Federal Trade Commission
Privacy Impact Assessment

FTC Wi-Fi Networks (Wi-Fi)

Reviewed and Updated

February 2025

Table of Contents

1 System Overview

1.1 Describe the project/system and its purpose.

The FTC's Office of Chief Information Officer (OCIO) handles the Commission's various information technology (IT) and infrastructure needs. As a component of its IT program, OCIO operates Wi-Fi[1] Networks at all FTC locations to support Commission activities and to meet specific agency needs. The following components represent the FTC's Wi-Fi Networks:

Wi-Fi Network (SSID)	*Description*
WIFI-User	The WIFI-User SSID provides wireless connectivity for FTC users to the FTC internal network. Access is restricted to government-owned equipment. Information maintained by the WIFI-User network is the same as that maintained by the wired network.
WIFI-Phones	The WIFI-Phones SSID provides wireless connectivity for FTC desk phones to the FTC internal network. Access is restricted to government-owned equipment. Information maintained by the WIFI-Phones network is the same as that maintained by the wired network. This network does not have Internet access.
WIFI-Printers	The WIFI-Printers SSID provides wireless connectivity for FTC printers to the FTC internal network. Access is restricted to government-owned equipment. Information maintained by the WIFI-Printers network is the same as that maintained by the wired network. This network does not have Internet access.
WIFI-Guest	The WIFI-Guest network provides Wireless Internet connectivity to visitors and employee personal devices at FTC offices. Access is restricted to those with the current passphrase, which changes twice monthly and is posted in the Service Now instance. The WIFI-Guest network logs the MAC addresses of all devices that connect or attempt to connect to the network.
WIFI-Meet	The WIFI-Meet network provides wireless Internet connectivity to participants at FTC public events. Access is restricted to those with the event passphrase provided in a handout. unrestricted, but is limited to the location and duration of the event. The WIFI-Guest network logs the MAC addresses of all devices that connect or attempt to connect to the network.

[1] Wi-Fi is a technology that allows electronic devices to connect to a network. That network may or may not have access to the Internet. This PIA discusses how the FTC collects and uses information affiliated with use of its Wi-Fi networks: any collection or use of FTC Wi-Fi information by the Internet service provider supplying the FTC's Guest Wi-Fi functionalities is beyond the scope of this PIA. For information about the Internet service provider's collection and use of data, see the Zayo Customer Privacy Statement.

Although the following component is part of the FTC's Wi-Fi Networks, it is a closed network with no Internet access and does not collect, maintain, or disseminate personally identifiable information (PII).

Wi-Fi Network	*Description*
AV Wi-Fi	The AV Wi-Fi network provides connectivity between the handheld touch panels used in the large conference rooms to control the room's audiovisual and other equipment. This isolated network maintains the SSID, passphrase, and list of authorized MAC addresses of the AV components used by the FTC.

The FTC employs monitoring and management tools to ensure the security of FTC operations, to protect the equipment connected to the networks, and to preserve the privacy of staff and guest users. The following security components are used in varying degrees on the FTC's Wi-Fi Networks:

Security Component	*Description*
Authentication Management System (AMS)	AMS manages user authentication to validate access to the WIFI-User network. It issues PKI certificates to FTC-owned devices to allow connection to the network. The name of the workstation, which incorporates the FTC username, is collected by AMS whenever the workstation connects to the network. PKI certificates for FTC mobile devices are issued by the Mobile Device Management System (MDMS) for the device and the user by utilizing the FTC username and password. AMS collects and logs the device name and IP address when the certificate is used to connect to the network. For the WIFI-Guest and WIFI-Meet networks, the AMS presents a web form via captive portal to the user to accept the terms of service. The AMS collects the MAC addresses of connections to the captive portal.
Wi-Fi Firewall[2]	The Wi-Fi Firewall controls the incoming and outgoing network traffic by analyzing the data packets and determining whether or not they should be allowed through based on a set of rules. The rules prevent communications between the various Wi-Fi networks and between devices on each network. The Wi-Fi Firewall logs IP header information for network activity.

[2] Firewalls determine access based on the contents of the IP header relative to configured rules and the protocol and ports employed.

