Federal Trade Commission
Privacy Impact Assessment

ServiceNow
Administrative E-Filing Application

August 2020

Table of Contents

1 System Overview

1.1 Describe the project/system and its purpose.

The Federal Trade Commission (FTC) has updated its system for receiving and managing electronic filings in FTC administrative proceedings under Part 3 of its Rules of Practice, by incorporating a web-based application developed on the ServiceNow platform[1]. Part 3 sets forth the procedures for competition and consumer protection cases tried before an Administrative Law Judge (ALJ) of the FTC, and appeals of the ALJ's initial decision to the full Commission. During Part 3 proceedings, electronic filings and public documents are received and served electronically.

Administrative E-Filing, or Admin E-Filing, allows users to submit public and nonpublic pleadings and motions in Part 3 administrative litigations before the ALJ and the Commission. Submitting these documents electronically speeds up the process for circulating these filings to the relevant offices within the Commission and reduces costs incurred for scanning and courier fees.

In order to use the Administrative E-Filing application, a user (i.e., lawyers representing respondents or third parties in the Part 3 matter) must register with a unique user ID and password. The user's name, company name, work address, work telephone number, work email address, and bar admission number (if applicable) are required to register. The user is then required to enter a Notice of Appearance[2] in a specific administrative litigation. Once the Notice of Appearance has been approved, the user may submit filings electronically through the system for that specific matter.

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 FTC Act, 15 U.S.C. §§ 41-58, the Rules of Practice, 16 C.F.R. §§ 0.1 *et seq.*, and other laws and regulations the Commission enforces.

[1] For more information about ServiceNow, refer to the Privacy Impact Assessments available online.
[2] Available online at https://www.ftc.gov/system/files/attachments/faqs/file-documents-adjudicative-proceedings/ftc-232.pdf.

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	☐ Investigation Report or Database
☐ Sex	☐ Passport Number	☐ Driver's License/State ID Number (or foreign country equivalent)
☒ Email Address		☒ Other *(Please Specify)*: Login and logout times, Company name, Bar admission jurisdiction, Bar admission number (if applicable), User password[4]
☒ 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.

The user is able to enter the title of the filing being submitted and upload a copy of the document being filed. This information will be retained in the system for 90 days after the

[3] 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.

[4] Passwords for FTC users are authenticated through the Active Directory system; passwords for external users are collected and stored in OKTA, another third-party commercial identity and access management solution service used by the FTC. A separate PIA is maintained for the agency's use of OKTA.

filing has been successfully submitted. After 90 days, this information will be deleted from the system.

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

It is necessary to collect this information (i.e., Notices of Appearance) from filers in order to submit public and nonpublic pleadings and motions in Part 3 administrative litigations. The user registration information is collected and maintained in order to authenticate the user in the systemAs noted in 2.2, the system also collects non-PII from users (i.e., pleadings and other documents filed on behalf of users or their clients) for purposes of Part 3 administrative litigation.

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***
Filing individual (External non-FTC user)	The filer must register with the Admin E-Filing system by providing their name, company name, work address, work telephone number, and work email address, and bar admission number (if applicable). The filer must also submit the Notice of Appearance form. The filer enters the "Document Title" for the E-Filing submission and select the confidentiality status of the submission. Login credentials are maintained in the OKTA identity management system.
FTC employees and contractors	As with the external user, an FTC staff person filing must also submit the Notice of Appearance form (see 2.3), enter the "Document Title" for the E-Filing submission, and select the confidentiality status if the submission. The FTC Review and Administration team inputs the docket information and reviews/updates the status of filings. The FTC user's login information (user ID, time of login and logout), as well as roles and access permission levels, are maintained within the ServiceNow system.

