Federal Trade Commission
Privacy Impact Assessment

Capital Reporting/Veritext Legal Solutions (MyVeritext, Veritext Virtual, Exhibit Share)

Reviewed January 2026

Table of Contents

1 System Overview

1.1 Describe the project/system and its purpose.

The Federal Trade Commission (FTC or agency) enforces competition and consumer protection laws and regulations to promote competition and protect consumers. Towards that end, FTC staff investigate proposed transactions and conduct, as well as allegations of unfair or deceptive practices in violation of the FTC Act. As part of the investigation process, FTC staff issue subpoenas and civil investigative demands seeking sworn testimony from witnesses, in the form of investigational hearings or depositions. These investigational hearings and depositions must be conducted in accordance with FTC Rules of Practice and, for federal court depositions, the Federal Rules of Civil Procedure. These investigational hearings and depositions are typically conducted by FTC staff throughout the Bureau of Competition (BC) and the Bureau of Consumer Protection (BCP).

It is critical for FTC staff to be able to continue their investigative work, even if such activities must be conducted remotely or through virtual means. The FTC has contracted with Veritext, a deposition and litigation support solution. To request stenographic services, the FTC uses MyVeritext, the online web portal. To conduct online depositions in a safe remote environment, the FTC uses Veritext Virtual, a remote deposition video conferencing platform and electronic exhibit management tool used to display documents to witnesses during investigational hearings and virtual depositions. Veritext Exhibit Share (the virtual exhibit platform) allows parties to upload documents (typically nonpublic) and remotely share and discuss such documents with a deponent. These documents can include (but are not limited to) copies of strategic plans, marketing materials, emails, and financial information. Additionally, use of Veritext Exhibit Share permits attorneys and witnesses to annotate documents and mark exhibits.

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

The FTC is permitted by law to collect these documents, typically pursuant to a subpoena or a civil investigative demand, and the agency uses such information in the course of its investigations. Depending on the matter, these laws may include 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, 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)[1] may be collected or maintained in the system/project. Check all that apply.

In order to provide customer services to its clients, Veritext collects the following PII from FTC users for billing and contact purposes: first name, last name, work email address, work phone number, and work mailing address.

Files, attachments, and exhibits uploaded onto the system may potentially include any and all types of PII (e.g., name, title, address, personal financial data or statement, DOB, SSN, or other information about the individual whose oral testimony is being taken, or about other third-party individuals who are the subject of such testimony).

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
☒ Personal Phone Number(s)	☒ Certificates (e.g., birth, death, marriage, etc.)	☒ Employee Identification Number (EIN)
☒ Work Phone Number(s)	☒ Legal Documents, Records, Notes (e.g., divorce decree, criminal records, etc.)	☒ Salary
☒ Place of Birth	☒ Vehicle Identifiers (e.g., license plates)	☒ Military Status/Records/ ID Number
☒ Age	☒ Financial Information (e.g., account number, PINs, passwords, credit report, etc.)	☒ IP/MAC Address
☒ Race/ethnicity	☒ Geolocation Information	☒ Investigation Report or Database
☒ Alias	☒ Passport Number	☒ Driver's License/State ID Number (or foreign country equivalent)
☒ Sex		☒ Other *(Please Specify)*: _____
☒ Email Address		
☒ Work Address		
☒ Taxpayer ID		
☒ Credit Card Number		
☒ Facsimile Number		
☒ Medical Information		
☒ Education Records		
☒ Social Security Number		
☒ Mother's Maiden Name		

Administrative data. The system collects and stores administrative data, including the names of the FTC case file, the filenames of documents, and the names, usernames, and passwords for MyVeritext users (Bureau staff, Outside Counsel, and Witnesses).

Log data. All system log data is collected within a centrally managed Security Information and Event Management (SIEM) platform and retained for a period of one year. Log data includes but is not limited to authentication events, errors, system process status notifications, user access times. Logs do not contain customer or court data.

[1] 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.

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.