Security Component	*Description*
Wired Firewall	The Wired Firewall controls the incoming and outgoing network traffic by analyzing the data packets and determining whether they should be allowed through based on a set of rules. This firewall is used to prevent unauthorized inbound traffic from accessing the Wi-Fi networks from the Internet. The Wired Firewall logs IP header information for network activity.
Intrusion Prevention & Rogue Device Detection	Intrusion Prevention & Rogue Device Detection continually monitors the Wi-Fi Networks; detects, classifies, and isolates unauthorized Wi-Fi Access Points; and protects FTC Wi-Fi Networks against denial-of-service (DoS) and client attacks. It collects records of unauthorized Wi-Fi device activity (SSID, MAC address, frequency, associations with FTC equipment (if any), time of detection, and which Access Points detected the activity, thereby implying a general location of the unauthorized device) that may represent an intentional network intrusion within FTC premises and its Wi-Fi perimeter.
Content Filtering	Content Filtering restricts access to certain types of Internet content (e.g., gambling, adult entertainment, known malware sites, etc.). WIFI-User is protected by the same content filter as the FTC wired network. WIFI-Guest and WIFI-Meet content filtering and Internet connections are separate from the FTC production network.

1.2 What specific legal authority allows for the collection, maintenance, or dissemination of information for this project/system?

The Federal Information Security Modernization Act of 2014.

2 Data Type, Sources, and Use

2.1 Specify in the table below what types of personally identifiable information (PII)[3] may be collected or maintained in the system/project. Check all that apply.

PII Elements: This is not intended to be an exhaustive list. Specify other categories of PII as needed.		
☒ Full Name	☐ Biometric Identifiers (e.g., fingerprint, voiceprint)	☒ User ID
☐ Date of Birth	☐ Audio Recordings	☐ Internet Cookie Containing PII
☐ Home Address	☐ Photographic Identifiers (e.g., image, x-ray, video)	☐ Employment Status, History, or Information
☐ Phone Number(s)	☐ Certificates (e.g., birth, death, marriage, etc.)	☐ Employee Identification Number (EIN)
☐ Place of Birth	☐ Legal Documents, Records, Notes (e.g., divorce decree, criminal records, etc.)	☐ Salary
☐ Age	☐ Vehicle Identifiers (e.g., license plates)	☐ Military Status/Records/ ID Number
☐ Race/ethnicity	☐ Financial Information (e.g., account number, PINs, passwords, credit report, etc.)	☒ IP/MAC Address
☐ Alias	☒ Geolocation Information (within FTC spaces only)	☐ Investigation Report or Database
☐ Sex	☐ Passport Number	☐ Driver's License/State ID Number (or foreign country equivalent)
☒ Email Address		☒ Other *(Please Specify)*: PIN/Password
☐ Work Address		
☐ Taxpayer ID		
☐ Credit Card Number		
☐ Facsimile Number		
☐ Medical Information		
☐ Education Records		
☐ Social Security Number		
☐ Mother's Maiden Name		

2.2 What types of information other than PII will be collected, disseminated, or maintained by the project/system? Provide a general description below and be sure to include all data elements.

For each of the Wi-Fi networks, the Service Set Identifier (SSID) is maintained by the network. The Authentication Management System (AMS) collects MAC addresses for all users and devices and user ID information for FTC users. User's acceptance of the Terms of Service for network use is logged against the MAC address. The Intrusion Prevention & Rogue Device Detection collects records of unauthorized Wi-Fi device activity (SSID, MAC address, frequency, associations with FTC equipment (if any), time of detection, and which Access Points detected the activity, thereby implying a general location of the unauthorized device) that may represent an intentional intrusion within FTC premises and its Wi-Fi perimeter.

[3] Per OMB M-07-16, personally identifiable information (PII) refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date or place of birth, mother's maiden name, etc.

2.3 What is the purpose for collection of the information listed above?

Information collected by the Wi-Fi Networks is maintained for the purposes of controlling access to and logging activity on the networks.

Security Component	*Reason for Collection, Use and Maintenance*
Authentication Management System (AMS)	For the WIFI-User network, the system queries PKI certificates to validate access. For the WIFI-Phones and WIFI-Printers, the system ensures that the devices have the proper WPA-2 pre-shared key to validate access. For the WIFI-Guest and WIFI-Meet networks, the system ensures that users accept the terms of service. To allow access.
Wi-Fi Firewall	The Wi-Fi Firewall logs IP header information for network activity to monitor and document activity that violates FTC policy or indicates network malfunction.
Wired Firewall	The Wired Firewall logs IP header information for network activity to monitor and document activity that violates FTC policy or indicates network malfunction.
Intrusion Prevention & Rogue Device Detection	Records generated by Intrusion Prevention & Rogue Device Detection are maintained to monitor and document activity that may represent an intentional network intrusion on FTC premises.
Content Filtering	Records generated by Content Filtering activities are maintained to monitor and document blocked access to prohibited Internet sites by Wi-Fi Network users.

