Federal Trade Commission
Privacy Impact Assessment

StenTrack Database System (StenTrack)

October 2019

Table of Contents

1 System Overview

1.1 Describe the project/system and its purpose.

The Federal Trade Commission (FTC) protects America's consumers. As part of its work investigating potential violations of law, enforcing compliance with law, and in connection with its other work (e.g., holding workshops related to consumer protection and maintaining competition) FTC schedules numerous orders for stenographic reporting services. For example, the FTC uses stenographic services to report and prepare transcripts of depositions of witnesses in investigations. The Records and Information Management Office (RIM) is responsible for administering and coordinating all aspects of stenographic activities for the FTC. This requires RIM to collect, verify, process, and maintain information in a variety of formats.

RIM developed StenTrack specifically for this purpose. StenTrack is a database that allows the requester of stenographic services to enter specific details pertaining to the request: for example, when and where a stenographer is needed, what data/material needs to be transcribed, whether an interpreter is needed, etc. StenTrack comprises a series of modules that guide the user through the stenographic order process. The first module collects general information about the type of order, the matter number/name and the requester's contact information. The remaining three modules collect information pertaining to the deponent, choice of end product formatting from various options and shipping details. Importantly, transcripts of depositions and the corresponding exhibits from those depositions are not stored in StenTrack or linked to StenTrack.

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

The FTC Act and other laws the Commission enforces permit the collection of this information.

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.

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		

StenTrack collects and stores only the information necessary for processing stenographic requests, arranging a deposition or scheduling a necessary service related directly to a specific stenographic request, and delivering an end product to FTC staff. The information maintained by RIM in the database will include names and phone numbers of individuals being deposed as well as the address where the deposition will be taken. Typically, the address is a business address: for example, the business address of the entity the deponent represents. On rare occasions when a deposition is taken at a deponent's home, his/her address will be "flagged" in the system. RIM will perform periodic searches to delete the home address when it is no longer needed. If the deponent requires an interpreter or other special services, that information will be collected and maintained in the system as well. In addition to collecting minimal information about the individual deponent, StenTrack also will collect and maintain information about the FTC staff person requesting the stenographic services, including the requester's name, office, FTC organization code, date of request and contact information. The system also collects the names of individuals eligible to purchase transcripts from the court reporting vendor (typically, counsel representing deponents in investigations or counsel for respondents in administrative litigation under Part 3 of FTC's Rules of Practice)[2]. The FTC staff member requesting stenographic services or the FTC attorney on the matter must authorize the sale in order for an individual to be eligible. Importantly, transcripts and the corresponding exhibits are not stored in StenTrack or linked to StenTrack.

[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] 16 CFR Part 3.

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.

StenTrack also includes information such as the matter name for which a stenographer is needed, when and where a stenographer is needed, what data/material needs to be transcribed, and information about purchasing transcripts. See also sections 1.1 and 2.1 above.

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

The information in StenTrack is collected so that RIM can schedule stenographic services and perform related functions (e.g., obtaining transcripts of depositions) in a professional, efficient and timely manner. Once RIM verifies the order and funding, RIM will forward the order to the appropriate vendor for processing. In addition, data in the system will be used to compile reports for RIM to more effectively manage the process. For example, RIM can review specific Bureau expense reports in an effort to identify spending trends and coordinate with the Bureaus and FTC's Financial Management Office to adjust funding levels accordingly. Miscellaneous data about deponents (e.g., name, contact information) is used for transcript identification and other administrative purposes, such as contacting the deponent, where appropriate, to review and approve the transcript.

StenTrack will be used to manage and maintain data on every stenographic service request in order to schedule stenographic services and perform related functions (e.g., budgeting). All uses of the data are both relevant and necessary for which it was collected.

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 members	Information generally is collected directly from the FTC staff member requesting stenographic services. RIM will initially input the information into StenTrack when it is provided by the FTC staff requesting stenographic services. In the future, FTC staff will input the information directly into StenTrack.
Deponents	The FTC originally obtains information about the deponents directly from them or otherwise as part of its investigative work.
Individuals eligible to purchase transcripts	FTC staff collect information about individuals eligible to purchase transcripts from those individuals.

Other FTC applications (MMS2 and StaffID)	StenTrack is linked to the Matter Management System 2 (MMS2)[3] and the FTC StaffID Database for the purpose of auto-populating certain fields in an attempt to eliminate possible order entry errors. For example, when RIM or the requester enters a matter number, StenTrack will use MMS2 to match the number and then auto-populate the matter name and FTC program code. FTC StaffID confirms the staff member's name and then auto-populates the staff member's phone, mailstop and email address.

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***
Requester Role (Any FTC employee with an Oracle Password).	Can enter and access their orders only
Administrator Role	Can read and modify orders in the Request Module; all other modules are read-only.
Funds Manager Role	Can read and modify orders in the Invoice Module; all other modules are read-only.
System Administrator	Has read and modify rights in all modules.

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.

See section 5.2.

☐ Not Applicable.

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.

