Federal Trade Commission
Privacy Impact Assessment

for the:
Video Teleconferencing Pilot

June 2012

1 System Overview

Congress passed, and the President signed, the Telework Enhancement Act of 2010, which requires agencies to encourage and improve teleworking. Teleworking can help the FTC carry out its mission by permitting FTC employees to continue working during inclement weather and other situations that may disrupt normal operations or require employees to take leave. Telework can also help save time, money, and other resources; reduce greenhouse gas emissions associated with commuting; and improve job satisfaction and work/life balance.

There are, however, technological and other barriers to teleworking. In particular, some FTC managers and employees may resist telework because communicating and coordinating with teleworkers can be challenging.

This Privacy Impact Assessment (PIA) discusses the FTC's deployment of an advanced video teleconferencing system that could reduce these barriers. The new technology would allow more FTC employees to video teleconference with each other, at work and at home. Video teleconferencing provides face-to-face visual interaction that is missing from phone conversations and email exchanges that take place during telework communications.

This PIA applies to a pilot study to test whether providing more video teleconferencing equipment to staff will improve the amount and quality of teleworking. With the assistance of the FTC's Office of the Chief Information Officer (OCIO), we will provide new video teleconferencing hardware and software to two teams of attorneys who have at least one member who regularly teleworks. The attorneys will use the video teleconferencing system for a designated amount of time, and then they will be surveyed to measure the impact of the equipment on teleworking conditions and to assess whether the use of video teleconferencing has changed the team members' impressions of teleworking. At the conclusion of the study period, the findings and recommendations will be presented to the FTC's Executive Director and OCIO.

2 Information Collected and Stored within the System

The following questions are intended to define the scope of the information in the system, specifically the nature of the information and the sources from which it is obtained.

2.1 What information is to be collected, used, disseminated, or maintained by the system?

The video conferences will be live and ephemeral, and the system will not monitor, record, or otherwise collect or maintain images that are disseminated by the video conferences.

Separate from the live video, the video teleconferencing system – Cisco Jabber Video for Telepresence (previously called "Movi") – maintains a searchable call log that is comparable to call detail information compiled and maintained by a telephone system

when a telephone call is made. The searchable video call log will contain the following information:

Display name
Direction of the call (inbound/outbound)
Remote Uniform Resource Identifier (URI)
Date
Start time
End time
Duration (in hrs./minutes)
Status (*e.g.*, ended)

As noted above, this log data will pertain exclusively to FTC teleworking employees who have been authorized to use the system in this pilot, and not to any non-FTC individuals.

2.2 What are the sources of the information in the system?

The log data compiled about users is automatically generated and compiled by the system. The data maintained and utilized by the teleconferencing management software (TMS) for this video teleconference system incorporates existing data in the form of user profiles from internal FTC phone or network user directory files.

2.3 Why is the information being collected, used, disseminated, or maintained?

The searchable call log described above in 2.1 documents each video teleconference, supports functionality, and allows usage to be monitored and audited, if necessary.

2.4 How is the information collected?

As noted previously in section 2.2, the system will access and use the user profile information in the TMS that will run the video-teleconferencing system. No new user information is collected, other than system usage data (e.g., session date and time).

2.5 How will the information be checked for accuracy and timeliness (currency)?

The user information in the TMS will be checked for accuracy and timeliness by updates from the source data (i.e., FTC internal network user directory files, see section 2.2).

2.6 Is the system using technologies in ways that the FTC has not previously employed (e.g., monitoring software, Smart Cards, etc.)? If so, how does the use of this technology affect individuals' privacy?

The FTC has used video teleconferencing equipment in the past, but not this particular technology and not for teleworking. Specifically, the video teleconference system that will be employed for this pilot will require new software and hardware. Although it is not believed that the new technology will affect individuals' privacy, its use in private

homes creates a possibility that the technology may affect privacy. For example, it is possible that other members of the FTC employee's family may inadvertently appear or wander through a video teleconference or that the employee's home or possessions may be viewable.

The employee will have control over what the camera focuses on. In addition, the teleworker can turn the camera on or off; once the camera has been physically turned off and the shutter has been closed it cannot be turned on remotely and thus there is no risk, other than employee error, that an accidental live-feed will occur.

In any event, as already noted, no video data are recorded or maintained by the system, and the system logs do not reflect data about any individual other than the user and the user's session.