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 employees and contractors	FTC staff in the Records and Information Management (RIM) office and Office of the Secretary (OS) access the E-Filing application to review and process the filing. Authorized users in these offices have access to all documents submitted. FTC staff in the Office of Administrative Law Judges (ALJ) performs the initial adjudicative fact-finding in the agency's administrative complaint proceedings. They have access to all the data in the system in order to review the information as well as to upload documents. FTC staff in their roles as complaint counsel have limited access to the application to submit documents for Commission and/or ALJ consideration. FTC support contractors also have access to all the information in the E-Filing application in order to review and process the data.
ServiceNow Administrators	For troubleshooting and maintenance purposes, authorized ServiceNow system administrators have access to data in E-Filing.
Non-FTC parties (Respondent/Third parties appearing in Part 3 matters)	External respondents and third parties may have access to E-Filing in order to submit documents for Commission and/or ALJ consideration. They will only have access to those documents that they (the non-FTC party) submit.

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, FTC contractors will have access to data in the system. Contractors must use FTC-issued laptops to access the system, using their PIV cards. All FTC contractors are required to sign non-disclosure agreements (NDA), complete security and privacy training prior to

obtaining access to any FTC systems, and complete annual security and privacy training to maintain network access and access to those systems.

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 with access rights to the ServiceNow E-Filing application are subject to the same rules and policies as FTC staff, including adherence to the FTC 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.

☒ 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*): Every external user is required to sign the FTC Rules of Behavior (ROB) prior to use of the Application.

☐ 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)?

No. Users who do not register to use the system are not able to file electronically using the Admin E-Filing system. Additionally, users who decline to accept the Rules of Behavior (ROB) cannot register for system access and are therefore unable to use the system.

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

Yes. Individuals can log into their account and access limited personal information about themselves, such as their password and security questions. They do not have the ability to change their profile information or access log details about their activity. An individual may make a Privacy Act request to the FTC for access to additional information maintained about them in the ServiceNow Admin E-Filing application. See Commission Rule 4.13 (Privacy Act request procedures). Access to the information under the Privacy Act may be subject to certain exemptions. See Commission Rule 4.13(m). Individuals may also file Freedom of Information Act (FOIA) requests for agency records about them (if they are not exempt from

disclosure to them under those laws). 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 ServiceNow Admin E-Filing application. As stated above in 4.3, individuals can file requests with the FTC under the FOIA and the Privacy Act for access to any agency records that may be about them and are not exempt from disclosure to them under those laws. 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.

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.

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?

It is incumbent upon the person submitting the filing to ensure that the information contained therein is accurate and up to date. Additionally, all Notices of Appearances submitted through the system are reviewed by the FTC OS administrator. Additionally, all other filings submitted through the E-Filing application are reviewed by the RIM office and OS reviewers; filings that are not in compliance are returned/rejected.[5] Once the RIM office and OS reviewers return a filing due to non-compliance, then the system sends a notification to the filer detailing the reason for rejection. The rejected filing is deleted from the system immediately.

[5] Examples of why a filing may be rejected due to noncompliance may include the following: Filing before the Commission with the wrong caption before the ALJ or vice versa; not appropriately labeling the filing (public or confidential); submitting a filing when the relevant hearings is stayed; or when the filing does not comply with the Commission's Part 3 and Part 4 Rules.

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.

Yes, below are some examples of administrative procedures, technical safeguards, and controls in place to protect and ensure proper use of data in ServiceNow Admin E-Filing application.

The principle of least privilege is used to grant access to FTC staff and contractors, and user actions are tracked in the system audit logs. All FTC positions are assigned a risk designation that has associated criteria for personnel screening. All potential FTC staff, contractors, and volunteers are subject to background investigations and suitability reviews in accordance with OPM guidance.

All authorized users are required to use two-factor authentication to access the application. Authorized FTC users of the application must use their PIV cards along with a PIN to access data in the system. External users must authenticate with a registered username and password and agree to receive a one-time passcode (OTP) by voice or use an OTP token authenticator app on their smartphone in order to use the application. Additional safeguards for FTC users include role-based access controls at the application level to control who has access to what data in the application.

