



**Federal Trade Commission
Privacy Impact Assessment**

for the:

W120023 ONLINE FAX SERVICE

December 2012

1 System Overview

The Federal Trade Commission (FTC, Commission or the agency) is an independent federal government law enforcement and regulatory agency with authority to promote consumer protection and competition through the prevention of unfair, deceptive and anti-competitive business practices; to enhance informed consumer choice and public understanding of the competitive process; and to accomplish these missions without unduly burdening legitimate business activity.

The Online Fax Service provides an effective and efficient alternative to the traditional manual fax method using existing agency fax machines. Particularly for faxes that are being sent to multiple destinations, that contain a high volume of information, or that are transmitting material that is already in electronic format, the Online Fax Service reduces the time, effort, cost, and risks associated with more traditional manual fax methods. Currently, FTC users can use the Online Fax Service to send, but not receive, faxes.

The Online Fax Service permits authorized FTC employees and contractors to use their web browser to securely upload materials to the contractor's fax portal for fax transmission to designated recipients.

Some of the information sent via the Online Fax Service may include nonpublic or otherwise sensitive information, including personally identifiable information about members of the public (e.g., individual defendants, consumers, or others) or FTC employees or contractors. Accordingly, we have conducted this "privacy impact assessment" (PIA) and are making it available to the public, as required by section 208 of the E-Government Act of 2002, to explain how the FTC has considered the possible privacy risks of such a system and how we have addressed those risks before putting the system online.

2. Information Collected and Stored within the System

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

Information uploaded to, transmitted by and temporarily maintained in the Online Fax Service is not restricted to a specific category or subset of FTC matters, and may relate to any authorized, official FTC matter, such as an FTC law enforcement investigation, lawsuit, or study.

Information uploaded to, transmitted by, and temporarily maintained in the Online Fax Service may include materials that the FTC has previously collected voluntarily (e.g., access letter or discovery) or through compulsory process (e.g., subpoenas, civil investigatory demands, court orders) from various businesses or individuals (see section 2.2 below), as well as materials that the FTC staff themselves have compiled or generated (e.g., drafts of joint motions or briefs, attachments, or exhibits, being uploaded and shared with opposing counsel for review). These materials will frequently consist, in whole or part, of nonpublic information, including confidential business data or other privileged or internal matters. In addition, the materials may contain personal information about specific defendants, consumers, or other individuals, some of which could raise privacy issues if they were to be improperly handled or disclosed (e.g.,

personal financial statements, bank records, credit card numbers, customer lists, consumer complaints or affidavits, personal contact data).

The system also collects, uses, and maintains account information for FTC staff with access to the service. This information includes email address, password, and user preferences.

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

The information uploaded to, transmitted by, and temporarily maintained in the Online Fax System may include copies of materials that have been collected, gathered, or generated in connection with the FTC's legal, investigatory, administrative, and other activities, as well as orders issued by courts in connection with FTC litigation. Sources of materials include targets of investigations (businesses and individuals) and their lawyers and representatives; companies or organizations not under investigation; consumers, witnesses, and informants; and others (e.g., data acquired by the FTC from commercial, academic or governmental sources); and FTC staff (e.g., nonpublic drafts or memoranda, briefs, attachments, exhibits authored by FTC attorneys).

User IDs will be created by the System Administrator. Staff will provide their own passwords and user preferences.

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

Information uploaded to, transmitted by, and temporarily maintained in the Online Fax Service is used for law enforcement and other agency activities. As noted earlier, Online Fax Service provides a secure alternative to traditional manual fax methods used by the FTC, particularly when transmitting material to multiple recipients or sending voluminous materials or materials that already exist in electronic form.

User account information is collected to allow users to securely use the Online Fax Service.

2.4. How is the information collected?

Materials to be transmitted by the Online Fax Service will be securely uploaded from the FTC network by authorized users to the contractor's portal, together with the transmission information for the recipient(s), as encrypted electronic files (attachments).

User IDs will be created by the System Administrator. Staff will enter their own passwords and user preferences directly into the secure system.

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

Files are uploaded to the Online Fax Service's secure storage area "as is" without verifying their accuracy or timeliness. Instead, the underlying information that is used by the FTC as part of its law enforcement and other activities is reviewed for accuracy and timeliness as required by, and in the course of, the particular activity.

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. The Online Fax Service is a new technology that the FTC has not previously employed. Although this technology may require the transfer of potentially sensitive information, including nonpublic information and PII, over the internet, the system protects the confidentiality and integrity of such information by using authentication and encryption, by limiting storage of uploaded materials by the contractor to the time required to confirm transmission and receipt of the facsimile, and by using secure fax transmission to minimize the risk of interception and unauthorized access and use.

