



**Federal Trade Commission  
Privacy Impact Assessment**

**for:**

**BCP Business Center Website and Blog**

**January 2011**

## **1 SYSTEM OVERVIEW**

The Federal Trade Commission's Division of Consumer and Business Education (DCBE) developed the [Business Center](http://business.ftc.gov) website (business.ftc.gov) to help businesses and organizations understand how to comply with consumer protection laws the FTC enforces. The site includes plain-language guidance publications; links to public information like FTC cases, reports, events and workshops; downloadable audio and video files with compliance tips; and RSS feeds. (No data is collected from users who download audio or video files or subscribe to an RSS feed.)

The Business Center website and [blog](http://business.ftc.gov/blog) (business.ftc.gov/blog) were developed using a content management system (CMS). Using a CMS provides benefits that lead to a better experience for site visitors and increased efficiency for DCBE web developers and other staff. Specifically, a CMS:

- allows us to present content dynamically,
- gives us more flexibility to feature new content,
- provides an enhanced search functionality for users, and
- lets non-technical staff from DCBE update content easily and regularly.

Using a CMS also allowed us to integrate additional functionality, like the Business Center blog. The blog allows us to communicate with readers in a more informal, conversational way and encourages dialogue between readers and the FTC. The blog features timely articles about complying with FTC law and information about upcoming FTC events, like workshops and roundtables. It allows moderated comments submitted through an online form. A prominent commenting policy states that we will not post comments that divulge personal information about an individual, are off-topic or include misinformation, use offensive language, or promote a commercial product or website. FTC blog moderator guidelines help staff determine which comments should be posted. Comments will not be made public until FTC administrators have reviewed and approved them.

Both the website and blog are hosted by a contractor on an external server that runs on a Linux platform. We chose a web hosting provider that supports a LAMP (Linux, Apache, MySQL, and PHP) architecture and meets our project needs.

The Business Center website and blog are publicly available.

## **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 user name. The blog commenting policy advises users not to share personal information.

The CMS collects user names 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.

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

The information in the blog is obtained from users who voluntarily submit a comment on the blog.

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

The web hosting provider's servers automatically collect log information from visitors to the site as described in Section 2.1.

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

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

FTC moderators' user names 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 site and better serve visitors.

## **2.4 How is the information collected?**

Users who want to leave a comment can do so through an online comment form that will be available at the bottom of each blog post. The form includes a link to our commenting policy, a Privacy Act statement, and fields for users to input a self-selected user name and their comment. Users do not register at the blog site and will complete the form each time they submit a comment. The blog does not use persistent cookies and will not remember user names.

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

Web log files are automatically collected by the web hosting provider's servers.

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

Blog comments will be reviewed by FTC moderators. Any comments that are off-topic or 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 their comments be removed.

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

DCBE staff download web log files from the web hosting providers' servers on a monthly basis and review their accuracy.

## **2.6 Is the system using technologies in ways that the FTC has not previously employed (e.g., monitoring software, Smart Cards, etc.)? If so, how does the use of this technology affect individuals' privacy?**

The website makes use of technology the FTC has not previously employed in that it incorporates AddThis, an online sharing service. To share a link or information, visitors to the Business Center may click on the AddThis icon. When they choose the site or service they want to use (e.g., Facebook, MySpace, LinkedIn, Twitter, etc.), a new browser window will open up and they will log in using their user name and password for the service or site selected. Once logged in, the content they choose to share or save will be "pre-populated" and they can share or save the link. After sharing the information, the new browser window will close and they will go back to browsing the Business Center.

If a visitor chooses to share Business Center content through the AddThis email functionality, they will provide their email address and the email address(es) of the recipient(s). They also will have the option to write a message to recipients. AddThis uses this personal information to send the email. It is not merged or otherwise combined with any non-personally identifiable information they collect. The FTC does not have access to log in credentials or email addresses provided by website visitors who use AddThis to share content. AddThis does not use this information to deliver targeted advertising in connection with the Business Center 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. Per this agreement, AddThis agrees not to use

cookies, web beacons, or other persistent tracking technology that could collect user information at the Business Center website because it resides on a .gov domain.

Though AddThis will not use cookies on the Business Center, 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 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 about themselves or others in their comments and the risk that those without authorization will access the website content or blog comments.

The former is mitigated through the commenting policy, as well as by DCBE's internal guidelines for posting comments so that those comments that contain 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. In addition, if a comment that contains, for example, a business email address or telephone number, is posted and the user later determines that this information should not have been posted, the [commenting policy](#) allows the moderators to remove 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 will enhance DCBE's ability to have a dialogue with readers who are interested in learning what laws apply to their business and what they must do to comply. They also will allow communication between readers who choose to comment.

FTC administrators' user names 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 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 hosting provider's web log information.

### **3.3 Which external entities will have access to the information?**

The web hosting provider will not have access to comments submitted for review or to user names and passwords of the FTC moderators. They will have access to the server's log information but will not access it routinely.

