Federal Trade Commission
Privacy Impact Assessment

for the

Collection of Public Comments Filed Electronically

November 2011

Introduction

Congress has empowered and directed the Federal Trade Commission (FTC or Commission) to prevent the use of unfair methods of competition, and unfair or deceptive acts or practices, in or affecting commerce, pursuant to the Federal Trade Commission Act, 15 U.S.C. §§ 41-58, *as amended*. Congress has also empowered and directed the Commission to prevent mergers, acquisitions, price discrimination, and certain other practices that may "substantially lessen competition" or "tend to create a monopoly," in violation of the Clayton Act, 15 U.S.C. §§ 12-27, *as amended.* In addition, Congress has directed the Commission to enforce or assist with implementing a large number of other statutes.[1]

As one important vehicle for executing its responsibilities under these statutes, the Commission conducts rulemaking proceedings, pursuant to both the notice and comment procedures established by Section 553 of the Administrative Procedure Act (APA), 5 U.S.C. § 553, and the procedures prescribed by Section 18 of the Federal Trade Commission Act, 15 U.S.C. § 57a. Comments from members of the public concerning proposed rules constitute an important source of information, and the Commission has therefore incorporated the solicitation and systematic consideration of such comments into those of its Rules of Practice which govern rulemaking proceedings.[2] Moreover, Section 553(c) of the APA, 5 U.S.C. § 553(c), expressly requires agencies to give "interested persons an opportunity to participate in the rule making through submission of written data, views, [and] arguments . . ." Similarly, Sections 18(b)(1)(B) and 18(e)(1)(B) of the FTC Act, 15 U.S.C. § 57a(b)(1)(B), (e)(1)(B), respectively require the Commission to "allow interested persons to submit written data, views, and arguments, and make all such submissions publicly available. . ." and define "any written submissions" as part of the rulemaking record. Commission Rule 4.9(b)(3)(iii) consequently provides that the public record of the Commission includes, *inter alia*, "written statements filed with or forwarded to the Commission in connection with [all rulemaking] proceedings."[3]

---

[1] The Commission has enforcement or administrative responsibilities under more than seventy laws. *See* the FTC Web site at the following location: http://www.ftc.gov/ogc/stats.shtm.

[2] The rules governing the solicitation of public comments in Trade Regulation Rule proceedings, pursuant to Section 18 of the FTC Act, are set forth in Subpart B of the Commission Rules of Practice at 16 C.F.R. §§ 1.10(b)(2), 1.11(a)(5), 1.13(a) (2011). The analogous requirements for rules promulgated under authority other than Section 18 of the FTC Act are set forth in Subpart C of the Commission Rules of Practice at 16 C.F.R. § 1.26(b)(4) (2011).

[3] 16 C.F.R. § 4.9(b)(3)(iii)(2011).

The Commission has also incorporated the solicitation and consideration of public comments into the Commission Rules of Practice governing administrative consent agreements;[4] applications for approval of proposed divestitures, acquisitions, or similar transactions subject to Commission review under outstanding orders;[5] and requests to reopen and modify Commission rules and orders.[6] In addition, the Commission solicits and considers public comments as part of its preparation of reports and its sponsorship of workshops and other types of public proceedings.

Sections 206(c) and 206(d) of the E-Government Act of 2002, 44 U.S.C. § 3501 note Sec. 206(c), (d), respectively require the Commission, to the extent practicable, to accept rulemaking comments electronically, and to establish an online system through which members of the public can access rulemaking comments submitted both electronically and in paper form. The Commission has determined to accept public comments in the other types of proceedings described above in the same way. Members of the public submit comments on a voluntary basis in all these types of Commission proceedings.

1 System Overview

The CommentWorks System is a web-based application that the FTC will use to collect and store comments from members of the public when it solicits and considers public comments in the proceedings described above. It is a commercially available off-the-shelf software application. The FTC Records and Filings Office (RFO), located within the Office of the Executive Director, utilizes this system on a subscription basis. The system is operated by a contractor on behalf of the FTC.

CommentWorks utilizes a web-based form for comment submission and the system stores the comments in a database that is both secure and readily accessible to members of FTC and contractor staff. Staff examine submissions for review and analysis and to separate home contact information for individuals submitting comments in their personal capacity, thereby greatly facilitating the placement of the remaining information in each comment on the FTC Web site (FTC.gov).

2 Information Collected and Stored within the System

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

---

[4] 16 C.F.R. §§ 2.34(c), (e), 3.25(f) (2011).

