Federal Trade Commission
Privacy Impact Assessment

Azure

Microsoft Cloud Service

Published

November 2021

Table of Contents

1 System Overview

1.1 Describe the project/system and its purpose.

The Federal Trade Commission (FTC, Commission, or Agency) is an independent federal law enforcement and regulatory agency with the authority to promote consumer protection and competition through the prevention of unfair, deceptive, and anti-competitive business practices. Within the FTC, the Office of the Chief Information Officer (OCIO) operates and maintains the necessary Information Technology (IT) services to support the mission, including the network, servers, applications, databases, computers, and communication facilities.

As part of the agency's plan to modernize the existing IT infrastructure, the FTC utilizes the Microsoft Azure cloud environment and its affiliated products. Azure is an open and flexible cloud platform that provides Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (Saas), allowing the FTC to build, test, deploy, and manage applications, services, and product development across a vast network of datacenters within the U.S. The Azure commercial cloud provides the FTC with various services like computing, analytics, and networking (see table below).

Azure Data Factory (ADF)	ADF is used for data transformation and loading between different cloud data sources. ADF uses the built-in connectors and Integration Runtime Engine (IRE) to connect and transfer data within the Azure cloud in a secure manner.
Azure Synapse Analytics (ASA)	Previously known as Azure SQL, ASA is the enterprise analytics service that provides insight across data warehouses and big data systems.
PowerBI	This Business Intelligence (BI) tool is used to create and share meaningful reports and dashboards.
InTune	InTune is a cloud-based service that focuses on mobile device management (MDM) and is used by the agency to monitor and track FTC mobile phones.

Implementation of the Azure cloud architecture design addresses the FTC's data warehouse requirements, which includes planning and creating structures that will support future Azure utilization when required, while minimizing additional cloud expenses. The existing Azure cloud connects to other third-party cloud services like Okta and ServiceNow for data migration, authentication, and monitoring purposes. Azure services are used as part of the application and management infrastructure within the FTC. Azure's Active Directory (AD) is connected and synced with the FTC's on-premise AD services, and role-based access controls are implemented for accessing Azure. Azure is integrated with the FTC's Okta[1] Single Sign On (SSO) authentication service, and end user domain credentials are validated through the FTC's directory services.

[1] For more information about Okta, see the Okta Privacy Impact Assessment, available online.

Currently, the FTC considers Azure to be a subset of its existing General Support System (GSS)[2] with most of the control structure remaining unchanged. At the time of this publishing, the FTC's Premerger Notification Office (PNO) maintains the ServiceNow Premerger Application in the Azure cloud.[3] This PIA will be updated as the agency transfers more of its GSS applications and functions to the Azure cloud.

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

The information in this system is collected, maintained and disseminated pursuant to the Federal Trade Commission Act, 15 U.S.C. §§ 41-58 and other laws and regulations the Commission enforces.

2 Data Type, Sources, and Use

2.1 Specify in the table below what types of personally identifiable information (PII)[4] may be collected or maintained in the system/project. Check all that apply.

☒ 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	☐ Investigation Report or Database
☒ Sex	☐ Passport Number	☒ Driver's License/State ID Number (or foreign country equivalent)
☒ Email Address		☒ Other *(Please Specify)*: Company revenue, annual audit reports, financial share holdings, and the Central Index Key (CIK) number
☒ Work Address		
☒ Taxpayer ID		
☒ Credit Card Number		
☐ Facsimile Number		
☒ Medical Information		
☐ Education Records		
☒ Social Security Number		
☒ Mother's Maiden Name		

[2] For more information about the GSS, refer to the FTC's GSS Privacy Impact Assessment, available online.
[3] Click here for more information about the FTC's Premerger Notification Program, which examines large mergers and acquisitions as part of the agency's antitrust mission.
[4] Per OMB Circular A-130, personally identifiable information (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.

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.

Not applicable.

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

Azure's cloud services are used as part of the application and infrastructure management at the FTC. Azure collects information such as userID, IP address, and other PII from FTC employees and contractors for authentication and verification purposes.

Currently, the agency's premerger application resides on the Azure cloud. Premerger data is collected in order to ascertain whether a larger merger or acquisition is able to proceed or whether it violates antitrust laws.

