



**Federal Trade Commission  
Privacy Impact Assessment**

**for the:**

**National Consumer Protection Week Blog**

**November 2010**

## 1 System Overview

The Federal Trade Commission's Division of Consumer and Business Education (DCBE) plans to develop a blog to share consumer and business education resources, publications and ideas with members of National Consumer Protection Week (NCPW) Planning Committee (which primarily consists of government agencies, and organizations with a consumer education focus), as well as other government agencies, organizations and individuals across the country that have an interest in consumer protection issues. The blog will be hosted on a public site at [www.ncpw.gov](http://www.ncpw.gov) and exist within the public domain. The intended audiences are organizations and government agencies that disseminate information to the public as well as individual consumers.

The blog will feature short, timely articles that focus on specific topics and link to more detailed information on the Planning Committee organizations' websites. Only select FTC staff will be authorized to post blog articles, including posts submitted by members of the Planning Committee. We will use the blog to promote consumer protection resources, share examples of successful partnerships and outreach efforts, help partners (organizations and agencies taking an interest in NCPW) develop new outreach ideas, and get feedback from our partners about these ideas. In addition, the site will incorporate an online sharing service that will enable visitors to share content via various social networking and bookmarking sites. This feature, AddThis, is currently being used on the BCP Business Center website. Visitors to the site will also be able to download videos from the FTC's video page, from blog posts and from other web pages on the site. Downloading videos from the blog or any other part of the NCPW website does not require the system to collect any PII from the visitor.

The blog will allow moderated comments, which will be submitted through an online form generated by a secure web application. All comments will be reviewed by a DCBE staff member before posting. The full commenting policy for NCPW is currently available at <http://www.ncpw.gov/commenting-policy/>. This policy will be included on the NCPW 2011 website. DCBE's internal process for posting blog comments mirrors this policy and guides the manner in which comments are edited and posted. In addition, DCBE has developed a guideline for bloggers that provides direction on subject matter, content, length, privacy issues and the review process.

The blog software will be hosted by a contractor on an external server. We plan to launch the blog in December 2010 and to continue blogging from that point onward as [ncpw.gov](http://ncpw.gov) will be a permanent website and blog. This will allow us to share ideas and communicate with participating organizations and the general public in preparation for NCPW 2011 (March 6-12), to provide event summaries and feedback afterward, and to continue to build momentum for future NCPW observances.

This project, including the blog, builds upon the successful experience of the NCPW 2010 website and blog as well as the Business Center blog, launched in September 2010. With website traffic in excess of 400,000 visits, there were no negative incidents related to the privacy and security of personal information during NCPW 2010. The NCPW 2011 blog will be virtually the same as the 2010 blog, for which there is currently an existing PIA on the FTC intranet.

## **2 Information Collected and Stored within the System**

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

Bloggers who submit a comment will provide their comment and a self-selected user name. The blog commenting policy advises users not to share their personal information. The CMS collects user names and passwords from FTC administrators who log in 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 system will be obtained from individuals who voluntarily submit comments to blog posts. DCBE staff who serve as FTC moderators will input their user names and passwords into the system. The website server automatically collects log information of those who visit the site.

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

Blog comments and self-selected user IDs are collected in order to create an online community for organizations interested in participating in National Consumer Protection Week, specifically those that wish to use NCPW consumer education resources in their outreach efforts. Blog comments will allow FTC employees and members of the Planning Committee to interact with consumers and our partners, answer questions, and share ideas. In addition, blog comments will allow our partners to be included in NCPW planning and outreach. Allowing users to voluntarily specify their states and organizations will help us create a national online community and allow us to analyze the impact of NCPW.

Log information is automatically collected in order to analyze traffic to the site and better serve site visitors.

FTC moderators' user names and passwords are collected to ensure that only authorized staff access and post users' comments.

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

Users who wish to leave a comment can do so through an online comment form. The form will be available at the bottom of each blog post and will contain fields for users to complete, including user name, and comment. A brief Privacy Act statement with a link to the FTC's full privacy policy as well as an abbreviated commenting policy with a link to the full NCPW blog commenting policy will be positioned prominently next to the form, at the point of collection. When a user hits "submit," the comment is queued for review by a DCBE staff member. Once approved, the comment will be posted. Users do not register at the blog site and will complete the form each time they submit a comment. Log information is automatically collected by the website server.

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

Blog comments will be reviewed by an authorized FTC employee and posted within one business day. As stated in the commenting policy, those comments that contain false or misleading information or that are off-topic will not be posted.

Users who discover errors in their comments after they are posted will be able to contact the FTC moderators and request that their comments be removed.

**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 NCPW 2011 website and blog will not use technologies in ways not previously employed by the FTC. The blog will use the same hosting service used for NCPW 2010 and for the Business Center site as well as the same content management system (CMS) used for NCPW 2010.

The NCPW blog and website will now feature AddThis, an online sharing service. AddThis is currently being used on the [Business Center website](#). To share a link or information, visitors to the NCPW 2011 website would 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 NCPW website.

If a visitor chooses to share content from the NCPW 2011 website 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 NCPW website or blog.

Add This 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 NCPW website because it resides on a .gov domain. Though AddThis will not use cookies on NCPW.gov, 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. See 15 U.S.C. 45, 46(a), (f).

