



Federal Trade Commission
Privacy Impact Assessment

Everlaw

March 2026

Table of Contents

1	System Overview	3
2	Data Type, Sources, and Use	4
3	Data Access and Sharing	6
4	Notice and Consent	8
5	Data Accuracy and Security.....	10
6	Data Retention and Disposal.....	11
7	Website Privacy Evaluation.....	11
8	Privacy Risks and Evaluation	12

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 In addition, the FTC conducts internal investigations, defends itself against legal actions, and responds to Freedom of Information Act (FOIA), Government Accountability Office, Congressional, and other requests. These activities all involve electronic discovery – specifically, the review, analysis, and use of electronically stored information (ESI). The FTC obtains a significant amount of ESI from external parties as part of its law enforcement and other activities. This information may contain personally identifiable information (PII) as well as other types of sensitive data. The FTC’s matters also involve data created by agency staff and contractors, and the FTC collects this information from its own computer systems.

The FTC has procured Everlaw, a Software as a Service (SaaS) product that enables staff to review, analyze, and produce ESI. Everlaw is a web application that is FedRAMP certified and hosted in the Amazon Web Service (AWS) GovCloud. Authorized FTC staff and contractors, and occasionally, law enforcement partners granted use by the FTC, access Everlaw using dual factor authentication. The data is placed in case-specific databases, and users are granted access to data based on their work assignments.

With Everlaw, the FTC will also have access to Everlaw AI Assistant (Everlaw^{AI}), a generative artificial intelligence (genAI) tool that combines large language models (LLMs) developed by AI service providers with the data inside Everlaw’s platform. The Everlaw^{AI} Assistant allows FTC users to quickly summarize large data sets, search large databases in seconds, and more efficiently conduct document reviews without compromising the confidentiality of FTC data.

1.2 What specific legal authority allows for the collection, maintenance, or dissemination of information for this project/system?

A number of statutes authorize the FTC to collect and store the information contained in Everlaw, including the Federal Trade Commission Act, 15 U.S.C. §§ 41-58; 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. These statutes not only authorize the collection of information, but also have provisions that limit the disclosure of the data.

¹ For a detailed discussion of the FTC’s mission and activities, see *About the Federal Trade Commission*, <https://www.ftc.gov/about-ftc>.

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.

<i>PII Elements: This is not intended to be an exhaustive list. Specify other categories of PII as needed.</i>		
<input checked="" type="checkbox"/> Full Name	<input checked="" type="checkbox"/> Biometric Identifiers (e.g., fingerprint, voiceprint)	<input checked="" type="checkbox"/> User ID
<input checked="" type="checkbox"/> Date of Birth	<input checked="" type="checkbox"/> Audio Recordings	<input checked="" type="checkbox"/> Internet Cookie Containing PII
<input checked="" type="checkbox"/> Home Address	<input checked="" type="checkbox"/> Photographic Identifiers (e.g., image, x-ray, video)	<input checked="" type="checkbox"/> Employment Status, History, or Information
<input checked="" type="checkbox"/> Phone Number(s)	<input checked="" type="checkbox"/> Certificates (e.g., birth, death, marriage, etc.)	<input checked="" type="checkbox"/> Employee Identification Number (EIN)
<input checked="" type="checkbox"/> Place of Birth	<input checked="" type="checkbox"/> Legal Documents, Records, Notes (e.g., divorce decree, criminal records, etc.)	<input checked="" type="checkbox"/> Salary
<input checked="" type="checkbox"/> Age	<input checked="" type="checkbox"/> Vehicle Identifiers (e.g., license plates)	<input checked="" type="checkbox"/> Military Status/Records/ ID Number
<input checked="" type="checkbox"/> Race/ethnicity	<input checked="" type="checkbox"/> Financial Information (e.g., account number, PINs, passwords, credit report, etc.)	<input checked="" type="checkbox"/> IP/MAC Address
<input checked="" type="checkbox"/> Alias	<input checked="" type="checkbox"/> Geolocation Information	<input checked="" type="checkbox"/> Investigation Report or Database
<input checked="" type="checkbox"/> Sex	<input checked="" type="checkbox"/> Passport Number	<input checked="" type="checkbox"/> Driver's License/State ID Number (or foreign country equivalent)
<input checked="" type="checkbox"/> Email Address		<input type="checkbox"/> Other (<i>Please Specify</i>): _____
<input checked="" type="checkbox"/> Work Address		
<input checked="" type="checkbox"/> Taxpayer ID		
<input checked="" type="checkbox"/> Credit Card Number		
<input checked="" type="checkbox"/> Facsimile Number		
<input checked="" type="checkbox"/> Medical Information		
<input checked="" type="checkbox"/> Education Records		
<input checked="" type="checkbox"/> Social Security Number		
<input checked="" type="checkbox"/> Mother's Maiden Name		

Note: Everlaw processes any information that the FTC might obtain as part of its law enforcement and other activities, and which the FTC chooses to upload into the Everlaw platform. This may include all types of PII and sensitive information and is not limited to the data elements identified in the above table.