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

FTC staff and contractors	FTC employees and contractors use Azure cloud services for securely accessing the required applications, such as the premerger application or the mobile device management system (InTune). Employees' names, email addresses, work phone numbers, user IDs, and PIN/passwords are used to validate users. They are authenticated through an enterprise directory associated with the FTC's Active Directory (AD) and granted role-based access. Azure is also integrated with the FTC's Okta authentication service. Azure requires creation of privileged accounts for access to the backend of the Azure cloud for administrative purposes. Access is managed through the Azure portal, which is only available to authorized FTC system administrators.
External/Commercial Entities	The Hart-Scott-Rodino Act established the federal premerger notification program, which provides the FTC and the Department of Justice with information about larger mergers and acquisitions before they occur. Outside parties and commercial entities submit premerger notifications online via the ServiceNow Premerger E-Filing Application, which is hosted in the Azure cloud. These notifications generally include the company name, business contact information (mailing address, email address, and phone numbers), as well

Source of Data	
	as financial information (company revenue, financial share holdings, annual audit reports, etc.). The FTC Premerger Notification Office and the U.S. Department of Justice access the ServiceNow application to manage the data from the filings for investigations and analysis.
Okta	Azure is configured to connect to the FTC's onsite AD through Azure's AD and OKTA SSO services for access authentication, identification, and validation purposes. Azure connects to Okta, ServiceNow, and Zscaler for data migration, authentication and monitoring purposes.
InTune	InTune is used for the monitoring, tracking, and management of the FTC's mobile phones. The data collected includes employee name, affiliated FTC mobile phone number, and device identifiers.

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.

FTC Staff and Contractors	Azure acts as the backend repository for various types of data collected from the public and other external sources. Only authorized FTC staff have direct access to information in the Azure cloud.
Department of Justice/Other Law Enforcement Partners	Authorized DOJ staff have access to the ServiceNow Premerger Application for investigation and analysis purposes. They do not have direct access to information in the Azure system.

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.

Authorized FTC contractors have access to information in the various applications housed in the Azure cloud. FTC contractors are required to sign nondisclosure agreements, complete security and privacy training prior to obtaining access to any systems, and complete annual security and privacy training to maintain network access and access to those systems. FTC contractors must follow the same guidelines and policies as FTC employees.

Other authorized federal agencies (e.g., Department of Justice) or law enforcement partners that have access to information store in the Azure cloud must agree to terms of use and non-disclosure agreements prior to access. Use is subject to authorization and approval by the FTC.

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.

FTC contractors who access the Azure cloud are subject to the same rules and policies as FTC staff, including the FTC's Breach Notification Response Plan. Azure staff do not have access to FTC data.

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 ☒ Verbal)
- ☒ FTC Website Privacy Policy
- ☒ Privacy Notice (e.g., on Social Media platforms)
- ☒ Login banner
- ☐ Other (*explain*):_____

☐ Notice is not provided (explain): _____

The FTC uses the Azure cloud to house various types of information collected by the agency. Whenever possible, the FTC's Privacy Act notices are included on all forms, websites, and other instruments by which Privacy Act information is collected from individuals, either in written or oral form, at the time of collection. For those occasions where the FTC cannot provide notice at the time the information is collected (e.g., when the information is collected by another law enforcement agency or another organization), the FTC provides notice via its privacy policy, its Privacy Act system of records notices (SORNs), and its PIAs, including this one.

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)?

The opportunity or right depends on how the information is collected and the purpose for the collection. For example, commercial entities filing electronically through the Premerger Application are required to provide information that includes business PII. The FTC needs this information to perform the due diligence and analysis required by the Hart-Scott-Rodino Act. Companies that are legally required to submit premerger filing information through ServiceNow. Similarly, an authorized FTC employee who wishes to access the backend of the application must provide their authentication information.

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

An individual may make a request under the Privacy Act for access to information maintained by the FTC about themselves in the Privacy Act systems that are hosted in the Azure cloud. The FTC's privacy policy provides links to the FTC's SORNs, as well as information about making Freedom of Information Act (FOIA) requests and the online FOIA request form. Individuals must follow the FTC's Privacy Act rules and procedures, published in the Code of Federal Regulations (C.F.R.) at 16 C.F.R. 4.13. Access to information under the Privacy Act is subject to certain exemptions set out in 16 C.F.R. 4.13(m).

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.

