Federal Trade Commission
Privacy Impact Assessment

FTC Public Websites

October 2016

Table of Contents

1 System Overview

1.1 Describe the project/system and its purpose.

The Federal Trade Commission (FTC) relies on multiple public web properties to:

- Inform and engage the public about its mission, activities and cases
- Provide resources to consumers and businesses
- Enable consumers to file complaints and take other actions
- Enable the public to comment on actions and submit FOIA requests
- Enable businesses and practitioners to file required documents electronically

The primary agency website, FTC.gov, is essentially an informational website. It is the main point of entry for access to other FTC public web properties and is the central resource for the agency's public information. Content is stored in and managed with the Drupal content management system by FTC staff. This PIA is for the FTC's informational website and sub-sites.

The agency also has a variety of transactional websites that enable the public to perform tasks such as file complaints and submit phone numbers to the do not call list. Most of these sites are managed by different contractors under the direction of FTC staff and are hosted in environments separate from the FTC's informational website. These sites, most of which gather sensitive PII, have their own PIAs.

FTC PUBLIC WEBSITES WITH THEIR OWN PIAS			
Site Name	**Address**	**Purpose**	**PIA Link**
Admongo	admongo.gov	Game teaches children about advertising	Admongo.gov PIA
Complaint Assistant	ftccomplaintassistant.gov	Consumers submit fraud complaints for investigation.	Sentinel Network Services PIA
Consumer Sentinel	consumersentinel.gov	Law enforcement access to consumer complaint data	
National Do Not Call Registry	donotcall.gov	Consumers submit phone numbers to registry	
Identity Theft	identitytheft.gov	Public submits identity theft complaints	
Econsumer Complaint Assistant	econsumer.gov	Consumers submit complaints that cross international borders	
E-filing	ftcefile.gov	Attorneys submit documents for cases before FTC	E-Filing System PIA
FOIA Request Form	foia.ftc.gov/ftc/foia.htm	Public submits requests via online form	FOIAXpress System PIA

Public Comments	ftcpublic.commentworks.com	Public submits comments regarding matters before FTC	Collection of Public Comments Filed Electronically PIA
Publication Bulk Order	bulkorder.ftc.gov	Public can order free publications	Bulk Order PIA
Registered Identification Number (RN) Database	rn.ftc.gov/pls/textilern	Textile manufacturers can request an ID number	Textile RN PIA (forthcoming)

The FTC also relies on social media and other third-party digital tools and platforms to execute its communications and outreach. These tools also have their own PIAs.

SOCIAL MEDIA/THIRD PARTY DIGITAL TOOLS WITH PIAS			
Name	**Address**	**Purpose**	**PIA Link**
Facebook	facebook.com/federaltradecommission	Outreach and engagement via social media	Facebook PIA
Google Analytics	digitalgov.gov/services/dap/	Website traffic measurement	Google Analytics PIA
Gov Delivery	public.govdelivery.com/accounts/USFTC/subscriber/new?preferences=true	Outreach and engagement via email	GovDelivery Communications Management System PIA
LinkedIn	linkedin.com/company/federal-trade-commission	Outreach and recruiting via social media	LinkedIn PIA
Reddit	reddit.com	Outreach and engagement via social media	Reddit PIA
Skype	skype.com	Outreach via video conferencing	Skype PIA
Twitter	twitter.com/FTC	Outreach and engagement via social media	Twitter PIA
Video Hosting	ftc.gov/news-events/audio-video	Outreach and engagement via video (live and on-demand)	Video Hosting PIA
Web Customer Satisfaction Survey	foresee.com	Customer satisfaction survey for websites	Web Customer Satisfaction Survey PIA

YouTube	youtube.com/user/FTCvideos	Consumer and business education and public outreach via video	YouTube PIA

The FTC informational website has a variety of content types. Examples of typical content includes legal documents (usually in PDF form) such as case files and rules, as well as policies, press releases, speeches and testimony, articles, video, RSS feeds, datasets, audio and game files, tutorials, educational materials, live webcasts of workshops and press events, and blogs. The public may submit comments to the blogs, but the comments are moderated by FTC staff before posting. Members of the public also may subscribe to a variety of email newsletters and alerts via the GovDelivery system. GovDelivery is a web-based system that manages email subscriptions and delivers emails for various FTC newsletters, blogs, press releases, and other communications, such as email alerts, to subscribers. See GovDelivery Communications Management System PIA.

