Federal Trade Commission
Privacy Impact Assessment

Collection of Public Comments Filed Electronically (CommentWorks)

Updated April 2018

Table of Contents

1 System Overview

1.1 Describe the project/system and its purpose.

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]

The CommentWorks system is a web-based application that the FTC uses 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 Information Management (RIM) office, located within the Office of the Chief Administrative Services Office (CASO), utilizes this system on a subscription basis. The FTC has contracted with a third party company, ICF Technologies, to operate the CommentWorks system 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 accessible to members of FTC and ICF staff. Staff examine submissions for review and analysis, as well as to separate home contact information for individuals submitting comments in their personal capacity, and determine if the comments are germane to the FTC-announced initiatives. ICF conducts the PII redaction prior to submission to the

[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).

FTC for posting, thereby greatly facilitating the placement of the remaining information in each comment on the FTC website (www.ftc.gov).

1.2 What specific legal authority allows for the collection, maintenance, or dissemination of information for this project/system?

The FTC Act, the FTC Rules of Practice, and other laws and regulations that the Commission enforces or administers (see section 2.3 below) permit the collection of the information. For more information, see www.ftc.gov/ogc/stats.shtm.

The Federal Information Security Modernization Act (FISMA) and other information security laws authorize the FTC to collect user data for IT security purposes.

2 Data Type, Sources, and Use

2.1 Specify in the table below what types of personally identifiable information (PII)[4] may be collected or maintained in the system/project. Check all that apply.

PII Elements: This is not intended to be an exhaustive list. Specify other categories of PII as needed.

☒ Full Name	☐ Biometric Identifiers (e.g., fingerprint, voiceprint)	☒ User ID
☒ Date of Birth	☐ Audio Recordings	☒ Internet Cookie Containing PII
☒ Home Address	☒ Photographic Identifiers (e.g., image, x-ray, video)	☒ Employment Status, History, or Information
☒ Phone Number(s)	☒ Certificates (e.g., birth, death, marriage, etc.)	☒ Employee Identification Number (EIN)
☒ Place of Birth	☒ Legal Documents, Records, Notes (e.g., divorce decree, criminal records, etc.)	☒ Salary
☒ Age	☒ Vehicle Identifiers (e.g., license plates)	☒ Military Status/Records/ ID Number
☒ Race/ethnicity	☒ Financial Information (e.g., account number, PINs, passwords, credit report, etc.)	☒ IP/MAC Address
☒ Alias	☒ Geolocation Information	☐ Investigation Report or Database
☒ Sex	☒ Passport Number	☒ Driver's License/State ID Number (or foreign country equivalent)
☒ Email Address		☒ Other *(Please Specify)*: See Below
☒ Work Address		
☒ Taxpayer ID		
☒ Credit Card Number		
☒ Facsimile Number		
☒ Medical Information		
☒ Education Records		
☒ Social Security Number		
☒ Mother's Maiden Name		

Submitters are explicitly advised not to submit additional PII on the comment form; however, individuals may still choose to include a variety of PII elements in their comments, including many of the PII elements listed above. Though reasonable measures are taken to redact the PII prior to

[4] Per OMB Circular A-130, personally identifiable information (PII) means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

posting, the CommentWorks system maintains both the redacted and the unredacted versions of each public comment.

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

Metadata. The system collects information that is maintained and associated with each individual comment (i.e., "metadata"). This includes: "Title," "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 last name and state.

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 (RIMRIM and contractor staff).

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

2.2 What types of information other than PII will be collected, disseminated, or maintained by the project/system? Provide a general description below and be sure to include all data elements.

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.

Review information. RIM 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.

2.3 What is the purpose for collection of the information listed above?

The purpose of CommentWorks 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). 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 review information 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 maintained for system security and maintenance purposes.

2.4 What are the sources of the information in the system/project? How is the information collected?

Source of Data	*Type of Data Provided & How It Is Collected*
Individual Members of the Public	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 FTC web-based comment form; in others, RIM 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. Typically, only the commenter's last name and state are posted publicly on FTC.gov. However, any information placed in the following data fields for submission – "Title," "First Name," "Organization Name," "Comments," and "Attachment" will be collected and maintained in the CommentWorks system.
RIM and CommentWorks Staff	Review information and administrative data is entered by RIM and ICF staff.
CommentWorks System	Log data is generated and maintained automatically by the system.

3 Data Access and Sharing

3.1 In the table below, specify the systems/applications and groups (both FTC and non-FTC) that will have access to or share data in the system/project.

Data Will Be Accessed By and/or Provided To:	*How and Why the Data Will Be Accessed/Shared*
FTC staff and contractors	The Commission will serve as the official custodian and owner of electronic comments submitted through the electronic comments system. RIM and ICF staff will have access to data contained in the electronic database for the purposes of maintaining the information filed for each comment and posting the data in those comments on the FTC Web site. Before the comments are publicly posted, authorized FTC staff will have access to nonpublic data or information for processing and review. 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 website. 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.
ICF Staff	The CommentWorks system is maintained and operated on behalf of the FTC by a contractor (ICF). 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.

