Federal Trade Commission
Privacy Impact Assessment

Relativity

Updated August 2022

Reviewed February 2023

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 has contracted with FedLabs Complete Discovery Source (CDS), to obtain a commercial ediscovery software application known as Relativity, to review, analyze, and produce ESI. CDS administers and maintains the software application and all physical systems, and securely hosts FTC data.[2] CDS utilizes two geographically diverse data centers for disaster recovery purposes. FTC staff provides data to CDS either on encrypted hard drives that are hand-carried to CDS facilities or sent via secure file transfer protocol (SFTP) from the FTC production network.[3] In addition to providing software as a service, CDS may also assist the FTC with other ediscovery 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. 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 Relativity, 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 Improvements Act, 15 U.S.C. § 18a; and the Robinson-Patman Act,

[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 CDS 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.

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.

☒ 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.)	☒ SMS4Ns5MPID
☒ Alias	☒ Geolocation Information	
☒ Sex	☒ Passport Number	
☒ Email Address		
☒ Work Address		
☒ Taxpayer ID		
☒ Credit Card Number		
☒ Facsimile Number		
☒ Medical Information		
☒ Education Records		
☒ Social Security Number		
☒ Mother's Maiden Name		

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.

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) CDS 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 dai supT ayont (t)-2 t7) C

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.

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 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 stat

5 Data Accuracy and Security

5.1 Are there procedures in place to ensure that the information maintained is accurate, complete, and upto-date?

CDS deletes FTC data at the request of authorized FTC staff. CDS initiates data deletion with complete and final deletion occurring within ten business days of the FTC request. CDS 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

8 Privacy Risks and Evaluation

8.1

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. FTC staff log in with user names and will be validated using a dual factor authentication method which is