The informational site is comprised of sub-sites with a variety of functions, audiences and owners. Some of these sub-sites are translated into Spanish. All the sub-sites listed below are covered by this PIA. Each site's content is managed by the relevant FTC Owner.

FTC INFORMATIONAL WEBSITES COVERED UNDER THIS PIA			
Site Name	**Address**	**Purpose**	**FTC Owner**
Agency Website	ftc.gov	Agency information and gateway to other FTC websites (informational and transactional)	Office of Public Affairs. Bureaus and Offices contribute their own content.
Agency Website in Spanish	ftc.gov/es	Agency information and gateway to other FTC websites in Spanish (informational and transactional)	Office of Public Affairs and Division of Consumer and Business Education
Business Center	ftc.gov/tips-advice/business-center	Guidance for business on how to comply with law, rules, and best practices	Division of Consumer and Business Education
Consumer Center	consumer.ftc.gov	Advice, tips and resources for consumers regarding their rights, fraud and other issues	Division of Consumer and Business Education
Consumer Center in Spanish	consumidor.ftc.gov	Advice, tips and resources for consumers regarding their rights, fraud and other issues in Spanish	Division of Consumer and Business Education

Consumer.gov	consumer.gov	Advice, tips and resources for consumers with literacy challenges	Division of Consumer and Business Education
Consumidor.gov	consumidor.gov	Advice, tips and resources for consumers with literacy challenges in Spanish	Division of Consumer and Business Education
National Consumer Protection Week	ncpw.gov	Consumer topics and materials	Division of Consumer and Business Education and non-agency partners
Military Consumer	militaryconsumer.gov	Tips, advice and materials for members of the military	Division of Consumer and Business Education

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

The FTC is authorized to disseminate government information and data online by the E-Government Act of 2002, Section 207 and the Digital Government Strategy (May 2012).

The FTC is authorized to disseminate information to consumers in Spanish on its websites by Executive Order 13166, Improving Access to Services for People with Limited English Proficiency (August 2000).

The FTC is authorized to enable the public to publish comments on its website's blogs by the Office of Management and Budget Memorandum on Social Media, Web-Based Interactive Technologies, and the Paperwork Reduction Act (April 2010).

The FTC is authorized to use Google Analytics to collect aggregated, anonymous data about website visitor behavior by the Office of Management and Budget Memorandum OMB M-10-22, Guidance for the Online Use of Web Measurement and Customization Technologies (June 2010) and Executive Order 13571 – Streamlining Service Delivery and Improving Customer Service (2011).

2 Data Type, Sources, and Use

2.1 Specify in the table below what types of personally identifiable information (PII)[1] 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)*:_____
☒ Work Address		
☐ Taxpayer ID		
☐ Credit Card Number		
☐ Facsimile Number		
☐ Medical Information		
☐ Education Records		
☐ Social Security Number		
☐ Mother's Maiden Name		

The other types of PII collection include the following:

- Blog Comments: A member of the public who submits a comment to a blog on an FTC website will publish their comment and a self-selected username. The blog commenting policy advises users who choose to comment not to include personal information in their comments. If they do so, the FTC staffer moderating the blog can remove this information before publishing the comment or can opt not to publish it.

- Emails: The FTC publishes a variety of email addresses, e.g. webmaster@FTC.gov on its websites for the purposes of allowing the public to provide comments and make requests. These emails are received and stored in the FTC's email system for 45 days. They are forwarded to the appropriate Bureau or Office for response.