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.

Everlaw processes information that the FTC obtains as part of its law enforcement and other activities, and which the FTC chooses to upload into the Everlaw platform. This information is in electronic format and in a variety of file types, such as word processing files, spreadsheets, and email. The information may include many types of sensitive 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.

including Controlled Unclassified Information (CUI),³ that may be other than PII. For example, during a merger case, the FTC's Bureau of Competition (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). The Bureau of Consumer Protection (BCP) also may obtain large volumes of sensitive and proprietary business information, such as planning information, sales data, and data security requirements.

The FTC will have access to Everlaw^{AI} Assistant, though platform administrators retain the authority to disable generative AI features at any time. When enabled, the FTC maintains full control over which specific data are processed using generative AI functionality.

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?

Typically, 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 companies that wish to merge, or from consumers who file complaints with the FTC), through compulsory process (e.g., pursuant to an FTC-issued Civil Investigative Demand, subpoena, or other requests), or during formal discovery processes in federal or administrative litigation proceedings. The FTC also may forensically acquire electronic information directly from a defendant's business premises pursuant to federal court order. The FTC also obtains data created by its employees and contractors and stored on the FTC's production network. In addition, the FTC obtains information from public sources such as the Internet.

³ CUI is information the U.S. Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. See 32 C.F.R. § 2002.4(h).

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.

<i>Data Will Be Accessed By and/or Provided To:</i>	<i>How and Why the Data Will Be Accessed/Shared</i>
FTC Staff	<p>Certain FTC staff (litigation support specialists) with elevated privileges have access to the system to load data into the application, create databases, assign access rights to databases, and create production sets. The litigation support specialists have access to all of the data for the particular Bureau or Office with which they are working.</p> <p>Authorized FTC staff will have web-based access to Everlaw’s environment to use e-discovery software applications. FTC staff obtain access using dual factor authentication. Data is stored in case-specific databases. The FTC’s litigation support staff provide access rights to staff to particular databases based on their work assignments. Once staff no longer needs access, the FTC’s litigation support specialists remove that access.</p>
Everlaw	<p>Only authorized Everlaw staff have access to the FTC’s data. These staff have completed FTC-approved background checks and security clearances.</p> <p>When FTC staff use Everlaw^{AI} Assistant, each data request is sent to one Everlaw’s subprocessors over an SSN encrypted service, to process and send back to Everlaw. All data is maintained in servers in the US. FTC data submitted to Everlaw and responses received via Everlaw^{AI} are not used to train or improve any of its LLM models, nor is any FTC data maintained by the LLMs or shared with other entities.</p>
Other External Users	<p>For a particular case or matter, the FTC may grant its law enforcement partners access to data for that case within Everlaw. These partners will be provided access to only the data relevant to the case and will have web-based access to the data using dual factor authentication.</p> <p>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.⁴ When the</p>

⁴ See, e.g., 16 C.F.R. § 4.11 (c), (d) and (j) for information regarding FTC rules for sharing information with law enforcement partners.

<i>Data Will Be Accessed By and/or Provided To:</i>	<i>How and Why the Data Will Be Accessed/Shared</i>
	<p>FTC shares information with external entities, it typically does so pursuant to non-disclosure agreements, court-approved protective orders, and contract provisions regarding privacy and security, or similar data protection controls. These external entities will have no web-based or other online access to the system or system data.</p>

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 and third-party service providers may have access to data in the system. The level of access granted is commensurate with the contractor’s duties. There are three types of contractors who may have access to data: (1) FTC contractors assigned to work on a specific case; (2) FTC contractors serving as litigation support specialists for the agency; and (3) Everlaw staff. Contractors who are assigned to work on a specific case will be granted access only to data relating to that matter. Contractors supporting the FTC’s litigation support specialists will have access to the data for the Bureau or Office with which they are working. Authorized Everlaw staff provide technical assistance to the FTC, and therefore, have access to all the data in the system.

The first two types of FTC contractors are required to complete the FTC’s Annual Information Security and Privacy Awareness Training. This interactive online training provides guidelines for properly handling PII and other data, online threats, social engineering, and the physical security of documents. Everlaw provides security awareness training to its staff as part of initial training and annually thereafter. This training includes the proper handling and protection of PII.

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 data within the system are subject to the same rules of usage and incident response as FTC employees. Everlaw has developed a comprehensive Incident Response Plan for addressing adverse computer-security related events. The plan discusses the company’s vulnerability mitigation and threat mitigation. Everlaw’s Incident Response Plan contains a framework for responding to information security incidents, including communications, restoring system components and services, and providing breach notifications. The FTC’s contract with Everlaw requires the company to immediately notify the FTC of all breaches. Moreover, Everlaw’s Incident Response Plan further states that for incidents related to unauthorized access of PII, Everlaw will report the

incident to the FTC within one hour of the security incident being positively identified by Everlaw's team.

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 request, 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.⁵ 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.⁶ With regard to information collected from internal FTC systems for internal investigations or for the defense of lawsuits 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

⁵ See, e.g., notices provided to consumers who file a complaint via [ReportFraud.gov](#). See also the [FTC Privacy Policy](#).