Files, attachments, and exhibits uploaded and shared in the system also may include non-PII, mainly business records, such as strategic plans, marketing materials, emails, and corporate financials. These documents are typically nonpublic in nature.

Counsel can mark-up and provide comments on the exhibits, and the system maintains the marked-up version as a separate copy from what the witness originally submitted. These comments and mark-ups do not generally include or involve any additional PII.

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

The purpose of collecting and uploading documents to Veritext Virtual is to permit FTC attorneys to electronically view, share, and annotate documents during remote depositions and investigational hearings. The purpose of the collection of administrative data from FTC employees is for the administration and security of the system (e.g., password recovery) by Veritext.

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

Source of Data	***Type of Data Provided & How It Is Collected***
FTC staff	FTC staff provide their PII (e.g., full name, e-mail address) to MyVeritext to register for system access, then upload their documents (exhibits) onto Exhibit Share for use during the Veritext Virtual deposition/investigational hearing. Documents are uploaded to case-specific folders. Authorized FTC staff are provided access to folders based upon their case assignments. The uploaded documents are typically obtained from the subject (e.g. target) of the investigation and/or third parties.
FTC External Counsel	External counsel working with the FTC (e.g., local counsel retained under contract) must create their own accounts in order to access marked exhibits and upload documents to Exhibit Share during a deposition/investigational hearing. In order to register an account, they must provide their name, email address, party they represent, and the name of their law firm, and create a password. They are permitted to mark and share those documents with the deponent/witness and with FTC counsel. The uploaded documents are obtained from the subject (i.e., target) of the investigation or third parties.

Source of Data	*Type of Data Provided & How It Is Collected*
Law Enforcement Partner Agencies	Authorized law enforcement partners from other federal, state or local government agencies can discretionarily be provided access to specific files by FTC officials after authorization to share records is granted pursuant to Section 21(b)(6) of the Federal Trade Commission Act, 15 U.S.C. § 57b-2(b)(6). Also see Rule 4.11(c), 16 C.F.R. 4.11(c).
Non-FTC Users	Opposing counsel who have their own MyVeritext account and are not using it as guests have the capability to upload documents and introduce them in a specific deposition.
System-Generated Data	Veritext Virtual automatically generates and maintains the log data on system usage and users.

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	Authorized FTC staff can access documents for use in a deposition/investigational hearing specific to a case and share such documents with the witness, co-counsel, and opposing counsel. Each FTC staff person assigned to that particular case also has the ability to view any annotations (notes) that may have been added to the originally uploaded documents. Per FTC policy, escalated privileged accounts are reviewed every 30 days; non-privileged accounts are reviewed annually to determine whether users need to continue to have access.
FTC External Counsel	Authorized External Counsel working with the FTC (e.g., local counsel retained under contract) can access documents for use in a specific deposition/investigational hearing (IH) in a particular case and may share documents with the witness, co-counsel, and opposing counsel. However, external counsel is not provided access to the case-specific folders that FTC staff use. External counsel is permitted to view only those documents that (a) external counsel uploads or (b) FTC staff reveals in Exhibit Share during a specific deposition/investigational hearing.
Law Enforcement Partner Agencies	Authorized law enforcement partners from other federal, state or local government agencies can discretionarily be provided access to specific files by FTC officials after authorization to share records is granted pursuant to Section 21(b)(6) of the Federal Trade Commission Act, 15 U.S.C. § 57b-2(b)(6). Also see Rule 4.11(c), 16 C.F.R. 4.11(c).

