Federal Trade Commission

Privacy Impact Assessment

for:

DCBE Websites and Blogs – Consumer.ftc.gov, Consumidor.ftc.gov, OnGuardOnline, AlertaenLinea, Consumer.gov, Consumidor.gov and the BCP Business Center

December 2012

1 SYSTEM OVERVIEW

The Federal Trade Commission's Division of Consumer and Business Education (DCBE) developed the websites **Consumer.ftc.gov** and **consumidor.ftc.gov** to help consumers understand their rights in the marketplace and avoid frauds and scams; **OnGuardOnline** (OnGuardOnline.gov) and **AlertaenLínea** (AlertaenLínea.gov) to help consumers be on guard against internet fraud, secure their computers, and protect their personal information; **Consumer.gov** and **Consumidor.gov** to give consumers information in a simple and direct style; and the **BCP Business Center** (business.ftc.gov) to provide information to help companies comply with the law. The sites include: articles; downloadable video, audio and game files; tutorials; blogs; and RSS feeds. (No data is collected from users who download audio or video files or subscribe to an RSS feed.)

These sites and blogs were developed using the content management system (CMS) Drupal. The CMS enables authorized FTC staff to electronically administer (e.g., upload, revise, delete) the content of these sites (e.g., articles, video, blog comments). This Privacy Impact Assessment (PIA) is an analysis of how information is handled by the CMS: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. The sites and blogs are hosted on the FTC's Public WEB Hosting General Support System (GSS), which has been authorized to process at the moderate level using National Institute of Standards and Technology (NIST), Office of Management and Budget (OMB), and Department of Homeland Security (DHS) guidance.

In addition to viewing, downloading, and commenting, visitors to the CMS-managed sites can sign up for email alerts, through a commercial e-mail subscription service (GovDelivery) or share information from these sites with others using an application (app) (AddThis). AddThis is covered by this PIA, while GovDelivery is covered by its own Privacy Impact Assessment. See GovDelivery Communications Management System Privacy Impact Assessment.

Visitors to the sites can contact the FTC by clicking on a link to a generic FTC email address on a "Contact Us" or "Help for You" page.

2 INFORMATION COLLECTED AND STORED WITHIN THE SYSTEM

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

Blog users who submit a comment will provide their comment and a self-selected username. The blog commenting policy advises users who choose to comment to not include personal information in their comments.

The CMS collects usernames and passwords from FTC administrators who login to manage content.

The web hosting provider's servers collect the following information: IP address, date and time of visit, referrer, entry page, exit page, browser, and operating system.

Visitors who click on a link to email FTC staff will open an email in the users' own email client. Their email address and the content of the emails they send to the FTC are not stored on the site or server, but both are maintained and used within the FTC email system.

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

Users voluntarily submit comments to the blogs. Users may voluntarily email FTC by clicking on the email link.

FTC administrator login credentials are submitted by staff who post blog entries, moderate blog comments, or manage website content.

The web servers automatically collect log information from visitors to the sites as described in Section 2.1.

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

Blog comments (and email communications) allow FTC employees and our federal partners to interact with consumers, answer questions and share ideas, and help develop an online community that promotes online safety and security and fraud prevention.

A username is required to verify that a real person is submitting the comment. This reduces the amount of comment spam received.

FTC moderators' usernames and passwords are collected to ensure that only authorized staff are able to post blog entries, moderate blog comments, or manage website content.

Web log files are collected to analyze overall traffic to the sites and better serve visitors.

2.4 How is the information collected?

Users who want to leave a comment do so by using the online comment form available at the bottom of each blog post. Users do not register at the blog site and must complete the form each time they submit a comment.

Users who choose to email can do so by clicking on a link. FTC staff monitor the mailboxes and respond to emailed questions or comments.

FTC administrators' usernames and passwords are collected through a secure login screen.

Web log files are collected automatically.

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

Blog comments are not checked for accuracy or timeliness but will be reviewed by FTC moderators before they are posted. Any comments that are off-topic, contain personally identifiable information, include misinformation, use offensive language, or promote a commercial product or non-Federal website will not be posted. Users who discover errors in their comments after they are posted may contact FTC moderators and request that their comments be removed.

FTC administrator login credentials are verified by the CMS software. Administrators are required to change their password every 60 days.

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 Drupal content management system and AddThis share function both have been used in the BCP Business site (business.ftc.gov) since 2010. Consumer.ftc.gov, consumidor.ftc.gov, OnGuardOnline.gov and AlertaEnLinea.gov also use AddThis.