- IP Addresses: The web servers routinely capture in log files session information from computers and devices that visit FTC websites. This includes IP addresses, date, time, duration of session, referrer, entry and exit pages, browser, and operating system. The purpose of this data collection is to enable technical and security staff to analyze the performance and security of these systems. This information is routinely deleted after six months.

[1] Per OMB M-07-16, personally identifiable information (PII) refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date or place of birth, mother's maiden name, etc.

- Event Registration: In support of its general law enforcement, rulemaking, and community education and outreach programs, the FTC conducts workshops, seminars, and events. The FTC webpages for these events sometimes include an FTC e-mail address for individuals who wish to register voluntarily in advance of the event. Individuals are asked to provide only basic information, such as name, e-mail, and telephone number. See Data Center GSS PIA.

- Community Engagement Projects: In support of its education and outreach programs, the FTC occasionally invites the public to submit stories, comments, or other feedback that may be shared in whole or in part with other members of the public. For these projects, the FTC creates webpages with submission and content instructions, which include a Privacy Act statement and a link to the FTC's Privacy Policy. Individuals who choose to participate may be asked to provide basic information, such as name and e-mail address, along with their submission. This PII is used by the organizers to identify and process submissions, and, if necessary, to follow up with submitters.

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 FTC publishes a huge range of content in connection with its mission, activities, and outreach. The following items could contain PII.

- Public Comments: Comments that have been submitted to the FTC are published on the FTC website. Each comment identifies the individual who submitted the comment, their organization (if any) and their state. Comments are retained in an archive on the site.

- Staff Biographies and Testimonials: Biographies, including photos, are published on the website for the Commissioners, senior staff, and other agency staff. Video and text testimonials from FTC staff about working at the FTC are also published on the website. See Video Hosting PIA.

- Workshop and Event Videos: FTC archives its live webcasts. Workshops feature FTC staff and the public (as speakers/presenters) so these participants are identifiable in the videos. See Video Hosting PIA.

- Case Studies: Some consumer stories are used as case studies to educate others about the dangers of certain scams or fraud. These individuals are sometimes named and are featured in videos that are available on the web.

- Case Proceedings: The FTC sometimes takes actions against individuals, who are named in case materials, including press releases, that are published on the web.

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

See Section 2.2.

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	A member of the public who submits a comment to a blog on an FTC website will publish their comment and a self-selected username. The submission is reviewed by an FTC staff moderating the blog before publishing. The blog commenting policy advises users who choose to comment not to include personal information in their comments. If they do so, the FTC staffer moderating the blog can remove this information before publishing the comment or can opt not to publish it.
Individual members of the public	The FTC conducts workshops, seminars, and events in support of its law enforcement, rulemaking, and community education and outreach programs. The FTC webpages for these events may include an FTC email address for individuals who wish to register voluntarily in advance of the event. Individuals are asked to provide only basic information, such as name, email, and telephone number.
Individual members of the public	Individuals who choose to participate in a community engagement project in support of FTC education and outreach programs may be asked to provide basic information, such as name and email address, along with their stories, comments, or other feedback. This PII is used by the organizers to identify and process submissions and, if necessary, to follow up with submitters.
Individual members of the public	The FTC publishes a variety of email addresses, e.g. webmaster@FTC.gov, on its websites for the purposes of allowing the public to provide comments and make requests. These emails are received and stored in the FTC's email system for 30 days. They are forwarded to the appropriate Bureau or Office for response.
Computers or devices used by individual members of the public	The web servers routinely capture in log files session information from computers and devices that visit FTC websites. This includes IP addresses, date, time, duration of session, referrer, entry and exit pages, browser, and operating system. The purpose of this data collection is to enable technical and security staff to analyze the performance and security of these systems.
FTC Personnel	FTC administrator login credentials are submitted by staff who post blog entries, moderate blog comments, or manage website content.

