



**Federal Trade Commission
Privacy Impact Assessment**

for the:

FOIAXpress System

August 2009

1 System Overview

This Privacy Impact Assessment (PIA) discusses the Federal Trade Commission (FTC) FOIAXpress system. The FTC's Office of General Counsel (OGC) uses this electronic system to track and fulfill requests filed by members of the public seeking access to nonpublic FTC records under the Freedom of Information Act (FOIA), and requests from individuals seeking access under the Privacy Act of 1974 (PA) to nonpublic FTC records, if any, about themselves. This PIA explains what information about individuals is maintained in the FOIAXpress system, how we collect that information, who is allowed to use it and for what purposes, and what steps the FTC has taken to identify, secure, and reduce any privacy risks to that information.

The FOIAXpress system is a commercial off-the-shelf web-based application that the FTC runs on its secured internal servers. The system allows the FTC to log and track the processing of each FOIA or PA request, using data entered by FTC staff or automatically generated by the system about the request, the requester, or the FTC staff assigned to process the request. The system records the status of the request, relevant deadlines, and other key events or data, such as the agency's response to the request, and any related administrative appeals or court litigation if the request was denied. The FTC also uses FOIAXpress to store and manage copies of the nonpublic agency records that have been gathered in response to each access request. In some cases, these copies contain personally identifiable information about the requester or about other individuals mentioned or discussed in the scanned records.

2 Information Collected and Stored within the System

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

Correspondence Log. Communications (e.g., letters, e-mails and facsimiles) to and from the requesting party are entered into the correspondence log portion of the system. Personally identifiable information (PII) captured here can include but is not limited to names, addresses, telephone numbers, e-mail addresses, fax numbers, and other contact information of the requester or the person filing on behalf of the requester. Documents that contain social security numbers ("SSNs") (such as the original FOIA request) may be scanned into the correspondence log section of the system (see 8.1 for how data is retrieved).

File Cabinet/Document Management. As noted in Section 1, the system also maintains copies of materials responsive to the access request that have been gathered from other FTC offices and entered into the system. These documents consist of legal, investigatory, administrative, or similar nonpublic agency records, some of which may contain PII about investigatory targets or other individuals (e.g., witnesses, complainants, FTC staff, other consumers, or the requester) depending on the type and nature of the

record. For example, such PII can include names, addresses, telephone numbers, or other information about an individual (e.g., a complaint by a consumer or description of an alleged violation by the subject of the investigation).

Review Log and Case Folder. Once responsive records within Document Management are redacted by a FOIA Professional they are sent to the Review Log section for supervisory review and approval. After redacted records are approved for an outgoing response to the Requester, the records are sent to the Case Folder before delivery to the Requester. The documents found within the Review Log and the Case Folder are copies of documents in Document Management.

System Users. FOIAXpress also stores information on the identity of system users (those with password protected access as explained in Section 3.2), including the specific access requests they worked on. FOIAXpress maintains records showing who has access, who the active users are, and what access requests the users have been assigned to process.

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

The principal source of PII in the system about requesters is from individuals' own access requests. FTC staff may enter additional information into the system in the course of processing, considering, and responding to these access requests (e.g., notes about when staff discussed the request with the requester, user ID and password when staff accesses the system). Some information in the system is generated or compiled by the system itself (e.g., deadlines for responding to an individual's FOIA request; date, time and other information about system users).

As noted in Sections 1 and 2.1, other records in the system about individuals consist of documents that have been identified as responsive to these access requests. Depending on the particular record (e.g., affidavit, court filing, investigatory record, personnel file), the PII in such records will have come from the individual requester, from some other individual (e.g., investigatory targets, requesting witnesses, consumer complaints, employees), or from other sources (e.g., public media, commercial databases, other companies or non-individual entities).

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

The information collected in the system is used to respond to access requests under the FOIA or the PA, to track these requests in order to maintain compliance with statutory response times, and to maintain documents responsive to these requests, regardless of whether they are exempt from disclosure to the requester under the FOIA or the PA. The information is also used to generate annual reports to the Department of Justice as

required by FOIA.

2.4 How is the information collected?

As noted in Section 2.1, PII about FOIA and PA requesters is compiled and entered into the system by FOIA staff. The information entered is obtained from the requesters' initial FOIA or PA requests as well as from follow-up correspondence or other communications.

PII in responsive documents that are entered into the system is collected either by voluntary or mandatory means (e.g., subpoena) either directly from the relevant individual or from third-party sources, as explained earlier in Section 2.2.

