Federal Trade Commission
Privacy Impact Assessment

FTC Access Control System

Updated April 2019

Table of Contents

1 System Overview

1.1 Describe the project/system and its purpose.

The Access Control System is a combination of hardware (e.g., workstations, servers), software (e.g., security management software), and paper-based information collections (i.e. visitor logs). The Access Control System secures, monitors, and controls access by employees, contractors, visitors, and others to the FTC Headquarters Building (HQ), Constitution Center (CC), warehouse, and designated areas within those facilities.[1]

The Access Control System comprises four major functions: visitor management, physical access control, intrusion detection, and video surveillance. The Access Control System contains personally identifiable information (PII) from FTC employees, contractors, and members of the public who access or attempt to access FTC facilities.

Several individual components comprise the Access Control System, which include (see table):

[1] This PIA addresses the access control measures that are specific to the FTC, but it does not necessarily address access control measures undertaken by entities such as GSA, FPS, or local building security, that apply to all offices in shared buildings (such as CC) in which the FTC has an office. Unless specifically noted in this PIA, security controls in the Regional Offices (RO) are managed by by other entities (such as GSA, FPS, or local building security).

Component		Description	Location			
			HQ	CC	RO	Notes On Location
A	PACS Server/Application	Server and application for the Physical Access Control System (PACS)	√			Located in the HQ Data Center
B	Card Key Readers* (Card scanner only)	Turnstiles and readers	√	√		Located at entrances/exits, elevator lobbies, secure storage, data centers
C	FTC Badge (PIV Badge and Proximity Card capabilities)	PIV: A card that provides identification, authentication, and storage of personal data Proximity: Used to grant or restrict access to FTC facilities.	√	√	√	All employees, contractors, visitors, etc., are issued a PIV or Proximity Card. Regional Office (RO) employees use PIV cards for access if they work in GSA-managed buildings. The FTC participates in the GSA USAccess program.
D	CCTV Cameras* (Transmit Only)	Digital (IP based) and analog cameras	√	√		Located in corridors/hallways, lobbies, entrances/exits, and building perimeter.
E	CCTV Network Video Recorder (NVR)	Network video recorders for cameras	√			Located in the HQ Data Center
F	Intrusion Detection System Sensors*	Used to alert security personnel of an actual or attempted intrusion into an area. Alert data is stored on the PACS server.	√	√		Installed on select doors and windows
G	Electronic High-Security Key System	A key assigned to an individual that provides access to a specific room(s) (office, storage room, war room, office suite) The electronic key system logs the date and time of when a room was accessed or unlocked by any individual. A person's name and organization is stored in a secured database. Room numbers and location are also collected.	√	√		Installed on internal doors at facilities located in the National Capitol Region
H	AIPHONE*	Visual intercom system installed on all RO entrances. A component of the device external to the door has a camera and buzzer so internal staff can see who is asking for entrance to the office. Staff can electronically open the door via the console installed at the reception desk. Camera footage is not stored and AIPHONE information is not tracked. Managed by the FTC.			√	Currently installed atmost regional offices.
I	Guard Post Workstation*	FTC provisioned workstation used to view card key scan results and camera feeds.	√			Located at all HQ Guard Posts
J	Physical Security Specialist Workstation	FTC provisioned workstation used to view card key scan results and camera feeds. The workstations connect to the PACS server but are not used for data storage.	√	√		Deployed at Physical Security Specialist Workspace
K	Visitor Management - Logs	Paper visitor sign-in logs and parking garage records.	√			Used by HQ Guards. Any logs maintained by CC and RO are beyond the scope of this PIA: see footnote 1.

*** These components are not used for data collection, but are pass-through devices without autonomous authorization or logging responsibility, and thus, these devices will not be included in any further discussion.**

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

- Executive Order 12977, *Interagency Security Committee*
- Homeland Security Presidential Directive-12, *Policies for a Common Identification Standard for Federal Employees and Contractors*, August 2004
- Office of Management and Budget (OMB) M-05-24, *Implementation of HSPD-12 – Policy for a Common Identification Standard for Federal Employees and Contractors*
- National Institute of Standards and Technology (NIST) 800-116, *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)*
- 41 Code of Federal Regulations (CFR) 102-74, *Facility Management*

2 Data Type, Sources, and Use

2.1 Specify in the table below what types of personally identifiable information (PII)[2] may be collected or maintained in the system/project. Check all that apply.

