Federal Trade Commission
Privacy Impact Assessment

GovDelivery Communications

Cloud E-mail Marketing

(GovDelivery)

Updated May 2019

Table of Contents

1 System Overview

1.1 Describe the project/system and its purpose.

The GovDelivery Communications Cloud (GovDelivery) is a web-based email-subscription management application, provided by Granicus, that allows members of the public to subscribe to get information from the FTC via email.

Subscribers can choose from numerous subscriptions offered by the FTC, including, but not limited to:

- press releases
- blog posts
- case-related notifications

To facilitate redress in cases where the defendant data includes consumer email addresses, but does not include a physical mailing address, the FTC may email the list of potential redress recipients and ask them to provide their mailing address. The FTC uses GovDelivery for this purpose because that application is an authenticated sender for the FTC.

The FTC also uses GovDelivery for internal email communications with FTC staff (for instance, to invite staff to events).

Users can subscribe, via a secure Web page, to receive FTC emails through various sign-up pages on FTC website properties, including:

- www.ftc.gov
- www.consumer.ftc.gov
- www.consumidor.ftc.gov
- www.militaryconsumer.gov

For a list of the topics currently available to subscribers through ftc.gov, see www.ftc.gov/stay-connected and www.ftc.gov/es/conectese.

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

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 offers these subscription services as part of its public education efforts.

Web log information is collected and maintained under information security laws, including the Federal Information Security Modernization Act (FISMA).

2 Data Type, Sources, and Use

2.1 Specify in the table below what types of personally identifiable information (PII)[1] may be collected or maintained in the system/project. Check all that apply.

☐ Full Name	☐ Biometric Identifiers (e.g., fingerprint, voiceprint)	☒ User ID
☐ Date of Birth	☐ Audio Recordings	☐ Internet Cookie Containing PII
☐ Home Address	☐ Photographic Identifiers (e.g., image, x-ray, video)	☐ Employment Status, History, or Information
☐ Phone Number(s)	☐ Certificates (e.g., birth, death, marriage, etc.)	☐ Employee Identification Number (EIN)
☐ Place of Birth	☐ Legal Documents, Records, Notes (e.g., divorce decree, criminal records, etc.)	☐ Salary
☐ Age	☐ Vehicle Identifiers (e.g., license plates)	☐ Military Status/Records/ ID Number
☐ Race/ethnicity	☐ Financial Information (e.g., account number, PINs, passwords, credit report, etc.)	☒ IP/MAC Address
☐ Alias	☐ Geolocation Information	☐ Investigation Report or Database
☐ Sex	☐ Passport Number	☐ Driver's License/State ID Number (or foreign country equivalent)
☒ Email Address		☒ Other *(Please Specify)*: Optional passwords for web-based profile page, backend user passwords
☐ Work Address		
☐ Taxpayer ID		
☐ Credit Card Number		
☐ Facsimile Number		
☐ Medical Information		
☐ Education Records		
☐ Social Security Number		
☐ Mother's Maiden Name		

The application collects e-mail, IP address, and optional passwords from members of the public. Of these PII elements, only e-mail is available to the FTC in an identifiable form.

In addition to information collected from members of the public, GovDelivery collects the username and password of FTC employees using the application from application administrators. For these users, there is also a log of user actions that includes information such as username and information about login attempts. This information is not anonymized and is available to the FTC. Furthermore, to the extent that the FTC uses GovDelivery to send internal e-mail notifications, e-mail and IP address are collected.

[1] Per OMB Circular A-130, personally identifiable information (PII) means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

2.2 What types of information other than PII will be collected, disseminated, or maintained by the project/system? Provide a general description below and be sure to include all data elements.

The application collects:

- Web log information including
  - pages accessed
  - pages requested
  - time of access
  - date of access
- email opens
- email link clicks

The FTC only has access to this information in anonymized form.