Data Will Be Accessed By and/or Provided To:	*How and Why the Data Will Be Accessed/Shared*
Members of the Public	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.
Other External Parties	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.

3.2 Do contractors and/or third party service providers have access to data in the project/system? If yes, explain what privacy requirements are in place to ensure that data is properly protected.

Yes, FTC contractors who support RIM staff have access to the CommentWorks system as authorized when required to fulfill their work assignments. All FTC contractors are required to complete the FTC's IT security and privacy training before obtaining access to the FTC network and systems.

The CommentWorks system is maintained and operated by ICF on behalf of the FTC. ICF system administrators have 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. Additionally, a limited number of authorized ICF personnel have access to data in the system for the purpose of assisting the FTC in processing comments received and posting them to the FTC's website. As part of ICF's mandatory annual security training, all ICF staff are required to complete data privacy training that emphasizes the importance of safeguarding personal data handled or maintained by ICF staff in the course of supporting its clients.

3.3 If you answered "yes" to 3.2, describe the privacy incident response plan maintained by the contractor's organization or third party service provider.

ICF maintains incident response procedures that are implemented by its Corporate IT Information Security (CIT InfoSec) Team. These procedures are applied to incidents arising with ICF-owned systems as well as customer-hosted systems that do not have their own specified incident response protocols. The FTC systems hosted by ICF are subject to government-wide policies regarding

breach notification and planning; as such, ICF has prepared an FTC-specific set of incident response procedures that apply to the CommentWorks system regarding notification timelines, a reporting matrix, roles and responsibilities, emergency communication procedures and up-to-date contact information.

4 Notice and Consent

4.1 How are individuals provided with notice prior to the collection of their PII? If notice is not provided, explain why.

☒ Notice is provided via (*check all that apply*):
- ☒ Privacy Act Statement (☒ Written ☐ Oral)
- ☒ FTC Website Privacy Policy
- ☐ Privacy Notice (e.g., on Social Media platforms)
- ☐ Login banner
- ☐ Other (*explain*):

☐ Notice is not provided (explain): _____

The system utilizes the FTC's public comment filing web form to request information from the user and provide notice about what information is collected, and how it is used and disclosed. The comment submission form contains a link to the FTC Privacy Policy.

4.2 Do individuals have the opportunity to decline to provide information or to consent to particular uses of their information (other than required or authorized uses)?

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.

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).

4.3 Are there procedures in place to allow individuals access to their personally identifiable information? Explain.

All comments and documents filed and posted electronically (with the exception of duplicate submissions and documents that are not germane to any FTC proceeding) are publicly available on the FTC website, as provided under Commission Rule 4.9(b).

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.) The rules and procedures for making these requests are published in the Code of Federal Regulations, 16 C.F.R. 4.13, and on the FTC's website.

4.4 Are there procedures in place to allow individuals the ability to correct inaccurate or erroneous information? What is the process for receiving and responding to complaints, concerns, or questions from individuals? Explain.

Yes. As specified above in Section 4.3, the FTC provides a process for individuals to obtain access to their records under FOIA and the Privacy Act, and, to the extent permitted under the Privacy Act, to correct or amend any inaccurate PII maintained by the Agency.[5] The FTC's privacy policy provides links to the FTC's Privacy Act system of records notices (SORNs), see section 8.3 below, which also include information about how to correct or amend records. . Additionally, individuals may contact the FTC with any complaints, questions or concerns via phone or email available on www.ftc.gov or contact the Chief Privacy Officer directly. Where appropriate, the FTC disseminates corrected or amended PII to other authorized users of that PII, such as external information sharing partners.

5 Data Accuracy and Security

5.1 Are there procedures in place to ensure that the information maintained is accurate, complete, and up-to-date?

FTC contractors and ICF staff do not check the accuracy or integrity of the information submitted by an individual commenting on a specific matter, and would not be authorized to modify or alter the content of an individual's comment. Instead, FTC and ICF staff may review the comment to ensure it does not contain any confidential or sensitive personal information, but they do not attempt to verify the information for accuracy or timeliness. Commenters are solely responsible for the contents of their comments and for ensuring that the information they provide is accurate and current when filing a comment with the FTC.

5.2 Are there administrative procedures and technical safeguards in place to protect the data in the system/project? What controls are in place to ensure proper use of the data? Please specify.

Yes. The system is intended to collect comments for posting to the FTC's public website, so those comments do not generally require safeguards to protect their confidentiality. However, because the system may collect some information in identifiable form (e.g., e-mail or specific postal address) that is normally redacted and not disclosed on the public record, the system has access restrictions and other security measures (e.g., encryption both in transit and at rest) to protect all system data. Likewise, safeguards are in place to ensure the integrity and availability of system data (e.g., publicly posted comments) from unauthorized modification or deletion.

