Federal Trade Commission
Privacy Impact Assessment

ServiceNow
Print Tracking Application for FTC Consumer and Business Publications Bulk Order Data

(Print Tracking)

April 2020

Table of Contents

1 System Overview

1.1 Describe the project/system and its purpose.

The Division of Consumer and Business Education (DCBE), a division within the FTC Bureau of Consumer Protection (BCP), develops print publications to inform consumers of their rights and to educate businesses about their responsibility to comply with laws enforced by the FTC. The FTC provides these materials to a variety of customers, which include individual members of the public, libraries, credit counseling services, police departments, Congressional offices, community-based organizations, trade associations, corporations, as well as federal, state, and local government offices and institutions. These orders are received via bulkorder.ftc.gov, a web-based order system that allows customers to select and order materials from a catalog of FTC publications.[1] In order to ensure that the FTC is well-stocked with the necessary publications and to maintain the capability to report analytical data, the agency uses the Print Tracking application developed on the cloud-based ServiceNow platform to track the type and number of publications printed, as part of the agency's ongoing migration of various on-site IT business support applications to ServiceNow.
Inventory levels are maintained and monitored by the FTC's publication distributor, the Government Publishing Office (GPO) in Pueblo, Colorado. On a weekly basis, FTC staff receive this information from GPO Pueblo and upload it to the Print Tracking application. A separate XML report containing all publication orders and associated publication data is generated from the Bulk Order system and also imported into the Print Tracking application. This information is used to create reports, identify trends, and ensure inventory levels in the Print Tracking application.

This PIA discusses the privacy impact of the agency's use of Print Tracking to compile, analyze, and report data about bulk print publications that members of the public may order online from the FTC.

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.

[1] For additional information, refer to the Publication Bulk Order Privacy Impact Assessment available at www.ftc.gov.

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: 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)*:_____
☒ Work Address		
☐ Taxpayer ID		
☐ Credit Card Number		
☐ Facsimile Number		
☐ Medical Information		
☐ Education Records		
☐ Social Security Number		
☐ Mother's Maiden Name		

The application contains open text fields where FTC users have the option to input additional information if necessary.

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 Print Tracking application maintains the following types of data related to publications printed: GPO Pueblo code publication title, language, packing options, format, pages, dimensions, and counts per carton. Other information maintained in the system pertaining to publication orders include: order type, order status, date of order, estimated cost, actual cost, and budget information.

[2] 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.

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

Information is mainly collected and utilized within the ServiceNow Print Tracking application for the purpose of tracking print publication inventory, budget, and order information so the agency can maintain inventory, minimize costs, and report on outreach efforts.

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*
Publication Bulk Order System	Publication order data including the publication name and contact information for the entity, including email address, phone number, organization, shipping address, and opt-in status are all collected via an XML export accessible only to authorized users of the bulkorder.ftc.gov website. The Print Tracking application has an import function, allowing an authorized system administrator to load the XML document into the application.
GPO Pueblo	Inventory data from GPO Pueblo is sent via XML to FTC staff on a weekly basis; authorized FTC system administrators then upload it to the Print Tracking application.
FTC employees and contractors	Usernames of FTC employees and contractors with access to the system are maintained, as well as their roles and access permission levels.

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	Authorized FTC administrators will have access to the system with an assigned role and set of permissions to manage the FTC's print distribution needs. Division of Consumer and Business Education (DCBE) Staff will have read/view only access to the data to perform their business needs, but will not have the ability to update/edit data.

Data Will Be Accessed By and/or Provided To:	*How and Why the Data Will Be Accessed/Shared*
ServiceNow administrators	ServiceNow administrators (also considered FTC contractors) have access to system data in order to perform Operations and Maintenance responsibilities.

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, contractors have access to data in the Print Tracking application.

All FTC contractors are required to sign NDAs, 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 and authorized ServiceNow system administrators who have access to the Print Tracking application are subject to the same agency rules and policies followed by FTC staff. All contractors must also abide by the FTC's Breach Notification Response Plan in the event of an incident or breach.