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

The application collects:

- web log information to analyze traffic to the site and better serve site visitors
- email addresses to deliver email messages from the FTC to subscribers
- passwords in order to give subscribers access to their subscriber preferences page
- email opens and email clicks to evaluate performance
- application administrator log information to detect unauthorized application use or other technical problems

2.4 What are the sources of the information in the system/project? How is the information collected?

Source of Data	***Type of Data Provided & How It Is Collected***
Subscribers	Subscribers submit email addresses and optional passwords through a secure sign-up page as described in 1.1.
E-mail recipients at the FTC	FTC administrators provide email addresses for FTC staff to distribute internal (staff only) email communications (e.g. FTC Daily)

Source of Data	*Type of Data Provided & How It Is Collected*
Granicus	Granicus collects: • IP address, pages accessed, pages requested, time of access, date of access through web log files, to monitor usage and performance of their email management system • Email opens and clicks by including unique, customized links in each email.
FTC application administrators	FTC application administrators submit their username and password upon login, and the application automatically collects information about their actions within the application for logging/auditing purposes.

3 Data Access and Sharing

3.1 In the table below, specify the systems/applications and groups (both FTC and non-FTC) that will have access to or share data in the system/project.

Data Will Be Accessed By and/or Provided To:	*How and Why the Data Will Be Accessed/Shared*
FTC administrators	FTC administrators will have access to the GovDelivery Communications Cloud, where they can access subscriber email addresses and aggregate-level analytics data. Administrators will use analytics data to analyze the effectiveness of the FTC's email messages.
Granicus support staff	Granicus support staff will have access to the GovDelivery Communications Cloud where they can access subscriber email addresses and analytics data. Granicus employees may access this data to provide FTC administrators customer support.

3.2 Do contractors and/or third party service providers have access to data in the project/system? If yes, explain what privacy requirements are in place to ensure that data is properly protected.

Yes. Granicus employees who are members of the support team will have access to the data in the application. Granicus implements a role-based access model, so only employees that are required to have access to data will have that access.

FTC onsite contractors may also have access to the data in the application. Such contractors are subject to the vetting, access control, and contractual safeguards described in 8.1 below.

3.3 If you answered "yes" to 3.2, describe the privacy incident response plan maintained by the contractor's organization or third party service provider.

Granicus has a written Incident Response Plan (IRP). All incidents (including privacy) are handled following the steps in the IRP, which includes communicating with the FTC about the root cause of the incident.

FTC onsite contractors are subject to the FTC's Breach Notification Response Plan.

4 Notice and Consent

4.1 How are individuals provided with notice prior to the collection of their PII? If notice is not provided, explain why.

☒ Notice is provided via (*check all that apply*):
- ☒ Privacy Act Statement (☒ Written ☐ Oral)
- ☒ FTC Website Privacy Policy
- ☐ Privacy Notice (e.g., on Social Media platforms)
- ☐ Login banner
- ☐ Other (*explain*):_____

☐ Notice is not provided (explain): _____

4.2 Do individuals have the opportunity to decline to provide information or to consent to particular uses of their information (other than required or authorized uses)?

If someone subscribes for email updates, they do not have the opportunity to consent to particular uses of their email address. They have the ability to unsubscribe at any time they choose. Members of the public are not required to use GovDelivery, and may manually search and access relevant FTC information from the FTC's websites, which enables them to avoid submitting PII to GovDelivery.

FTC application administrators must provide their username and password in order to access the application, and are not provided a choice to consent or opt-out of particular uses of that information, as described elsewhere in this PIA.

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

Once users subscribe, they will have access to a web page where they can manage their email subscriptions. They can access the page by clicking on the "Manage Preferences" link in the footer of emails they receive from the FTC or by visiting the FTC subscriptions page at https://www.ftc.gov/stay-connected and clicking on "Manage Your Subscriptions." Once there, subscribers must enter the email address to manage their current subscriptions. Subscribers who have chosen to password-protect their web-based

subscriber preferences page must enter the password to gain access to the page. Subscribers can also contact customer service by email or phone for any questions or problems they may have.

