Federal Trade Commission
Privacy Impact Assessment

Litigation Support System (LSS)

February 2018

Table of Contents

1 System Overview

1.1 Describe the project/system and its purpose.

The Federal Trade Commission (FTC or agency) conducts investigations and litigates cases to accomplish its competition and consumer protection missions.[1] For these matters, the FTC obtains a significant amount of electronically stored information from external parties voluntarily, in response to compulsory process, and through the forensic acquisition of data pursuant to court orders in certain cases. This data may contain personally identifiable information (PII) and sensitive business information, among other things. In some instances, the data may contain viruses or malware.

FTC staff use the Litigation Support System (LSS) to extract, process, analyze, and maintain data in a secure, isolated environment, as part of the FTC's Electronic Discovery Support System (EDSS).[2] The LSS contains several commercial off-the-shelf software applications that allow FTC staff to perform specialized analysis and processing of the data. These applications include forensic, e-discovery, accounting, and data analysis tools. The LSS contains a firewall that blocks non-security related traffic to the Internet. This protection ensures that staff can analyze and maintain forensically-acquired data in a forensically sound manner. A bridge server connects the LSS to the FTC's production network.[3] Staff may manually transfer data from the LSS to the FTC production network so that it can be loaded into a document review platform or incorporated into a case file. All data from the LSS undergoes anti-virus scanning prior to being loaded onto the FTC's production network.

Although FTC staff primarily use the LSS to process data received from external parties, the LSS also is used to analyze and process data created by agency staff or contractors. This data may be responsive to discovery in FTC law enforcement actions as well as Freedom of Information Act (FOIA) and other requests. The data also may be used in internal investigations or in defense of legal actions brought against the agency.

The Office of the Chief Information Officer (OCIO) serves as the system owner of the LSS, and OCIO staff and contractors manage the system. The LSS is used by authorized staff and contractors in the Bureau of Consumer Protection (BCP), the Bureau of Competition (BC), and the Office of the General Counsel (OGC). Authorized individuals access the LSS either by using a computer that is connected solely to the LSS or a virtual private network (VPN) from the FTC's production network.

---

[1] For a detailed discussion of the FTC's mission, see About the Federal Trade Commission, https://www.ftc.gov/about-ftc.

[2] The EDSS, which includes the LSS, the EDSS Review System, and the Department of Justice (DOJ) ORCA application, provides the FTC with various customized hardware and software tools and resources to accomplish its e-discovery tasks. For more information, refer to the EDSS PIA.

[3] The FTC production network is a wide area network and is the networking "backbone" of the agency – connecting computers, servers, printers, scanners, network storage devices, etc. together into a seamless computing environment. The FTC production network is part of the agency's Data Center General Support System (Data Center GSS). For more information, see the Data Center GSS PIA.

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 FTC enforces.

2 Data Type, Sources, and Use

2.1 Specify in the table below what types of personally identifiable information (PII)[4] 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)*: Password
☒ Work Address		
☒ Taxpayer ID		
☒ Credit Card Number		
☒ Facsimile Number		
☒ Medical Information		
☒ Education Records		
☒ Social Security Number		
☒ Mother's Maiden Name		

The LSS may collect or maintain any information the FTC may obtain as part of its law enforcement and other activities. This may include any and all types of PII. The system also collects and maintains the user ID and password of the FTC staff person or contractor logged into the LSS.

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.

[4] 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.

The LSS will maintain any information that the FTC might obtain as part of its law enforcement and other activities, including Controlled Unclassified Information (CUI). This information is in a variety of electronic formats and file types, such as word processing files, email, spreadsheets, databases, and audio and video files. The information may include many types of sensitive information. For example, during a merger case, the BC may obtain large volumes of sensitive and proprietary business information, including pricing information, planning information, financial reports, strategic plans, contracts, sales reports, securities filings, organization charts, emails, sales data, invoices, and specific project information about individuals (e.g., employee information or detailed customer data). BCP also may obtain sensitive and proprietary business information, such as planning information, sales data, and data security requirements.

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

The FTC collects information as part of its law enforcement and other activities. These activities may include investigating potential or alleged violations of anticompetitive practices; enforcing statutes that protect consumers against fraudulent, deceptive, or unfair practices in the marketplace; locating victims and potential witnesses; assisting with redress; investigating internal FTC matters; and defending the FTC in suits brought against the agency.

2.4 What are the sources of the information in the system/project? How is the information collected?

Information in the LSS is created or obtained by FTC staff in connection with the agency's law enforcement and other activities. The FTC obtains information directly from targets of its law enforcement activities and from individuals and entities with information that may be relevant to the FTC's investigations. The FTC may obtain this information voluntarily (e.g., from consumers who file complaints with the FTC), through compulsory process (e.g., pursuant to an FTC-issued Civil Investigative Demand), or during formal discovery processes in federal or administrative proceedings. The FTC also may forensically acquire electronic information directly from a defendant's business premises pursuant to a federal court order. The LSS also may contain data created by FTC employees and contractors. The system also maintains information pertaining to the system users, such as their user IDs and passwords. This information is collected directly from FTC staff.

