Federal Trade Commission
Privacy Impact Assessment

for the:

Secure Investigations Lab
(SIL)

Updated
March
2019

1 Overview

The mission of the Federal Trade Commission (FTC or agency) is to enforce the Federal Trade Commission Act by preventing the use of unfair methods of competition and unfair or deceptive acts or practices; to enforce many other consumer protection and antitrust statues; and to enhance informed consumer choice and public understanding of the competitive process. In support of these activities, the FTC often receives data sets to conduct investigations and perform long-term studies. Some of these data sets may be designated for special handling because of the nature or the volume of the data, the analysis required, or other considerations. For example, a data set may contain significant volumes of personally identifiable information (PII) or it may require analysis of sensitive PII[1] or Sensitive Health Information (SHI).[2]

The Office of the Chief Information Officer (OCIO) created the Secure Investigations Lab (SIL) to allow FTC staff to work with certain data sets while supporting the agency's investigations, litigation, and studies. The SIL is a secure computing environment--isolated from the FTC's production, development, and test lab networks--that is configured with statistical and analytic software and sufficient processing power to allow the efficient analysis of the extremely large and/or sensitive data sets that are collected to support the agency's mission and regulatory activities.

The SIL allows authorized FTC users to securely import, store, work with, and export data sets that are received by FTC staff in connection with investigations, litigation, and other authorized projects and that are designated for special handling. The SIL is maintained by authorized administrators: it cannot be accessed directly from the Internet, and it cannot be accessed by third parties; only authorized FTC users can access SIL.

2 Information Collected and Stored within the Application

2.1 What information is to be collected, used, disseminated, or maintained by the application?

The SIL is used to store and analyze data sets that have been designated for special handling because of the nature or volume of the data, the analysis required, or other considerations. The FTC obtains this information in

[1] For purposes of this PIA, sensitive PII refers to the following information, whether in paper, in electronic form, or communicated orally:

(1) An individual's Social Security Number (SSN);
(2) Sensitive Health Information;
(3) a Biometric Identifier; or
(4) an individual's name or address or phone number in combination with one or more of the following: date of birth; driver's license number or other state identification number, or foreign country equivalent; military identification number; passport number; financial account number; or credit or debit card number.

[2] For purposes of this PIA, SHI includes medical records and other individually identifiable health information, whether on paper, in electronic form, or communicated orally. Sensitive Health Information relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

connection with its law enforcement and other activities, and the SIL contains data in a variety of electronic formats, including:

- word processing files
- spreadsheets
- databases
- emails
- images
- videos
- audio files

Personal information obtained by the FTC and stored in the SIL may, for any particular matter, include names, home/work addresses, telephone numbers, e-mail addresses, birth dates, age, race/ethnicity, sex, social security numbers / tax identification numbers, military ID numbers, driver's license/state ID numbers, place of birth, geolocation information, bank account numbers, credit card numbers, other financial information, audio recordings, , employment and salary information, employee identification number (EIN), military status/records, education records, medical record identification numbers, and other health diagnosis and treatment details. Given the varied data sets that are stored in the SIL, the list above may not be exhaustive. This personal information is located in financial transaction data, loan files, credit reports, consumer complaints, affidavits, hospital and patient records, and other similar records produced during litigation, investigations, and other FTC matters.

2.2 What are the sources of the information in the application?

Typically, the FTC obtains information stored in the SIL from targets of its law enforcement activities, companies filing under the Hart-Scott-Rodino (HSR) Act, and from individuals and entities with information that may be relevant to the FTC's enforcement and other activities. Sources may include consumers; local, state, federal, and foreign government agencies; and private sector entities, including financial institutions, hospitals, and insurance companies. Information may be provided to the FTC voluntarily (e.g., from companies that wish to merge, or from consumers who file complaints with the FTC), via compulsory process (e.g., subpoenas or civil investigatory demands), or through discovery in matters in litigation. Information for other activities, such as economic analyses, may, in limited cases, be obtained from third parties.

2.3 Why is the information being collected, used, disseminated, or maintained?

The data sets stored in the SIL are collected, used, and maintained in connection with the FTC's law enforcement and other activities. Law enforcement activities include investigations of potential or alleged violations of anticompetitive practices as well as investigations and enforcement actions related to alleged violations of statutes protecting consumers against fraudulent, deceptive, or unfair practices in the marketplace. Other activities include studies, rulemakings, and economic analyses.

2.4 How is the information collected?

The data sets stored in the SIL are obtained from a variety of sources, including information provided to the FTC voluntarily, via compulsory process or discovery, purchased from data vendors, and through other investigative sources. Voluntary submissions may include information provided to the FTC by consumers, private sector entities, law enforcement partners, regulatory agencies, and others. Information obtained via compulsory process includes information provided to the FTC pursuant to any one of the mechanisms available to the agency for compelling an individual or entity to provide information, including CIDs, access orders, and subpoenas.