PII Elements:

☒ Full Name
☐ Date of Birth
☐ Home Address
☐ Phone Number(s)
☐ Place of Birth
☐ Age
☐ Race/ethnicity
☐ Alias
☐ Sex
☒ Email Address
☒ Work Address
☐ Taxpayer ID
☐ Credit Card Number
☐ Facsimile Number
☐ Medical Information
☐ Education Records
☐ Social Security Number
☐ Mother's Maiden Name

☐ Biometric Identifiers (e.g., fingerprint, voiceprint)
☐ Audio Recordings
☒ Photographic Identifiers (e.g., image, x-ray, video)
☐ Certificates (e.g., birth, death, marriage, etc.)
☐ Legal Documents, Records, Notes (e.g., divorce decree, criminal records, etc.)
☒ Vehicle Identifiers (e.g., license plates)
☐ Financial Information (e.g., account number, PINs, passwords, credit report, etc.)
☐ Geolocation Information
☐ Passport Number

☒ User ID
☐ Internet Cookie Containing PII
☒ Employment Status, History, or Information
☐ Employee Identification Number (EIN)
☐ Salary
☐ Military Status/Records/ ID Number
☐ IP/MAC Address
☐ Investigation Report or Database
☐ Driver's License/State ID Number (or foreign country equivalent)
☒ Other *(Please Specify)*: See Below

[2] Per OMB Circular A-130, PII means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

PIV/Proximity Card

The following data elements are collected from the FTC employee/contractor PIV card and entered into the PACS database at the time of PIV card issuance:

1. Last Name, First Name, Middle Name
2. Agency Code: A four-digit code that is part of the Federal Agency Smart Credential Number (FASC-N) on the card and is assigned by the certificate authority
3. System Code: A two-digit number that is part of the FASC-N
4. Card Number: The number embossed on the PIV card
5. Certificate Number: The certificate number assigned by the certificate authority
6. Personnel Type: Employee or contractor
7. Record ID: A unique number assigned by the PACS and associated with the employee profile
8. Activation Date: Date the profile was entered into the PACS database
9. Expiration Date: Expiration date of the PIV card
10. Employee or Contractor Photograph
11. Date and time the profile was entered into the PACS database

HQ Visitor Management - Paper Log

The FTC's visitor management function authorizes and records the entry and exit of visitors requiring temporary access to the HQ building. The security guard verifies the individual's name from any local, State, or Federal government-issued identification (ID) card and enters the information into a hand-written visitor log as a record of the visit. The visitor management function at HQ is governed by the Administrative Manual, Chapter 4: Section 800 – Physical Security. The PII collected from each visitor includes:

1. Date
2. Time of Arrival and Departure
3. Name
4. FTC Point of Contact
5. Name of Firm or Agency
6. Purpose of Visit
7. Security Guard Initials

For FTC employees and visitors authorized to use the FTC Headquarters garage, the FTC collects the following via paper logs:

1. Name
2. Vehicle make
3. License Plate Number
4. Date
5. Model
6. State

7. Time entered/exited

Electronic High-Security Key System

The following information is collected and maintained for the key management system:

1. Name of FTC employee/contractor
2. Date/Time individual accesses the room
3. Key number
4. Room(s) individual can access/room location
5. Organization

HQ Network Video Recorder (NVR) and CCTV Cameras

The cameras used for the FTC CCTV systems provide the greatest possible range and area of monitoring. The cameras do not store PII; rather, they transmit the images to the NVR for retention. Additionally, cameras are located at the entrance and exits.

The FTC uses the video feeds to detect and respond to potentially unlawful activities in real time in the areas using CCTV. The video feeds may also be used to support law enforcement investigations to the extent that they contain information relevant to a criminal (or potential criminal) activity.

Cameras are not placed in locations where individuals have a reasonable expectation of privacy, such as restrooms, offices, or locker rooms.

CC CCTV Cameras (Other than FTC-designated Space)

CCTV cameras and any associated recording devices at CC are managed by non-FTC facility management personnel and are not included in this PIA. However, CC video recordings may be provided to the FTC via a justified investigative request. In the regional offices, any CCTV cameras are managed by FPS, GSA, or the local security, and are outside the scope of this PIA.

PACS System Administration

Physical Security Branch Personnel – Administrative user IDs and passwords are used to manage the PACS application. The Application System Administrators provide their first and last names.

OCIO IT Support Personnel – System Administrator user IDs and passwords are used to manage the operating system and hardware. The IT support personnel provide their first and last names.

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.

The system may contain video footage of the interior of FTC buildings. See also section 2.4.

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

The Access Control System is used for employee, intrusion detection, and video surveillance functions at FTC facilities as outlined in this PIA. The Access Control System also serves as a repository for all employee PII required for authorizing and monitoring physical access at FTC facilities.