2.4 What are the sources of the information in the system/project? How is the information collected?

For all the FTC's Wi-Fi Networks, some information is entered using the administrative console of the respective Wi-Fi systems. For WIFI-User, machine certificates are created and installed when the device is joined to the domain. For WIFI-Phones & WIFI-Printers, passphrases are entered manually at the device. MAC addresses are set by manufacturers and supplied by devices as their device connects to the Guest Network.

Source of Data	*Type of Data Provided & How It Is Collected*
System Administrators	System administrators set the SSID for all the FTC Wi-Fi networks. For Wi-Fi networks other than WIFI-User, system administrators set the passphrase as well. For the AV Wi-Fi network, system administrators are also responsible for entering the authorized MAC addresses of the AV components.

Source of Data	*Type of Data Provided & How It Is Collected*
Authentication Management System	The Authentication Management System queries FTC-issued PKI certificates to validate device access to the WIFI-User network. The PKI certificate is presented to the system by the device as part of the authentication process. o FTC Workstations – PKI device certificate is issued by the Windows Certificate Authority when the workstation joins the domain. This certificate can only be seen by administrators. Per FTC policy, workstation names include the username of the person to whom the workstation is assigned. o FTC Mobile Devices – PKI device certificate is issued by MDMS. Guest MAC address information is collected as part of the Acceptance of Terms of Service.
Wi-Fi Firewall	The Wi-Fi Firewall logs of IP header information are generated as a part of communications on the Wi-Fi Networks. Network activity is collected as part of the normal operating process of the Wi-Fi Firewall.
Wired Firewall	The Wired Firewall logs of IP header information are generated as a part of communications on the Wi-Fi Networks. Network activity is collected as part of the normal operating process of the Wired Firewall.
Intrusion Prevention & Rogue Device Detection	Intrusion Prevention & Rogue Device Detection generate records of unauthorized Wi-Fi device activity within FTC premises and its Wi-Fi perimeter. Rogue Device information is created when an unapproved Wi-Fi Access Point (one that attempts and/or provides unauthorized Wi-Fi connection to the FTC networks) is detected by the system. Network activity is analyzed as part of the normal operating process of the Intrusion Protection system. Activity records of suspected rogue devices are logged automatically.
Content Filtering	Content Filtering activities generate records of Internet use, User ID for WIFI-User and MAC address for WIFI-Guest & WIFI-Meet.

3 Data Access and Sharing

3.1 In the table below, specify the systems/applications and groups (both FTC and non-FTC) that will have access to or share data in the system/project.

Data Will Be Accessed By and/or Provided To:	*How and Why the Data Will Be Accessed/Shared*
FTC Staff and Contractors	All information collected is directly accessible only by authorized system administrators for authorized purposes. In addition, information regarding unapproved inappropriate activity may be requested by the FTC Office of General Counsel (OGC), Human Capital Management Office (HCMO), and/or the Office of the Inspector General (OIG) as part of an investigation. Information regarding security-related issues may be provided to the appropriate FTC Cybersecurity personnel within the OCIO. FTC Wi-Fi is accessible for all FTC-issued laptops using the PKI certificate issued when the workstation is connected to the domain. FTC staff and contractors must sign the FTC Rules of Behavior and use of Wi-Fi Networks is subject to supervisor approval. Access is limited to authorized devices, and access to device configuration (except for employee personal devices) is restricted to administrative personnel, as documented in standard operating procedures.
External non-FTC Entities	In some cases, information regarding potential security-related issues may be provided to the Department of Homeland Security (DHS) and the US Computer Emergency Response Team (US-CERT). Information collected by the FTC's Wi-Fi Networks is not routinely shared with outside entities, but may be shared, if necessary, where authorized or required by law (e.g., confidential disclosures to other law enforcement authorities for investigations and proceedings, mandatory release of information that is not privileged or exempt from Freedom of Information Act (FOIA) requests, discovery in litigation, subpoenas or other compulsory process, official requests of Congress or the General Accountability Office (GAO), etc.). This PIA discusses how the FTC collects and uses information affiliated with its Wi-Fi networks: any collection or use of FTC Wi-Fi information by the Internet service provider supplying the Guest & Meet Wi-Fi functionalities is beyond the scope of this PIA. For information about the internet service provider's collection and use of data, see the Zayo Customer Privacy Statement.

3.2 Do contractors and/or third-party service providers have access to data in the project/system? If yes, explain what privacy requirements are in place to ensure that data is properly protected.