The FTC provides a process for individuals to correct or amend any inaccurate PII maintained by the Agency. The FTC's privacy policy provides links to the FTC's SORNs, which include information about how to correct or amend records. An individual may make a request under the Privacy Act for access to information maintained by the FTC about themselves in the applicable Privacy Act systems that are hosted in the Azure cloud. Access to the information under the Privacy Act is subject to certain exemptions set out in 16 C.F.R. 4.13(m). Individuals may also file requests with the FTC under the FOIA for agency records that may be about them (if they are not exempt from disclosure to them under those laws) or contact the Chief Privacy Officer directly. Where appropriate, the FTC disseminates corrected or amended PII to other authorized users of that PII, such as external information sharing partners. 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.

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?

Information in the Azure cloud that is used by the FTC as part of its law enforcement, policy, and other activities will be reviewed for accuracy and timeliness in accordance with the specific needs of that particular FTC activity.

Information in the Azure cloud is also subject to appropriate information security controls, as further described in Section 5.2 below. These controls will ensure that sensitive information is protected from any undue risk of loss and that the contents of evidentiary materials remain unchanged from the point-in-time they are included in the Azure.

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.

Azure is a cloud system housed in FedRAMP-certified data centers. Users from the internal FTC network are allowed to access Azure and other provided services based on roles and responsibilities.

Before any new FTC employee or contractor can access any information in the Azure cloud, that individual must complete new employee orientation and successfully complete the FTC's Privacy and Security Awareness training. All employees are granted basic network access to include email services, the Internet, the Intranet, network shared drives, network-based applications, and are assigned their own home directory. There are specific procedures to address access restrictions for higher-risk categories of employees such as interns and International Fellows.

Supervisors and/or Contracting Officer's Representatives (CORs) must identify and approve employee requests to access network applications and specify the appropriate user role and level of access privileges. Network and application access is based on: (1) a valid access authorization, (2) intended system usage, and (3) other attributes based on the system's business function. All network and application access is based on least-privilege and need-to-know security models.

Auditing measures and technical safeguards are in place commensurate with the National Institute of Standards and Technology (NIST) Recommended Security Controls for Federal Information Systems and Organizations Moderate-Impact Baseline Special Publication (SP) 800-53.

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?

☒ Not Applicable. PII is not used for 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?

Disposition of general technology management records and information system security records is authorized under National Archives and Administration (NARA) General Records Schedules 3.1 and 3.2. The disposition of the data will be covered by NARA-approved records disposition schedules of the FTC.

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.

Access to the Azure cloud is managed through the Azure portal, which is only accessible to authorized system administrators on the FTC network. The website is not open to members of the public.

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?

Unauthorized Access to Data (Logical and Physical Access)	Access to information is limited to authorized administrators and users that are given the smallest amount of system and data access necessary to accomplish their authorized tasks. Each new network user receives the most restrictive set of privileges and network access, and additional privileges and access must be authorized when appropriate. Only administrator(s) can access and modify the data. Those who develop reports have read only access. Physical access to the Azure is controlled, logged, and monitored by Microsoft.
Unauthorized Transmission of Sensitive PII	To address this risk, FTC policy generally requires that electronic documents (including emails) containing sensitive PII must be transmitted using an approved secure file transmission solution. Transfer of sensitive PII must also be preapproved and logged appropriately in accordance with FTC policy.
Use of Personally Owned IT Equipment	Personally owned devices are not allowed to be connected to any IT asset within the FTC's network. Access to the Azure cloud is only permissible on authorized FTC equipment to those with authenticated and verified user accounts.

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

Access to information in the Azure cloud system is only allowed via the FTC network, which:

- enforces system lock-out after several failed login attempts;
- logs all session activity with username along with the IP addresses or domain names of the system components accessed; and

• requires two-factor authentication for elevated access to the network.

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 Azure cloud itself is not considered to be a Privacy Act System of Record. However, the systems and applications supported or hosted in the Azure cloud have the appropriate SORN(s) as necessary. For example, to the extent any premerger filing data is about an individual and retrieved by that individual's name or other personal identifier, that data is part of the nonpublic investigative records system (FTC-I-1).

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?

The collection, use, and disclosure of information in this system are consistent with the FTC's Privacy Policy. Access logs, storage logs, and firewall logs are periodically reviewed to ensure that users are complying with GSS policies and procedures. In addition, all FTC staff and contractors must review and sign the FTC Rules of Behavior on an annual basis.