2.7 What law or regulation permits the collection of this information?

The agency manages and establishes working conditions for its employees, including providing teleworking opportunities, pursuant to the FTC Act (15 U.S.C. § 45 et seq.) and Federal law, regulation, and policies encouraging the use of teleworking in the Federal workplace. See www.telework.gov.

2.8 Considering the type of information collected and sources of collection, what privacy risks were identified and how were these risks mitigated?

As discussed above in 2.6, the risk of inadvertent display of family members, home, or possessions can be minimized by training all individuals to use the equipment properly. The FTC has not identified any significant privacy risks with the log data: it is limited to date, time, and relatively non-sensitive data concerning the user's session, and the authorized users in the pilot are all FTC employees, not members of the public.

3 Use and Access to Data in the System

The following questions are intended to clearly describe how the information in the system will be used, and who will use it.

3.1 Describe how information in the system will or may be used.

The video teleconferencing system will be used by the teams during the workday to discuss legal strategy, to assign work, to prepare for litigation, to review documents and procedures for a case or investigation, and to facilitate the group dynamic of the team. Log data will be used, as needed, to enable functionality and track or audit usage.

3.2 Which internal entities will have access to the information?

Other than those FTC employees participating in a video teleconference, no internal entities will be permitted access to the call. Log data will only be accessible to authorized FTC system administrators.

3.3 Which external entities will have access to the information?

Other than those third parties participating directly in a video teleconference, no external entities will be permitted access to the call. No external entities will have access to system log data.

4 Notice and Access for Individuals

The following questions are directed at how or whether the individual is notified of the scope of information collected. They also concern the individual's right to consent to uses of information, right to decline to provide information, ability to ensure the accuracy of the information collected, and right to access their information.

4.1 How will individuals be informed about what information is collected, and how this information is used and disclosed?

The Rules of Behavior that each user will have to sign will include a description consistent with 2.1, above, about what information is being collected.

4.2 Do individuals have the opportunity and/or right to decline to provide information?

Individuals can decline to use the video teleconferencing system if they do not wish to provide the information described above in 2.1. If they use the system, it will automatically compile the log data described earlier, which the user cannot decline.

4.3 Do individuals have the right to consent to particular uses of the information? If so, how would an individual exercise this right?

No.

4.4 What are the procedures that allow individuals to gain access to their own information?

Individual users will not have routine access to log data in the system about their sessions. To the extent, if any, that the log data constitute Privacy Act records, access could be granted by the agency to its employee users without a formal Privacy Act request, and the FTC's rules contain formal access procedures for such records, where an

agency declines to grant such access voluntarily. *See* 16 C.F.R. 4.13.

4.5 Discuss the privacy risks associated with the process of providing individuals access to their own records and how those risks are mitigated.

Not applicable, since the data maintained by the system (i.e., log data) are not accessible through the system by individuals and are accessible only by designated system administrators.

5 Web Site Privacy Issues

Complete this section only if the new system or project creates or modifies an FTC Web site, page, or online form accessible through the Internet.

5.1 Describe any tracking technology used by the Web site and whether the technology is persistent or temporary (e.g., session cookie, persistent cookie, Web beacon). Currently, persistent tracking technology is not approved for use by the FTC (see 5.2).

Not applicable.

5.2 If a persistent tracking technology is used, ensure that the proper issues are addressed (issues outlined in the FTC's PIA guide).

Not applicable.

5.3 If personal information is collected through a Web site, page, or online form accessible through the Internet, is appropriate encryption used? If not, explain.

Not applicable.

5.4 Explain how the public will be notified of the Privacy Policy.

Not applicable.

5.5 Considering any Web site or Internet issues, please describe any privacy risks identified and how they have been mitigated.

Not applicable.

5.6 If the Web site will collect personal information from children under 13, or be directed at such children, explain how it will comply with the Children's Online Privacy Protection Act (COPPA).

Not applicable.

6 Security of Information in the System

The following questions are intended to describe technical safeguards and security measures.

6.1 Are all IT security requirements and procedures required by federal law being followed to ensure that information is appropriately secured?

The FTC follows all applicable Federal Information Security Management Act (FISMA) requirements to ensure the information contained in the system is appropriately secured.