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

As mentioned in Section 2.4, information stored in the system about requesters has been collected from the requesters themselves (i.e., their access requests and related communications) or is generated and entered by staff. OGC staff checks the accuracy and timeliness of this information (e.g., contact information, precise scope of the request) as necessary to allow FTC staff to respond to or contact a requester and to ensure that FTC staff accurately interpret and respond to the request. Furthermore, as set out by 16 CFR Part 4.13, when the request is from an individual seeking access to his or her own records under the Privacy Act (e.g., a consumer seeks a copy of a complaint they previously submitted or an FTC employee seeks access to or a copy of his or her own personnel records), OGC staff may require additional verification of that requester's identity when reasonably necessary to assure that records are not disclosed to someone other than the submitter or their representative.

The OGC staff does not check the accuracy or timeliness of responsive documents that are scanned into the system, including any PII that may be contained in such documents. The FTC is required under the FOIA to grant or deny access to responsive records "as is," without alteration. The accuracy and timeliness of the information (including any PII) contained in such records, would be governed by other laws and authorities, if any, applicable at the time the agency compiles those records (e.g., FTC Act, personnel laws, administrative or court evidentiary rules and procedures).

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?

The system does not employ technologies that create any new or significant privacy risks at the FTC. As noted earlier, the FOIAXpress software is a commercially available tracking system for managing FOIA and PA requests and agency documents responsive to such requests.

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

The FTC's collection and maintenance of information in FOIAXpress relating to FOIA and PA access requests is authorized by the FOIA, 5 U.S.C. § 552, as amended, and the Privacy Act of 1974, 5 U.S.C. § 552a, both of which require the FTC to respond to requests and appeals filed under those statutes. *See* also 16 C.F.R. §§ 4.11 and 4.13 (FTC rules implementing the FOIA and PA, respectively). The FOIA, the PA, and the Federal Records Act require that responsive records be temporarily or permanently maintained. Certain information is also needed to generate annual reports to the Department of Justice as required by FOIA. Information, including PII, in responsive documents scanned into the system is collected under, and its handling governed by, other laws and regulations (e.g., FTC Act), as discussed in Section 2.5.

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

The main privacy risk associated with the collection and maintenance of PII in the system about FOIA and PA requesters is that individual requesters may, when filing their access request, include sensitive personal information about themselves, or about other individuals in their request. Similar risks are presented by the entering of responsive documents into the system. This information could then be compromised by unauthorized access or disclosure. To mitigate this risk, the FTC has taken steps to minimize the amount of information that the agency collects and maintains about such individuals. For example, the FOIA Office only asks for the minimum amount of contact information from individual requestors necessary to communicate with them and respond to their requests as required by law. At the weblink to our online request form, we alert requesters not to provide sensitive PII unless necessary to authenticate a specific request. To avoid unauthorized access or disclosure, this information is logged into the database, but system access is limited (by software licenses) to a small number of specified FTC professionals who need system access to do their jobs. Each user must have a valid and current password. Only the user and other designated FOIA professionals with Administrator rights can change these passwords.

In other cases, if the responsive document is especially sensitive, it may be omitted from the process entirely.

An additional potential privacy risk could arise when certain information is extracted from the system for placement on the public record (See Commission Rule 4.9(b), 16 C.F.R. § 4.9(b), for a list of all FTC public records, which includes copies of FOIA requests.). Personal addresses and telephone numbers are redacted prior to placing the information on the public record, as is more sensitive PII that may be included in the request. See Section 3.1 for further details.

Furthermore, when the FTC provides documents in response to an access request, the FTC redacts sensitive personal information from the documents where the information,

if publicly disclosed, would cause a “clearly unwarranted invasion of personal privacy.” See 5 U.S.C. 552(b)(6). When a requester is seeking his or her own information under the Privacy Act, the FTC properly authenticates the individual’s identity before disclosing the Privacy Act records to him or her. Finally, to guard against unauthorized or inadvertent disclosure, FOIA/PA staff also follow special internal agency procedures for working with, storing, sharing, sending, transporting, and destroying sensitive personal information.

3 Use and Access to Data in the System

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

System information will be used to respond to access requests under the FOIA or the PA, to track the status of responses, to grant or deny access to documents responsive to these requests and to maintain these documents. System information is also used to generate annual reports to the Department of Justice as required by FOIA.