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

Source of Data	*Type of Data Provided & How It Is Collected*
PACS (Server and Database)	• **<u>Employee/Contractor Profiles</u>**. These are manually entered into PACS by Physical Security Branch personnel for each employee/contractor issued a PIV or proximity card. These profiles are used by the card readers to authorize and/or deny access. The information collected is included in Section 2.1 above. • **<u>System Audit Logs</u>**. The PACS server logs all activity to support the requirement to record sufficient information to uniquely identify individuals and the time of access. The system data is never overwritten. • **<u>Physical Security Branch System Administrator and OCIO IT Specialist User IDs</u>**. These are manually entered by OCIO IT Specialists for each employee or contractor who manages employee/contractor profiles, and include individual user names, user IDs, and passwords. • **<u>Contract Security Maintenance Personnel User IDs</u>**. These are manually entered by OCIO IT Specialists and include individual user names, user IDs, and passwords.
NVR	• **<u>HQ and CC Camera Footage</u>**. The cameras collect video images through real-time monitoring on the associated NVR. The NVR records video from a variety of cameras, which allows the Security Officer monitoring the video feed to adjust the camera in real-time.
Visitor Management	• **<u>Paper Logs</u>.** Visitors to the HQ building provide the data elements identified in Section 2.1 above. • **Parking Garage Information**. The Security Officers in the

	Headquarters parking garage obtain information on vehicles parking in the garage from the vehicles entering the garage and directly from FTC employees and contractors who are permitted to use the garage.
Electronic High-Security Key	• The information in the key management database is collected from CADapult workorders or electronic key requests forms, which are submitted by FTC Administrative Officers or FTC personnel. Request forms submitted outside of CADapult are subject to Supervisor approval before the keys are issued.

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***
PACS Server and Database	• **FTC Physical Security Branch Personnel** – Data may be accessed daily to (1) input/modify/delete and/or audit employee profiles, (2) review/monitor access logs, (3) review/monitor alert logs, and (4) when necessary, to export data for use in internal or external investigation. • **Contract Physical Security Personnel** – Data may be accessed daily to input/modify/delete employee profiles. • **Contract Security Maintenance Personnel** – Access to troubleshoot or apply necessary upgrades. • **FTC IT Specialist and/or Contract IT Specialist** – Access to troubleshoot or apply necessary upgrages.
PACS Application (Live Streaming Video and Alert Data)	• **Contract Security Guards** – Read-only access via an application installed in each workstation. • **FTC Physical Security Branch Personnel** – Read-only access via an application installed on their assigned workstation located in their office/workspace.
CCTV Cameras (Physical Access)	• **FTC Physical Security Branch Personnel** – When necessary, will be accessed to troubleshoot or replace. • **Contract Security Maintenance Personnel** – Routinely accessed to perform maintenance, upgrades, and/or replacement.
NVR	• **FTC Physical Security Branch Personnel** – When necessary, data may be accessed (1) to review access or movement of employees and/or others, or (2) to export data for use in internal or external investigations upon approval. • **Contract Security Maintenance Personnel** – Accessed to troubleshoot or apply necessary upgrades – access is non-routine.

Visitor Logs	• **FTC Physical Security Branch Personnel –** Daily logs and parking garage records are collected from Guard Posts and securely stored in the HQ Physical Security Office. • **Contract Security Guards –** Security guards posted at visitor entrances collect information from visitors on paper logs.
Electronic High-Security Key	• **FTC Facilities Branch--**The FTC Facilities Branch personnel have administrative access to the data.

The FTC's Inspector General or an external investigative entity may be provided with data from access control system components for use in an investigation upon appropriate approval.

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.

Yes.

1. The Physical Security Branch uses FTC employees and contractors to input Employee/Contractor Profiles into the PACS database. Account privileges are established based on the FTC's Access Control Policy. All contractor personnel with access to the FTC's network are required to take the annual Information Security and Privacy Awareness training, and all profiles created by contractor personnel are audited regularly by Physical Security Branch employees for accuracy.

2. The OCIO uses contractor personnel as system administrators to maintain servers, workstations, and enterprise software for all agency IT equipment. Account privileges are established based on the FTC's Access Control Policy. OCIO contractor personnel are required to take the annual Information Security and Privacy Awareness training. OCIO applies the appropriate security controls (e.g., technical, operational, physical) as required by the Federal Information Security Modernization Act (FISMA).

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.