6.2 Has a Certification & Accreditation been completed for the system or systems supporting the program?

The system is part of the FTC's Data Center General Support System (GSS), which has received a Certification and Accreditation (C&A) using NIST (National Institute of Standards and Measures) and Office of Management and Budget (OMB) guidance**.**

6.3 Has a risk assessment been conducted on the system?

A risk assessment was completed on the Data Center GSS as part of the C&A. Appropriate security controls have been identified to protect against risk and such controls have been implemented.

6.4 Does the project employ technology that may raise privacy concerns? If so, please discuss its implementation.

Except as described above in 2.6 and 2.8, the project does not employ technology that raises privacy concerns.

6.5 What procedures are in place to determine which users may access the system and are they documented?

Access to the video teleconference system is controlled by the standard FTC user authentication system and is limited to designated users and administrators. Users can initiate, receive, and participate in video teleconferences but cannot access or alter the system's administrative or security settings. Administrators can access and alter the system's administrative and security settings, but only through designated portals, and all such administrative access and changes in settings are monitored and recorded.

All users will receive training on the proper use of the video teleconferencing system. The users will also review and sign a Rules of Behavior form before they are allowed to use the system. Likewise, system administrators are subject to FTC rules and procedures and routinely receive training regarding proper system access and the restrictions on use and disclosure of nonpublic FTC data.

6.6 Describe what privacy training is provided to users either generally or specifically relevant to the program or system.

All FTC staff and all contractors are required to complete computer security training and privacy awareness training annually.

6.7 What auditing measures and technical safeguards are in place to prevent the misuse of data?

The information collected, as described above in 2.1 is minimal; log data may enable the FTC, as needed, to monitor usage and conduct audits.

Any questions regarding the security of the system should be directed to the FTC's Chief Information Security Officer.

7 Data Retention

This section addresses how long data is maintained, and how and when it is disposed of.

7.1 For what period of time will data collected by this system be maintained?

The system log data will be kept for 30 days. (This retention period is comparable to the standard retention period for call detail logs, which is also 30 days.) User profile information in the TMS is deleted when user profiles are removed from FTC internal network user directory files (e.g., when an employee leaves the FTC).

7.2 What are the plans for destruction or disposal of the information?

The logs are automatically erased from the system after 30 days. User profile information is automatically deleted from the TMS when user profiles are removed from FTC internal network user directory files. All data will be deleted/destroyed in accordance with OMB, National Archives and Records Administration and NIST regulations and guidelines.

7.3 Describe any privacy risks identified in the data retention and disposal of the information, and describe how these risks have been mitigated.

Any privacy risk in the retention of the data is minimal. See Section 2.8. No privacy

risks have been identified in the disposal of the data.

8 Privacy Act

This section addresses the applicability of the Privacy Act of 1974 to the system, and whether or not the system is covered by a System of Records Notice (mandated for some systems by the Privacy Act of 1974).

8.1 Will the data in the system be retrieved by a personal identifier?

Yes. Data in the system will be retrieved by a personal identifier to the extent that the video call log data as described above in 2.1 will be maintained and retrieved by the names of individuals who use the system.

8.2 Is the system covered by an existing Privacy Act System of Records Notice (SORN)?

Yes. The call log data maintained by the system will covered by the Privacy Act SORN FTC-VII-3 (Computer Systems User Identifiable and Access Records), to the extent such data are about an individual and are retrieved by that individual's name or other personal identifier. This SORN is available at: http://www.ftc.gov/foia/sysnot/vii-3.pdf.

9 Privacy Policy

This section confirms that the information handling practices of the system are consistent with the FTC's privacy policy.

9.1 Confirm that the collection, use, and disclosure of the information in this system has been reviewed to ensure consistency with the FTC's privacy policy.

This system has been reviewed to ensure consistency with FTC's privacy policy.

10 Approval and Signature Page

Prepared for the Business Owners of the System by:

_____ Date: _____
Sarah Mackey Mathias
Assoc. General Counsel for Proj. Mgt.

Reviewed by:

_____ Date: _____
Alexander C. Tang, Attorney
Office of the General Counsel

_____ Date: _____
Peter Miller
Acting Chief Privacy Officer

_____ Date: _____
Jeffrey Smith
Information Assurance Manager

_____ Date:_____
Jeff Nakrin
Director, Records and Filings Office

Approved:

_____ Date: _____
Jeff Huskey
Chief Information Officer