[5] 16 C.F.R. § 2.41(f)(2)(2011).

[6] 16 C.F.R. § 2.51(c)(2011).

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

Comments. The system permits each commenter to type in information he or she believes to be relevant to the proceeding, and also permits up to three files to be attached. In some matters and proceedings, the system may also collect additional relevant information as set forth in the request for public comment.

Metadata. In addition, the system collects additional information that is maintained and associated with each individual comment (i.e., "metadata"). This includes: "Title," "First Name," "Last Name," "Organization Name," "Mailing Address," "City," "State," "Postal Code," and "Country." Although the system has the ability to collect metadata for all of these fields, the only required fields for submission are name and state.

Review information. RFO and contractor staff will attach certain review information to each comment submission that is received. This information includes the classification (e.g., unique, duplicate, form letter, not germane) and other additional review data.

Administrative data. The system collects and stores administrative data, including a list of the FTC initiatives and the names, user names, and passwords for CommentWorks system users (RFO and contractor staff).

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?

Comments are submitted by the members of the public. In some instances, these comments are submitted directly to the system by the commenters via the web-based comment form; in others, RFO staff and their support contractors will scan and upload documents into the system when the documents have been submitted by another method (e.g., in paper form). Third party organizations also compile and submit comments on behalf of their members.

Metadata contained in the documents comes from the individuals to whom it pertains.

Review information is entered by RFO and contractor staff.

Administrative data is entered by RFO and contractor 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 Public Comments filed electronically is to facilitate the submissions and web posting of public comments as required by the Administrative Procedure Act, the E-Government Act of 2002, and Commission Rule 4.9(b), 16 C.F.R. 4.9(b).

Review information is used by FTC and contractor staff to determine which comments will get processed for posting to the public via the Web.

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?

See Section 2.2.

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

Commenters are responsible for submitting accurate information. Data is not checked for accuracy or timeliness.

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. The FTC has employed similar Windows-based technologies, including HTTPS/SSL, Microsoft SQL Server and .NET, to collect public comments via web-based forms since at least 2004. For discussion of how the use of the technology affects individuals' privacy, see Section 2.8 and 4.5.

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

The FTC Act, the FTC 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.shtm.

The Federal Information Security Management Act and other information security laws authorize the FTC to collect user 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 warning to users that the system is only intended to collect public comments, and that comments will become part of the public records of the Commission and will be posted on FTC.gov. As a matter of discretion, the FTC makes every effort to remove home contact information for individuals from the public comments it receives before placing those comments on the FTC Web site.

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).

To reduce the risk of alteration, comments submitted through the system are saved in their original format, separate from the working copies that are accessible to FTC and contractor staff in the database. Access to in-process documents in the system is granted only to FTC staff, contractors and subcontractors as authorized when required to fulfill their work assignments. For more information on who will have access to system data, see Sections 3.2 and 3.3.

3 Use and Access to Data in the System

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

Any information placed in the following data fields for submission – "Title," "First Name," "Last Name," "Organization Name," "State," "Comments," and "Attachment" – will be publicly available on FTC.gov, subject to the exception described in Section 4.3.

For any given electronic comment, the information provided will be used to help determine the course of action the Commission should pursue in the rulemaking proceeding or other proceeding or matter. The personal information provided by the commenter will facilitate assessments of the validity and significance of the comment, permit storing the comment alphabetically by last name, and permit the Commission or its staff or contractors to contact the commenter, should that become necessary.

FTC and contractor staff will have access to data contained in the electronic database for the purposes of maintaining the information filed for each comment and placing the data in those comments on the FTC Web site. As noted, the Commission makes every effort to remove home contact information for individuals submitting comments in their personal capacity, prior to posting their comments on the Web site. Access to the data is also necessary for the purpose of analyzing and evaluating the typed-in comment, any attachment, and any other information requested as relevant to the matter.

The General Counsel of the Commission may give federal and state agencies access to home contact information of individuals for law enforcement or other purposes, provided

that the agencies certify that they will maintain this information in confidence. The Commission does not expect that any other entities will have access to the individual home contact information in the system, except as may otherwise be required or authorized by federal law or regulation.

In that regard, the Commission cannot rule out possible requests for public disclosure of individual home contact information pursuant to the Freedom of Information Act (FOIA), 5 U.S.C. § 552. Under this Act and the agency's FOIA rules, the agency may be required to make such information publicly accessible unless it is determined that such disclosure would constitute a clearly unwarranted invasion of personal privacy within the meaning of FOIA Exemption 6, 5 U.S.C. § 552(b)(6), or some other exemption applies. The Commission has determined that all of the above uses or disclosures of the data are authorized and both relevant and necessary to the purposes for which the data are collected.

