Federal Trade Commission
Privacy Impact Assessment

for the:

E-Filing System

May 2010

1. System Overview

The E-Filing System is a web-based application that the Federal Trade Commission will use to receive public filings in adjudicative proceedings conducted under Part 3 of the Commission's Rules of Practice, 16 CFR Part 3. These public filings will be submitted by FTC staff acting as complaint counsel, outside attorneys representing respondents, and others with an interest in the proceeding, such as those filing amicus briefs.

To date, parties in these proceedings have filed their motions, memoranda, briefs, exhibits and other submissions in paper form. The Commission has, however, recently amended its Rules of Practice to provide that if a document is labeled as "Public" an electronic version must be submitted through such system the Secretary directs. See Rule 4.2(c)(3)(i).

All Part 3 filings, except for confidential portions, are treated as part of the agency's public record, and are routinely made available in the agency's public reading room. Public Part 3 filings, with the exception of very lengthy attachments, are posted on the FTC's public web page. The E-Filing System, by enabling parties to use a web site to submit public filings electronically over the Internet, will reduce the time, expense, and burden associated with filing for the FTC and other parties in Part 3 proceedings, while continuing to ensure the security, integrity and availability of such filings. The E-Filing System also implements the Government Paperwork Elimination Act, which requires that agencies, where feasible, offer electronic alternatives for agency filing requirements.

The E-Filing System will be operated by a contractor on behalf of the FTC. The system comprises components or modules that will enable parties to register with the system, to complete the "notice of appearance" form in order to participate in a particular proceeding, and to submit documents in that proceeding. Other system components or modules are designed for FTC staff to process and review the public filings and to export them for posting on the FTC.gov web site.

The System Owner for the FTC's E-Filing System is the Records and Filings Office, which is located in the Office of the Executive Director.

2. Information Collected and Stored within the System

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

The following are collected, used, disseminated, or maintained by the system:

Filings. Public filings, including motions, memoranda, briefs, exhibits, notices of appearance, and other submissions from parties to FTC Part 3 adjudicative proceedings and others. These documents may contain the names, addresses, and/or telephone numbers of individuals, including parties to the proceedings as well as witnesses and consumers.

Registration information. Those who use the non-public system are required to

register and provide the following registration information: first name; last name; title (optional); name of law firm or employer, if applicable; phone number; fax number (optional); and e-mail address. Filers will also specify a login user name and password, which will be maintained in the system as part of their registration data. A set of "password recovery" questions are asked, for the sole purpose of recovering forgotten passwords. The questions chosen and answers provided by the filer will also be maintained by the non-public system.

Metadata. In addition, the system collects additional information that is maintained and associated with each individual filing (i.e., "metadata"). This includes the filer's system user name, the name(s) of the party or parties on whose behalf the public filing is submitted, a filer-defined document title, a document type (from a preset list), and whether the document contains "physical" exhibits.

Review information. FTC staff will attach certain review information to each public document filed. This information includes the receipt date, the document status (pending; filed (accepted), returned (rejected) and web posted) and any other additional comments.

Administrative data. The system will also collect administrative data, including a list of Part 3 Adjudicative Proceedings (by name and docket number) and the names, user names, and passwords for all users (including filers, FTC staff and potentially, FTC contractors).

Log data. In addition, the system collects web log data, including IP addresses and date and time information.

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

Filings are submitted by registered users of the system ("registrants"). In some instances these filings are submitted directly to the system by the registrants; in others, staff in the FTC Records and Filings Office will scan and upload documents into the system when the documents have been filed in a Part 3 matter in paper form. Personal information contained in the documents comes from the individuals to whom it pertains or, in some instances, from other individuals, such as employees of respondents in a Part 3 matter, and consumers who may have done business with respondents.

Registration information and metadata is provided by the registrants themselves. Registrants include FTC complaint counsel, representatives for respondents, and any other users who will be submitting filings through the system.

Review information is entered by FTC Records and Filings Office staff.

Administrative data is entered by FTC Records and Filings Office staff.

Log data is generated and maintained automatically by the system.

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

The purpose of the E-Filing System is to facilitate the submission and web posting of public documents in Part 3 adjudicative proceedings via electronic means.

Review information is used by FTC Records and Filing Office staff, the Office of the Secretary, and the Administrative Law Judge to determine the status of a document.

Administrative data is collected to administer the system (e.g., password recovery).

Log data is collected for system security purposes.

2.4. How is the information collected?

With the exception of log data, all information in the E-Filing System is collected via a web-based form. All users, including registered users and FTC staff, enter or upload the information directly into the web-based form.

Log data is generated by the system automatically.

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

Filers are responsible for submitting accurate information and for updating it as appropriate during the proceeding.

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?

Yes. This web-based system utilizes Windows-based technologies, including HTTPS/SSL, Microsoft SQL Server and .NET. For discussion of how use of the technology affects individuals' privacy, see Sections 2.8 and 4.5.

