



Adapted Privacy Impact Assessment

Medium

September 7, 2016

Contact

Departmental Privacy Office
U.S. Department of the Interior
1849 C St. NW, MIB-7456
Washington, DC 20240
(202) 208-1605
DOI_Privacy@ios.doi.gov



One Privacy Impact Assessment (PIA) may be prepared to cover multiple websites or applications that are functionally comparable as long as agency or bureau practices are substantially similar across each website or application. However, any use of a third-party website or application that raises distinct privacy risks requires a complete PIA exclusive to the specific website or application. Department-wide PIAs must be elevated to the Office of the Chief Information Officer (OCIO) for review and approval.

SECTION 1: Specific Purpose of the Agency's Use of the Third-Party Website or Application

- 1.1 What is the specific purpose of the agency's use of the third-party website or application and how does that use fit with the agency's broader mission?

Medium is a web-based privately owned third party social media application that is open to members of the public. Medium is a publishing tool where anyone can express her/his ideas. It's similar to a blog, but this platform makes it easy to integrate photos, audio, video and social media content into the stories people create. Users can easily share their perspectives with the Medium community. The Medium community in turn can provide thoughtful comments on the post, highlight phrases or sentences and share posts with others.

Medium is a network of thinkers and storytellers who thoughtfully engage with, share, and build on ideas. By becoming a member and using the Medium platform, the Department of the Interior (Department or DOI) will reach new audiences and better educate the public about the Department's work. DOI will utilize Medium to share information, facilitate dialogue, improve customer service, and encourage public participation and collaboration with the Medium community.

Medium users can create posts and add photos, videos, and audio, and can comment on other users' posts and stories. The content can be viewed (but not downloaded) through the application by other users or by members of the public without Medium accounts.

The Department does not actively seek personally identifiable information (PII) through the use of the Medium application, and will only receive minimal amounts of PII in order to fulfill a user's request. For example, when a Medium user responds to a DOI post asking about the content of the post, DOI will be able to view the user name and profile photo of the individual asking the question. DOI is a user of Medium and has the same level of access as other users. DOI's official use and presence on Medium does not constitute an endorsement or preference for the services, products or information on Medium.

- 1.2 Is the agency's use of the third-party website or application consistent with all applicable laws, regulations, and policies? What are the legal authorities that authorize the use of the third-party website or application?

Authorities supporting DOI's use of this networking application include:



The President's January 21, 2009 Memorandum on Transparency and Open Government; Presidential Memorandum on Building a 21st Century Digital Government, May 23, 2012; OMB M-10-06, Open Government Directive, December 8, 2009; OMB Memorandum M-10-23, Guidance for Use of Agency Third-Party Websites and Applications, June 25 2010; OMB Memorandum for the Heads of Executive Department Agencies, and Independent Regulatory Agencies, Social Media, Web-Based Interactive Technologies; the Paperwork Reduction Act of April 7, 2010, 44 U.S.C. 3501; and 110 Departmental Manual 5.

SECTION 2: Any PII that is Likely to Become Available to the Agency Through the Use of the Third-Party Website or Application

2.1 What PII will be made available to the agency?

DOI does not actively seek or collect PII from Medium users; however, DOI will be able to view any PII that users make available to the Medium community through interactions on the official DOI Medium account. DOI uses third-party social media applications to engage the public and provide content in formats that may be useful or interesting, and DOI has the same level of access to Medium as other users.

Users are required to provide an email address, full name and a username in order for them to register for the Medium application. Users may also associate a profile image with their user account and a biography, though these aren't required. When a Medium user recommends a story, or posts or highlights a line, the user's username and profile image will become available to the Medium community and will be visible to DOI. When a Medium user responds to a story or post, the user's username, first and/or last name (if they've opted to use it), profile image, and comments will be visible to DOI and the Medium community. Clicking on a username will lead to other images, stories, or posts associated with the user. Users are reminded that they are using a third-party application and are subject to Medium's terms and policies. Users should take care when registering and selecting privacy settings to determine the level of interaction and visibility they want when posting messages, placing comments, and other information for public viewing.

Medium users also have the option of creating Medium accounts using their Facebook, Twitter or Google accounts, in which case, Medium would pull the user information from those other third-party applications to register. Users may provide more than the required information such as profile photo, biography, and website. Medium users can control or limit the personal information shared with other users by blocking accounts and turning off private notes. Unless individuals opted to block DOI, the Department would be able to see the usernames, and any other information users voluntarily provide, such as their names, profile photo, biography, and website.

Information provided to Medium during registration is not collected or used by DOI, and DOI does not ask individuals to provide personal information to view DOI stories.



Medium does not share user information with DOI. Any information that individuals voluntarily submit as part of the registration process is not the property of DOI and Medium users are subject to the Medium privacy policy and terms of service regarding use of their data and how information may be handled and shared.