Data Will Be Accessed By and/or Provided To:	*How and Why the Data Will Be Accessed/Shared*
Non-FTC Users	Non-FTC users can view only (1) the documents FTC staff reveal in Exhibit Share for a specific deposition and/or IH; and (2) (if external or opposing counsel, with those permissions) only the documents that external or opposing counsel upload to the specific deposition/IH.
Veritext Staff	Authorized Veritext staff have access to the data based on their roles and privilege group. Scheduling staff have access to names, email addresses, and user data for the purpose of granting access to FTC users. The transcript production team have access to FTC user data and transcripts for the purpose of finalizing documents and distributing them to the FTC. Technical support staff have access to FTC data for contract support, platform access, and troubleshooting. Veritext reviews account access to its systems on an annual basis. Veritext is responsible for managing and monitoring passwords and system security. For users needing access to the virtual exhibit platform, Exhibit Share, credentials are established via a unique one-time activation email. Exhibit Share can be easily linked to the users MyVeritext account, providing access to both the deposition and to the exhibits with a single username and log-in. For non-frequent users, such as witnesses, Veritext offers an Exhibit Share "viewer/guest only" access option through a secure link that restricts document access to viewing (not downloading) only while the deposition is active.

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.

Authorized Veritext staff have access to FTC data in the system and are required to undergo annual training in privacy and security. Select third parties may have access to FTC data as required to deliver services. This includes contractors and affiliate court reporters and legal videographers. Third parties that have access to data are required to align with Veritext security policies and privacy standards, and sign confidentiality/non-disclosure agreements.

To ensure third-party compliance with Veritext security standards and as part of overall Veritext Enterprise Risk Management (ERM) and third-party risk management programs (TPRM), all Veritext third parties utilized in delivering customer services that process, store, or transmit court materials/customer data are required to undergo a risk assessment in the form of Third Party Risk Assessment (TPRA), completed and approved by Veritext. This review consists of a combination of review methodologies including system review of third-

party service infrastructure, interviews with third party representative and subject matter experts (SMEs), and document review of supporting vendor security artifacts, certifications and audit reports.

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.

Veritext encrypts all data at rest and in transit. Veritext allows for distribution of files via secure links rather than as attachments in clear text emails. Veritext also supports delivery of encrypted files directly from within the MyVeritext portal. This approach allows users to securely share files with the inherent encryption, without having to download and email them. Within the Exhibit Share platform, files are similarly secure. Veritext does not allow users the ability to share files directly through Zoom or other third-party meeting platforms. Such sharing of data is inherently risky as the file is distributed locally to all participants; in addition to losing control of the file, it also creates the potential to distribute malicious files.

Veritext leverages Amazon Web Services (AWS) as the backbone for its cloud-based services and conducts systems maintenance around off-peak, weekend hours, and posts notices on its website of any potential impact to users. A dedicated staff composed of programmers, network operations technicians and security personnel are available to respond to any disruption in that time period.

Veritext maintains its own Security Incident Management Plan as part of its Global Information Security Policy. If it is reasonably determined that a breach has occurred involving FTC data, Veritext will notify the FTC of the breach within 24 hours.

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 ☐ Verbal)
- ☒ FTC Website Privacy Policy
- ☐ Privacy Notice (e.g., on Social Media platforms)
- ☐ Login banner
- ☒ Other (*explain*): The MyVeritext Portal and/or Veritext website posts its own privacy policy. There is a requirement to check an "I Agree" box on the user agreement when each FTC user registers his/her account. That agreement includes a reference and link to the Veritext privacy policy.

☐ Notice is not provided (explain): _____

For those documents that the FTC uploads to the Veritext platform, the FTC provides notice to individuals about its policies regarding the use and disclosure of such

documents at the time information is collected pursuant to a CID or subpoena or voluntarily in lieu thereof. Notice is provided as part of the request (e.g., in a letter request, or in the document outlining the compulsory process request). This notice may include a Privacy Act Statement, when that statute applies. See section 8.3 below.

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)?

Unless specified otherwise, user data required to register with MyVeritext is mandatory, and failure to provide this information may make it impossible for the user to access and upload documents, and/or participate in virtual depositions/investigational hearings via Exhibit Share. This includes a valid user ID (email address), full name, and unique activation link to create a registered account. In certain cases where the Exhibit Share application specifically states that some data is not mandatory, users are not obligated to provide the data, and it does not interfere with the availability or the functioning of the service.

Users have the choice at any time to refrain from providing personal information to Veritext. However, choosing not to provide certain information may limit or prevent Veritext from providing services to the user.