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

The Federal Trade Commission Act, 15 U.S.C. §§ 41-58, the Commission Rules of Practice, and other statutes and regulations enforced by the agency authorizes the FTC to collect the information that is sent, received, and maintained temporarily in the system.

For system user information, see the Federal Information Security Management Act, 44 U.S.C. 3541 *et seq.*

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

The FTC has identified several risks that could affect the privacy of individuals whose information may be uploaded to, transmitted by, and temporarily maintained in the Online Fax Service.

Such information could be intercepted in transit over the Internet. The web-based application addresses this risk by using enhanced encryption and authentication methods. The Online Fax Service's configuration requires information to be transferred from the authorized FTC user to the fax portal in encrypted form using secure socket layer (SSL) technology, and the user's Web browser verifies the digital signature (i.e., authentication) of the secure Web page where files are uploaded and downloaded. In addition, the contractor's storage of uploaded materials is temporary. After the contractor, transmits the fax, confirms its receipt by the recipient(s), and notifies the FTC sender that the fax has been received by its intended recipient(s), the contractor securely and irreversibly deletes the uploaded material from its system.

There is a risk that users may inadvertently transfer sensitive data (including Sensitive PII) to unintended recipients, but this risk also exists with manual fax transmission. This risk is addressed by administrative and technical controls adopted by the FTC as well as security and process controls inherent in the Online Fax Service. To become an authorized FTC user of the Online Fax Service, FTC employees must be approved for access by DPI, must complete an online training module, and must also comply with specific user guides for internal (FTC) users that explain the proper use of the system.

In addition, to help ensure that materials are sent to the correct recipient, the Online Fax Service requires manual entry of the recipient fax number(s). Therefore, when users type the recipient fax number(s) into the "To" field in the Online Fax Service's portal, there is no "auto-complete" function unless the user has previously sent a fax to the same recipient using the Online Fax Service system.

Furthermore, all FTC Online Fax Service users must verify that the recipient fax number(s) that appear in a confirmation box on the user's screen are correct before the fax can be sent from the system, and after the fax is sent, the user receives e-mail confirmation that the fax was sent and may verify that the fax was sent to the correct recipient.

To prevent FTC users and administrative users from exceeding their authorized access and viewing documents or files from other accounts, FTC users cannot access other accounts and system administrators do not have access to files that have been uploaded to the Online Fax Service. Administrators can only view logs of each transaction for auditing purposes.

3. Use and Access to Data in the System

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

As discussed in the introduction and system overview (see Section 1), information in the system may be used to support the FTC's law enforcement and other activities, including to investigate and enforce statutes and regulations protecting consumers against fraudulent, deceptive, or unfair practices in the marketplace; to locate victims; to assist with redress; to investigate internal matters; and to defend against suits brought against the agency.

User account information will be used to allow approved FTC staff to securely access and use the Online Fax Service.

3.2 Which internal entities will have access to the information?

Only authorized FTC employees and FTC contractors who have received either classroom or one-on-one training on the proper use of the system will be approved for use of the Online Fax Service at the FTC. User IDs can only be created by a System Administrator, and authorized users will retain access rights until they no longer have a business need for the Online Fax Service or they leave the agency. The system owner for the Online Fax Service is the Information Assurance Branch in the Office of the Chief Information Officer.

3.3 Which external entities will have access to the information?

None. Only authorized FTC employees and contractors have access to the FTC's account and the information it contains. All FTC materials uploaded to and transmitted by the Online Fax Service are transmitted telephonically as ordinary faxes to the intended recipient(s), and those recipients cannot access the information while it is in the fax portal. System administrators do not have access to files that have been uploaded to the Online Fax Service, but can only view logs of each transaction for auditing purposes. After the contractor transmits the fax, confirms its receipt by the recipient(s), and notifies the FTC sender that the fax has been received by its intended recipient(s), the contractor securely and irreversibly deletes the uploaded material from its 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?

Wherever required, the FTC provides notice to individuals about its policies regarding the use and disclosure of information at the time information is collected (e.g., in voluntary access letters, civil investigatory demands, or agency forms or questionnaires that were originally used to request or collect the information uploaded to the system).

For the Online Fax Service users, appropriate notice is given at the secure webpage where their user login information is collected. On those occasions where the FTC cannot provide notice at the time information is collected (e.g. information collected and maintained by other organizations that have then shared such information with the FTC), the FTC provides notice via its privacy policy, its Privacy Act Systems of Records (SORNs), and its PIAs, including this one.

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).

The Online Fax Service uses session cookies for site functionality, performance, and quality. It also uses three persistent cookies: “remember job type,” “fastTrackState,” and “sa_user_id.” The first associates a user with previous online fax send preferences, the second is used to remember the user’s starting page, and the third is used to remember user id. All cookies are owned by and associated solely with the Online Fax Service, and the cookies are only functional on the Online Fax Service portal. Although some customers of the Online Fax Service may receive additional persistent and third-party cookies, as well as other tracking technologies, all such tracking technologies have been inactivated with regard to FTC users of the Online Fax Service

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?