DOI does not actively solicit, collect, maintain, or disseminate sensitive PII from individuals who interact on Medium. In very limited circumstances, DOI may receive and use the minimum amount of PII voluntarily provided by a user if it is necessary for the proper performance of an agency function. For example, if a user requests information or a service and provides an email address, DOI may use the email address to communicate for the purpose of providing information or customer service.

DOI receives notifications when a Medium user recommends DOI's Medium posts, responds to a story, or highlights a story, and would be able to see the username, image, or comments shared with DOI. If Medium users tag DOI in their stories or respond on a DOI Medium story, DOI can view their user profile. Users can limit what DOI or others see by not including personal information in their profile, by not interacting with DOI on Medium, or by utilizing Medium's account settings.

2.2 What are the sources of the PII?

Any PII on Medium is voluntarily provided by users when they register to create an account, create stories, follow, recommend, or otherwise interact with the Medium community, and is publicly available unless the user enables the privacy setting in their account.

2.3 Will the PII be collected and maintained by the agency?

DOI does not actively solicit, collect or maintain PII from individuals who interact on Medium. In very limited circumstances, DOI may receive and use the minimum amount of PII voluntarily provided by a user if it is necessary for the proper performance of an agency function. For example, if a Medium user or member of the public interacts with DOI through its official Medium account, including responding to a DOI story, requests information, or submits feedback through Medium, the user's username as well as other information the user makes public will become available to DOI and may be used to provide the requested information or service. In these cases DOI may use PII to provide the requested service through the Medium application where possible and will not collect or maintain the PII.

Any DOI bureau or office that collects PII or uses Medium in a way that creates a system of records must complete a separate PIA to address the privacy implications for the specific use and collection of information, and must maintain the records in accordance with DOI-08, Social Networks, system of records notice or other applicable system of records notice.

2.4 Do the agency's activities trigger the Paperwork Reduction Act (PRA) and, if so, how will



the agency comply with the statute?

No, DOI is not using Medium to survey the public in any manner that would trigger the requirements of the Paperwork Reduction Act. The activities of DOI are carried out under the general solicitation exclusion of the PRA. Under the general solicitations exclusion, the PRA does not apply to notices published in the Federal Register or other publications that request public comments on proposed regulations, or any general solicitation for comments “regardless of the form or format thereof.” 5 CFR 1320.3 (h)(4).

SECTION 3: The Agency’s Intended or Expected Use of the PII

3.1 Generally, how will the agency use the PII described in Section 2.0?

DOI’s official presence on Medium is to promote the Department’s work and provide better services to the general public, develop community engagement, and increase government transparency. DOI does not collect, maintain or disseminate PII from individuals who interact with DOI utilizing the Medium application. DOI may use a person’s username or other information provided by the user to respond to a specific comment or question directed to or about agency activities, or to fulfill a request. In such a situation, only the minimum required information that is needed to appropriately respond is used. See examples in Section 3.2 below.

There may be unusual circumstances where user interactions indicate evidence of criminal activity, a threat to the government, a threat to the public, or an employee violation of Departmental policy. In these cases information about the user interaction, including username, name, profile photo, images, contents of postings, and other personal information available to DOI through Medium, may be used to notify the appropriate agency officials or law enforcement organizations as required.

3.2 Provide specific examples of the types of uses to which PII may be subject.

DOI may recommend other Medium users’ stories with DOI followers to show the Department’s work and increase engagement with the Medium community. DOI may also respond to or highlight other Medium users’ stories to increase engagement with the Medium community. In that case, DOI’s responses and highlights will appear on that post and also be listed at the bottom of the Department’s account homepage. In addition, if a Medium user or member of the public interacts with DOI through its official Medium account — including commenting on DOI stories, requesting information, or submitting feedback through Medium — their username, name, profile photo, images, and contents of postings will become available to DOI and may be used to communicate and interact with the user or provide information or requested services.

SECTION 4: Sharing or Disclosure of PII



4.1 With what entities or persons inside or outside the agency will the PII be shared, and for what purpose will the PII be disclosed?

Medium is a third-party social media application and a smartphone mobile application. DOI does not collect and maintain PII from Medium users, or share PII with other agencies, and is not responsible for how Medium may access or use data posted on the platform. Users understand that whenever they upload and share content, the entire content of the posting is publicly displayed and available to all visitors for viewing, sharing, and commenting, unless the user utilizes the privacy setting. Users are encouraged to exercise care when posting information on this application as information shared with the Medium community may be viewed by all members of the public.

Information posted on third-party social media websites and applications is considered to be public by its very nature. By choosing to post information, Medium users voluntarily choose to share information publicly. DOI does not own or control the third-party sites, and accesses them as a user. The public will have access to content posted and published by DOI, and will be able to submit comments or questions about the posted content.

When a Medium user or member of the public interacts with DOI through its official Medium account by following, recommending, highlighting or responding to DOI stories, requesting information, or submitting feedback through Medium, their username, name, profile photo, images, and contents of postings will become available to DOI, and may be used internally to communicate and interact with the user, or provide information or requested services.