1. The contractor's privacy incident response plan is not applicable. Instead, the contractor is subject to the FTC's Breach Notification Response Plan.

2. OCIO contractors perform all of their work on an FTC-owned equipment These contractors are not permitted to remove data from the database. The contractor's privacy incident response plan is not applicable. Instead, the contractor is subject to the FTC's Breach Notification Response Plan.

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.

Sign-in sheets at FTC HQ visitor entrances are accompanied by a Privacy Act statement to inform individuals entering the building of their rights under the act. (For information about logs in shared buildings, see footnote 1.) When FTC employees or contractors are issued high-security electronic keys, they sign a form accepting responsibility for the key and agreeing to abide by applicable Rules of Behavior and FTC policies. That form includes a Privacy Act statement. Though not required, as a matter of policy, signs are posted in the FTC HQ lobby to provide notice of surveillance activities via CCTV cameras. In addition, as previously explained, notice is provided to employees and contractors assigned PIV or proxy cards at the time they are issued, and in the applicable Privacy Act System of Records Notice (SORN). (See Section 8.3 of this PIA regarding Privacy Act SORNs.)

☒ 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):____

☐ 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)?

PACS Server/Database – Employees and Contractors

No. HSPD-12 requires federal agencies to use a standard smart credential to verify the identities of all employees and contractors accessing federal buildings and information systems. The directive mandates all government personnel obtain PIV cards, which enhance security, increase government efficiency, reduce identity fraud and protect personal privacy.

PACS Server/Database – System Administrators

No. System Administrators provide PII when their accounts are established. Failure to do so may result in no establishment of their accounts.

NVR (Video Recording)

No. Individuals who enter onto Federal property or are in public space around such property do not have a reasonable expectation of privacy and therefore no consent is required. However, as a matter of policy, signs are posted in the FTC headquarters lobby to provide notice of surveillance activities via CCTV cameras.

Visitor Management Paper Log

No. Visitors who decline to provide information will not be permitted access to FTC facilities.

Electronic High-Security Key

No. FTC employees and contractors who require key-controlled access to FTC facilities must provide certain information to be assigned a key, and the system automatically records when the individual uses the key.

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

Yes. An individual may make a request under the Privacy Act for access to information maintained by the FTC about themselves in the Access Control System. Access to the information under the Privacy Act is subject to certain exemptions. Individuals may also file FOIA requests for agency records about them (if they are not exempt from disclosure to them under those laws).[3] Additionally, individuals may contact the FTC with any complaints, questions or concerns via phone or email available on www.ftc.gov or contact the Chief Privacy Officer directly.

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.

Yes. The FTC provides a process for individuals to correct or amend any inaccurate PII maintained by the FTC, including any information that may be stored in the Access Control System. The FTC's Privacy Policy provides links to the FTC's SORNs, which include information about how to correct or amend records. Where appropriate, the FTC disseminates corrected or amended PII to other authorized users of that PII, such as external information sharing partners. See also section 4.3.

[3] See 16 C.F.R. 4.11(a) (FTC FOIA rules), 4.13(m) (FTC Privacy Act rules).

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?

PACS Server/Database

FTC employee and contractor profiles are regularly reviewed and audited by Physical Security Branch personnel, and when necessary and approved, updates and/or deletions of information are completed. Information is regularly backed-up as required per the OCIO Contingency Planning Policy.

Visitor Management (Paper Logs)

Visitors are required to present some form of official identification to the HQ security guard to ensure that the log contains accurate information about the visitor's identity for security purposes.   Changes are not made to the visitor-provided information once entered in the log by the security guard. As noted earlier, visitors can review their log entry to ensure that the HQ security guard has recorded the correct information in the log during their sign-in process.

NVR (Camera Footage)

Cameras collect real-time video of the activities occurring within their reviewing space in or near an FTC facility.   Cameras may only record what is occurring in real time; there is no editing feature or ability to change the image.

Electronic High-Security Key

The FTC employee or contractor signs a form accepting responsibility for the key, and the Facilities or Security Office confirms that the name in the system matches the name on the form. The name and key assignment(s) can later be revised or corrected by the employee's or contractor's Administrative Officer or the Security Office.

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.

PACS Server/Database

Supervisors and/or Contracting Officer's Representatives (CORs) must identify and approve employee/contractor requests to access the PACS server/database and specify the appropriate user role and level of access privileges. Access is based on a valid access authorization and intended system use. All access is based on least-privilege and need-to-know security models. Additionally, auditing measures and technical safeguards are in place commensurate with the Moderate-Impact control Baseline of the National

Institute of Standards and Technology (NIST) Security and Privacy Controls for Federal Information Systems and Organizations Special Publication (SP) 800-53.

