Federal Trade Commission
Privacy Impact Assessment

GovDelivery Communications Cloud (GovDelivery)

Reviewed February 2022

Table of Contents

1 System Overview

1.1 Describe the project/system and its purpose.

The GovDelivery Communications Cloud (GovDelivery) is a web-based software system, provided by Granicus, that allows several FTC offices, including the Division of Consumer and Business Education, the Office of Public Affairs, and the Office of International Affairs, to deliver emails to subscribers and manage subscriptions. GovDelivery allows people to subscribe to a variety of email updates from the FTC including press releases, blog posts, and e-newsletters based on their individual needs and interests. The FTC also uses GovDelivery to distribute the FTC Daily News and FTC Daily Clips internally to its employees.

The FTC develops custom-designed email templates, integrated graphics and multimedia content, and delivers emails to hundreds of thousands of subscribers.

Individuals can subscribe, via a secure Web page, to receive FTC emails in English (www.ftc.gov/stay-connected) or in Spanish (www.ftc.gov/es/conectese). They also can subscribe through various sign-up pages on FTC website properties including www.ftc.gov, www.consumer.ftc.gov, and www.military.consumer.gov. Below is a list of the topics currently available to subscribers through ftc.gov:

- **Newsletters**
  - Penn Corner
- **FTC Blogs**
  - Tech@FTC
  - Competition Matters
- **Business Center Updates**
  - Business Center Blog Updates
- **Press Releases**
  - Competition and Antitrust Press Releases Information
- **Consumer Protection Press Releases**
  - Consumer Fraud Press Releases
  - Credit and Debt Press Releases
  - Do Not Call/Robocalls Press Releases
  - Mobile Press Releases
  - Privacy and Data Security Press Releases
  - Advertising Press Releases
- **Consumer Updates**
  - Money & Credit
  - Homes & Mortgages
  - Health & Fitness
  - Jobs & Making Money
  - Privacy, Identity & Online Security
  - Scam Alerts

Granicus collects subscriber emails and subscription preferences (i.e. the list of topics to which the user has subscribed) to deliver emails about the topics subscribers have chosen.

Subscribers are provided with the option to add a password to protect their web-based subscriber preferences page. In those instances, Granicus maintains the subscriber's password. However, subscribers are not required to provide a password. If at any time, subscribers wish to change

their account settings, they can do so by clicking on the "Manage my email subscriptions" link at www.ftc.gov/stay-connected. They are prompted to enter their email address to subscribe or edit their current subscriptions, but a password is not required unless they have previously created one for their account.

The system maintains the user's email address, subscriptions, and password until they are changed or deleted by the user. Following standard security protocols, GovDelivery sign-up pages collect basic web log information, including IP address, pages accessed, pages requested, and time and date of access. The web log information is not linked to any individual accounts.

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.

PII Elements: This is not intended to be an exhaustive list. Specify other categories of PII as needed.		
☐ 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
☐ Work Address		
☐ Taxpayer ID		
☐ Credit Card Number		
☐ Facsimile Number		
☐ Medical Information		
☐ Education Records		
☐ Social Security Number		
☐ Mother's Maiden Name		

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.

GovDelivery sign-up pages collect log information, including IP address, pages accessed, pages requested, and time and date of access.

Granicus collects passwords for subscribers who have chosen to protect their subscriber preferences with an optional password.

Granicus collects aggregate-level data about which messages are opened and which links in emails are clicked. These reporting statistics are provided to the FTC through the GovDelivery Communications Cloud and are not associated with the activity of any particular subscriber.

[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.

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

Granicus collects subscriber emails and subscription preferences to deliver emails about the topics subscribers have chosen.

For those subscribers who have chosen to password-protect their web-based subscriber preferences page, Granicus collects passwords in order to give subscribers access to their subscriber preferences page.

Web log information is collected automatically in order to analyze traffic to the site and better serve site visitors. The web log information is not linked to any individual's data.

The FTC reviews aggregate-level analytics data to better understand what FTC content GovDelivery subscribers are most interested in and to help refine the FTC's use of this service.