AddThis is an online sharing service. To share a link or information, visitors to the FTC site clicks on the AddThis icon. AddThis displays a menu of third-party sites or services that the user can select and use for sharing FTC content with others (e.g., Facebook, MySpace, LinkedIn, Twitter, etc.). After the user makes a selection, a new browser window will open up and the user will log into the selected site or service with his or her user name and password for that site or service. Once logged in, the FTC content that the user wants to share or save will be "pre-populated" (e.g., in a draft email message screen) on the selected site or service and the user can share or save the link there. After sharing or saving the FTC content, the new browser window will close, the user will exit the sharing site or service, and the user will go back to browsing the FTC's site.

If visitors choose to share FTC site content through the AddThis email functionality, the service(s) or site(s) they are using will require them to provide their email address and the email address(es) of the recipient(s), so the email can be delivered through those services or sites. They also will have the option to include a message to recipients, with the shared content. AddThis does not maintain, merge, or otherwise combine email addresses or messages with any non-personally identifiable information they may collect. The FTC does not have access to the log-in credentials, email addresses, or messages sent by site visitors who use AddThis to share FTC content. AddThis does not use this information to deliver targeted advertising in connection with any FTC website or blog.

AddThis provides the FTC with aggregate level data about how visitors use the service. These reports tell us:

- how many times our content is shared,
- what content is shared,
- what services are being used to share our content, and
- usage by country.

The General Services Administration negotiated an amendment to the AddThis terms of service applicable to U.S. government agencies. In accordance with these amended terms, , AddThis will not use cookies, web beacons, or other persistent tracking technology that could collect user information from the Business Center, OnGuard Online, and Alerta en Linea websites because they all reside on a .gov domain.

Though AddThis will not use cookies on the FTC's sites, the third-party services available through AddThis (e.g., Facebook, Twitter, MySpace, etc.) often use both session and persistent cookies. Site visitors who choose to share content through these third-party services may be providing such services or other non-government parties access to their personal information and may have cookies placed on their computers.

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

The FTC Act authorizes the FTC to prevent unfair and deceptive acts and practices in interstate commerce and, in furtherance of this mission, to gather, compile, and make information available in the public interest.

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

The privacy risks identified are the risk that users will include personally identifiable information (PII) about themselves or others in their comments and the risk that those without authorization will access the website content or blog comments.

The former risk is mitigated by posting the commenting policy near the comment form to remind users not to share PII. In addition, DCBE's internal guidelines require review of all comments before they are posted for public view, and comments with PII will not be posted. If there is any question about whether the individual intended to post contact information, the FTC administrator will contact the individual before posting the comment.

The risk of unauthorized access is mitigated by having only a small number of FTC employees with login credentials and password protected access to the CMS, and by requiring users to change their password every 60 days.

3 USE AND ACCESS TO DATA IN THE SYSTEM

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

Comments that are posted (and emails that are received) enhance DCBE's ability to have a dialogue with people interested in consumer protection news and tips. Comments also will allow communication between readers who choose to comment.

FTC administrators' usernames and passwords are collected to provide access to the CMS to post blog entries, moderate blog comments, or manage website content.

Web log files are collected to analyze overall traffic to the site and better serve visitors.

3.2 Which internal entities will have access to the information?

If user comments are approved by FTC moderators, they will be publicly viewable on the blog. A limited number of FTC staff will monitor the email accounts.

A limited number of FTC administrators selected by DCBE management will have access to the CMS to post blog entries, moderate blog comments, or manage website content.

A limited number of DCBE staff who provide internal reports on visits to DCBE-managed websites will have access to the web log information.

3.3 Which external entities will have access to the information?

A limited number of staff from Fleishman Hillard, a communications firm contracted by the FTC to help develop and maintain these websites and blogs, will have access to the database and the information stored there. All contract staff who have access to this information have signed a non-disclosure agreement.

4 NOTICE AND ACCESS FOR INDIVIDUALS

4.1 How will individuals be informed about what information is collected, and how is this information used and disclosed?

The blog links to the FTC's privacy policy and contains an appropriate Privacy Act statement on the blog comment form explaining the authority, purpose, and uses of the information collected by the blog. The commenting policy clearly informs users that the comments will be made public and that comments should not include personally identifiable information.

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

Posting a comment in response to an article is voluntary. A user who chooses to post a comment must provide a self-selected username. Sending an email to an FTC account also is voluntary.

All site visitors agree to the automatic collection of web log information, as described in the FTC privacy policy.

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

Users who choose to submit comments agree to make their comments public, subject to moderator approval.

All site visitors agree to the automatic collection of web log information, as described in the FTC privacy policy.