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.

The system automatically disposes of the following PII elements 90 days after a document has been uploaded to the system: Bar admission jurisdiction, Bar admission number, and work address.

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

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?

Electronic input source records (filings) will be retained in the Administrative E-Filing Application for 90 calendar days in accordance with National Archives and Records Administration (NARA) GRS 5.2, item 020, Intermediary Records.

During this time, the filings will be uploaded, validated, and stored within ServiceNow. Documents that do not meet the administrative filings requirements will be rejected and deleted from the system immediately.

The metadata associated with a Notice of Appearance (NOA) will be maintained for 90 days until the corresponding proceeding is closed in order to allow users to further submit filings beyond the initial 90-day period.

Help desk and related customer service desk operation records will be retained per NARA GRS 5.8, item 010, Technical and administrative help desk operational records, for 1 year after resolution of request, or when no longer needed for business use, whichever is appropriate.

In order to dispose of the data, the authorized FTC administrator submits a ServiceNow request for the deletion of the data. The ServiceNow O&M Contractor performs the task of manually deleting the defined data from the E-Filing application.

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.

Yes, the application does employ the use of a Website. ServiceNow utilizes session-based cookies to enable core site functionality. ServiceNow refers to these as "required" cookies. ServiceNow may use required cookies to authenticate user access to various areas of the site. Other cookies allow ServiceNow to enhance the user's browsing experience, tailor content to the user's preferences, and make user interactions with ServiceNow more meaningful.

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***
Misuse of data by authorized users	Prior to receiving access to the FTC's network, all users must agree to the FTC Rules of Behavior, which includes consenting to monitoring and restrictions on data usage.
Unauthorized system access	All FTC users must have an FTC account and government-issued personal identity verification (PIV) card to access ServiceNow. FTC's user identity management processes include authentication with enterprise directory to control and manage access restrictions to authorized personnel on an

Risk	*Mitigation Strategy*
	official need-to-know basis. The FTC utilizes a combination of technical and operational controls to reduce risk in the ServiceNow environment, such as encryption, passwords, audit logs, firewalls, malware identification, and data loss prevention policies. As a FedRAMP-approved cloud service provider, ServiceNow undergoes regular reviews of its security controls. External users will be required to authenticate using two-factor authentication: username/password and OTP passcode delivered to user (voice or token authenticator app on their smartphone).
Data leakage	Non-FTC ServiceNow system administrators are not allowed to review, audit, transmit, or store FTC data, which minimizes privacy risks from the vendor source.
Eavesdropping	The users interact with the Admin E-Filing application over the TLS protocol (https), an authenticated protected channel.

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

The Admin E-Filing application inherits all privacy controls from the parent ServiceNow application. This includes an automatic logoff after 15 minutes of inactivity, deactivating users after 35 days of account inactivity, and locking user accounts after 3 incorrect password attempts. External users can only view and access information and data that they have submitted into the application. External users can only file attachments after their Notice of Appearance (NOA) has been approved by an OS administrator.

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).

Information collected about users from their Notices of Appearances is considered part of FTC VII-3 -- Computer Systems User Identification and Access Records – FTC. Pleadings or other filings and documents submitted by users through the system are part of FTC I-1 -- Nonpublic Investigational and Other Nonpublic Legal Program Records – FTC. To the extent such pleadings or other documents are placed on the public record of the Part 3 administrative proceeding (i.e., posted on the FTC's public web site), such materials are part of FTC I-6 -- Public Records -- FTC. These SORNs may be read and downloaded at https://www.ftc.gov/site-information/privacy-policy/privacy-act-systems.

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 administrative and technical controls described in section 5.2 of this document provide assurance that the collection, use, and maintenance of the information will be conducted as described in this PIA. This PIA aligns with the FTC's existing privacy policies and procedures, and is subject to periodic review by the Office of the Chief Privacy Officer (OCPO), in consultation with relevant program staff and other relevant agency officials.