A limited number of staff from a communications firm contracted by DCBE to develop and maintain the Business Center website and blog will have access to information on the website and blog, including user comments. 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. If a user posts a comment, they are required to provide a self-selected user name.

All site visitors agree to the automatic collection of weblog 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 submit a comment are agreeing to make that comment public upon approval.

All site visitors agree to the automatic collection of weblog 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. If a commenter has included PII in the form of an email address or telephone number and later determines that the information should not have been included, the commenter can contact the FTC at the email address provided in the [commenting policy](#) to request that the comment be deleted from the blog.

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 blog is 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). Currently, persistent tracking technology is not approved for use by the FTC (see 5.2).**

The public website and blog are hosted through a web hosting provider on an external server that does not use persistent cookies or other persistent tracking technology. The site uses session cookies for certain functionality: to determine whether the visitor is a site administrator, to enable visitors to post comments, and to enable advanced features to load faster.

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.**

Neither the contractor nor the FTC will use persistent cookies or other persistent tracking technology (persistent cookies) for visitors. Visitors, therefore, do not need to be notified about this technology.

The persistent cookies for administrators will use the same technologies that were used for the NCPW 2010 website. FTC administrators understand that persistent cookies 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.

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 website and blog include a prominent link to the FTC's Privacy Policy in the top navigation bar, as dictated by FTC web best practices. The blog comment form includes 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 website and blog 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.

**6 SECURITY OF INFORMATION IN THE SYSTEM**

**6.1 Are all IT security requirements and procedures required by federal law being followed to ensure that information is appropriately secured?**

The FTC follows all applicable Federal Information Security Management Act (FISMA) requirements to ensure that information in the website and blog is appropriately secured. The information contained in the website and blog is categorized as low for confidentiality, integrity and availability, using the Federal Information Processing Standard (FIPS) 199 *Standards for Security Categorization of Federal Information and Information System*.

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

Per FTC policy, Web 2.0 technologies with a FIPS 199 categorization of low do not require a C&A.

**6.3 Has a risk assessment been conducted on the system?**

We conducted an abbreviated System Security Plan and have determined that the security risk of hosting the business website and blog through the selected vendor is low.

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

Because the technology for the website and blog is being expressly used to disseminate comments and other material to the public, the privacy risks of the technology are considered low in terms of integrity, confidentiality, and availability.

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

Access is granted on a need-to-know and least privilege basis. DCBE management determines who will have access to the system. These include a limited number of DCBE staff responsible for moderating comments and managing website content, and a limited number of staff from a communications firm contracted by DCBE to develop and maintain the website and

blog. A DCBE administrator has the ability to remove or add administrators who can login to the site.

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

FTC administrators complete annual FTC privacy training and are required to read and sign rules of behavior, acknowledging their responsibilities in accessing and managing the website and blog. In addition, DCBE staff responsible for reviewing comments must demonstrate a thorough understanding of the blog's commenting policy, the guidelines for interpreting this policy, and the privacy implications of comments that reveal PII. In addition, site administrators are required to read and sign rules of behavior, acknowledging their responsibilities in accessing and managing the blog.

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

The CMS automatically sends email alerts to site administrators when changes are made — including new blog posts, changes to the site settings, and password resets. These alerts will allow us to monitor changes to the site and respond if an unauthorized user makes changes.

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

Any questions regarding the security of the system should be directed to the FTC's Chief Information Security Officer.

**7 DATA RETENTION**

**7.1 For what period of time will data collected by this system be maintained?**

The FTC has submitted to the National Archives and Records Administration (NARA) a new comprehensive records retention schedule. The FTC will begin retaining and disposing documents and data in accordance with the new schedule when NARA has approved it. Pending NARA approval, the FTC will manage the data in a manner consistent with 44 U.S.C. Ch. 31, 44 U.S.C. 3506, 36 CFR Ch. XII, Subchapter B, Records Management, and Office of Management and Budget (OMB) Circular A-130, par. 8a1(j) and (k) and 8a4. In the interim, blog content that includes aggregate data about site visits will be kept indefinitely, but will not contain any personally identifiable information.

## **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 National Institute of Standards and Technology (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.**

The privacy risks are minimal because the information collected by the system is intended for publication. Any PII that is submitted and is not determined to be appropriate for publication is immediately deleted.

## **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.

### **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. See <http://www.ftc.gov/foia/listofpaysystems.shtm>.

In compliance with the Privacy Act, the blog comment form 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: \_\_\_\_\_  
Carolyn Shanoff, Associate Director  
Division of Consumer and Business Education

Review:

\_\_\_\_\_ Date: \_\_\_\_\_  
Alexander C. Tang  
Office of the General Counsel

\_\_\_\_\_ Date: \_\_\_\_\_  
Marc Groman  
Chief Privacy Officer

\_\_\_\_\_ Date: \_\_\_\_\_  
Margaret Mech  
Chief Information Security Officer

\_\_\_\_\_ Date: \_\_\_\_\_  
Jeffrey Nakrin  
Records and Filings Office

Approved:

\_\_\_\_\_ Date: \_\_\_\_\_  
Patricia Bak  
Acting Chief Information Officer