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 Users	FTC staff must have an authorized account that requires a username and password to obtain access to the LSS. BC, BCP, and OGC litigation support staff (and contractors performing similar duties) have access to data for the particular Bureau or Office in which they are working. These staff members access the LSS to copy, process, and analyze data. BCP data analysts and forensic accountants have access to only specific subfolders, which contains the data needed to accomplish their work. BCP case teams (e.g., attorneys, investigators, and paralegals) occasionally access the LSS to preview data. These staff are given access to a subset of data for the case to which they are assigned. FTC contractors who provide system and case team support may also have access to the system (see section 3.2 below for further details).
Non-FTC Users	The FTC may extract information from the system to share with courts, opposing counsel, defendants, law enforcement partners, or other individuals as authorized by law.[5] Except as described below, these parties do not have access to the LSS. On occasion, law enforcement partners may obtain access to the LSS on a temporary basis to review data for a particular case. This access must take place in an FTC office.

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 may have access to data in the LSS. The level of access granted is commensurate with the contractor's duties. Certain contractors support OCIO in maintaining and operating the LSS, and given the nature of their duties, they have access to the entire system. Contractors supporting BC, BCP, and OGC litigation support specialists have access to the data for the particular Bureau or Office with which they are working. Contractors who are assigned to work on a specific case are granted access to only data relating to that matter.

[5] See, e.g., 16 CFR § 4.11 (c), (d) and (j) for information regarding FTC rules for sharing information with law enforcement partners.

All FTC contractors are required to complete information security and privacy awareness training prior to obtaining access to any systems and on an annual basis. FTC contractors also are required to sign nondisclosure agreements.

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.

Authorized FTC contractors who have access to the LSS are subject to the same rules of use and as FTC employees and also are bound by the FTC's 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*):_____

☐ Notice is not provided (explain): _____

Wherever possible, the FTC provides notice to individuals about its policies regarding the use and disclosure of information at the time information is collected. For information that is collected pursuant to a request from the FTC, notice is provided as part of the request (e.g., in a letter or in the document outlining the compulsory process request). For information that is collected via an FTC-sponsored website or telephone call center, notice is given at the point of collection. On those occasions where the FTC cannot provide notice at the time information is collected (e.g., information contained in systems maintained by other organizations), the FTC provides notice via its Privacy Policy, its Privacy Act system of records notices (SORNS), and its PIAs, including this one. With regard to information collected from internal FTC systems for internal investigations or for the defense of suits brought against the agency, all staff are informed that the agency's computing systems are monitored and that personal information may be collected. Notices are provided to staff at logon, and are also provided in administrative manuals, agency policy documents, and during employee training.

Individuals who provide the FTC with information pursuant to discovery or a related court order are not provided with specific notice by the FTC as to how information will be used or disclosed, other than the FTC's general Privacy Policy and related FAQs. In addition, the use and disclosure of this information is governed by applicable discovery rules and court orders.

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)?

Individuals who provide the FTC with information on a voluntary basis may choose to decline to provide that information. However, individuals do not have a right to decline to provide information that is required by law or that is required to be provided via compulsory process, and refusal to provide the information may result in legal action by the FTC.

Individuals do not typically have a right to consent to particular uses of their information. Data sources who submit their information in FTC law enforcement investigations and mark their submissions confidential, however, may be afforded prior notice and opportunity to object to further disclosure, to the extent provided under Section 21 of the FTC Act and the FTC's Rules of Practice (see, e.g., 16 C.F.R. 4.10 & 4.11).

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

Individuals may make a request under the FOIA and Privacy Act for access to information maintained about themselves in the LSS or other FTC record systems. Individuals must follow the FTC's Privacy Act rules and procedures, published in the Code of Federal Regulations at 16 C.F.R. 4.13, for requests for information. Privacy Act requests must be made in writing and submitted to the FTC's Office of General Counsel. See the FTC FOIA website and online FOIA request form. However, due to the law enforcement nature of the LSS, records in the system about certain individuals, such as defendants, may be exempt from mandatory access by such individuals. See 16 C.F.R. 4.13(m) (exemptions applicable to certain FTC Privacy Act systems of records). To prevent the risk that the agency releases records it is legally required to withhold from public disclosure to an individual purporting to be the subject of such records, the FTC may require additional verification of a requester's identity when such information is reasonably necessary to assure that records are not improperly disclosed.

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.

As stated above, individuals seeking records about themselves do not have direct access to the system. They may make a request under the FOIA and Privacy Act for access to information maintained about themselves in any FTC system. However, due to the law enforcement nature of the system, records in the system about certain individuals, such as defendants, may be exempt from mandatory access by such individuals. See 16 C.F.R. 4.13(m) (exemptions applicable to certain FTC Privacy Act systems of records**.**

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?