Information obtained via discovery includes information provided to the FTC pursuant to any one of the mechanisms available to parties litigating matters in the Federal Courts of the United States, including court orders, requests for admissions, sworn statements (e.g., declarations, affidavits, depositions, and interrogatories), and electronic and documentary evidence.

Information required for FTC studies may be obtained in a variety of ways, including via solicitations to relevant external parties or pursuant to section 6(b) of the Federal Trade Commission Act.

2.5 How will the information be checked for accuracy and timeliness (currency)?

The data sets that are collected and stored in the SIL are not systematically checked for accuracy and timeliness. However, information that is used by the FTC as part of its law enforcement and other activities will be reviewed for accuracy and timeliness as appropriate to the particular FTC activity. For example, staff performing a merger or fraud investigation may confirm that the information in the SIL data set for that particular matter is timely and accurate, and FTC staff analyzing information from a SIL data set for use in an economic study may cross-check their results in the aggregate against publicly available information.

The SIL, like other FTC network environments, is subject to appropriate security controls and OCIO policies and procedures. SIL procedures, controls, and Rules of Behavior (RoB) help protect SIL data sets against undue risk of loss and ensure that the contents of evidentiary materials remain unchanged from the point-in-time they are included in the SIL.

2.6 Is the application using technologies in ways that the FTC has not previously employed (e.g., monitoring software, Smart Cards, etc.)? If so, how does the use of this technology affect individuals' privacy?

No. The SIL uses technologies that are deployed elsewhere within the FTC production, development, and test lab network environments.

2.7 What law or regulation permits the collection of this information?

Several statutes authorize the FTC to collect and store the information that is maintained in SIL data sets, including the Federal Trade Commission Act, 15 U.S.C. §§ 41-58; the Privacy Act of 1974, 5 U.S.C. § 552a; the Sherman Act, 15 U.S.C. § 1–7; the Clayton Act, 15 U.S.C. § 12–27, 29 U.S.C. § 52–53; the Hart-Scott-Rodino Antitrust Improvements Act, 15 U.S.C. § 18a; and the Robinson-Patman Act, 15 U.S.C. § 13.

2.8 Considering the type of information collected and sources of collection, what privacy risks were identified and how were these risks mitigated?

There is a risk that the original digital media used to load data sets into the SIL may be lost after initial receipt from external parties. To address this risk, the FTC has put in place a chain of custody for media and has established policies, procedures, and RoB, all of which ensure that SIL data is properly copied, transported, and stored. Additionally, all original digital media, when not in use, is locked in a safe that is located in a locked room.

There is a risk of unauthorized access, modification, and/or misuse of personal information in SIL data sets by FTC personnel. To address this risk, SIL networking components and computing resources are physically accessible only by authorized administrators. Authorized FTC users can only connect to the SIL from their internal FTC workstations via an SSL VPN using two-factor authentication. The SSL VPN technology is deployed on the FTC internal network and provides the only logical access to the segregated SIL network. Authorized SIL users cannot access the SIL directly from the Internet, and third parties do not have direct access to SIL. In addition, SIL users are granted access to data sets in matter-specific SIL folders on a need-to-know and least privilege access basis. SIL users cannot access SIL data sets for matters that they are not working on, and a Bureau of Economics representative requests that the SIL administrator remove the user's permissions from folders once the user no longer needs access to the folder. Matter-specific SIL folders are deleted when the data are no longer required for the investigation or for studies. Additionally, the FTC Personnel Security Office performs various types or levels of background investigations on every FTC employee. The SIL is accessible only by authorized administrators and authorized FTC users, all of whom have received a Minimum Background Investigation (MBI) and Criminal History and Credit Checks.

There is a risk that digital copies made of SIL data sets may be removed or lost. To address this risk, the FTC has put in place a chain of custody for digital copies of SIL data sets. All requests for digital copies of SIL data sets must be initiated by designated individuals, and movement of SIL data sets must be properly documented. Finally, all digital copies of SIL data sets must be encrypted using FIPS 140-2 standards.

There is a risk that printed documents or reports containing data from SIL data sets may be lost. To address this risk, the FTC has deployed multiple media protection controls, including limiting physical access to the SIL printer, enforcing print logging (SIL users must save the cover sheet of every document printed in the SIL), providing secure hard copy disposal methods (shredder and burn bags), RoB, and signs in the SIL printer room

reminding SIL users of their responsibilities.

There is a risk that software to be used in the SIL may contain malware that could run in the SIL environment. To reduce this risk, security scans are run on the software before it is used in the SIL.