Copies of request and appeal letters, and agency responses thereto, are placed on the FTC’s public record and made available to the public for routine inspection and copying. As discussed earlier, the FTC redacts personal addresses and contact numbers of requesters from these materials before they are placed on the public record. As required by the FOIA, copies of records in the system that have been “frequently requested” within the meaning of the FOIA and disclosed to requesters under that law are made available to the public for routine inspection and copying from the agency’s public record room and its Web site.

See Section 8 of this PIA for additional “routine uses” of system records that are retrieved from FOIAXpress by the name or other personal identifier of an individual (e.g., requester, system user, investigatory target mentioned in a scanned document). These “routine uses” are described in the applicable system of records notices (SORNs) published by the FTC under the PA. *See, e.g.,* FTC-V-1 (Freedom of Information Act Requests and Appeals–FTC).

3.2 Which internal entities will have access to the information?

FOIA/PA professionals in the FTC’s OGC have User ID and password-protected access to the records as necessary to prepare responses to FOIA/PA requests and appeals and to prepare periodic reports as required by law, executive order or agency directive. FOIA/PA liaisons in other sections of the FTC do not have access rights to the FOIAXpress System. Administrator rights are limited to a few supervisory or senior level FOIA/PA staff in OGC to ensure the proper functioning of the system. FTC Office of Information Technology Management professionals have access as necessary to administer and support FOIAXpress operations.

3.3 Which external entities will have access to the information?

External entities do not have user access to the system; contractors have access as necessary for the proper functioning of the system. FOIA/PA requesters have access to responsive records in the system only when OGC staff retrieves them from the system and discloses them in electronic or paper format to such requesters. Before such disclosure, staff may share such documents with other law enforcement agencies or the original submitters in order to determine whether the materials are confidential or otherwise exempt from mandatory FOIA or PA disclosure. In addition, as noted earlier, the PA also allows the FTC to disclose information in the system for other “routine uses” compatible with the purpose for which the record was collected, as set forth in the applicable Privacy Act SORNs. See Section 8 below.

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 FTC notifies the public, including FOIA/PA requesters, and FOIAXpress system users about what information is collected in the system, and how it is used and disclosed, through applicable system of records notices that the FTC has published in the *Federal Register* and posted online. As required by the FOIA, the Commission also sets out in its regulations at 16 CFR 4.11 and in the agency’s FOIA Handbook (<http://www.ftc.gov/foia/foiahandbook.pdf>) what information the FTC needs from a requester to process an access request.

Additional notice about what the FTC collects from individuals when they file a FOIA request is provided on the FTC’s online FOIA request form (<https://www.ftc.gov/ftc/foia.htm>). The FTC’s Web site also contains a Privacy Policy explaining what the FTC does with personal information that it may collect and maintain on individuals (<http://www.ftc.gov/ftc/privacy.shtm>).

In contrast, notice to individuals whose information may be contained in responsive documents entered into the FOIAXpress system is provided to such individuals, where appropriate or legally required, at the time that information is collected from him or her (e.g., by subpoena, civil investigatory demand or other compulsory process, by voluntary access request in an investigation). In some cases (e.g., court cases), an individual may also receive notice when the FTC collects his or her information from other sources (e.g., when the FTC serves a subpoena on another person or entity for information about the individual and the court rules require the FTC to notify that individual as well).

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

FOIA/PA requesters: All information provided by FOIA/PA requesters to the FTC is voluntary. Individuals may freely decline to provide any information they do not wish to provide, but it could adversely affect the FTC's ability to process a FOIA or PA response if the contact information is inadequate or the individual's identity cannot be authenticated.

FOIAXpress system users: System users must enter their user ID and passwords (in the login screen) in order to be given access to the FOIAXpress system. If the user declines to provide this information, the system does not grant access. The user has no right or opportunity to decline to provide other usage data in the system (e.g., date, time of user session), which is generated and maintained automatically by the system itself.

Other individuals: The right or opportunity of individuals to provide information that is contained in responsive documents scanned into the FOIAXpress system depends on how the information was collected and whether applicable laws or other legal authorities give the individual a right or opportunity to decline to provide the information. In some cases, individuals will have the right to decline to provide information (e.g., voluntary requests), while in other cases, individuals have no such right (e.g., subpoenas), although they may have the legal right in those cases to challenge the request (e.g., by filing a motion to quash the subpoena).

