



Federal Trade Commission Privacy Impact Assessment

for the:

GovDelivery Communications Management System

August 2010

1 System Overview

The FTC's Division of Consumer and Business Education (DCBE) plans to implement an online ordering system for our monthly e-newsletter for consumers and our quarterly newsletter for community organizations available by email and postal mail. DCBE will develop a web page on ftc.gov that describes our newsletter options and allows visitors to sign-up. To manage the subscription lists for these publications, DCBE will use the GovDelivery email management service.

GovDelivery is a web-based software system that manages and delivers email subscriptions. The GovDelivery system allows website visitors to subscribe quickly and easily based on their individual needs and interests. With GovDelivery, DCBE can develop and save branded email templates, integrate graphics and multimedia content, and efficiently deliver newsletters to a much larger audience than is currently possible.

GovDelivery also allows the FTC to accommodate website visitors who wish to receive email notifications when certain web pages are updated. These are referred to as email alerts. Subscribers can choose which web pages interest them and how often (i.e., weekly, monthly) they would like to receive such emails.

GovDelivery collects and stores data in a secure data center.

2 Information Collected and Stored within the System

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

To receive e-newsletters and email alerts, subscribers will provide an email address and select which e-newsletters and email alerts they wish to receive; user also may choose to create a password to protect their email preferences. The system will maintain the user's preferences and password until they are changed or deleted by the user.

Subscribers who wish to receive our quarterly newsletter by mail will be asked to provide their name, mailing address, and organization name (optional). The system will then assign them a random, unique user ID

number.

The FTC subscriptions web page will collect certain log information, including IP address, pages accessed, pages requested, and time and date of access. None of this log information will be linked to personally identifiable information.

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

All subscriber information and preferences will be voluntarily supplied by the subscriber.

The server for the subscription page automatically collects log information (IP address, date and time of visit, etc.) of individuals who visit the page.

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

The system collects subscriber information and preferences in order to deliver the services specifically requested by the subscriber (e-newsletters, email alerts, and/or mailed newsletters). Passwords are optional and are collected to protect the users' email preferences.

Log information is collected automatically in order to analyze traffic to the site and better serve site visitors as well as for other administrative and security purposes.

2.4 How is the information collected?

Subscription information and preferences are supplied voluntarily by the user through the subscriptions web page and through the User Profile page, once an individual has subscribed.

Log information is collected automatically by the website server.

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

The FTC will not check the information for accuracy and timeliness. The information is presumed to be accurate and timely because it is being submitted by the subscriber who is seeking to receive publications. Users can change and/or verify their subscription information and preferences at any time through their User Profile page. Any email sent via GovDelivery will include links for users to “manage their subscriptions,” “unsubscribe,” and “report spam.” There will also be a customer service number subscribers can call.

Newsletters that are mailed via postal mail will include information for how users can unsubscribe from the mail list. GovDelivery will be responsible for removing subscribers who choose to unsubscribe from the list.

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?

Yes. The FTC currently sends out newsletters and e-newsletters via contact databases that are manually updated by FTC employees. The GovDelivery management system will leverage technology to make the process more efficient and allow the FTC to offer this service to a much broader audience. Bounce back emails and subscribe and unsubscribe requests will be handled automatically by GovDelivery. Users will have more control of their own information and subscription preferences because they will be able to access their own information at any time to make changes.

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). The FTC will offer these subscription services as part of its public education efforts.

Log information is collected and maintained under information security laws, including the Federal Information Security Management Act (FISMA), Pub.

L. No. 107-347, t.3.

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

One privacy risk is that users will provide their contact information without understanding that they are signing up for an email message service. This risk will be mitigated by the subscription page – which will clearly explain how the information will be used – and by the confirmation email.

Furthermore, users can unsubscribe at any time even after they respond to the confirmation email.

Another risk to privacy is a possible breach of the GovDelivery database. The security of the subscriber data is a priority for GovDelivery. The company has developed a comprehensive security plan that has been reviewed and approved by several federal executive agencies, and has completed a successful Certification and Accreditation process for the National Institute of Standards and Technology. Security controls include:

- The data is hosted in a secure center that includes five levels of physical security.
- The System is protected by state of the art firewalls.
- The Company logs, maintains, and audits as necessary application, network, server, and database activity.
- Access to the data is limited to GovDelivery employees who need access to perform their duties. never send or
- Administrator sessions automatically time out.
- Account administrators create strong, unique passwords and do not share their passwords.

