Federal Trade Commission
Privacy Impact Assessment

for the:

StenTrack Database System

September, 2011

1 System Overview

The Federal Trade Commission (FTC) protects America's consumers. As part of its work investigating potential violations of the laws it enforces,1 enforcing compliance with those laws, 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. An example is the reporting and preparation of a transcript of a deposition of a witness in an investigation. The Records and Filings Office (RFO)2 is responsible for administering and coordinating all aspects of stenographic activities for the FTC. This requires RFO to collect, verify, process, and maintain information to effectively provide FTC staff with timely, professionally prepared transcripts and/or transposed media in a variety of formats. RFO developed StenTrack specifically for this purpose. StenTrack is a database that will allow 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.

2 Information Collected and Stored within the System

2.1 What information is to be collected, used, disseminated, or maintained by the system?

StenTrack will collect and store 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 RFO in the database will include names and phone numbers of individuals being deposed as well as the address were 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. RFO 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).3 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.

2.2 What are the sources of the information in the system?

The information generally is collected directly from the FTC staff member requesting stenographic services. The FTC originally obtains information about deponents directly from them or otherwise as part of its investigative work. RFO staff and contractors (and, in the future, the requester) will input the information into the system on a request-by-request basis. StenTrack is linked to the Matter Management System 2 (MMS2)4 and the FTC StaffID

---

1 A list of the statutes enforced or administered by the FTC is available at http://www.ftc.gov/ogc/stats.shtm
2 Information about the FTC's Records and Filings Office may be found at http://www.ftc.gov/ftc/oed/rfo/index.shtm
3 16 CFR Part 3.
4 The Matter Management System (MMS) is used to record, track, and report administrative and statistical information about FTC matters. The MMS PIA is located at http://www.ftc.gov/os/2007/12/mmspia.pdf

Database for the purpose of auto-populating certain fields in an attempt to eliminate possible order entry errors. For example, when RFO 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 e-mail address.

2.3 Why is the information being collected, used, disseminated, or maintained? How is the information collected?

The information in StenTrack is collected so that the RFO can schedule stenographic services and perform related functions (e.g., obtaining transcripts of depositions) in a professional, efficient and timely manner. Once RFO verifies the order and funding, RFO will forward the order to the appropriate vendor for processing. In addition, data in the system will be used to compile reports for RFO to more effectively manage the process. For example, RFO 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.

2.4 How is the information collected?

Information on deponents is collected directly from them or otherwise as part of FTC's investigative work. FTC staff collect the names of individuals eligible to purchase transcripts (see Section 2.1) from those individuals. RFO 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.

2.5 How will the information be checked for accuracy and timeliness (currency)?

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). RFO staff and contractors review the orders as part of the scheduling process.

2.6 Is the system using technologies in ways that the FTC has not previously employed (e.g., monitoring software, Smart Cards, etc.)? If so, how does the use of this technology affect individuals' privacy?

No. StenTrack is a database programmed using Oracle 10g, which is currently used in other FTC systems.

2.7 What law or regulation permits the collection of this information?

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

2.8 Considering the type of information collected and sources of collection, what privacy risks were identified and how were these risks mitigated?

The privacy risks identified are 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. 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. RFO will perform periodic searches to delete this information when it is no longer needed.

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.

3 Use and Access to Data in the System

3.1 Describe how information in the system will or may be used.

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 to the purpose for which it was collected.

3.2 Which internal entities will have access to the information?

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.

3.3 Which external entities will have access to the information?

None. The system is only accessible internally by authorized FTC staff and contractors.

4 Notice and Access for Individuals

4.1 How will individuals be informed about what information is collected, and how this information is used and disclosed?

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,5 its Privacy Act system of records notices (SORNs)6 and its PIAs, including this one. See also Section 8.2.