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

FOIA/PA requesters: Requesters do not have a right to consent to whether the FTC places copies of their requests on the public record, which is mandatory under the Commission's rules. Requesters, however, can complete and submit a certification of identity to OGC staff in order to authorize other individuals (e.g., personal attorney) to act as their personal representative in order to access their request records and pursue the FOIA/PA requests on their behalf and to obtain copies of the agency records that have been requested.

FOIAXpress system users: These individuals do not have a right to consent to or otherwise determine how the agency uses the information collected by the system regarding their login, access, or usage of the system.

Other individuals: Individuals who have provided information in agency records that have been entered into the FOIAXpress system for disclosure to a FOIA/PA requester do not have rights to consent to such use. The FOIA and PA legally determine whether the FTC is required to disclose, or whether it may withhold, such records from a requester seeking access under those laws.

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

Individuals may file an access request under the PA or the FOIA, depending on how the information is maintained and retrieved. The PA provides a procedure for individuals to request their own information, if the agency maintains and retrieves that information by the individual's name or other personal identifier (e.g., Social Security number). The FTC's Privacy Act procedures are published at 16 C.F.R. 4.13, which may be viewed online at <http://ecfr.gpoaccess.gov/>. The request must be made in writing and, if mailed, it must be addressed as follows:

Privacy Act Request
Office of the General Counsel
Federal Trade Commission
600 Pennsylvania Avenue, NW.
Washington, DC 20580.

PA Requests may also be made electronically using the FTC's online FOIA request form, <https://www.ftc.gov/ftc/foia.htm>.

If information about an individual is not maintained and retrieved by his or her name, Social Security number, or other personal identifier, the individual's request must be made under the FOIA, rather than the Privacy Act. The procedures for making a FOIA request are similar to making a Privacy Act request, and are published at 16 C.F.R. 4.11, which can also be viewed online at <http://ecfr.gpoaccess.gov/>. Individuals who use the FTC's online FOIA request form to file a PA or FOIA request will also have their request treated as a FOIA request for any records that fall outside the PA.

Requesters should note that some records may be legally withheld from individuals for investigatory or other reasons under the FOIA and/or the PA. See Section 8 of this PIA for additional details.

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 FTC, as noted earlier, does not provide individuals with user access to their own records through FOIAXpress. Rather, the only way an individual can obtain records from the system is if OGC staff electronically retrieve those records from the system and provide them manually (electronically or on paper) to the requester. Thus, there are no privacy risks associated with allowing individuals themselves to obtain records from the system, since they are not allowed to do so.

5 Web Site Privacy Issues

FOIAXpress does not create or modify any FTC web site, page or online form. One of the sources of PII in the system is the existing FOIA online request form. However, the form itself is not part of the system and is not linked to the system. When a new FOIA

Requester submits the online form, that form is transmitted to an FTC e-mail account, FOIA@ftc.gov, that is accessible only to designated FOIA professionals. The transmission of the online FOIA request form (<https://www.ftc.gov/ftc/foia.htm>) is protected with Secure Socket Layer (“SSL”) encryption. For this particular web link, the connection is currently 3.0 SSL with 128-bit encryption.

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 to ensure that information in FOIAXpress is appropriately secured. FOIAXpress is a Minor Application that rides on the Infrastructure General Support System (GSS) which is categorized as a moderate using Federal Information Processing Standard (FIPS) 199.

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

FOIAXpress resides within the FTC Infrastructure General Support System (GSS), which has received a Certification and Accreditation (C&A). The FTC conducts a C&A for major information systems, including the General Support System underlying FOIAXpress, but not for FOIAXpress itself, which is a minor application.

6.3 Has a risk assessment been conducted on the system?

Not for FOIAXpress, but for the underlying GSS. See section 6.2 above.

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

No. See section 2.6 above.

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

Before access is granted to a new user, Standard Form 255 is filled out and signed by the FOIA/PA Program Director and submitted to Information and Technology Management. Once this form is completed, the software is loaded onto the user’s machine.

A FOIAXpress Supervisor creates an account for the user and assigns them to a group.

Each user group has different privileges, and the FOIAXpress system has the capability to grant privileges on a user level. Currently the program director, the lead paralegal, and the program assistant are the only users with administrative privileges. The FOIA user group, which contains all FOIA specialists, does not have administrative rights. Therefore they cannot engage in administrative processes such as creating user names, changing passwords, or changing the fee structure.