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

The FTC Act, the Commission's Rules of Practice, and other laws and regulations that the Commission enforces permit the collection of the information. For more information, see www.ftc.gov/ogc/stats .

The Federal Information Security Management Act and other information security laws authorize the FTC to collect user and log data for IT security purposes.

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

Two privacy risks have been identified.

The first risk is that a public document that is filed via the system, and placed on FTC.gov, could contain sensitive personal information, such as social security numbers. The risk that documents will contain sensitive personal information is mitigated by clear instructions and warnings to users that the system is only intended to collect public documents, and that filings will become part of the public records of the Commission and will be posted on FTC's publicly accessible web site.

The system provides specific instructions that each document filed must be clearly marked "PUBLIC DOCUMENT" and must not contain any *in camera* or other otherwise confidential information. Commission Rule of Practice 4.2 (c)(4) prohibits the inclusion of sensitive personal information in a public filing. It is the responsibility of the filer, and not the Federal Trade Commission, to ensure that the document is properly marked, that it contains no confidential or sensitive personal information, and that all redactions are complete, permanent, and irreversible.

Prior to submission of any documents, the user is required to respond, on a document-by-document basis, to the question, "Does this document contain non-public information?" If the user answers "yes" for any document, the system displays a message that the document cannot be submitted. Prior to submission, users must also affirmatively acknowledge that they have followed the filing instructions, including the prohibition on filing any non-public materials through the system.

The second risk identified is that information in the system will be viewed or altered by unauthorized parties. This risk is mitigated in several ways.
The system utilizes encryption technology, particularly in the transmission of data across the Internet (HTTPS/SSL). All users are required to login with a user name and password, based on the FTC's strong password requirements.
To reduce the risk of alteration, filings submitted through the E-Filing system include the full text and graphics of the filed document and are filed in Adobe Portable Document Format (pdf). Access to in-process documents in the system (ones that have not been submitted) is granted only to FTC staff, contractors and subcontractors as authorized when required to fulfill their work assignments. See Sections 3.2 and 3.3. In addition, FTC staff and contractors and subcontractors are subject to security background checks.

3. Use and Access to Data in the System

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

The system is designed to collect, maintain and facilitate web posting of public versions of the filings submitted by parties to FTC adjudicative proceedings.

Filings will initially only be viewable by authorized FTC staff, potentially including FTC contractors. Only once a document, including the relevant metadata, is designated as "filed" will it become part of the public record and be posted to the public website at ftc.gov. With the exception of date stamping, documents are provided to the public exactly as received.

Registration information and metadata are used to ensure that only authorized individuals have access to and submit filings to the system.

Review information is used by FTC Records and Filing Office staff, the Office of the Secretary, and the Administrative Law Judge to determine the status of a document.

Administrative data is collected to administer the system (e.g., password recovery).

Log data is collected for system security purposes.

3.2. Which internal entities will have access to the information?

FTC staff who serve as Complaint Counsel, have registered with the system, and have submitted a Notice of Appearance in a particular matter will have the ability to review and modify their documents in the system prior to filing them. Filers, including FTC Complaint Counsel, cannot use the system to access or edit their filed documents. Once the documents are posted, they can be accessed on the FTC's website.

Authorized FTC Records and Filings Office staff will have access to information for processing, review and administration (e.g., adding a new user account or proceeding). Read only access will be available to authorized Office of the Secretary staff and to staff in the Office of the Administrative Law Judges.

3.3. Which external entities will have access to the information?

External filers (e.g., counsel for respondents) who have registered with the system and have submitted a Notice of Appearance in a particular matter will have the ability to review and modify their documents in the system prior to filing them. Filers cannot use the system to access or edit their filed documents. Once the documents are posted, they can be accessed on the FTC's website.

The system is maintained and operated on behalf of the FTC by a contractor. The system administrator has full access rights to all documents and metadata in the system in order to assist with maintenance of and enhancements to support the system's operations.

Registration information and information about a particular transaction (e.g., any error messages the filer may have received) will be available to FTC contractors in order to provide help desk support and to maintain the operations of the system. This access will be read only, except for passwords and user IDs which they may have to reset as part of their support and maintenance of the system.

Information collected by the E-filing System is not provided to the general public via the system.

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?

The system utilizes web forms to ask the user for the information and provide notice about what information is collected, and how it is used and disclosed.

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

Yes. If the individual does not want to provide information through the system, then, under the Commission's Rules of Practice, the individuals may file documents in paper form.

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

Individuals do not have the right to consent to particular uses of the information stored in the system except by declining to provide the information.

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

All documents filed via the system (i.e. submitted and marked as filed) are posted to the publicly available FTC web site FTC.gov and are available in the FTC's public reading room. Internal and external filers can access their nonpublic registration information and a history of filings (but not the documents themselves) via the system. They also can access their own in-process documents prior to filing them. FTC staff and contractors who are system users (e.g., reviewers) can access registration information, a history of filings and documents filed.

