Federal Trade Commission
Privacy Impact Assessment

for the:

Secure Investigations Lab
(SIL)

5HYLHZHG)HEUXDU\

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 or Sensitive Health Information (SHI).[1][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

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, drivers' license/state ID numbers, place of birth, geolocation information, bank account numbers, credit card nu

2.4 How is the information collected?

The data sets stored in the Salesforce 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

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

Several statutes authorize the FTC to collect and store 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 the 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 au[illegible]

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 F-17 ([b0 Te)6 (x)-p7ft abpeion on th,

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

4 N

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

T>>BD

6.4 Describe what privacy training is provided to users either generally

7 Data Retention

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

SIL i