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*
Individual subscribers	Subscribers provide an email address via a secure sign-up page as described in 1.1.
Granicus	Granicus will automatically collect aggregate-level data about which messages are opened, which links in emails are clicked on, and how much our reach has increased (or decreased) over time. Granicus will also automatically collect web log information (IP address, date and time of visit, etc.) This is not linked in individual account information.

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 at https://admin.govdelivery.com/ 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 employees	Granicus employees will have access to the GovDelivery Communications Cloud at https://admin.govdelivery.com/ where they can access subscriber email addresses and aggregate-level 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.

Granicus employees who are members of the support team will have access to the data in the system. All Granicus employees who will have access to the system 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.

Granicus implements a role-based access model, so only employees that are required to have access to data will have that access.

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

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.

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): _____

Privacy Act Statement on GovDelivery Sign-up Pages
PRIVACY ACT STATEMENT: It is your choice whether to subscribe to our email updates. If you do, you must provide an email address, or we will not be able to send you updates. The Federal Trade Commission Act authorizes this information collection for the purpose of distributing information to the public. Email addresses are part of our mailing list system of records, and we may routinely use these records as described there and in Appendix I for our Privacy Act system notices. For more information on how we handle information that we collect,

please read our privacy policy. We use GovDelivery, a contractor, to help us provide this service. According to our agreement, GovDelivery will not share your information with third parties. To learn more, read their privacy policy.

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)?

Subscribers must provide an email address in order to use GovDelivery's subscription services. Users who do not wish to provide this information would not be able to subscribe to GovDelivery's email services. Users may unsubscribe at any time by clicking on the "unsubscribe" link included in every email or by visiting a web-based subscriber preferences page where they can modify their email addresses, add, change, or delete a password, review their subscriptions, set delivery preferences, or delete their profile entirely.

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 are also provided with a customer service email address and phone number for any questions or problems they may have.

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 that they have successfully subscribed. Users who fail to submit a valid email address will not be able to subscribe to GovDelivery services.

It is possible for a malicious actor to enter an email address and change or delete a subscriber's email preferences if the subscriber has not set a password on their account. In such cases, if the subscriber notices that they are receiving inaccurate subscription emails or no emails at all, the subscriber must access their own account and update or reactivate their preferred settings.

Granicus does not require users to set passwords on their accounts when they sign up for subscription services via GovDelivery. Due the minimal (and non-sensitive) personal information maintained in the system, Granicus has determined that requiring users to set passwords would be too burdensome on the customer. However, Granicus does give the user the option to set a password, if he/she so chooses. The user can use their email address to access

their subscription settings, and if they feel there has been erroneous activity on their account, the user can contact Granicus to report complaints, concerns, or any questions the user may have.

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.

Granicus's access to the data is limited to employees who need access to perform their duties. Administrator sessions automatically time out after a set period of inactivity.

FTC administrators are given access on an as-needed basis. Each FTC system 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.

5.3 Has the system/project undergone the appropriate security risk assessment and received authority to operate?

In April 2016, GovDelivery received a Joint Authorization Board (JAB) Provisional Authorization to Operate (PATO). The FTC reviewed the PATO package and is currently designing and implementing the customer controls required under the PATO. An FTC ATO will be granted pending agency validation of customer controls.

5.4 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

PII is not used for any testing, training, or research.

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, 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 on a daily basis and incremental backups are executed every five minutes. 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.

Risk	*Mitigation Strategy*
Unauthorized access to user data	Granicus logs, maintains, and 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. 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. If the user wishes to, they can create a password to protect their account and prevent 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 system 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.

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 system is covered by an existing Privacy Act SORN, Mailing and Contact Lists–FTC-VI-1, 73 FR 33591 (June 12, 2008).

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.

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 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.

9 Approval and Signature Page

Prepared By:

_____ **Date: _____**
Alvaro Puig
Chief of Staff
Division of Consumer and Business Education

Reviewed By:

_____ **Date: _____**
Katherine Race Brin
Chief Privacy Officer (CPO)

_____ **Date: _____**
Alexander C. Tang, Attorney
Office of the General Counsel (OGC)

_____ **Date: _____**
Jaime Vargas
Chief Information Security Officer (CISO)

_____ **Date: _____**
Jeffrey D. Nakrin
Director, Records and Filing Office

Approved By:

_____ **Date: _____**
Raghav Vajjhala
Chief Information Officer (CIO)