⁶ See [FTC Privacy Policy](#), [SORNs](#), and [PIAs](#).

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 seeking records about themselves do not have direct access to Everlaw, so no privacy risks are associated with the process of providing individuals with access to their own records through the system. Individuals may make a request under the FOIA and Privacy Act for access to information maintained about themselves in Everlaw or other FTC record systems. Individuals must follow the FTC's Privacy Act rules and procedures, which are 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](#). However, due to the law enforcement nature of the Privacy Act system that includes the records on the Everlaw platform or derived from Everlaw services,⁷ 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 records that the agency would be legally required to withhold from public disclosure may be improperly released 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 applicable Privacy Act system, records in the system about certain individuals, such as defendants, may be exempt from mandatory access by such

⁷ See section 8.3 below which describes the applicable Privacy Act System, FTC-I-1, Nonpublic Investigational and Other Nonpublic Legal Records, that is exempt from certain access provisions otherwise required by the Privacy Act.

individuals. See 16 C.F.R. § 4.13(m) (exemptions applicable to certain FTC Privacy Act systems of records). If individuals have questions or concerns about any information in the system, they would raise those questions or concerns in the context of the FTC investigation or litigation in which they are involved.

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 as part of its 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 incorporated into the Everlaw system 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.

FTC data stored within Everlaw is encrypted at rest and is maintained separately from other Everlaw client data. Data also is encrypted in transit. Everlaw utilizes various types of automated continuous monitoring of its system.

Authorized FTC staff obtain access to Everlaw using dual factor authentication. FTC staff log in with usernames and are validated using a dual factor authentication method that is selected by FTC and integrated with Everlaw environment. The system also terminates sessions after 30 minutes of inactivity. Staff are given system access to the least amount of data needed to perform their duties.

The Everlaw platform can provide audit records of successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes.

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. Dummy data is used in the course of system testing, training, and research.

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 received, retained and destroyed/deleted in accordance with applicable FTC policies and procedures and with the FTC records retention schedule approved by the National Archives and Records Administration (NARA), as well as the instructions in the FTC Rules of Practice Section 4.12, Disposition of Documents Submitted to the Commission.

The FTC can delete its own data from the Everlaw platform at any time. In addition, Everlaw can delete FTC data at the request of authorized FTC staff. Everlaw initiates data deletion with complete and final deletion occurring within a commercially reasonable time of the FTC request. Everlaw can provide the FTC with a Certificate of Deletion.

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.

Authorized FTC staff access Everlaw through a secured website that they have set up specifically for the FTC's use. FTC staff use a specific URL to access Everlaw from the FTC or remotely. This URL is not posted online or otherwise made publicly available. However, when working with external law enforcement partners on jointly prosecuted cases, the FTC shares the URL with authorized law enforcement personnel to access Everlaw. Everlaw uses session cookies to track user sessions in the web browser; there are no persistent cookies in use. The cookies are always encrypted with Secure Socket Layer (SSL)/Transport Layer Security (TLS) protection.

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.

<i>Risk</i>	<i>Mitigation Strategy</i>
Unauthorized access to data before it is loaded into Everlaw	Data is transferred to Everlaw via hard drives that are encrypted with National Institute of Standards and Technology (NIST)- certified cryptographic modules. These hard drives are hand carried to Everlaw's offices and are subject to strict chain-of-custody controls. Alternatively, the FTC transfers data to Everlaw via secure electronic transfer methods such as SFTP.
Unauthorized access to data in Everlaw	Authorized staff obtain access to the data using dual factor authentication. Data is loaded into case-specific databases, and authorized users must be granted access to the case folder in order to view the data. FTC staff are granted permission to access only those databases needed to accomplish their work. Everlaw employs continuous monitoring and utilizes automated intrusion detection and prevention systems. Everlaw audits successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes.
Unauthorized alteration or dissemination of information	Everlaw audits user activity in the system. These audits include successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes.

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

Only authorized FTC staff, contractors, and law enforcement partners are granted access to the system. These users access Everlaw using dual factor authentication. FTC staff log in with usernames and will be validated using a dual factor authentication method which is selected by FTC and integrated with Everlaw environment. The system also terminates sessions after 30 minutes of inactivity. Staff are given system access to the least amount of needed to perform their duties. Staff is given the minimal access necessary to perform their duties.

The Everlaw platform provides audit records of successful and unsuccessful logon attempts and user activity in the system. These audits include account management events, policy change, privilege use, data access, data deletions, data changes, permission changes, and all administrator activity.

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 SORN applicable to this system is I-1, Nonpublic Investigational and Other Nonpublic Legal Records.⁸ 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). Login and other data, if any, compiled by the system on individual system users would be covered by FTC SORN VII-3 -- Computer Systems User Identification and Access Records – FTC, to the extent, if any, that Everlaw maintains and retrieves such individual system user data for or on behalf of the FTC.

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.

⁸ All FTC SORNs are available online on the [FTC SORN page](#).