Visitor Management (Paper Log)

Daily, the visitor logs and parking garage records are retrieved from Guard Posts and stored in a locked cabinet for two years, after which time they are shredded by Physical Security Branch personnel.

NVR

Only Physical Security Branch (federal personnel) are authorized to access the stored video data, which resides on the NVR hard drives which are physically located in the HQ Data Center. The Data Center is physically accessed via a PIV card and such access is logged on the PACS database. Access to the NVR requires a user ID and password that follows FTC's Access Control Policy. The misuse of any FTC system will subject employees to administrative and potentially criminal penalties. Each user (Physical Security Branch federal employees) has a separate user ID and password for accessing the NVR's data.

Electronic High-Security Key

Only Facilities personnel have access to the key software program, which is password protected. The information in the key system is not highly sensitive.

5.3 Has the system/project undergone the appropriate security risk assessment and received authority to operate?

Yes. The FTC's Access Control System and its components, all of which are located on FTC premises and managed by FTC personnel, are included in the authorization to operate (ATO) for the Datacenter GSS.

The FTC follows all applicable FISMA requirements. The data is categorized as moderate using Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems.

5.4 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?

☒ Not Applicable

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 in the Access Control System, including information, if any, that may be incorporated into or otherwise required to be preserved as Federal records, is retained and destroyed in accordance with National Archives and Records (NARA) General Records Schedule (GRS) 5.6, Security Records..

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.

☒ 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*
PACS Server/Database **Inadvertent or unauthorized access to or disclosure of FTC employee or contractor data**	To reduce privacy risks, employee profiles are created using only the minimum amount of PII necessary to verify and grant physical access to FTC facilities and other restricted areas. Access to the system is based on a valid access authorization and intended system use. All access is based on least-privilege and need-to-know security models. Data stored on backups is encrypted.
NVR - Cameras **Collecting more information than is necessary**	The security cameras could collect more information than is necessary to accomplish the security and law enforcement purposes for which they are used. This risk is reduced by placing security cameras in public places only, as opposed to areas such as bathrooms and similar areas where individuals have a reasonable expectation of privacy. Only authorized Physical Security Branch personnel and Security Guards have access to live video feeds and stored images.
PACS Server/ Database and/or NVR	This risk is reduced by the Office of the Chief Administrative Services Officer (OCASO) Chain of Custody and Evidence Storage policy and procedure, which establishes guidance

Loss of Exported Investigative Data	regarding the collection, chain of custody, storage, and disposition of controlled materials collected by OCASO physical security office employees and contractors.
Electronic High-Security Key **Access by Unauthorized User**	The main privacy risk is the use of a valid key for access by an unauthorized user, whether by borrowing another user's key or finding a lost, misplaced, or stolen key, if such use is then mistakenly attributed to the employee or contractor who was assigned the key. This risk is mitigated by having FTC employees or contractors sign Rules of Behavior (RoB), which requires them to maintain possession and control of the key, limit lending or borrowing keys to very narrow circumstances, and require, consistent with FTC incident reporting policy, prompt notification to the Help Desk of a lost key. Upon notification, the EKM manager initiates an immediate protocol to deactivate a misplaced, lost, or stolen key, to prevent unauthorized access.

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

PACS Server/Database and NVRs

Yes. Access to the server/database occurs via the FTC network. The FTC network enforces system lock-out after several failed login attempts and logs all session activity with username.

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).

Yes: FTC II-11, Personnel Security, Identity Management, and Access Control Records System -- FTC, and VII-3 -- Computer Systems User Identification and Access Records -- FTC (for login credentials of system administrators). These system notices also explain the individual's rights and procedures for reviewing and accessing any records about themselves in the system.

FTC II-11 does not apply to CCTV, since these video records are not retrieved from the system by name or other personally assigned identifier subject to the Privacy Act to the extent that the Office of Inspector General (OIG) retrieves information from PACS, and CCTV.

All FTC SORNs are listed and can be downloaded from our public SORN page: http://www.ftc.gov/foia/listofpaysystems.shtm.

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?

Security managers annually review the log of security employee access to PACS and may conduct other reviews more frequently, as needed. PIAs, including this one, are reviewed routinely to ensure accuracy. In addition, all FTC staff and contractors must review and sign the FTC Rules of Behavior form and take privacy and security training on an annual basis.

The collection, use, and disclosure of the identification, authorization, and access data and login credentials described above are consistent with the privacy policy that the FTC provides to the public.