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*):_____

☒ Notice is not provided (explain): The ServiceNow Print Tracking application will not be the collection point for PII. Information is downloaded from the FTC Bulk Order website, where customers are provided with a Privacy Act statement and a link to the FTC's privacy policy on the online order form.

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, individuals do not have the opportunity to decline to provide information or consent to particular uses of their information in the Print Tracking application. Customer information imported from the FTC Bulk Order website is maintained in the Print Tracking application for the purposes of tracking orders and maintaining inventory. Members of the public may decline to provide information for the Publication Bulk Order system, but orders for FTC publications cannot be processed without accurate personal information required for shipping and communications.

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 ServiceNow Print Tracking application. 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 ServiceNow Print Tracking application. 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.

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?

Due to the nature of the ServiceNow system, information that is imported into the Print Tracking application generally will not be checked for accuracy or completeness. The application only accepts valid XML files, and the XML files must be in a specific predefined format. If the file is not valid, the application will not make any changes to the data. The

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

XML files have attributes such as that, if the same file is imported twice, the application will automatically update the records that are changed. Data imported from the FTC's Bulk Order website and Pueblo inventory is relied upon for accuracy, timeliness, and completeness of the data in the Print Tracking application.

System administrators ensure user information is complete and accurate for access privileges through enterprise direct authentication; however, data entered or created by end users will not be validated or reviewed by system administrators for accuracy or completeness.

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.

There are administrative procedures, technical safeguards, and controls in place to protect the data in the system and ensure proper use of the ServiceNow Print Tracking application. FTC authorized users are required to use two factor authentication to access the application, which includes the use of their PIV card. Additional safeguards include role based access controls at the application level to control who has access to what data in the application.

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

Yes, PII data is used for testing the application in the test environment, which is separate from the production environment. The test environment is restricted to only a limited number of authorized testers and the development contractor. This data is deleted from the test environment within 90 days of the system going into production mode.

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?

PII data will be disposed of every 3 years or sooner as required by the National Archives and Records Administration (NARA) General Records Schedule (GRS) 6.5, item 020, Customer Records.
Procedure for disposing the data:

- The FTC Print Tracking authorized administrator will submit a ServiceNow request for the deletion of the data
- The Print Tracking ServiceNow O&M Contractor on receipt of the authorized request will perform the task of deleting the defined data.
- Depending on the requirement for data deletion the data will be deleted through the UI or a script will be executed for deleting the data.

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 ServiceNow Print Tracking application is a web-based application, and utilizes both session-based and persistent-based cookies to enable core site functionality. The application is only accessible to internal FTC users on the FTC network, and members of the public do not have the ability to access the website. Thus, these cookies do not track or collect any data about them, and only about internal FTC users of the app.

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 consent to monitoring and restrictions on data usage.
Unauthorized system access	All 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 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.
Data leakage	The contract between FTC and ServiceNow does not allow the service provider to review, audit, or transmit, or store FTC data outside of the FTC ServiceNow instance, which minimizes privacy risks from the vendor source.

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

User access is managed through the FTC's enterprise directory infrastructure, which uniquely identifies, authenticates, and applies permissions to authorized user sessions based on FTC policies and procedures. This allows the FTC to leverage organizational multifactor authentication solutions, including HSPD-12, already deployed to meet internal identification and authentication requirements. The use of enterprise directory service also allows automatic enforcement of certain policies and requirements, such as password complexity and maximum-log in attempts, for organizational users.

Additionally, FTC security policies require automated monitoring of information system components with regard to flaw remediation.

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 ServiceNow Print Tracking application does not qualify as a system of record as users do not retrieve records using any personal identifier (e.g., name of individual who ordered the publication). The application, however, processes ordering data collected by the bulk ordering system, which is subject to the Privacy Act and has a SORN. See FTC VI-1 (Mailing and Contact Lists—FTC), which can be viewed on the FTC's web site, see 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.