Anyone with Internet access may access the web-based comment forms and submit a comment, which is collected using secure Web transfer protocols (see section 7.1 below). Designated FTC and contractor staff with valid user names and passwords can access the secure database to review, analyze, and process the comments for posting on FTC.gov. RIM has procedures in place to grant access to FTC staff, and access is granted only if needed to perform official work.

[5] See 16 C.F.R. 4.11(a) (FTC FOIA rules), 4.13(m) (FTC Privacy Act rules).

The system has been assessed according to Federal Information Processing Standards (FIPS) security categorization and the National Institute of Standards and Technology (NIST) Security Control guidance. It has been designed to prevent unauthorized access to the data contained in the system, including unauthorized access by administrators and developers. The system has undergone a security assessment process to validate the integrity of the access controls. The application's access controls include regular auditing and testing of the system.

5.3 Has the system/project undergone the appropriate security risk assessment and received authority to operate?

Yes. A security risk assessment has been conducted on the system, and the system has received authority to operate.

5.4 Is PII used in the course of system testing, training, or research? If so, what steps are taken to minimize and protect PII during this process?

Yes, PII may be used in the course of system testing, training, or research. Only authorized FTC staff or contractor staff with valid system user accounts to the electronic database have access to unredacted comments (i.e., comment entries that may contain PII) during testing, training, or research. These authorized users are trained within the system with close supervision and must also undergo the annual FTC privacy and security awareness training.

6 Data Retention and Disposal

6.1 Specify the period of time that data is retained in the system/project. What are the specific procedures for disposing of the data at the end of the retention period?

Redacted public comments incorporated or used in the course of FTC initiatives are retained with the related initiative case files. The initiative case files are managed in accordance with the National Archives and Records Administration (NARA) approved FTC records disposition schedule, N1-122-09-1, Schedule 2, Mission Records. The data in the CommentWorks system and the comments posted to FTC.gov are managed in accordance with NARA General Records Schedule (GRS) 5.2, item 020, Intermediary Records.

All data will be deleted/destroyed in accordance with OMB, NARA, and NIST regulations and guidelines.

7 Website Privacy Evaluation

7.1 Does the project/system employ the use of a website? If so, describe any tracking technology used by the website and whether the technology is persistent or temporary (e.g., session cookie, persistent cookie, web beacon). Describe the purpose of using such tracking technology.

Yes, the CommentWorks system employs the use of a website. The system uses a session cookie to collect 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. Data transmission via the Internet is encrypted via a secure connection (HTTPS/SSL), using an appropriately validated encryption module.

8 Privacy Risks and Evaluation

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

Risk	*Mitigation Strategy*
Public documents filed via CommentWorks and placed on FTC.gov may contain sensitive personal information (e.g., Social Security Numbers)	The risk that comments or 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 individuals' personal information from the public comments it receives before placing those comments on the FTC Web site.
Information in the system may be viewed and altered by unauthorized parties	This risk is mitigated in several ways. The system utilizes encryption technology, both in the transmission of data across the Internet (HTTPS/SSL) and at rest. 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. FTC staff (including RIM staff) do not have the ability to alter comments in the system. ICF staff redact PII before submitting the comments to FTC for posting.

8.2 Does the project/system employ the use of automated privacy controls or enhanced capabilities designed to support privacy? Explain.

Authorized FTC and ICF staff with valid user names and passwords can access the secure database to review, analyze, and process the comments for posting on FTC.gov. Users are automatically logged off the system after some period of inactivity, and user accounts are locked after three incorrect attempts to login. The number of authorized user accounts granted to FTC staff is limited by the RIM office in compliance with contract and cost management guidelines.

8.3 Has a Privacy Act System of Records Notice (SORN) been published in the Federal Register for this system/project? If so, list the applicable SORN(s).

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 contains 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.

8.4 How does the project/system ensure that the information is collected, used, stored, or disseminated in accordance with stated practices in this PIA?

The FTC and its contractors follow applicable FTC policies and procedures to ensure that all information maintained by or on behalf of the agency is collected only for official purposes and secured appropriately. The collection, use, and disclosure of information in the system have been reviewed to ensure consistency with the FTC's privacy policy.

9 Approval and Signature Page

Prepared By:

_____ **Date: _____**
Jack Gabriel
Customer and Project Management Office

Reviewed By:

_____ **Date: _____**
John Krebs
Acting Chief Privacy Officer (CPO)

_____ **Date: _____**
Alexander C. Tang, Attorney
Office of the General Counsel (OGC)

_____ **Date: _____**
Jaime Vargas
Chief Information Security Officer (CISO)

_____ **Date: _____**
Yvonne K. Wilson
Records and Information Management Office (RIM)

Approved By:

_____ **Date: _____**
Raghav Vajjhala
Chief Information Officer (CIO)