☒ Not Applicable. There are no third-party service providers who have administrative access to the Wi-Fi Networks or the security components used to monitor the networks. However, see the chart in 3.1 above for information about Internet service provider data collection. FTC contractors who are employed by the agency are subject to the same policies and guidelines that FTC staff members must follow. As such, contractors must adhere to existing FTC guidelines when using the Wi-Fi Networks and comply with established Rules of Behavior.

3.3 If you answered "yes" to 3.2, describe the privacy incident response plan maintained by the contractor's organization or third party service provider.

☒ Not Applicable.

4 Notice and Consent

4.1 How are individuals provided with notice prior to the collection of their PII? If notice is not provided, explain why.

☒ Notice is provided via (*check all that apply*):

☒ Privacy Act Statement (☒ Written ☐ Oral)
☐ FTC Website Privacy Policy
☐ Privacy Notice (e.g., on Social Media platforms)
☐ Login banner
☒ Other (*explain*): Individuals, including members of the public, who choose to use the WIFI-Guest or WIFI-Meet networks are given notice about the FTC's Wi-Fi network monitoring in writing when acknowledging the online Terms of Service for those networks. This PIA also acts to provide public notice of the configuration and security information collected by the networks.

☐ Notice is not provided (explain): _____

4.2 Do individuals have the opportunity to decline to provide information or to consent to particular uses of their information (other than required or authorized uses)?

Individuals are not required to provide their information; however, if they wish to utilize the Wi-Fi Network services, they must provide the necessary information. Similarly, individuals may choose to use their own communication solutions when visiting the FTC as guests or conference attendees; however, if guests or conference participants wish to use the WIFI-Guest or WIFI-Meet networks, then they must provide the required information.

Once individuals choose to use any component of the FTC Wi-Fi Networks, they cannot decline to provide information necessary for the security components associated with that Wi-Fi network. Individuals do not have the right to consent to particular uses of the information except by declining to use the Wi-Fi Networks provided by the FTC.

4.3 Are there procedures in place to allow individuals access to their personally identifiable information? Explain.

Individuals do not have direct access to information collected and issued by the Wi-Fi Networks. FTC employees and contractors may contact the FTC Enterprise Service Desk (Help Desk) and request their account information. Guest users and Conference attendees may request access to collected information, if any, through the FTC FOIA/Privacy Act Office, www.ftc.gov/about-ftc/foia/foia-request.

4.4 Are there procedures in place to allow individuals the ability to correct inaccurate or erroneous information? What is the process for receiving and responding to complaints, concerns, or questions from individuals? Explain.

As stated in 4.3 above, individuals do not have direct access to information collected about themselves. FTC employees and contractors can receive their account information by calling the Enterprise Service Desk (Help Desk). If a Guest or Conference attendee wishes to request access to collected information, he/she may submit a request through the FOIA/Privacy Act Office, www.ftc.gov/about-ftc/foia/foia-request.

If an individual is aware that the information collected about them is inaccurate (e.g., wrong email address), then he/she can contact OCIO to correct or update the information as necessary.

5 Data Accuracy and Security

5.1 Are there procedures in place to ensure that the information maintained is accurate, complete, and up-to-date?

The minimal information collected about users is maintained by the Authentication Management System. FTC staff members may contact the FTC Help Desk to request their account information. If there is any inaccuracy in the information maintained, the individual can request corrections, and OCIO will update the information accordingly. Information access and amendment procedures for FTC Wi-Fi information may also be governed by FOIA and the Privacy Act.

5.2 Are there administrative procedures and technical safeguards in place to protect the data in the system/project? What controls are in place to ensure proper use of the data? Please specify.

FTC administrative staff members are bound by FTC policy regarding network and usage data collected by the monitoring and security tools mentioned in Section 1. Logs created by these tools are audited, as needed, as part of overall infrastructure security management. Any questions regarding the security of the system should be directed to the FTC's Chief Information Security Officer (CISO). The following technical safeguards are employed to prevent misuse of data transiting the network:

Security Component	***Technical Safeguards***
Authentication Management System	The Authentication Management System provides centralized management of rules and access control for the various Wi-Fi networks. It enables the use of PKI certificates across many of the networks, ensuring stronger and more efficient access control.
Wi-Fi Firewall	The Wi-Fi firewall controls the incoming and outgoing network traffic by analyzing the data packets and determining whether or not they should be allowed through, based on a set of rules. This tool prevents traffic flow between the FTC Wi-Fi networks and between connected Wi-Fi devices on the same FTC Wi-Fi network.
Wired Firewall	The wired firewall controls the incoming and outgoing network traffic by analyzing the data packets and determining whether or not they should be allowed through, based on a set of rules. This firewall is used to prevent inbound traffic from the Internet to the Wi-Fi networks.
Intrusion Prevention & Rogue Device Detection	Intrusion Prevention & Rogue Device Detection continually monitors the networks; detects, classifies and contains rogue Access Points; and protects against denial-of-service (DoS) and client attacks.
Content Filtering	Content filtering is used to restrict access to certain types of Internet content from the various Wi-Fi networks. The levels of filtering vary by the network purpose.