5 The FTC's privacy policy is available in both English and Spanish at http://www.ftc.gov/ftc/privacy.shtm
6 The FTC's Privacy Act System of Records Notices (SORN) are available at http://www.ftc.gov/foia/sysnot/i-8.pdf

4.2 Do individuals have the opportunity and/or right to decline to provide information?

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 contact 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 individual has the opportunity and right to decline to appear. Individuals eligible to purchase transcripts (see Section 2.1) provide their names voluntarily.

4.3 Do individuals have the right to consent to particular uses of the information? If so, how would an individual exercise this right?

No.

4.4 What are the procedures that allow individuals to gain access to their own information?

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.

5 Web Site Privacy Issues

Not applicable. The system is not made available for access or disclosure through any public web site.

6 Security of Information in the System

The following questions are intended to describe technical safeguards and security measures.

6.1 Are all IT security requirements and procedures required by federal law being followed to ensure that information is appropriately secured?

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.7

7 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. The Data Center GSS PIA is available at http://www.ftc.gov/os/2011/08/1108datacenter.pdf

6.2 Has a Certification & Accreditation been completed for the system or systems supporting the program?

Yes.

6.3 Has a risk assessment been conducted on the system?

Yes.

6.4 Does the project employ technology that may raise privacy concerns? If so, please discuss its implementation.

No.

6.5 What procedures are in place to determine which users may access the system and are they documented?

Only authorized FTC employees and contractors may obtain access to the system. An individual may secure access to the system – 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 application and if permissible grants the appropriate level of access permissions to the individual.

6.6 Describe what privacy training is provided to users either generally or specifically relevant to the program or system.

All FTC staff are required to complete a computer security and privacy awareness training annually. The interactive online training covers topics such as properly handling Sensitive PII and other data, online threats, social engineering, and the physical security of documents and electronics, such as laptops and mobile devices. Individuals with significant security responsibilities are required to undergo additional training tailored to their respective responsibilities.

6.7 What auditing measures and technical safeguards are in place to prevent the misuse of data?

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. 3.

6.8 **Questions regarding the security of the system.**

Any questions regarding the security of the system should be directed to the FTC's Information Assurance Manager.

7 Data Retention

7.1 For what period of time will data collected by this system be maintained?

The FTC has submitted to the National Archives and Records Administration (NARA) a new, comprehensive retention schedule that includes systems including StenTrack. Once NARA has approved the new schedule, records and data in StenTrack, including auxiliary information and data in the system, will be retained and destroyed in accordance with the new schedule. FTC has proposed a retention period of three years for the data in StenTrack. Pending NARA approval, the FTC will manage the data in a manner consistent with 44 U.S.C. Ch. 31, 44 U.S.C.

3506, 36 CFR Ch. XII, Subchapter B, Records Management and OMB Circular A-130, par. 8a1(j) and (k) and 8a4. Home address information for deponents is considered non-record material that FTC will destroy when no longer needed.

7.2 What are the plans for destruction or disposal of the information?

Information in the system will be destroyed in accordance with the new retention schedule. All data will be deleted/destroyed in accordance with OMB, NARA and NIST regulations and guidelines.

7.3 Describe any privacy risks identified in the data retention and disposal of the information, and describe how these risks have been mitigated.

Regarding privacy risks in data retention, see Section 2.8.

8 Privacy Act

8.1 Will the data in the system be retrieved by a personal identifier?

Yes, data in the system can be retrieved by the name of the FTC requester, lead attorney and funds manager (but not by the name of the deponent or individual eligible to purchase a transcript).

8.2 Is the system covered by an existing Privacy Act System of Records notice (SORN)?

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

9 Privacy Policy

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

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

10. Approval and Signature Page

Prepared for the Business Owners of the System by:

_____ Date: _____
Jeffrey Nakrin
Director, Records and Filings Office

Review:

_____ Date: _____
Alexander C. Tang, Attorney
Office of the General Counsel

_____ Date: _____
Marc Groman
Chief Privacy Officer

_____ Date: _____
Margaret Mech
Chief Information Security Officer

Approved:

_____ Date:
Jeffrey Huskey
Chief Information Officer