For files, attachments and exhibits that are uploaded into the system, individuals whose PII may be contained in such documents may have an opportunity to decline to provide information, except information that the FTC obtains by compulsory process, which is mandatory (e.g., subpoena, CID). If the individual is the submitter of a document, the individual may be entitled to notice an opportunity to object prior to disclosure (see, e.g., section 21 of the FTC Act). Once information is provided by an individual, however, use of his or her information by the FTC (e.g., uploading it to Exhibit Share) is not subject to individual consent, except as provided by law (see, e.g., routine uses under the Privacy Act of 1974, where applicable).

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

Users of Veritext Virtual do not have access to data about themselves in the Exhibit Share application, except to create or change credentials associated with their registered account.

Witnesses do not have direct access to any of the information that may be contained about them within the documents that FTC staff may have uploaded to the Exhibit Share platform. Each witness is provided access only to those documents that FTC staff choose to reveal to the witness during a specific deposition or investigational hearing. Following each deposition or investigational hearing, Veritext provides a copy of the transcript, as well as any documents revealed to the witness during that session, to the witness and the witness' counsel.

Any individual who is required to submit data to the FTC or to testify in a deposition or investigational hearing may request a copy of any document submitted under FTC Rule 2.9, 16 C.F.R. § 2.9. 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 section 8.3 below (Privacy Act).

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.

Yes. The information provided to Veritext by customers is limited to the following public contact information: First Name, Last Name, Business Telephone Number, Business Email Address, Business Physical Address. This information is used to provision customer MyVeritext user access to court reporting service deliverables, and it is the responsibility of the customer to communicate inaccurate or erroneous information to customer's Veritext account manager via telephone or email.

In the context of a witness providing testimony, a witness may submit changes to an official transcript in the form of an errata request sent to the court reporter prior to record certification.

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?

Records of testimony and legal proceedings are preserved in the system as required by courts or the Federal Trade Commission. Standard Operating Procedures (SOPs) and security policies are in place to ensure the integrity of digitized records on the Veritext platform.

Clients provide PII and contact information (e.g., the information provided to Veritext by its customers) is limited to the following public contact information: First Name, Last Name, Business Telephone Number, Business Email Address, Business Physical Address. This information is used to provision customer MyVeritext user access to court reporting service deliverables, and it is the responsibility of the customer to communicate inaccurate or erroneous information to Veritext via telephone or email.

In the context of a witness providing testimony, a witness may submit changes to an official transcript in the form of an errata request sent to the court reporter prior to record certification.

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.

Veritext uses reasonable security measures to maintain the security of the personally identifiable information that it may collect and process on behalf of the FTC. Veritext uses encryption, firewalls, password protection, and physical lock and key to help prevent unauthorized access to PII in its system. They may also place internal restrictions and access controls on Veritext employees to limit to help prevent unauthorized access to PII.

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. No PII is used in course of system training or 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?

Records of testimony and legal proceedings in all forms (e.g., transcripts, exhibits, and related text, audio/video, etc.) are retained by Veritext for a minimum of ten years unless a court order requires destruction of such records.

Additional information on destruction procedures:

- Physical portable media and paper copies of protected data are destroyed by shredding and certified as such by a third-party vendor that has been vetted & approved by Veritext.
- Internal computer storage devices, such as disk drives, solid state drives, and optical drives are removed from computing devices and separately destroyed by a vetted destruction supplier, with a certificate of destruction provided to Veritext by the supplier.
- Virtual storage utilized at hosting provider environments are destroyed by executing a file deletion on the administrative access level.
- AWS Cloud-hosted virtual storage is destroyed per AWS policy.
- Device and server storage backup media are purged of data per backup retention policy.
- A Data and Device Destruction Report or Certificate of Destruction is made available to and archived by Veritext whenever a device or data is destroyed.

Veritext has implemented reasonable physical, organizational, and technological security measures to protect personal information from unauthorized access or disclosure. The safeguards applied consider the sensitivity of the personal information, with the highest level of protection given to the most sensitive personal information.