For more information about GovDelivery security, see section 6.

3 Use and Access to Data in the System

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

Email addresses will be used to send subscribers the email alerts and e-newsletters that they have chosen to receive; these emails will be sent by FTC staff using the GovDelivery system. The names and addresses that are

collected for printed newsletters will be sent to a printer via a secure internet connection so the newsletters can be mailed to the subscribers who have requested them.

The log information that is automatically collected will be used to evaluate website traffic and better serve website visitors as well as for other administrative and security purposes.

3.2 Which internal entities will have access to the information?

DCBE staff who manage or help produce newsletters will have access to the information in order to send newsletters and e-mail alerts, and update user information if necessary.

3.3 Which external entities will have access to the information?

GovDelivery, FTC's contractor for this service, receives the email addresses directly from the subscriber. A notice will inform users that they are providing this information in order to receive email alerts and newsletters that they have elected to receive. A discussion of the security and access controls used by GovDelivery is included in Section 2.8.

The name and mailing address list for those users who elect to receive the printed newsletter will be exported by GovDelivery and sent via a secure internet connection directly to the newsletter printer, strictly for the purpose of mailing the newsletter. The printer will be contracted through the Government Printing Office and will not use the names or addresses for any other purpose, nor will the printer retain the names and addresses once the mailing is complete.

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?

Before users subscribe to the GovDelivery service, they are presented with a web page that details exactly how this information will be handled by GovDelivery and by the FTC. Links to the privacy policies of both

GovDelivery and the FTC are provided. In addition, a link to the FTC's Systems of Records notice, as published in the Federal Register, is included on the web page and in the Privacy Act notice where subscriber information is collected. Once they have subscribed, users will receive a confirmation email that will reiterate the purpose of the information collected. Users may choose to unsubscribe at any time by clicking unsubscribe in any of the emails or by visiting their User Profile page.

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

Yes, individuals may choose not to subscribe simply by choosing not to fill out the subscription form or by clicking on the cancel button. Subscribers may unsubscribe at any time, by clicking on the "unsubscribe" link included in every email or by visiting their User Profile page. The User Profile page details which alerts and newsletters the individual currently subscribes to and offers check boxes to unsubscribe to specific pages or to delete their profile entirely.

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

Individuals can control how their email addresses are used by deciding whether or not to sign up for the service, and then by choosing what updates they wish to receive and how often they want to receive them. When users first requests e-newsletters or email alerts, a confirmation email will be sent to them. Users must open this email and confirm that they want to subscribe before they are added to the subscriber list.

Subscribers can also modify their email addresses and mailing address at any time or unsubscribe from the service.

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

Once users subscribe, they will have access to a User Profile page where they can make changes to their subscription. They will be able to access their User Profile page by clicking on the "manage subscriptions" link in the emails

they receive or by visiting the FTC subscriptions page and clicking on “manage your subscriptions.” Subscribers are also provided with a customer service email address and phone number for any questions or problems they have.

Users who wish to subscribe only to a printed (offline) newsletter will not need to provide an email address and will not receive a confirmation email. Instead, once they enter their name and address, they will be presented with a confirmation page that will include their unique user ID number; they will be encouraged to print and/or save this confirmation page. Their unique ID number will be included on each printed newsletter they receive. They will use this number to make changes to their subscription. If they cannot locate their ID number when they want to make changes, they will be prompted to contact GovDelivery customer service by phone or email. GovDelivery representatives will be able to assist them in making their changes.

To minimize the risk that individuals might incorrectly enter their email address, users must confirm the email address during the subscription process. Then, they will receive a confirmation email.

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

The privacy risk associated with allowing individuals to access their information is relatively low because of the security protocols that are in place and because the information being collected is not sensitive information. It is possible that someone other than the user could access the User Profile page and view the user’s information. This risk is mitigated in several ways. The subscriber’s user name is self-selected. Links to the User Profile page will only be sent directly to the user’s email. In addition, if changes are made to a user’s subscription, an email will be sent automatically to the user to inform them of the change.

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).

Session cookies are used to allow subscribers to access and make changes to their profile. The session cookie stores the user's email address in order to identify the user and save changes. No persistent tracking is used in the emails, on the subscription page or on User Profile pages.

5.2 If a persistent tracking technology is used, ensure that the proper issues are addressed (issues outlined in the FTC's PIA guide).