Periodically the FTC is required to remove data from the SIL and transfer it to authorized third parties, such as expert witnesses, who must access this data outside of the FTC's network to complete their job functions. Sharing data with third parties in this way creates the risk that the third parties will store data in an insecure fashion. To address this risk, the FTC includes non-disclosure agreements and provisions in contracts (where appropriate) that mandate secure handling of the data the FTC stores in the SIL. Additionally, transfers to authorized third parties are made only by secure (e.g., encrypted) means.

3 Use and Access to Data in the Application

3.1 Describe how information in the application will or may be used.

FTC staff will use the SIL when a secure network environment is necessary to work with data sets that have been designated for special handling because of the nature or volume of the data, the analysis required, or other considerations. For example, the Bureau of Economics (BE) conducts economic studies, supports antitrust and consumer protection investigations and litigation, analyzes existing and proposed consumer protection rules, and studies the competitive impact of regulations for the Commission. Certain BE data sets may contain, for example, significant volumes of sensitive PII or SHI, and, as a result, those data sets would be stored in the SIL, and BE would conduct its analyses in the SIL.

3.2 Which internal entities will have access to the information?

As discussed in section 2.8, only authorized FTC users and authorized administrators will have access to the SIL. In addition, as discussed in 2.8, above, access to matter-specific folders are granted on a need-to-know and least privilege access basis, and matter-specific folders are deleted at the end of the investigation or study unless they are needed for further research.

3.3 Which external entities will have access to the information?

Although information in the SIL may be derived from external sources and in some cases may be used or incorporated into other confidential materials (e.g., *in camera* filings in litigation or discovery subject to protective orders), external entities will not have direct access to SIL. However, the FTC will transfer data stored in the SIL to authorized third parties, such as expert witnesses, if needed to complete their job functions. Data that the FTC stores on the SIL will be shared with external entities only as permitted by statute, FTC rules of practice, and data use agreements, where

applicable, or as required by court rules or court order.

4 Notice and Access for Individuals

4.1 How will individuals be informed about what information is collected, and how this information is used and disclosed?

Individuals who provide the FTC with information pursuant to discovery or a related court order are provided with notice of what information is being collected, and may in some cases be provided notice by the FTC as to how information may or will be used or disclosed (e.g., *in camera* or protective orders). Generally, the use and disclosure of this information is controlled by applicable discovery rules and court orders. Similarly, if such information is provided voluntarily, the FTC may provide notice about collection, use, and disclosure at the time the information is collected or through other means (e.g., negotiated agreements).

4.2 Do individuals have the opportunity and/or right to decline to provide information?

Yes, in some instances (e.g., by asserting privilege in response to discovery or court orders, or withholding the materials when the information has been requested by voluntary production). In such instances, the FTC has the right to pursue additional legal relief to compel provision of the information.

In other instances, an individual does not have the opportunity and/or right to decline to provide information that is stored in the SIL. For example, if an individual provides sensitive PII to an entity that the FTC subsequently subpoenas, the FTC may receive that sensitive PII and store it in the SIL without the individual's knowledge or consent.

4.3 Do individuals have the right to consent to particular uses of the information? If so, how would an individual exercise this right?

Yes, in some instances. When information is provided voluntarily, the use of such information may also be governed by mutual agreement. If the individual has a right to consent to particular use, this right will normally be exercised when determining whether to provide information to the FTC. Some uses of information are not subject to the consent of the individual providing the information (e.g., information provided pursuant to a court order or subpoena). In addition, uses of information may also be governed by specific laws (e.g., routine uses authorized under the Privacy Act of 1974).

4.4 What are the procedures that allow individuals to gain access to their own information?

Individuals may request access to their information, if any, that the FTC retrieves by a

personal identifier and that the FTC is required to disclose in accordance with the Freedom of Information Act (FOIA) and the Privacy Act of 1974. Requests can be submitted to the FOIA/Privacy Act Office in the Office of the General Counsel. See www.ftc.gov and Section 8, below.

4.5 Discuss the privacy risks associated with the process of providing individuals access to their own records and how those risks are mitigated.

Because individuals seeking access to their own records cannot, as a general rule, directly access the SIL, the primary risk is providing personal information to an unauthorized recipient upon request. In responding to such requests, the FOIA/Privacy Act Office has identity verification processes and procedures in place to reduce this risk.

5 Web Site Privacy

The SIL is not a website that is available to the public.

6 Security of Information in the Application

6.1 Are all IT security requirements and procedures required by federal law being followed to ensure that information is appropriately secured?