Additionally, an individual may make a request under the Privacy Act for access to information maintained by the FTC about themselves in FTC Privacy Act systems. The FTC's Privacy Policy provides links to the FTC's SORNs, as well as information about making Freedom of Information Act (FOIA) requests and the online FOIA request form. Individuals must follow the FTC's Privacy Act rules and procedures, published in the Code of Federal Regulations (C.F.R.) at 16 C.F.R. 4.13. Access to information under the Privacy Act is subject to certain exemptions.

4.4 Are there procedures in place to allow individuals the ability to correct inaccurate or erroneous information? What is the process for receiving and responding to complaints, concerns, or questions from individuals? Explain.

Subscribers must confirm their email address during the subscription process by entering it twice. Then they will receive a confirmation email alerting them that they have successfully subscribed. Users who fail to submit a valid email address will not be able to subscribe to GovDelivery services. See also the Privacy Act/FOIA information in 4.3 above.

FTC application administrators who enter the wrong user ID or password will receive an error message and/or denied system access until they re-enter the correct information to obtain such access.

5 Data Accuracy and Security

5.1 Are there procedures in place to ensure that the information maintained is accurate, complete, and up-to-date?

The FTC relies on users to check their information for accuracy and timeliness when subscribing. The information is provided directly by the subscriber, so it is up to the user to provide his/her email address accurately. Subscribers can change and/or verify their subscription information and preferences through their web-based subscriber preferences page.

Granicus does not have any additional methods of ensuring the user has entered his/her email address accurately; if an incorrect email address has been submitted, the user will not be able to receive subscriptions. Invalid email addresses will result in messages bouncing back to Granicus.

5.2 Are there administrative procedures and technical safeguards in place to protect the data in the system/project? What controls are in place to ensure proper use of the data? Please specify.

Yes. Some administrative procedures and technical safeguards apply specifically to GovDelivery:

- Each FTC application administrator will have a unique login and password and will not share their login credentials. Per FedRAMP requirements, passwords are changed every 60 days for Granicus employees and FTC administrators. Administrators will use strong passwords and will change them on a regular basis in accordance with FTC policy. FTC application administrators will have access to GovDelivery on a least-privilege basis.

- All Granicus employees who will have access to the application are required to take Granicus' Security Awareness training and Insider Threat training. In addition, all employees are required to sign a non-disclosure agreement as well as sign the Acceptable Use Policy.

- Technical controls include logging activities locally and on Granicus's centralized logging tool for analysis. Host-based and network-based intrusion detection applications look for malicious actors on the network and on servers.

Other administrative procedures and technical safeguards apply not only to GovDelivery, but to many other applications at the FTC, as well:

- All FTC positions are assigned a risk designation that has associated criteria for personnel screening. All potential FTC employees, contractors, and volunteers are subject to background investigations and suitability reviews in accordance with OPM guidance. Before any new employee, contractor, or volunteer can access FTC applications, that individual must first attend new employee orientation and successfully complete the FTC's Privacy and Security Awareness training. All employees are granted basic network access to include email services, the Internet, the Intranet, network shared drives, network-based applications, and are assigned their own home directory. Categories of employees deemed to be higher risk – such as interns and International Fellows – may have restricted access to network and physical space.

- Supervisors and/or Contracting Officer's Representatives (CORs) must identify and approve employee requests to access network applications and specify the appropriate user role and level of access privileges. Auditing measures and technical safeguards are in place commensurate with the Moderate-Impact Baseline of the National Institute of Standards and Technology (NIST) Security and Privacy Controls for Federal Information Systems and Organizations Special Publication (SP) 800-53.

- FTC staff is responsible for minimizing PII and disposing of it when the PII is

no longer needed and in accordance with appropriate records disposition schedules. The FTC ensures that all staff and contractors annually electronically certify their acceptance of FTC privacy responsibilities and procedures by requiring comprehensive Information Security and Privacy Awareness training. Moreover, all staff must annually acknowledge procedures for handling PII – including minimizing PII – and attest that all PII maintained by the individual has been properly secured and accounted for as part of the FTC's annual privacy and security training.