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	Blog Comments: FTC staff will view the original submission from the public and determine whether the post should be published. A limited number of FTC administrators will have authorization to post blog entries, moderate blog comments, or manage website content. Emails: FTC staff will review emails from the public to provide a response. A limited number of FTC staff will monitor the email accounts. IP Addresses: FTC staff will review web server log files to identify any performance issues or security risks.
CGI	IP Address: CGI provides web hosting services to the FTC. Its staff has access to the log files for the purposes of optimizing performance and identifying security risks.
Helpdesk Vendor	Emails: The Helpdesk staff has access to all Outlook email boxes so they are able to see public emails.

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.

☐ Not Applicable.

Yes. Contractors working on FTC systems and who have access to data undergo security clearances. Access to systems is tightly controlled and is provided after multiple FTC staff have reviewed the request and approved access. Contractors are required to complete the FTC's IT security and privacy training before obtaining access to the FTC network and systems.

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.

☐ Not Applicable.

CGI has implemented an incident response plan for its IaaS Cloud environment, which includes Preparation, Detection/Analysis, Containment Eradication and Recovery, and Post Incident Activity. Eradication steps are in place, which include account disabling, password change, patching, software/virus removal, and network perimeter enhancement. CGI's cloud also undergoes annual assessments and reviews for privacy and security risks.

4 Notice and Consent

As described in Section 1.1, the primary purpose of FTC.gov, and its associated sites, is to provide information to members of the public about the FTC's mission-related activities. The limited PII collected by ftc.gov generally is obtained directly from visitors to the site. Individuals may submit information voluntarily through blog comments or emails provided to the FTC for a variety of reasons. In addition, the FTC's web servers routinely capture IP address for security and site operations purposes, as described in Section 2.1 above. FTC websites that gather sensitive PII, or collect PII through other means – such as website forms – have separate PIAs and are therefore not covered by this document.

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*):___See below_____

Blogs: Blogs on FTC websites link to a Comment Policy that informs participants that all comments are reviewed before they are posted; that they can be edited to remove personal information or links to commercial websites; and that published comments are part of the public domain. See https://www.consumer.ftc.gov/comment-policy.

☐ Notice is not provided (explain): _____

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)?

Individuals have the option to provide blog comments or to send an email to the FTC. They cannot decline the automatic collection of technical information from their computer or device recorded in the web server's log files when individuals visit the FTC websites.

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

Individuals can view their blog posts and have copies of any email they send to the FTC in their email system's outbox.

Individuals who seek access to nonpublic records, if any, collected by the blog about themselves must submit such a request in writing to the FTC's Office of General Counsel, under the agency's Privacy Act access procedures.

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.

Individuals can contact the FTC about correcting a blog post comment or can post a new comment to correct the original post. Individuals can email the FTC as a follow-up.

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?

To ensure accuracy, completeness, and currency, users can see their comments once they are approved and posted, and can submit a follow-up comment to provide clarification. Likewise, for PII that is collected through the agency's Web site but not subject to public posting, individuals may always follow up with more accurate, complete and up-to-date information, if necessary. Accordingly, the FTC does not validate any PII that may be submitted through user comments.

All site visitors agree to the automatic collection of web log information, as described in the FTC privacy policy. Log data is used for website analytic purposes and is not verified for accuracy.

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.

Controls and safeguards are in place for protection of sensitive data. CGI, the FTC's web hosting vendor, implements two-factor authentication for administrators to the CGI cloud, which is FedRAMPed. Authorizations must be granted by management. Least privilege authorizations are also implemented providing only the necessary access rights to authorized users. CGI's Security Operations Center also performs 24x7 monitoring for detection of threats and potential risks. Secure destruction and disposal of data is implemented using data erasure, degaussing, and/or physical shredding. Encryption is in place using FIPS 140-2 AES-256. Transmissions of page requests are encrypted using HTTPS via TLS. Security controls are also reviewed and assessed on an annual basis and risk assessments are performed.