☒ Not Applicable.

[3] The Matter Management System (MMS) is used to record, track, and report administrative and statistical information about FTC matters. The MMS PIA is located in https://www.ftc.gov/system/files/attachments/privacy-impact-assessments/mmspia_0.pdf

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): _____

Whenever possible, the FTC provides notice to individuals about its policies regarding the collection, use and disclosure of information at the time the information is collected, for example, in the document outlining the compulsory process request issued in connection with an investigation. The FTC also provides notice via its privacy policy[4], its Privacy Act System of Records Notices (SORNs)[5], and its PIAs, including this one. See also Section 8.3.

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)?

The opportunity or right depends on how the information is collected. Those who provide information pursuant to compulsory process (e.g., an individual or company that has received compulsory process in an investigation and is providing the name and contract information on his or her own behalf or for a deponent representing the company) do not generally have a right to decline to provide the information. In other cases, a deponent may be asked to submit to a deposition voluntarily, where that the individual has the opportunity and right to decline to appear. Individuals eligible to purchase transcripts (see Section 2.1) provide their information voluntarily.

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

An individual may make a request under the Privacy Act for access to information maintained about themselves in StenTrack. Individuals must follow the FTC's Privacy Act rules and procedures published in the Code of Federal Regulations at 16 CFR 4.13. Access to the information under the Privacy Act is subject to certain exemptions.

[4] The FTC's privacy policy is available in both English and Spanish at https://www.ftc.gov/site-information/privacy-policy
[5] The FTC's Privacy Act System of Records Notices (SORN) are available at https://www.ftc.gov/site-information/privacy-policy/privacy-act-systems

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.

See section 4.3 above.

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?

FTC staff check information about deponents for accuracy and timeliness as part of their investigative work and also confirm the names of individuals eligible to purchase transcripts (see Section 2.1). RIM staff and contractors review the orders as part of the scheduling process.

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.

The FTC follows all applicable Federal Information Security Management Act (FISMA) requirements, ensuring that the StenTrack Database system is appropriately secured. The StenTrack Database system resides within the Data Center GSS which is categorized as moderate using Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems.[6]

Only authorized FTC employees and contractors may obtain access to the system. Individuals may obtain access to the system with an authorized Oracle account – with the approval of his or her supervisor (or, for contractors, the approval of the FTC employee who serves as Contracting Officer's Technical Representative on the contract) – by submitting the appropriate forms to the Commission's information technology office. The application administrator then reviews the applications and if permissible grants the appropriate level of access permissions to the individual.

Auditing measures and technical safeguards are in place commensurate with the National Institute of Standards and Technology (NIST) Recommended Security Controls for Federal information Systems and Organizations Moderate-Impact Baseline Special Publication (SP) 800-53, Rev. 4.

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

[6] The FTC Data Center General Support System (Data Center GSS) is the primary IT infrastructure used by the FTC to host information systems that collect, process, disseminate and store information in support of the agency's mission.

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?

This system deletes/destroys data in accordance with the National Archives and Records Administration (NARA) General Records Schedule (GRS) 5.2, item 020, Intermediary Records. Information in the system is destroyed upon successful creation of the final document or file, or when no longer needed for agency use, whichever is later.

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.

☒ Not Applicable

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***
Unauthorized access to Stentrack	One privacy risk identified is that information on a non-public FTC matter, such as an investigation, and/or non-public information about a deponent (e.g., contact information) could be obtained through unauthorized access. Although the potential for harm to individuals is relatively minimal, these risks have been mitigated in a number of ways. For instance, the system uses access controls to limit the ability to view, change, or delete information in the database and to protect the information from internal threats. Only authorized users from within the FTC will be granted access to the database. Authorized users will be required to have an Oracle ID and Password to gain access. Access is further limited based on an individual's role. The system is protected by other electronic or network controls (e.g., firewalls). In addition, agency staff and contractors are subject to security background checks. The contractors involved with the design, development and maintenance of StenTrack have confidentiality, Privacy Act and other privacy-related provisions in their contracts.
Over-collection of data	The information collected on deponents is the minimal amount needed to schedule stenographic services. On the rare occasion

	when the deposition is taken at a deponent's home, the home address will need to be collected and maintained in StenTrack. In an effort to mitigate the risk, any time a home address is collected it will be "flagged" in the system. RIM will perform periodic searches to delete this information when it is no longer needed.

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

Yes. See the information on access control technologies in Section 8.1.

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 system is covered by SORN FTC-I-8, Stenographic Reporting Services Request System – 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?

See Sections 5.2 and 8.1.

The collection, use, and disclosure of the information in this system has been reviewed to ensure consistency with the FTC's privacy policy.

The Privacy Office routinely collaborates with system/application owners as part of its Privacy Continuous Monitoring Strategy to ensure that the information in PIAs, including this one, is accurate and to mitigate any privacy risks, as needed. Members of the public with questions or comments on the FTC's privacy practices may contact the Chief Privacy Officer using the contact information at ftc.gov/privacy.