5.3 Is PII used in the course of system testing, training, or research? If so, what steps are taken to minimize and protect PII during this process?

☒ Not Applicable

6 Data Retention and Disposal

6.1 Specify the period of time that data is retained in the system/project. What are the specific procedures for disposing of the data at the end of the retention period?

Granicus will retain a user's settings and subscription records for as long as the user subscribes to its services. When users unsubscribe, Granicus immediately and permanently deletes their preferences. After one year, Granicus permanently deletes subscribers' email addresses.

Granicus replicates data in real-time between data centers. As such, any database activity (such as a profile deletion) is almost immediately incorporated in the backup structure. The FTC will retain aggregate analytics data for only as long as is necessary for operational purposes. The data will be maintained in accordance with FTC regulations, policies, and procedures.

7 Website Privacy Evaluation

7.1 Does the project/system employ the use of a website? If so, describe any tracking technology used by the website and whether the technology is persistent or temporary (e.g., session cookie, persistent cookie, web beacon). Describe the purpose of using such tracking technology.

The GovDelivery subscription pages use session cookies 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. The cookie is not shared with other websites and expires as soon as the user closes the browser.

Granicus analytics track whether users open an email or click on links in an email. Clicks are measured by including unique, customized links in each email. When a subscriber accesses his or her unique link, then that is recorded as one click. Each email includes a

unique, invisible image that is used to track whether users open an email. When a particular image is accessed, that is recorded as one "email open." The FTC can review this information in aggregate form through the GovDelivery Communications Cloud. No personal identifiers are associated or tagged with the email opened or the particular image associated with that email.

8 Privacy Risks and Evaluation

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

Risk	*Mitigation Strategy*
Granicus could suffer a data breach	GovDelivery received FedRAMP certification in April 2016, hosts data in a secure center that includes five levels of physical security, and employs state-of-the-art firewalls.
Unauthorized access to user data	Granicus logs, maintains, audits application, network, server, and database activity as necessary, and limits access to the data to those employees who need access to perform their duties. Administrator sessions automatically time out.
Unauthorized change or deletion of a subscriber's account	If a subscriber has not set a password on their subscriber preference page, it may be possible for a malicious actor to enter an email address and access that person's account settings. The malicious actor could potentially alter or delete the user's account settings. Due to the minimal (and non-sensitive) personal information maintained in the application, Granicus has determined that it is not necessary to require customers to set a password. If the user wishes to, they can create a password to protect their account and prevent unauthorized access. If the account owner notices unauthorized changes to their subscription services, they can log in with their email address and update/reactivate their settings. They can also contact Granicus to reset their account settings and report the unauthorized access.

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

All accounts, both for infrastructure access as well as application access, lock for 30 minutes after three failed attempts. All access to the Communications Cloud application (and the infrastructure it resides on) requires multifactor authentication. The application logs, both locally and to a centralized logging host, audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals associated with the event.

See also Section 5.2 above.

8.3 Has a Privacy Act System of Records Notice (SORN) been published in the Federal Register for this system/project? If so, list the applicable SORN(s).

Yes. The contact information maintained in the GovDelivery database is covered by an existing Privacy Act SORN, Mailing and Contact Lists–FTC-VI-1. 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. FTC SORNs are available on ftc.gov.

8.4 How does the project/system ensure that the information is collected, used, stored, or disseminated in accordance with stated practices in this PIA?

Granicus automatically logs application, network, server, and database activity. Unusual activity will result in an audit. Upon request or in the event of unusual activity, Granicus will provide log information to the FTC. The information stored in the application is not highly sensitive, and the FTC collects only the information needed in order to send subscribers the messages they request.

Furthermore, the Privacy Office routinely collaborates with system/application owners as part of its Privacy Continuous Monitoring Strategy to ensure that the information in PIAs, including this one, is accurate and to mitigate any privacy risks, as needed. Members of the public with questions or comments on the FTC's privacy practices may contact the Chief Privacy Officer using the contact information at ftc.gov/privacy.