No persistent tracking is used in the email, on the subscription page or on User Profile pages.

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.

Yes, GovDelivery uses 128 bit SSL encryption when collecting subscriber information.

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

The subscriptions page and the User Profile page will link to our Privacy Policy in the top navigation bar.

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 is not intended to collect any information from children under 13.

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?

Yes. All IT security requirements and procedures required by federal law are being followed to ensure that information is properly secured.

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

A C&A was performed by another Federal Government agency that subsequently authorized this system to operate. The FTC has reviewed this C&A documentation and other vendor supplied documentation, and find that there appears to be sufficient security controls in place to protect FTC information categorized as low.

6.3 Has a risk assessment been conducted on the system?

A risk assessment was completed by the Federal agency who authorized this system to operate, and was part of the C&A documentation reviewed by the FTC.

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

See Section 2.8.

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

FTC staff will have access to the system only as needed. Access is granted on a need-to-know and least privilege basis.

GovDelivery ESM administrators and technical staff are assigned roles based on their job function and are given only the permissions needed to perform

their work. This determination is made by the GovDelivery Director of Technical Operations.

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

FTC staff complete annual FTC privacy training, and those who use this system must demonstrate a thorough understanding of the privacy implications of the system.

All GovDelivery ESM administrators and technical staff are briefed on data integrity and confidentiality concerns at hiring and periodically throughout employment. GovDelivery employees are subject to the GovDelivery's Rules of Behavior.

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

Safeguards used internally by GovDelivery are discussed in 2.8. In addition, GovDelivery automatically logs application, network, server, and database activity. Unusual activity will result in an audit. Upon request or in the event of unusual activity, log information will be made available to the FTC. The information stored in the system is categorized as "low" impact in terms of sensitivity, and the FTC collects only the information needed in order to send subscribers the messages they request. Nevertheless, to safeguard the information, the FTC will allow access to staff only as needed. Each FTC system administrator will have a unique login and password and will not share login credentials with anyone else. We will use strong passwords and will change them on a regular basis in accordance with FTC policy. An administrator's password can only be changed through that administrator's FTC email. In addition, any significant change within the system will trigger an email to FTC system administrators. Similarly, whenever a message is sent to contacts through the GovDelivery system, administrators will receive a courtesy copy of the email. These measures will alert administrators to unauthorized use of the email messaging system.

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?

Records will be retained as long as the subscription service continues to be offered. When users unsubscribe, their email addresses are immediately removed from the subscription list. Their preferences are immediately and permanently deleted. After one year, their email addresses are permanently deleted as well. A full backup of the system is run early every morning and incremental backups every five minutes during the day, so any database activity (such as a profile deletion) is almost immediately incorporated in the backup structure.

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

The information will be disposed of (permanently deleted) when the email service is no longer available. User preferences are permanently deleted immediately when a user unsubscribes. User emails may be kept in the backup system for up to one year. After one year, unsubscribed email addresses are permanently deleted.

7.3 Describe any privacy risks identified in the data retention and disposal of the information, and describe how these risks have been mitigated.

GovDelivery's security measures are outlined in 2.8, including possible privacy risks and how they have been mitigated.

8 Privacy Act

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

Yes, it will be retrieved by a user's email address. Users who request only a printed newsletter will not be required to provide an email address. Instead, the system will automatically assign them a random user ID number. This number will be included on every newsletter the person receives and will be used to make changes to the user's account. If users cannot locate the ID number when they want to make changes, they will be prompted to contact GovDelivery customer service by phone or email. GovDelivery representatives will be able to assist them in making their changes.

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

The contact information maintained in the GovDelivery database system is covered by an existing Privacy Act System of Records Notice, Mailing and Contact Lists–FTC–VI–1, 73 FR 33591 (June 12, 2008)
<http://www.ftc.gov/foia/sysnot/vi-1.pdf>.

In compliance with the Act, the subscriptions page will contain the required notice of authority, purpose, routine uses, and state that the collection is voluntary.

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:

Carolyn Shanoff
Division of Consumer and Business Education

Date: _____

Review:

Alexander C. Tang, Attorney
Office of the General Counsel

Date: _____

Kellie Cosgrove Riley
Acting Chief Privacy Officer

Date: _____

Margaret Mech
Chief Information Security Officer

Date: _____

Approved:

Patricia Bak
Acting Chief Information Officer

Date: _____