3.2 Which internal entities will have access to the information?

The Commission will serve as the official custodian and owner of electronic comments submitted through the electronic comments system.

Before the comments are publicly posted, authorized FTC staff will have access to nonpublic data or information for processing and review.

3.3 Which external entities will have access to the information?

Except for certain portions for which there is a legal basis to redact the information, the comments are legally considered public records in accordance with the agency's Rules of Practice, 16 C.F.R. § 4.9(b), and will be routinely shared with the public on FTC.gov.

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.

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. Whether to file a public comment electronically, by mail, or at all, is voluntary. If an individual does not want to provide information through the system, then, under the FTC Rules of Practice, they may file a comment 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. Comments containing material for which confidential treatment is requested must be filed in paper form, must be clearly labeled "Confidential," and must comply with FTC Rule 4.9(c).

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

All documents filed via the system (with the exception of duplicate submissions and documents that are not germane to any FTC proceeding) are posted to the publicly available FTC Web site and are available in the FTC's public reading room.

Individuals seeking access to other data, if any, that has been collected, generated, or maintained in the system about themselves and not publicly posted on the FTC's web site may file a written access request under the FOIA and/or Privacy Act. (Data may be withheld if they are exempt from mandatory disclosure under these laws.) For further information on making a request, please see the FOIA page on the FTC's web site.

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. As described earlier, we address this risk by permitting only authorized internal entities to have access to nonpublic records in the system (i.e., unredacted comments). See Section 3.2. Access by external entities, including individuals who wish to access their own records (i.e., comments), is limited to public copies posted on the FTC's Web site only after home contact information (except for name and state) has been removed. See Section 3.3.

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.

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

5.2 If a persistent tracking technology is used, ensure that the proper issues are addressed.

Not applicable.

5.3 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), using an appropriately validated encryption module.

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

The comment submission form contains a link to the FTC Privacy Policy.

5.5 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 comments for posting to the FTC's public Web site. 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.

5.6 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. In accordance with those statutory and regulatory requirements, if Commission or contractor staff secure actual knowledge from reading a particular comment that it was submitted by a child (i.e., a person under 13 years of age), all personal information contained in the comment will be purged from the system.

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?

Anyone with Internet access may access the web-based comment forms and submit a comment. Designated FTC and contractor staff with a valid user name and password can access the secure database to review, analyze, and process the comments for posting on FTC.gov. The RFO has procedures in place to grant access to FTC staff, and access is granted only if needed to perform official 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 RFO will receive specific training on CommentWorks.

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 low 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 low

risk system. The application's access controls include regular auditing and testing of the system.

6.8 To whom should questions regarding the security of the system be addressed?

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. Once NARA has approved the new schedule, information and data will be retained and destroyed in accordance with the new schedule. Pending NARA approval, the FTC will manage the data in a manner consistent with 44 U.S.C. §§ 3301-3324, 44 U.S.C. § 3506, 36 C.F.R. Ch. XII, Subchapter B, Records Management and Office of Management and Budget (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 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.

See Section 2.8 for information regarding privacy risks identified in the data retention, 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?

Information submitted by the public is not retrievable by a personal identifier. FTC and contractor staff can access information contained in the database with 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 comments are covered by FTC I-6 (Public Records – FTC). Nonpublic system

data (i.e., undredacted comments) are covered by FTC I-1 (Nonpublic Investigational and Other Nonpublic Legal Program Records – FTC). Administrative system data (user IDs or other system login credentials) are covered by FTC VII-3 (Computer Systems User Identification and Access Records – FTC). These SORNs may be viewed and downloaded on the FTC's SORN page.

In compliance with the Act, the Web-based form used to collect the information will contain the required notice of authority, purpose, routine uses, and whether the collection is voluntary or mandatory and the consequences, if any, of not providing the information.

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 the system have been reviewed to ensure consistency with the FTC's privacy policy posted on the FTC Web site (http://ftc.gov/ftc/privacy.shtm).

10 Approval and Signature Page

Prepared for the Business Owners of the System by:

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

Review:

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

_____ Date: _____
Marc Groman
Chief Privacy Officer

_____ Date:_____
Jeffrey Smith
Information Assurance Manager

Approved:

_____ Date:_____
Jeff Huskey
Chief Information Officer