The FTC follows all applicable Federal Information Security Modernization Act (FISMA) requirements to ensure that the information residing in the SIL is appropriately secured. The SIL is designated as a subsystem within the Data Center General Support System (GSS). [3]

6.2 Does the project employ technology that may raise privacy concerns? If so, please discuss its implementation.

No. The SIL uses established technologies and controls for securing data and addressing privacy risks, while avoiding technologies that could raise additional privacy concerns. (For example, as noted earlier, the SIL does not directly connect to the Internet or host a Web site that might result in additional threats or vulnerabilities to the security and privacy of SIL data.)

6.3 What procedures are in place to determine which users may access the application and are they documented?

The FTC has a verification process for reviewing requests by FTC users to access SIL and for granting authorized SIL users the right to access matter-specific SIL folders, based on need and least privilege access.

[3] The Data Center GSS PIA is available here: http://www.ftc.gov/system/files/attachments/privacy-impact-assessments/1404datacentersystempia.pdf

6.4 Describe what privacy training is provided to users either generally or specifically relevant to the program or application.

All FTC personnel, including those who use the SIL, are subject to FTC procedures for safeguarding PII, including sensitive PII and SHI. All FTC personnel receive annual computer-based privacy and security training, as well as other guidance explaining how to safeguard information. In addition, SIL users receive SIL-specific training on receiving, handling, and securing SIL data.

6.5 What auditing measures and technical safeguards are in place to prevent the misuse of data?

The following in-place auditing measures and technical safeguards are applied to prevent misuse of SIL data. These controls include:

- Authenticator/Password Management – Application and monitoring of initial distribution, composition, history, compromise, and change of default authenticators.
- Account Management – Application and monitoring of account establishment, activation, modification, disabling, removal (including unnecessary/defunct accounts) and review.
- Access Enforcement – Application and monitoring of access privileges.
- Least Privilege – Application for a user to perform his/her function.
- Separation of functions – SIL users cannot import or export SIL data, but can only work with SIL data inside the SIL environment in matter-specific folders.
- Unsuccessful Login Attempts –Application automatically locks the account when the maximum number of unsuccessful attempts is exceeded.

Privacy risks associated with unauthorized disclosure of information are mitigated through implementation of technical and administrative controls that limit access to SIL data to those who must work with it. This need-to-know and least privilege access ensures that SIL users have no more privileges to data than required to carry out their official duties with regard to specific matters. In addition, deterrent controls in the form of warning banners, rules of behavior, and auditing are in place. Procedures are in place for designated individuals to properly dispose of or properly store SIL data at the end of each study or investigation.

6.6 Who is the point of contact for questions regarding the security of the application?

Any questions regarding the safeguarding of the SIL should be addressed to the FTC Chief Information Security Officer (CISO).

7 Data Retention

7.1 For what period of time will data collected by this application be maintained?

SIL information is retained and destroyed in accordance with applicable FTC policies and procedures, and with FTC records retention schedule N1-122-09-1, and the General Records Schedules (GRS) of the National Archives and Records Administration (NARA). The FTC records retention schedule, the NARA GRS, and FTC Rules of Practice 4.12 indicate that SIL data (working files) can be destroyed/deleted when no longer needed or returned to the submitter. In some cases, the time period for data retention and destruction may be governed by an applicable data use agreement.

SIL data is backed up on storage disks within the SIL environment. The backup data is kept for two weeks.

7.2 What are the plans for destruction or disposal of the information?

Disposal of all SIL information will be conducted in accordance with FTC policies and procedures and in compliance with Office of Management and Budget (OMB), NARA, and NIST guidelines.[4]

Internal procedures are in place for the destruction of original digital media used to load data into the SIL. For the destruction of external drives, the FTC has retained a vendor whose methods meet or exceed applicable standards for media sanitization and destruction.

7.3 Describe any privacy risks identified in the data retention and disposal of the information, and describe how these risks have been mitigated.

Risks associated with data retention and disposal of SIL data do not raise any special privacy concerns not already addressed.

8 Privacy Act

8.1 Will the data in the application be retrieved by a personal identifier?

Data may be retrieved from the SIL using a variety of factors, including personal identifiers. Actual retrieval methods will depend upon the content of the SIL data set, the nature of the matter, and the purpose for which the data set is used.

[4] See NIST Special Publication 800-88, Guidelines for Media Sanitization

8.2 Is the application covered by an existing Privacy Act System of Records notice (SORN)?

To the extent SIL data are about an individual retrieved from a system of records by name or other identifier assigned to the individual, the SIL is covered by SORN I-1, Nonpublic Investigational and Other Nonpublic Legal Program Records: http://www.ftc.gov/about-ftc/foia/foia-reading-rooms/privacy-act-systems.

9 Privacy Policy

9.1 Confirm that the collection, use, and disclosure of the information in this application has been reviewed to ensure consistency with the FTC's privacy policy.

The collection, use, and disclosure of the information in the SIL has been reviewed to ensure consistency with the FTC's privacy policy.