Information that is used by the FTC for law enforcement and other activities is reviewed for accuracy and timeliness as required by the particular activity. For example, staff performing an investigation based upon a "whistleblower" complaint may check the information that is obtained to ensure that it is timely and accurate. In other cases, the individual submitting the information may also be required to certify the accuracy of the information (e.g., witness or financial statements in court cases).

Information in the LSS is subject to appropriate security and chain-of-custody controls. In addition to protecting against unauthorized access, alteration, or dissemination, these controls reduce the risk of loss and assure the integrity of the evidentiary materials from the point at which they are included in the system.

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.

Only authorized staff and contractors are granted access to the LSS. Prior to accessing the LSS, users must create a password distinct from the password used to access the FTC production network. Users are locked out of the system after five failed attempts to log in. The LSS resets after 60 minutes to allow staff to attempt to log in again. The 60 minute reset is set up because the LSS does not have 24/7 help desk support and many users use the LSS after hours and on weekends. LSS administrators in OCIO and BCP have authority to reset passwords. User' access to information in the LSS is limited to only the data necessary to perform their designated tasks. If staff does not access the LSS for 90 days, their account is disabled. Before any new FTC employee or contractor can access any system, including the LSS, that individual must successfully complete the FTC's Privacy and Security Awareness training.

5.3 Has the system/project undergone the appropriate security risk assessment and received authority to operate?

Yes, the LSS has undergone a security risk assessment and been granted an authority to operate. The LSS is categorized as a moderate system using Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems.

5.4 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

PII is not used in the course of training or research in the LSS. Only dummy data is used for such purposes.

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?

Information is retained and destroyed in accordance with applicable FTC policies and procedures and with FTC records retention schedule N1-122-09-1 approved by the National Archives and Records Administration (NARA).

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.

☒ Not Applicable

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?

The FTC collects and stores large volumes of information that is obtained from various sources. Information may include sensitive business information and other nonpublic information/CUI, which if lost could result in significant monetary injury. In addition, the presence of PII within the system creates privacy risks. The primary risks posed by the storage of information in the system are associated with, and flow from, the potential loss of control of this information, including unauthorized access, alteration, or dissemination. To mitigate these risks, the FTC has implemented a number of safeguards, as discussed below.

Risk	***Mitigation Strategy***
Malicious Code	In some instances, electronic information received or forensically acquired by the FTC may contain viruses or other malware. To address the risk of data exportation or loss as a result of any malicious code, the LSS employs a firewall that blocks non-security related access to the

Risk	*Mitigation Strategy*
	Internet. If staff needs to transfer data from the LSS to the FTC production network, the data is scanned before being allowed on the FTC production network. In addition, the FTC production network employs a suite of tools and systems to detect, remove, and block malicious code and minimize the risk of exposure.
Unauthorized access to data in the LSS	Only authorized FTC staff and contractors have access to the LSS, and access is based on the individual's role. Access to the LSS requires a user name and unique password. Authorized individuals access the LSS either by using a computer that is connected solely to the LSS or a VPN from the FTC's production network On occasion, law enforcement partners may obtain access to the LSS on a temporary basis. This access must take place at the FTC. Only system administrators are permitted physical access to the LSS data center, and such access is controlled, logged, and monitored.

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

Only authorized staff are granted access to the LSS. Staff must create a password to access the LSS distinct from the password used to access the FTC production network. Staff are locked out of the system after five failed attempts to log in. The LSS resets after 60 minutes to allow staff to attempt to log in again. The 60 minute reset is set up because the LSS does not have 24/7 help desk support and many users use the LSS after hours and on weekends. LSS administrators in OCIO and BCP have authority to reset passwords.

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 FTC SORNs applicable to this system are: I-1, Nonpublic Investigational and Other Nonpublic Legal Records; and VII-3, Computer Systems User Identification and Access Records.[6] As noted earlier, subject individuals may make a request under the FOIA and Privacy Act for access, although some records may be exempt from disclosure, 16 C.F.R. 4.13(m), and the agency may require additional verification of the requester's identity to avoid improper disclosure of records to the wrong individual. See 16 C.F.R. 4.13(d).

[6] All FTC SORNs are available online on the FTC SORN page.

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?

Although the system does not operate any website that would require the posting of a privacy policy, the collection, use, and disclosure of the information in the system has been reviewed to ensure consistence with the FTC's Privacy Policy posted on its website.

9 Approval and Signature Page

Prepared By:

_____ **Date: _____**
Laura DeMartino, Associate Director
Division of Litigation Technology & Analysis
Bureau of Consumer Protection

Reviewed By:

_____ **Date: _____**
John Krebs
Acting Chief Privacy Officer (CPO)

_____ **Date: _____**
Alexander C. Tang, Attorney
Office of the General Counsel (OGC)

_____ **Date: _____**
Jaime Vargas
Chief Information Security Officer (CISO)

_____ **Date: _____**
Yvonne K. Wilson
Records and Filing Office (RFO)

Approved By:

_____ **Date: _____**
Raghav Vajjhala
Chief Information Officer (CIO)