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

The system has undergone a risk assessment and an Authorization to Operate has been issued.

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?

☒ Not Applicable

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?

The current policy for blog posts and comments is to retain them on the website in the blog archive until the agency determines they are no longer required for public information or preservation purposes.

FTC emails that have not been saved to an email archive are deleted after 45 days. See Data Center GSS PIA.

CGI implements the Commvault tool which stores data in encrypted chunks with unique encryption keys. All backups use a FIPS-140-2 AES-256 encryption module/algorithm. Retention of data is maintained on servers for 90 days and on tape for 6 months. Dates and records are maintained for backup and disposal information. For disposal, data erasure using a three-pass data wipe is used. Degaussing also is available to demagnetize electronic storage media. Physical shredding methods are also implemented for physical media that must be destroyed.

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.

☐ Not Applicable

The FTC's websites, including FTC.gov and its blogs, participate in the General Service Administration's (GSA's) Federal Digital Analytics Program, which uses a Federal government-specific version of Google Analytics Premium to collect and analyze data from website visitors to help the FTC improve its websites, share FTC information more effectively, and create a more engaging experience for website visitors. For more information, please see the Google Analytics through GSA's Digital Analytics Program PIA, which describes the use of persistent cookies and explains how the program anonymizes information before it is stored to prevent the collection of PII.

In addition to the Digital Analytics Program, the FTC also uses temporary ("session") cookies on FTC microsites, blogs, and tools to track information such as user IDs and preferences while the user is on an FTC site. The session cookies provide a particular functionality and/or a more streamlined experience for the user. For more information about cookies and the information that the FTC collects when you visit an FTC site, see the FTC's Privacy Policy and Cookie Page.

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*
Sensitive personal information such as a Social Security number is submitted in blog post	All blog comments are reviewed by a moderator (an FTC staffer) before they are published to the website. If someone submits a post with sensitive information, the moderator deletes the information from the comment before publishing it.
Sensitive information such as a Social Security number is submitted in an email sent to the FTC.	Emails from the public are reviewed by FTC staff. Sensitive information is removed from the email before it is forwarded to anyone for action.
Unauthorized access to the content management system.	Only a small number of FTC employees have login credentials and password protected access to the content management system. Users are required to change their password every 60 days.

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

Yes. The content management system times out after 15 minutes of inactivity, so the FTC user has to log back in to proceed. The system performs logging for content revisions and custom logging when permissions are changed.

Individuals must complete a captcha before they can submit a blog comment for posting. This prevents online spammers from spamming the comment section.

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).

To the extent, if any, that information about an individual is retrieved by a personal identifier, the electronic collection and storage of public comments is covered by existing Privacy Act System of Records notices. The FTC's SORN for public records (I-6) covers those comments that will be posted publicly.

FOIA Requests form data are covered by FTC IV-1 (and Privacy Act request data, if any, by FTC IV-2).

Event Registration Data are covered by FTC VI-1 (Mailing and Contact Lists).

All of the FTC's SORNs are on the public SORN page.

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?

Blogs: Staff in the Division of Consumer and Business Education and in the Office of Public Affairs ensure that comments submitted by the public are reviewed before they are published and that policies and procedures are followed. Access restrictions permit only authorized staff (e.g. administrators, site builders, web content managers) to moderate, edit, and publish the comments.

Emails: Only authorized FTC staff have access to the email accounts used to receive and manage emails from the public.

Log Files: Only authorized contractors and FTC staff have access to webserver log files.

9 Approval and Signature Page

Prepared By:

_____ **Date:** _____
Christine Noonan Sturm
Website Manager

Reviewed By:

_____ **Date:** _____
Katherine Race Brin
Chief Privacy Officer (CPO)

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

_____ **Date:** _____
Jeffrey M. Smith
Chief Information Security Officer (CISO)

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

Approved By:

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