whom? What should be the focus of these law enforcement efforts?
    - Can government-sponsored consumer education play a role in addressing spyware? Is there a special need for the government to educate teenagers and their parents about the risks of spyware, especially spyware disseminated through peer-to-peer file-sharing software?
    - What can government do to assist industry in addressing the harms caused by spyware?
- What can industry do to prevent the harms related to spyware?
    - Can technological tools reduce consumer concerns about spyware? If so, how and to what extent?
    - Can industry best practices or self-regulation decrease consumer concerns about spyware? If so, how and to what extent?
    - Can industry-sponsored efforts to educate consumers and employees help to reduce the harms related to spyware?
    - Can high-tech industry partner with the government to address spyware?
    - How can businesses work effectively with each other to address spyware?

- What would be the effect on the market for software if spyware were eliminated or reduced?

    - Would the elimination or reduction of spyware affect the price of software that is currently bundled with spyware?

    - Would the elimination or reduction of spyware affect the free distribution of peer-to-peer file-sharing software?

Requests to Participate as a Panelist in the Workshop

Parties seeking to participate as panelists in the workshop must notify the FTC in writing of their interest in participating on or before Friday, March 5, 2004, either by mail to the Secretary of the FTC or by email to spywareworkshop2004@ftc.gov. Requests to participate as a panelist should be filed in the same manner as comments (as detailed in the "Form and Availability of Comments" section below), and should be captioned "Spyware Workshop – Request to Participate, P044509." Parties are asked to include in their requests a statement setting forth their expertise in or knowledge of the issues on which the workshop will focus and their contact information, including a telephone number, facsimile number, and email address (if available), to enable the FTC to notify them if they are selected. An original and two copies of each document should be submitted. Panelists will be notified on or before Friday, March 19, 2004, whether they have been selected.

Using the following criteria, FTC staff will select a limited number of panelists to participate in the workshop:

1. The party has expertise in or knowledge of the issues that are the focus of the workshop.

2. The party's participation would promote a balance of interests being represented at the workshop.

3. The party has been designated by one or more interested parties (who timely file requests to participate) as a party who shares group interests with the designator(s).

In addition, there will be time during the workshop for those not serving as panelists to ask questions.

Form and Availability of Comments

The FTC requests that interested parties submit written comments on the above questions to foster greater understanding of the issues. Especially useful are any studies, surveys, research, and empirical data. Comments should be captioned "Spyware Workshop – Comment, P044509"; should be filed on or before Friday, March 19, 2004; and may be filed with the Commission in

either paper or electronic form.

1. A public comment filed in paper form should be mailed or delivered, with two complete copies, to the following address: Federal Trade Commission/Office of the Secretary, Room 159-H (Annex B), 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580. Both the comment itself and its envelope should be captioned "Spyware Workshop – Comment, P044509." If the comment contains any material for which confidential treatment is requested, it must be filed in paper (rather than electronic) form, and the first page of the document must be clearly labeled "Confidential."[1]

2. A public comment that does not contain any material for which confidential treatment is requested may instead be filed in electronic form (in ASCII, PDF, WordPerfect, or Microsoft Word format), as part of or as an attachment to an email message sent to the following email box: spywareworkshop2004@ftc.gov.

3. The FTC Act and other laws the Commission administers permit the collection of public comments to consider and use in this proceeding as appropriate. Regardless of the form in which they are filed, all timely comments will be considered by the Commission, and will be available (to the extent technologically possible, and with confidential material redacted) for public inspection and copying on the Commission web site at www.ftc.gov and at its principal office. As a matter of discretion, the Commission makes every effort to remove home contact information for individuals from the public comments it receives, before placing those comments on the FTC web site. More information, including routine uses permitted by the Privacy Act, may be found in the FTC's privacy policy, at http://www.ftc.gov/ftc/privacy.htm.

By direction of the Commission.

Donald S. Clark
Secretary

---

[1] Commission Rule 4.2(d), 16 CFR § 4.2(d). The comment must also be accompanied by an explicit request for confidential treatment, including the factual and legal basis for the request, and must identify the specific portions of the comment to be withheld from the public record. The request will be granted or denied by the Commission's General Counsel, consistent with applicable law and the public interest. *See* Commission Rule 4.9(c), 16 CFR § 4.9(c).