



Federal Trade Commission
Privacy Impact Assessment

RelativityOne

May 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.....	12
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 contracted with Federal Complete Discovery Source (FCDS) to obtain a commercial Software as a Service (SaaS) product called RelativityOne. RelativityOne is an e-discovery and legal data platform that is used to manage large volumes of information and evidence for litigation, investigation, and compliance. Using RelativityOne, FTC staff will be able to review, analyze and produce ESI in the course of their investigations and law enforcement activities. RelativityOne is a web application that is FedRAMP certified and hosted in the Microsoft Azure Government Cloud. The data is placed in case-specific databases, and users are granted access to data based on their work assignments.

RelativityOne also has built-in artificial intelligence functionality (Relativity aiR), automated analytics, and data-first workflows designed to accelerate document review, identify key facts, and efficiently meet discovery obligations. The AI features in the platform allow the FTC staff to summarize hefty data sets, quickly search large databases, and more efficiently conduct document reviews without compromising the confidentiality of FTC data. Platform administrators retain the authority to disable the AI features at any time; when enabled, however, the FTC maintains full control over which specific data are processed using the generative AI functionality.

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 RelativityOne, 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>		
☒ 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		

Note: RelativityOne 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 RelativityOne 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.

RelativityOne processes information that the FTC obtains as part of its law enforcement and other activities, and which the FTC chooses to upload into the RelativityOne 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

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.

information, 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.

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	Authorized FTC staff can upload the data to FCDS through the backend Virtual Machine (VM). Upon receiving the data, FCDS staff are responsible for performing the related review support functions, facilitating its transfer into RelativityOne, and notifying the case team once the data has been uploaded. Authorized FTC staff will have web-based access to the RelativityOne environment to use e-discovery software applications. FTC staff provide their names and email addresses to obtain access using Single-Sign On (SSO) integration with existing FTC authentication mechanisms. 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 need access, the FTC's litigation support specialists remove that access.
FCDS Staff	Only authorized FCDS staff have access to the FTC's data in RelativityOne. These staff have completed FTC-approved background checks and security clearances. All data is maintained in servers in the US. FTC data uploaded into the RelativityOne platform are not used to train or improve any of its AI models, nor is any FTC data shared with other entities.
Other External Users	For a particular case or matter, the FTC may grant its law enforcement partners access to data for that case within RelativityOne. These partners will be provided access only to the data relevant to the case and will have web-based access to the data using dual factor authentication. 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 FTC shares information with external entities, it typically

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>
	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.

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) FCDS staff authorized to access FTC data on the RelativityOne platform. 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 FCDS 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 have access to the FTC computer network and 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. FCDS provides its own 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 use and incident response as FTC employees. Relativity maintains a formal Privacy and Data Security Incident Response Program designed to identify, assess, contain, remediate, and communicate security and privacy incidents involving RelativityOne systems and Customer Data. The program is governed under Relativity's Information Security, Risk, and Privacy (ISRP) framework and is reviewed periodically by executive leadership.

Relativity employs continuous monitoring, centralized logging, and automated alerting mechanisms to detect suspected security or privacy events. Potential incidents are promptly

triaged by the Security team using documented procedures to determine scope, severity, and impact, including whether Customer Data or personal information may be affected. Relativity notifies affected customers without undue delay and no later than 24 hours after determination or reasonable suspicion of a data breach, unless delayed by law enforcement. Notifications include relevant details as information becomes available. Relativity cooperates with customers, regulators, and law enforcement as appropriate while maintaining confidentiality and legal compliance.

All incidents are formally documented, including investigative actions, decisions, and outcomes. Post-incident reviews are conducted to assess effectiveness, identify control improvements, and enhance incident response readiness. Incident response procedures are tested periodically through tabletop exercises and are subject to independent audit.

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

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

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

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, 15 U.S.C. § 57b-2, 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 RelativityOne; as such, there are no privacy risks 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 RelativityOne 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 and certify by signature that the requester is the individual to whom the record pertains or is the parent or guardian of a minor or the legal guardian of the individual to whom the record pertains. *See* the FTC [FOIA website](#). However, due to the law enforcement nature of the Privacy Act system that includes the records on the RelativityOne platform or derived from FCDS' 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

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.

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 RelativityOne platform. 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 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 RelativityOne platform 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 RelativityOne is encrypted at rest and is maintained separately from other RelativityOne client data. Data also is encrypted in transit. FCDS staff utilize various types of automated continuous monitoring of the RelativityOne system.

Authorized FTC staff provide their names and email addresses to obtain access to the system using Single-Sign On (SSO) integration with existing FTC authentication mechanisms. The system terminates user sessions after 30 minutes of inactivity. Staff are given system access to the least amount of data needed to perform their duties.

FCDS 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.

FCDS deletes FTC data at the request of authorized FTC staff. FCDS initiates data deletion with complete and final deletion occurring within ten business days of the FTC request. FCDS must provide the FTC with a Certificate of Deletion.

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.

FCDS deletes FTC data from Relativity at the request of authorized FTC staff. FCDS initiates data deletion with complete and final deletion occurring within ten business days of the FTC request. FCDS must 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 RelativityOne through a secured website that they have set up specifically for the FTC's use. FTC staff use a specific URL to access RelativityOne 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 RelativityOne. RelativityOne 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 in RelativityOne	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. RelativityOne employs continuous monitoring and utilizes automated intrusion detection and prevention systems. RelativityOne audits successful and unsuccessful account logon events, account management events, object access, policy

<i>Risk</i>	<i>Mitigation Strategy</i>
	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	RelativityOne 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 RelativityOne using dual factor authentication. FTC staff utilize single sign-on (SSO) to log into the system and will be validated using a dual factor authentication method which is selected by the FTC and integrated with RelativityOne environment. The system also terminates sessions after 30 minutes of inactivity. Staff are given the minimal access necessary to perform their duties.

The RelativityOne 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 and must certify their identity by signature, although some records may be exempt from disclosure, 16 C.F.R. 4.13(m), and the agency may require

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

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 RelativityOne 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 consistency with the [FTC's privacy policy](#) posted on its website.