Federal Trade Commission
Privacy Impact Assessment

Relativity

December 2017

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] 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 uses commercial off-the-shelf software applications to review, analyze, and produce ESI. The FTC has contracted with Innovative Discovery, LLC (ID) to obtain an e-discovery software application known as Relativity. ID administers and maintains the software application and all physical systems, and securely hosts FTC data.[2] ID utilizes two geographically diverse data centers for disaster recovery purposes. FTC staff provides data to ID either on encrypted hard drives that are hand-carried to ID facilities or sent via secure file transfer protocol (SFTP) from the FTC production network.[3] ID encrypts the data at rest. In addition to providing software as a service, ID may also assist the FTC with other e-discovery related services, such as ESI processing or loading, database creation, and ESI productions to third parties.

Users – including authorized FTC staff and contractors, and occasionally, law enforcement partners granted access by the FTC – access Relativity using dual factor authentication through a secure website. The data is placed in case-specific databases, and users are granted access to data based on their work assignments.

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 the agency's Electronic Discovery Support System (EDSS), of which Relativity is part, including the Federal Trade Commission Act, 15 U.S.C. §§ 41-58; 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

---

[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] For the purposes of this PIA, Relativity includes both the software provided by ID and the underlying data accessed and processed by the software.

[3] The FTC production network is a wide area network and is the networking "backbone" of the agency – connecting desktop 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.

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.

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)*:_____
☒ Work Address		
☒ Taxpayer ID		
☒ Credit Card Number		
☒ Facsimile Number		
☒ Medical Information		
☒ Education Records		
☒ Social Security Number		
☒ Mother's Maiden Name		

Note: Relativity will maintain any information that the FTC might obtain as part of its law enforcement and other activities. This may include any and 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.

Relativity will maintain information, including Controlled Unclassified Information (CUI),[5] that the FTC might obtain as part of its law enforcement and other activities. This

[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.

[5] CUI is information the 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).

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. For example, during a merger case, the FTC 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 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 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 Staff	Certain FTC staff (litigation support specialists) with elevated privileges have access to the system to load data into the application, assign access rights to databases, and create

Data Will Be Accessed By and/or Provided To:	*How and Why the Data Will Be Accessed/Shared*
	production sets. The litigation support specialists have access to all of the data for the particular Bureau or Office with which they are working. Authorized FTC staff will have web-based access to ID'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.
ID Staff	Only authorized ID staff have access to the FTC's data. These staff have completed FTC-approved background checks and security clearances.
Other External Users	For a particular case or matter, the FTC may grant its law enforcement partners access to data for that case within Relativity. These partners will be provided access to only the data relevant to the case and will have web-based access 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.[6] When the FTC shares information with external entities, it typically does so pursuant to non-disclosure agreements, court-approved protective orders, 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) ID 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

[6] 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.

will have access to the data for the Bureau or Office with which they are working. Authorized ID 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 on a yearly basis. This interactive online training provides guidelines for properly handling PII and other data, online threats, social engineering, and the physical security of documents. ID 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 use and incident response as FTC employees. ID has developed a comprehensive Incident Response Plan for addressing adverse computer-security related events. The plan discusses the company's vulnerability mitigation (including security applications that provide continuous monitoring, least privilege access, dual factor authentication, and logically separating web server, application server, and security manager functionality), and threat mitigation (including firewalls, intrusion detection and prevention systems, system component integrity monitoring, and log inspection). ID also utilizes a Next Generation Focus Incident Response tool that, in the event of a data breach, immediately identifies what data was breached, before encryption. ID'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 ID requires the company to immediately notify the FTC of all breaches. Moreover, ID's Incident Response Plan further states that for incidents related to unauthorized access of PII, ID will report the incident to the FTC within one hour of the security incident being positively identified by ID'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.[7] 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.[8] 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 seeking records about themselves do not have direct access to Relativity, 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 the EDSS 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

[7] See, e.g., notices provided to consumers who file a complaint via Complaint Assistant. See also the FTC Privacy Policy.
[8] See FTC Privacy Policy, SORNS, and PIAs.

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 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). 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 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 Relativity 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.

ID utilizes two geographically diverse data centers that have physical access controls, including the use of guards, identification badges, or entry devices such as key cards. FTC data is encrypted at rest and is maintained separately from other ID client data. Data also is encrypted in transit. The FTC provides data to ID either on encrypted hard drives that are hand carried to ID's offices or transferred using SFTP. ID utilizes various types of automated continuous monitoring of its system. ID replicates its customers' data between its two data centers for disaster recovery purposes.

The FTC will provide data to ID using encrypted hard drives, which ID will return to the FTC for media sanitization or disposal. In the event that ID uses its own encrypted hard drives to transfer FTC data, ID will overwrite the data using a DoD/NSA-approved process or physically destroy the hard drive.

Authorized FTC staff obtain access to Relativity using dual factor authentication. FTC staff log in with user names and passwords as well as a new unique code that is generated each time they log in. If there are more than three failed attempts to gain access to the system, users will be automatically locked out for at least 30 minutes. The system also terminates sessions after 30 minutes of inactivity. Staff are given the least amount of access to data in the system as they need to perform their duties.

ID audits 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.

ID deletes FTC data at the request of authorized FTC staff. ID initiates data deletion within 24 hours of the request, with complete and final deletion occurring within seven calendar days. ID must provide the FTC with a Certificate of Deletion.

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

Yes, Relativity has undergone a security risk assessment and received an authority to operate. The FTC Chief Information Officer (CIO) has accepted residual security risks associated with the operation of this system. The system is categorized as a moderate system using Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization for 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

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 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).

ID deletes FTC data from Relativity at the request of authorized FTC staff. ID initiates data deletion within 24 hours of the request, with complete and final deletion occurring within seven calendar days. ID 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 Relativity through a secured website that ID has set up specifically for the FTC's use. FTC staff use a specific URL to access Relativity 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 Relativity. Relativity 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.

Risk	***Mitigation Strategy***
Unauthorized access to data before it is loaded into Relativity	Data is transferred to ID via hard drives that are encrypted with National Institute of Standards and Technology (NIST)-certified cryptographic modules. These hard drives are hand carried to ID's offices and are subject to strict chain-of-custody controls. Alternatively, the FTC transfers data to ID via SFTP.
Unauthorized access to data in Relativity	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. ID employs continuous monitoring and utilizes automated intrusion detection and prevention systems. ID audits 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.
Unauthorized alteration or dissemination of information	ID audits user activity in the system. These audits include account management events, policy change, privilege use, data access, data deletions, data changes, data exports, permission changes, and all administrator activity.

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 Relativity using dual factor authentication. If there are more than three failed attempts to gain access to the system, users will be automatically locked out for at least 30 minutes. Relativity also terminates sessions after 30 minutes of inactivity. Staff is given the minimal access necessary to perform their duties.

ID audits 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.[9] 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 ID 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.

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

9 Approval and Signature Page

Prepared By:

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

Reviewed By:

_____ **Date:** _____
Katherine Race Brin
Chief Privacy Officer (CPO)

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

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

_____ **Date:** _____
Jeffrey D. Nakrin
Director, Records and Filing Office

Approved By:

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