

Federal Trade Commission
Privacy Impact Assessment

Azure

Microsoft Cloud Service

Published

November 2021

Updated

February 2022

Table of Contents

1	System Overview.....	1
2	Data Type, Sources, and Use	2
3	Data Access and Sharing.....	4
4	Notice and Consent	5
5	Data Accuracy and Security.....	6
6	Data Retention and Disposal.....	7
7	Website Privacy Evaluation.....	8
8	Privacy Risks and Evaluation	8

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 authority to promote consumer protection and competition through the prevention of unfair, deceptive, and 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 uses 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)

Application

Azure Data Factory (ADF)

Purpose

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.

Currently, the FTC considers Azure to be a subset of its existing General Support System (GSS) 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. 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](#) 192d-3.3 tarsons(nd d)10.4

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 user ID, IP address, and other PII from 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?

<p>FTC staff and contractors</p>	<p>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.</p> <p>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.</p>
<p>External/Commercial Entities</p>	<p>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 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</p>



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) we es by

7 Website Privacy Evaluation

- requires twofactor authentication for elevated access to the work.

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 about an individual and retrieved by that individual's name or other personal identifier, that data is part of the [nonpublic investigative records system](#) (ETC-I 0 TRNT