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

Users can see their comments once they are approved and posted to the blog. Users also can contact FTC site administrators by using the contact information on the site.

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.

4.5 Discuss the privacy risks associated with the process of providing individuals access to their own records and how those risks are mitigated.

There are no identifiable risks in providing individuals with access to their blog comments, since individuals are informed that their comments will be made publicly available

on the blog and will not be treated as confidential. The blogs are not configured to allow external users or other members of the public to gain access to any nonpublic information collected by the blog on individuals, and any requests by individuals for access to such information about themselves requires a formal written Privacy Act request, as noted in Section 4.4. See Section 6 for information regarding security measures.

5 WEB SITE PRIVACY ISSUES

5.1 Describe any tracking technology used by the Web site and whether the technology is persistent or temporary (e.g., session cookie, persistent cookie, Web beacon).

The sites use session cookies to enable visitors to post comments and to enable advanced features to load faster. OnGuardOnline.gov also uses session cookies in connection with an optional customer satisfaction survey.

The FTC administrator login screen uses a persistent cookie to encrypt and secure the information transmitted and to remember FTC administrators' passwords.

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

FTC administrators understand that the persistent cookies for administrators are implemented to make it easier for them to gain access to the CMS. The risk is minimal because persistent cookies will only be placed on the computers of a limited number of FTC administrators, with their knowledge. The risk that the login information stored by these cookies on the administrators' computers could be used by unauthorized individuals is minimal because their computers are also secured by other physical, administrative, and technical controls (e.g., password protection). The risk for site administrators will be additionally mitigated by encrypting all of their communications over the site, as described in 5.3.

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.

Encryption will not be used for the public facing website and blog. The information in the system is submitted voluntarily and is closely moderated before being made public. It therefore poses a low risk to privacy and encryption is not necessary. Other security controls have been put in place, however, to minimize the risk of unauthorized alteration or deletion. See Section 6.

The FTC administrator login page is encrypted using https or Secure Sockets Layer (SSL) technology. The only personal information that will be collected from this part of the website (not including the names of authors of articles and blog posts) will be the site administrator's username and password at login.

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

The websites and blogs include a link to the FTC's Privacy Policy in the footer and in other relevant places – when users are signing up for email updates or submitting blog comments. The blog comment form and email sign-up form also include a Privacy Act statement.

5.5 Considering any Web site or Internet issues, please describe any privacy risks identified and how they have been mitigated.

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 websites and blogs are not intended to collect any information from children under 13 years of age. If it becomes clear that a user under 13 has posted a comment, the FTC administrator will delete the post. The FTC does not ask the age of users who sign up to receive email updates. These email addresses are never made public. For more information on the FTC's email updates service, see the GovDelivery Communications Management System Privacy Impact Assessment.

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, ensuring that OnGuardOnline.gov AlertaenLinea, Consumer.gov, Consumidor.gov and business.ftc.gov are appropriately secured. These sites are hosted in the Public WEB Hosting General Support System (GSS), a data system that is categorized as "moderate" under Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems.

In addition, as mandated by *Office of Management and Budget (OMB) Memorandum M-08-23, Securing the Federal Government's Domain Name System (DNS) Infrastructure*, the FTC has deployed Domain Name System Security (DNSSEC). This provides cryptographic protections to DNS communication exchanges, removing threats of DNS-based attacks and improving integrity and authenticity of information processed over the Internet.

6.2 Has a Certification & Accreditation (security control assessment and authorization) been completed for the system or systems supporting the program?

These sites are maintained as part of the FTC's Public WEB Hosting General Support System (GSS), which has been authorized to process at the moderate level using National Institute of Standards and Technology (NIST), Office of Management and Budget (OMB), and Department of Homeland Security (DHS) guidance.

6.3 Has a risk assessment been conducted on the system?

A risk assessment was completed on the Public WEB Hosting General Support System (GSS) as part of the authorization. Appropriate security controls have been identified to minimize the risk associated with the system and such control have been implemented.

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

Yes, and the FTC has addressed risks and vulnerabilities as described elsewhere in this document. *See*, *e.g.*, Section 2.8.

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

Drupal Web Files: Only a small number of FTC contractors and staff have access to the Drupal install and other web files. These files are accessible via secure file transfer protocol (SFTP) and/or Secure Shell (SSH), with specific login credentials.

FTC contractors or staff will make any necessary updates to the website files through SFTP/SSH with a secure virtual private network (VPN) connection.

Therefore, in order to make changes to the web files, FTC contractors or staff need both the secure VPN login information, the SFTP, and optionally, the SSH login credentials for the Drupal site files.