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

All FTC personnel, including those FOIA/PA Professionals who use FOIAXpress, are subject to FTC procedures for safeguarding sensitive PII. All FTC personnel receive annual computer-based privacy and security training, as well as other guidance explaining how to safeguard information. The interactive online training covers topics such as how to properly handle sensitive PII and other data, online threats, social engineering, and the physical security of documents. In addition, all FOIA/PA professionals are required to complete a Mandatory Compliance Checklist for sensitive PII and SHI to confirm that they are handling such information in accordance with agency procedures. Furthermore, persons at the FTC with significant security responsibilities are required to undergo additional, specialized training, tailored to their respective responsibilities.

The Commission's Privacy Steering Committee (PSC) has also conducted privacy training specifically for FOIA/PA professionals, and will continue to conduct such training for FOIA/PA professionals periodically.

In addition, each FOIA/PA professional also takes periodic training on FOIA and Privacy Act issues provided by approved outside sources (e.g., Department of Justice, Department of Agriculture Graduate School, American Society of Access Professionals).

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

Access to nonpublic system records is restricted to FTC personnel or contractors whose responsibilities require access. Nonpublic paper records are retained temporarily, maintained in lockable file cabinets or offices, and returned to the submitter or destroyed once the request is complete. Access to all electronic records within the Agency is controlled by "user ID" and password combination and other electronic access or network controls (e.g., firewalls). FOIAXpress users have an additional "user ID" and password protected entry point into the system. FOIAXpress also keeps information on the identity of system users (those with password protected access as explained in Section 2.2), including the specific access requests they worked on. We also have the capacity to employ additional audit trail procedures about system users as necessary. FTC buildings are guarded and monitored by security personnel, cameras, ID checks, and other physical security measures. These and other information and physical security

measures currently in place are subject to periodic reviews and audits by the Commission's Inspector General.

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

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?

Records are retained and disposed of in accordance with General Records Schedule 14, issued by the National Archives and Records Administration (NARA), and other applicable schedules approved or issued by NARA.

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

Records are to be electronically purged and destroyed when appropriate under the NARA disposition schedules.

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

In addition to the privacy and security controls discussed in Section 2.8, the agency limits the number of staff with access to the records and access is restricted to those individuals with current IDs and passwords. Destruction of records occurs within the application by authorized personnel and does not create any additional risk. In particular, system users cannot delete or alter user audit trails, which are accessible only to system administrator(s).

8 Privacy Act

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

Yes, data is be retrieved by personal identifiers, the type of which varies according to which part of the system is being searched.

Correspondence Log. Information about FOIA and PA requests in the Correspondence Log can be retrieved by name of requesting party and subject matter of request, which may be an individual's name. Such records can also be retrieved by address, phone number, fax number, and e-mail of the requesting party, and staff member assigned to the request.

File Cabinet/Document Management. The text of responsive records that were entered into the File Cabinet/Document Management portion of the system from FY2004-FY2007 can be searched through a full text search; including name, address, SSN, if any, and other identifiers. Documents scanned into Document Management after that time cannot be retrieved except by FOIA Number or the folder name designated by the FOIA Professional when the folder was created. (This full-text search feature cannot be used to search any other portion of the system.).

Review Log and Case Folder. Records within the Review Log and the Case Folder sections can only be retrieved by FOIA number, the name or other contact information of the specific Requester, and then by FOIA Professional and folder name. These are the same identifiers used to retrieve records within the Correspondence Log.

System Users. Information about System Users could also be accessed by the system administrator and retrieved by user name or other user identifier.

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

Records pertaining to FOIA/PA requesters are covered by:

V-1 -- Freedom of Information Act Requests and Appeals -- FTC, and V-2 -- Privacy Act Requests and Appeals -- FTC.

Records pertaining to FOIAXpress system users are covered by: VII-3 -- Computer Systems User Identification and Access Records -- FTC.

Records pertaining to individuals whose information may be retrieved from some documents that have been scanned into the system for release to requesters would be covered by I-1 -- Nonpublic Investigational and Other Nonpublic Legal Program

Records -- FTC, or other applicable FTC SORNs.

Copies of all FTC SORNs can be viewed and downloaded at:
<http://www.ftc.gov/foia/listofpaysystems.shtm>.

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.

Although FOIAXpress does not involve the operation of any Web site that would require a 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: _____

Joan E. Fina
Assistant General Counsel for Information
& Legal Support

_____ Date: _____

Richard Gold, Attorney
Office of the General Counsel

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: _____

Stanley Lowe
Chief Information Officer