Veritext endeavors to destroy all copies of personal information related to client request; deleted information may continue to exist on Veritext infrastructure backup systems/media for up to one month per existing data backup processes & policies. Any personal data contained in system backups will not be used unless permitted by law.[2] While processing customer requests for destruction of personal information, Veritext technical personnel follow a standardized process to delete/remove electronically stored personal information from Veritext systems, and shred/destroy all tangible/paper materials containing personal information in scope of the request, while providing attestation/certification of destruction as needed.

Once it is no longer necessary to maintain case specific data on MyVeritext, FTC staff transfer the data to secure FTC systems. Data on FTC systems are deleted according to agency specific records retention policies and NARA guidelines.

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.

Veritext may collect anonymous information from visits to its sites through the use of web beacons, which do not access users' personal information, but rather allows Veritext to count the number of users who have visited its websites. Veritext or its vendors may use this data to analyze trends and statistics to help provide better customer service. Veritext uses web usage tracking software to log the IP address of each individual user. This information is used only to determine website usage, and at no time is there any attempt to associate these IP addresses with personally identifiable information such as names and addresses.

Cookies, which are packets of information sent from a Web service to a Web browser, are created for users who log in to the Veritext websites. The cookies do not store personal information beyond a user's name and email address and are removed when the user leaves the site.

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?

Risk	***Mitigation Strategy***
Documents may inadvertently remain in the system after the	All data in the Veritext platform is encrypted and is not directly accessible to anyone other than users with authorized access. Veritext maintains a strict 10-year

[2] Further details on Veritext's Privacy Policy can be found at https://www.veritext.com/privacy-policy.

Risk	*Mitigation Strategy*
conclusion of depositions/ investigational hearings	policy for the records of proceedings; Veritext may delete the content prior to the 10-year span if mandated by a court order or by written request by all parties in the case. FTC staff take all applicable measures to ensure that FTC data is transferred from MyVeritext when it is no longer necessary to maintain it in the system. The data is retained in FTC's secure systems and deleted as applicable per NARA's guidelines.
FTC staff inadvertently reveal a document to the wrong witness during a deposition/investigational hearing	Different users have different levels of access on the Veritext platform. FTC staff have the ability to view the document prior to revealing it in the course of the deposition/IH. Non-FTC users can view only (1) the documents FTC staff reveal in Exhibit Share for a specific deposition and/or IH; and (2) (if external or opposing counsel, with those permissions) only the documents that external or opposing counsel upload to the specific deposition/IH. For non-frequent users, such as witnesses, Veritext offers an Exhibit Share "viewer/guest only" access option through a secure link that restricts document access to viewing only while the deposition is active. FTC staff can claw back the document to prevent the witness from seeing it; additionally, witnesses have no ability to download the documents from the limited access they have.

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

Veritext employs privacy controls such as automated user session timeouts, use of web-application firewalls, and automated access controls. Only authorized FTC staff are granted accesso the system. FTC staff log in with a username and password. Staff are given access to the minimum level necessary to perform their duties on a specific case. Per FTC policy, escalated privileged accounts are reviewed every 30 days; non-privileged accounts are reviewed annually to determine whether users need to continue to have access.

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).

To the extent any records are retrieved by an individual's personal identifier, the FTC's SORN for investigational and other nonpublic program records applies. See FTC I-1. Additionally, the FTC's stenographic reporting services (FTC I-8) SORN may apply. This SORN may be viewed on the FTC's privacy policy page at www.ftc.gov.

Registration data collected and maintained solely by Exhibit Share and not on behalf of the FTC are not subject to the Privacy Act and do not require a SORN. Although the FTC considers that information confidential and nonpublic, the FTC's SORN for Computer Systems User Identification and Access Records (FTC VII-3) applies to system user records only for systems owned or operated by the FTC or by a third party 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?

Veritext undergoes regular external audits by accredited third-party auditor in the form of an SOC 2 Type II audit. The FTC also reviews its PIAs on an annual basis to ensure that the information presented therein is accurate and up to date.