Web Hosting: If a server-side change needs to be made, including taking the site down, a support ticket from the FTC's web hosting vendor is required. A small number of FTC staff and FTC contractors have credentials through the FTC's web hosting vendor which allow them to create and view support tickets. Support tickets also can be created by FTC's Office of the Chief Information Officer (OCIO) and the web hosting vendor.

When a support ticket is created, it has to pass through two tiers of approvers. The first-level approvers are OCIO operations staff or a DCBE assistant director, and the second-level approvers are the OCIO network security team. Support tickets are only created for server-side

issues and updates in the web hosting vendor's system and do not allow changes to the Drupal files themselves.

Posting and Publishing Content: A small number of FTC staff will have the ability to log into to the Drupal sites with a login and password.

These sites will be protected by limiting administrative access to the IP address ranges corresponding to the FTC and Fleishman Hillard (FH), and the entire backend will be secured via HTTPS. Future security developments may include use of a soft token module for log-in. Once logged in, authorized users will be able to create, modify, and delete content on the websites.

Authorizes users will have defined roles with access and control limited to the needs of their roles.

Each Drupal site will carry unique login credentials and user roles.

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

All FTC employees and designated contractor personnel are required to complete computer security training and privacy awareness training annually. 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.

Individuals with significant security responsibilities are required to undergo additional, specialized training, tailored to their respective responsibilities.

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

Auditing measures and technical safeguards are in place commensurate with the National Institute of Standards and Technology (NIST) Recommended Security Controls for Federal Information Systems and Organizations Moderate-Impact Baseline Special Publication (SP) 800-53, Rev. 3. These controls include but are not limited to:

- Authenticator/Password Management – Application and monitoring of initial distribution, composition, history, compromise, and change of default authenticators.
- Account Management – Application and monitoring of account establishment, activation, modification, disabling, removal (including unnecessary/defunct accounts) and review.
- Access Enforcement – Application and monitoring of access privileges.
- Least Privilege – Access to data is limited to data necessary for specific user to perform his/her specific function..

- Unsuccessful Login Attempts – System automatically locks administrator accounts when the maximum number of unsuccessful attempts is exceeded.
- Audit logs are reviewed for technical and administrative errors.

Privacy risks associated with unauthorized disclosure of information are mitigated through implementation of technical controls associated with need-to-know and least privilege, ensuring that users have no more privileges to data than required to affect their official duties. In addition, deterrent controls in the form of warning banners, rules of behavior, confidentiality agreements and auditing are in place. Procedures are in place to disable and delete user accounts at the end of use. Access to the server is password protected and access is granted on a very limited basis.

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) and NARA has approved a new comprehensive records retention schedule. The FTC will retain and dispose of data collected by the system, including blog comments and usernames, in accordance with the new schedule. Aggregate data about site visits will be kept indefinitely, but will not contain any personally identifiable information. Email that visitors to the sites send to FTC by clicking on the email link is generally deleted once FTC staff respond to the email.

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

All records and other information that includes inputs, outputs, system documentation, and system content will be disposed 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 regarding privacy risks identified in data retention and how those risks have been mitigated. The data will be disposed of in a manner that makes it impossible to recover.

8 PRIVACY ACT

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

No, unless a user chooses a user ID that is also a personal identifier within the meaning of the Privacy Act. The blogs are not indexed or otherwise configured to allow visitors or users to retrieve comments, usernames or other data by personal identifier.

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

To the extent, if any, that information is about an individual and retrieved by a personal identifier of such individual, the electronic collection and storage of public comments is covered by existing Privacy Act System of Records notices. System I-6 covers those comments that will be posted publicly and System VII-3 covers user ID and access records. System I-1 would cover any nonpublic emails collected and maintained by the agency in its program records if they are retrieved by name or other personal identifier. See http://www.ftc.gov/foia/listofpaysystems.shtm.

In compliance with the Privacy Act, blog comment forms used to collect the information will contain the required notice of authority, purpose, routine uses, and that the collection is voluntary (Privacy Act statement).

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 the information in this system has been reviewed to ensure consistency with the FTC privacy policy.

10. APPROVAL AND SIGNATURE PAGE

Prepared for the Business Owners of the System by:

_____ Date: _____
Nat C. Wood, Assistant Director
Division of Consumer and Business Education

Review:

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

_____ Date: _____
Peter Miller
Acting Chief Privacy Officer

_____ Date: _____
Jeffrey M. Smith
Information Assurance Manager

_____ Date: _____
Jeffrey Nakrin
Records and Filings Office

Approved:

_____ Date: _____
Jeffrey Huskey
Chief Information Officer