4.5. Discuss the privacy risks associated with the process of providing individuals access to their own records and how those risks are mitigated.

The privacy risk identified is that information in the system will be viewed or altered by unauthorized parties. To address this risk, the system utilizes encryption technology, particularly in the transmission of data across the Internet (HTTPS/SSL). In addition, users are required to login with a user name and password, based on FTC's strong password requirements.

5. Web Site Privacy Issues

5.1. Describe any tracking technology used by the Web site and whether the technology is persistent or temporary (e.g., session cookie, persistent cookie, Web beacon).
Currently, persistent tracking technology is not approved for use by the FTC

(see 5.2).

The system uses a session cookie to hold authentication information. This cookie is destroyed when the browser is closed or the user logs out of the system.

The system does *not* use persistent cookies, web beacons, or other persistent tracking technology.

If a persistent tracking technology is used, ensure that the proper issues are addressed (issues outlined in the FTC's PIA guide).

Not applicable.

5.2. If personal information is collected through a Web site, page, or online form accessible through the Internet, is appropriate encryption used? If not, explain.

Data transmission via the Internet is encrypted via a secure connection (HTTPS/SSL).

5.3. Explain how the public will be notified of the Privacy Policy

Every page of the web site will contain a link to the FTC Privacy Policy http://www.ftc.gov/privacy

5.4. Considering any Web site or Internet issues, please describe any privacy risks identified and how they have been mitigated.

The system is intended to collect only public information. However, because the system collects some information in identifiable form, the system has access restrictions and other security measures (e.g., encryption) to protect all system data. See Section 2.8.

5.5. If the Web site will collect personal information from children under 13, or be directed at such children, explain how it will comply with the Children's Online Privacy Protection Act (COPPA).

The system is not intended to collect information from children under 13. Therefore, COPPA does not apply.

6. Security of Information in the System

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

Yes. All IT security requirements and procedures required by federal law are being followed to ensure that information is properly secured.

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

Yes. A Certification and Accreditation has been completed.

6.3. Has a risk assessment been conducted on the system?

Yes. A security risk assessment has been conducted on the system. All risks are documented in the system's Security Risk Assessment document.

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

The system uses web-based forms, but precautions have been taken to ensure the security of such forms as described elsewhere in the PIA. See Sections 2.6 and 2.8.

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

A filer must complete the registration process and file a Notice of Appearance for a specific active proceeding to file documents in that proceeding. The Records and Filings Office has procedures in place to grant access to FTC staff (reviewers and read-only access for Office of the Secretary and ALJ staff). Access is granted only if needed to perform their work.

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

All FTC staff receive privacy training on an annual basis. Relevant staff in the FTC's Records and Filings office will receive specific training on the use of the E-Filing System.

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

The system is categorized based on Federal Information Processing Standards (FIPS) security categorization and on the National Institute of Standards and Technology (NIST) Security Control guidance as a moderate risk system. It has been designed to prevent all unauthorized access to the data contained in the system, including unauthorized access by administrators and developers. The system has undergone a certification process to validate the integrity of the access controls. The access controls comply with the Security Technical Implementation Guide (STIG) that NIST guidance sets out for a moderate risk system. The application's access controls include regular auditing and testing of the system.

6.8. State that any questions regarding the security of the system should be directed to the FTC's Chief Information Security Officer.

Any questions regarding the security of the system should be directed to the FTC's Chief Information Security Officer.

7. Data Retention

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

The Part III notice of appearance forms and documents are incorporated into the respective matter case file as Federal records subject to the retention period of the matter. During the E-Filing pilot phase expected to take place during the remainder of FY2010, all paper and electronic copies of forms, documents, outputs such as reports, metadata, and system documentation will be validated and disposition plans determined. The current records retention schedule specifies that the matter file be retained for 25 years after final action and close. The FTC has submitted to the National Archives and Records Administration (NARA) a comprehensive records disposition schedule, SF-115 Request for Disposition Authority. Pending NARA approval, FTC will manage the E-Filing system 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.

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

All E-Filing information 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 identified in data retention, see Section 2.8. No privacy risks have been identified in the disposal of the data.

8. Privacy Act

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

Yes. Information filed by users is tied to a user account, which is identified by a user-defined user name and password.

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

Public filings received through the system are covered by FTC I-6. System user data are covered by FTC VII-3. http://www.ftc.gov/foia/listofpaysystems.shtm

The FTC is considering whether to publish a SORN specifically for this system.

9. Privacy Policy

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

The collection, use, and disclosure of information in the system have been reviewed to ensure consistency with the FTC's privacy policy posted on the FTC's web site, www.ftc.gov .

10. Approval and Signature Page

Prepared for the Business Owners of the System by:

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

Review:

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

_____ Date: _____
Kellie Cosgrove Riley
Acting Chief Privacy Officer

_____ Date: _____
Margaret Mech
Chief Information Security Officer

Approved:

_____ Date: _____
Vance Allen
Acting Chief Information Officer