**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 that have been identified in connection with this system include the risk that users will provide personally identifiable information about themselves or others in the body of their comments and the risk that those without authorization will access the comments before the FTC moderators have made a determination as to whether they should be posted. The former is mitigated through a very clear commenting policy as well as by DCBE's internal process for posting comments so that those comments that contain PII will not be posted except in clearly enumerated circumstances. If there is any question about whether the individual intended to post contact information, the FTC employee 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 necessary FTC employees with login credentials and password protected access to the blog software.

**3. Use and Access to Data in the System**

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

As explained more fully in Section 2.3, blog comments from partners and consumers will be collected and posted to create an online community and to share ideas and questions about NCPW outreach. The weblog information that is automatically collected will be used to evaluate website traffic and better serve our visitors. The users names and passwords of DCBE staff who serve as FTC moderators are used to control access to the system.

**3.2 Which internal entities will have access to the information?**

Staff members in DCBE – designated by a DCBE manager – who must review, post, and respond to comments will have access to the information. Once posted, the comments will be public. Comments that cannot be posted because they do not comply with our commenting policy will be deleted.

DCBE employees who are site administrators will have password-protected access to the server's log files.

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

The contractor who will host the blog will not have routine access to the comments submitted by users before they are posted for the public, nor to the user names and passwords of the FTC moderators. The comments can be posted only by DCBE staff who serve as the FTC moderators and who have password access to the blog application. Once comments are posted, they will be available to the public and will become public information.

The contractor will have access to the server's log information.

## **4. Notice and Access for Individuals**

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

The blog will link to the FTC's privacy policy and will also contain an appropriate Privacy Act statement explaining the authority, purpose, and uses of the information collected by the blog. In addition, the commenting policy clearly informs users that the comments will be made public and that comments should not include personally identifiable information except in certain circumstances, as described in Section 2.1.

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

Participation in the blog is voluntary and those who choose to participate may decide what information to include in their comments.

Other information – namely, the user's IP address and the date and time of the visit – is collected automatically by the website server. Because this information is collected automatically by the server, and is needed for administrative and security purposes, users do not have the opportunity to decline to provide that information.

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

No. By submitting a comment to the blog, users are agreeing to make that comment public and to the automatic collection of weblog information.

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

Commenters can view their comments once they are 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 DCBE 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. For full details, see 16 CFR 4.13, <http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=bbdc64b9299e011d48bd7f4167072536&rgn=div8&view=text&node=16:1.0.1.1.5.0.5.13&idno=16>.

**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 such 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 above. See Section 6 for information regarding security measures applicable to this blog.

**5. Website Privacy Issues**

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

The FTC will host the blog on a contractor's external server and will capture log information on the server. The web hosting provider's servers collect IP address, date and time of visit, referrer, entry page, exit page, browser and operating system. The site uses session cookies for certain functionality: to enable flash fonts, to enable visitors to post comments, and to enable site visitors to toggle between English and Spanish language pages.

Neither the contractor nor the FTC will be using persistent cookies or other persistent tracking technology (persistent cookies) for visitors.

The login screen for site administrators does use persistent cookies so FTC administrators won't have to log in every time they go to update the website.

**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 and that are in use for the Business Center site. DCBE administrators understand the use of cookies to increase ease-of-use for

administrators. The risk here is minimal because the persistent cookies will only be placed on the computers of a handful of DCBE staffers, with their knowledge, and only for the sole purpose of easing their use of the site administrator tools. The risk that the login information stored by these cookies on the administrators' computers could be used by unauthorized individuals is minimal, since their computers are also secured by other physical, administrative, and technical controls (e.g., password protection). In addition, all of the site administrators' communications over the site will be encrypted, as described in 5.3.

**5.3 If personal information is collected through a Website, 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. 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.

We will be using encryption for the FTC administrator login area of the website. We will accomplish this 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 blog will link to the FTC's privacy policy in the top navigation bar. In addition, the blog Privacy Act statement with a link to the FTC's full privacy policy will be positioned prominently next to the blog commenting form, at the point of comment collection.

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

See Section 2.8.

**5.6 If the Website 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 is not intended to collect any information from children under 13. If it becomes clear that a user under 13 years of age has posted a comment, the moderator will immediately delete the comment..

**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 NCPW partner blog is appropriately secured. The information contained in the NCPW partner 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 Systems*.

**6.2 Has a Certification & Accreditation (C&A) 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?**

A risk assessment has been performed to determine the likelihood of a given threat-source exercising a particular potential vulnerability, and the resulting impact of that adverse event on the FTC.

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

Because the technology for this blog is being expressly used to disseminate comments and other material to the public, the privacy risks associated with the use of this 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?**

DCBE staff who are responsible for reviewing and posting comments will have access to the system. The application is password protected. Access is granted on a need-to-know and least privilege basis.

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

DCBE staff complete annual FTC privacy training. In addition, DCBE staff who will be responsible for posting 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 blog application automatically sends email alerts to the site administrator 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** 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 the 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 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: \_\_\_\_\_  
Nat Wood, Assistant Director  
Division of Consumer and Business Education

Review:

\_\_\_\_\_ Date: \_\_\_\_\_  
Bonnie Curtin  
Records Disposition Section

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

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

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

Approved:

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