The FTC follows all applicable Federal Information Security Management Act (FISMA) requirements with regard to the Online Fax Service.

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

Not applicable.

6.3 Has a risk assessment been conducted on the system?

This PIA serves as the risk assessment for the Online Fax Service.

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

Yes; the Online Fax Service uses the Internet to transmit information from the FTC to the contractor before converting that material into a traditional fax that is transmitted by telephone line. Use of the Internet potentially poses a privacy concern, however, as discussed in section 2.8, the Online Fax Service incorporates a number of measures to minimize the risks. The Online Fax Service uses several layers of authentication to ensure that only authorized recipients can access the files and that transmissions between the FTC and the contractor are encrypted, and a secure transfer protocol is used. In addition, the system utilizes various administrative and technical controls, as well as training to minimize the privacy risks identified and discussed earlier.

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

Authorized FTC employees and contractors must be pre-approved by their supervisor to access the Online Fax Service, and they must receive classroom or one-on-one training on the appropriate use of this technology. In addition, all authorized users must read and sign a 'Rules of Behavior' form, acknowledging their responsibilities while using the Online Fax Service.

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 computer security and privacy awareness training annually. The interactive online training covers topics such as properly handling of Sensitive PII and other data, online threats, social engineering, and the physical security of documents. Individuals with significant security responsibilities are required to undergo additional, specialized training, tailored to their respective responsibilities. In addition, as noted above, there is Online Fax Service-specific training for FTC users.

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

The Online Fax Service system tracks each fax that is sent, from whom the file is sent, to whom the file is sent, and the name of the file that was uploaded for transmission. There is also a documented list of authorized FTC users who can access the Online Fax Service and a comprehensive use log that can be filtered to identify file transfers, senders and recipients.

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?

After the information is uploaded to the Online Fax Service, the contractor transmits the fax, confirms its receipt by the recipient(s), and notifies the FTC sender that the fax has been received by its intended recipient(s). Once transmission is confirmed, the contractor securely and

irreversibly deletes the uploaded material from its system. If transmission cannot be completed for any reason, the uploaded material is deleted after the maximum retry attempts of three. Therefore, the Online Fax Service never maintains files. Uploaded files are not duplicated or transferred to other storage media during the normal course of transmitting the facsimile(s). Transmission information collected for the purpose of monitoring Online Fax Service usage, including access, system event, and device usage logs do not contain any message content. These system event and usage logs are not customer-specific and will be deleted or destroyed when the Online Fax Service provider deems appropriate.

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

See the response to Question 7.1

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

An overall discussion of the privacy risks associated with the Online Fax Service and the steps that the FTC has taken to mitigate those risks is provided in section 2.8, above. The privacy risk in disposal of information uploaded to and transmitted by the Online Fax Service is relatively low, because the uploaded information is only maintained temporarily and is deleted directly from the Online Fax Service system; the contractor does not retain the uploaded materials in other locations or formats.

8. Privacy Act

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

Documents temporarily awaiting transmission in the system are not (and will not be) retrievable by a personal identifier (e.g., name or other personally assigned number or identifier). The system does, however maintain user accounts that a system administrator can retrieve by a unique user ID (e.g., e-mail address).

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

Although the FTC, as noted in 8.1 above, does not maintain and cannot retrieve documents transmitted through the Online Fax Service by any subject individual's name or other personal identifier, the FTC maintains many of these documents as part one or more Privacy Act systems for which the FTC has published SORNs. *See, e.g.,* FTC I-1 (Nonpublic Investigational and Other Nonpublic Legal Program Records). The FTC has also published a SORN for computer systems user ID and access records maintained by or on behalf of the agency. *See* SORN FTC VII-3. All of the FTC's SORNs are available at <http://www.ftc.gov/foia/listofpaysystems.shtml>.

9. Privacy Policy

9.1 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 information in this system is consistent with the FTC's Privacy Policy.

10. Approval and Signature Page

Prepared for the Business Owners of the System by:

_____ Date: _____

Jack Gabriel
Assistant Director of Operations Assurance
Office of the Chief Information Officer

Review:

_____ Date: _____

Alexander C. Tang, Attorney
Office of the General Counsel

_____ Date: _____

Peter Miller
Chief Privacy Officer

_____ Date: _____

Jeffrey Smith
Information Assurance Manager
Office of the Chief Information Officer

_____ Date: _____

Jeffrey Nakrin
Director, Records and Filings Office

Approved:

_____ Date: _____

Jeffrey Huskey
Chief Information Officer