5.3 Is PII used in the course of system testing, training, or research? If so, what steps are taken to minimize and protect PII during this process?

Aside from instances when system administrators used their own PII for setup purposes, PII is not used in the course of system testing, training, or research.

6 Data Retention and Disposal

6.1 Specify the period of time that data is retained in the system/project. What are the specific procedures for disposing of the data at the end of the retention period?

Information collected as a part of the WIFI-User, WIFI-Guest, & WIFI-Meet is forwarded to the FTC SIEM and retained for a minimum of six months.

As specified by the National Archives and Records Administration (NARA) in General Records Schedule (GRS) 3.2, Information Systems Security Records, item 010, system and data security records, security records are maintained for as long as needed for agency/IT administrative purposes to ensure a continuity of security controls throughout the life of the system. Per FTC policy, the security records are maintained for a minimum of six months.

In accordance with NARA GRS 3.2, item 020, Computer security incident handling, reporting, and follow-up records, security incident records (e.g., attempts to gain unauthorized access to FTC Wi-Fi Networks) will be retained for a minimum of three years after all necessary follow-up actions have been completed.

7 Website Privacy Evaluation

7.1 Does the project/system employ the use of a website? If so, describe any tracking technology used by the website and whether the technology is persistent or temporary (e.g., session cookie, persistent cookie, web beacon). Describe the purpose of using such tracking technology.

The Wi-Fi Networks and the respective security components do not use tracking technology on behalf of the agency. The FTC's Authentication Management System (AMS), however, has the ability to log which users are no longer approved to access any of the Wi-Fi Networks; when Guest users connect to the Guest Wi-Fi network; and whether Guest users have appropriately accepted the Terms of Service. AMS collects MAC addresses for Guest and Meet network users. No other FTC Wi-Fi Network component collects personal information through a website. Persistent tracking technology is not applicable.

8 Privacy Risks and Evaluation

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

Risk	***Mitigation Strategy***
User information may be accessed, shared,	All collection and monitoring activities by the FTC Wi-Fi Networks and associated tools are related to securing the

Risk	*Mitigation Strategy*
used, maintained, or monitored by unauthorized persons or for unauthorized purposes.	networks. To mitigate privacy risks, the review of network activity is limited to authorized security personnel and does not include routine user-level data review, unless there is evidence of a potential security incident, in which case the additional user-level data may be reviewed by authorized FTC personnel for authorized purposes. Configurations and any information logged by components of the FTC Wi-Fi Networks are protected by access control lists at the network level and require administrative accounts and passwords to access or alter information. The FTC's WIFI-Guest and WIFI-Meet Networks are encrypted and password-protected with firewall protection, but as with any Wi-Fi network, the risk of intrusion from outside entities exists. Users should exercise caution when browsing the web and avoid suspicious content to protect their information and their devices. The Wi-Fi Networks are configured to prevent access to inappropriate sites, such as pornographic or gambling sites, and users are at their own risk while browsing other sites. The monitoring technologies help moderate these risks (although the risk of acquiring viruses or other malware cannot be completely eliminated).

8.2 Does the project/system employ the use of automated privacy controls or enhanced capabilities designed to support privacy? Explain.

There are systematic lock-outs in place to deter unauthorized access to security components monitoring the Wi-Fi Networks. For example, after four repeated incorrect login attempts of the Authentication Management System, a system user will be locked out of his/her account until an administrator resets the account. In addition, failed, non-FTC device connections will lock out the MAC address after 10 failed attempts.

8.3 Has a Privacy Act System of Records Notice (SORN) been published in the Federal Register for this system/project? If so, list the applicable SORN(s).

The information maintained is covered by existing Privacy Act System of Records Notices (SORNs): VII-3 -- Computer Systems User Identification and Access Records, VII-5 -- Property Management System. Information may also be incorporated into VII-7 -- Information Technology Service Ticket System, to the extent necessary to help track and resolve individual or network service issues.

8.4 How does the project/system ensure that the information is collected, used, stored, or disseminated in accordance with stated practices in this PIA?

FTC administrative staff members are bound by FTC policy regarding network and usage data collected by the monitoring and security tools put in place to prevent misuse of data transiting the network. Logs created by these tools are audited as needed as part of overall infrastructure security management.