There may be unusual circumstances where user interactions indicate evidence of criminal activity, a threat to the government, a threat to the public, or an employee violation of Departmental policy. This information may include username, name, profile photo, images, contents of postings, and other personal information available to the DOI through Medium, and may be used to notify the appropriate agency officials or law enforcement organizations as required.

4.2 What safeguards will be in place to prevent uses beyond those authorized under law and described in this PIA?

Only approved DOI staff members will have access to manage the official DOI Medium account and create official postings and stories. Except for official postings, DOI does not control the content or privacy policy on Medium. Medium is responsible for protecting its users' privacy and the security of user data within the Medium application. Medium users are subject to Medium's Privacy Policy and Terms of Use, and can utilize their own discretion with respect to the personal information they provide to Medium or make available to the Medium community.

DOI entered into Terms of Service for DOI's official use of the Medium application, which was previously negotiated by the General Services Administration (GSA) for U.S. government users, that includes the use of advertisements, endorsements, and system



security. The Terms of Service may be viewed at <https://medium.com/@Medium/amendment-to-medium-terms-of-service-applicable-to-u-s-government-users-fccb00db67d7#.p96foozgf>.

DOI employees are required to complete annual mandatory security, privacy and records management training to ensure an understanding of their responsibility to protect individual privacy and appropriately manage information.

Information posted on third-party social media websites and applications is considered to be public by its very nature. DOI does not own or control the Medium third-party site, and the public will have access to content posted on DOI's official Medium site and will be able to submit comments or questions about the posted content. Users should take care when registering and selecting privacy settings to determine the level of interaction and visibility they want when posting messages, placing comments, and other information for public viewing. Any PII or personal information posted is at the user's discretion.

SECTION 5: Maintenance and Retention of PII

5.1 How will the agency maintain the PII, and for how long?

DOI does not actively collect or maintain PII from interactions or use of the Medium application. Records published through Medium represent public informational releases by DOI, and must be assessed on a case-by-case basis depending on the office releasing the information and the purpose of the release. Retention periods vary as records are maintained in accordance with the applicable bureau or office records schedule for each specific type of record maintained by DOI. There is no single records schedule that covers all informational releases to the public at this time.

Comments and input from the public must be assessed by whether they contribute to decisions or actions made by the government. In such cases where input from the public serves a supporting role, the comments must be preserved as supporting documentation for the decision made. Approved methods for disposition of records include shredding, burning, pulping, erasing and degaussing in accordance with National Archives and Records Administration guidelines and 384 Departmental Manual 1.

5.2 Was the retention period established to minimize privacy risk?

Retention periods for official postings and informational releases by DOI may vary depending on agency requirements and the subject of the records for the DOI bureau or office maintaining the records. In cases where data serves to support agency business, it must be filed with the pertinent records they support and follow the corresponding disposition instructions. Comments used as supporting documentation will utilize the disposition instructions of the records they are filed with.



SECTION 6: How the Agency will Secure PII

6.1 Will privacy and security officials coordinate to develop methods of securing PII?

Yes. Privacy and security officials work with the Office of Communications to develop methods for protecting individual privacy and securing PII that becomes available to DOI.

6.2 How will the agency secure PII? Describe how the agency will limit access to PII, and what security controls are in place to protect the PII.

DOI does not collect, maintain or disseminate PII from Medium users, except in unusual circumstances where user interactions indicate evidence of criminal activity, a threat to the government, a threat to the public, or a violation of DOI policy. This information may include username, name, profile photo, images, contents of postings, and other personal information available to DOI through Medium, and may be used to notify the appropriate agency officials or law enforcement organizations as required. In these cases PII is secured in accordance with DOI Privacy Act regulations 43 CFR part 2, subpart K, and applicable DOI privacy and security policies. Access to the DOI network is restricted to authorized users with multi-factor authentication controls, servers are located in secured facilities behind restrictive firewalls, and access to databases and files is controlled by the system administrator and restricted to authorized personnel based on official need to know. Other security controls include continuously monitoring threats, rapid response to incidents, and annual mandatory employee security and privacy training.

SECTION 7: Identification and Mitigation of Other Privacy Risks

7.1 What other privacy risks exist, and how will the agency mitigate those risks?

Medium is a third-party website that is independently operated and controls access to user data within its system. Medium users control access to their own PII via system settings and through discretion with respect to the personal information users provide. Accordingly, users should take care to avoid disclosing sensitive PII, which could be used to commit fraud or identity theft, or for other harmful or unlawful purposes. To help reduce these risks, DOI will monitor comments on its official postings to the extent practicable. DOI does not have access to information within the application and has no control over access restrictions, privacy or security procedures, or how Medium manages information. Where possible, DOI will also provide appropriate notice to users on the official DOI Medium page warning them to avoid sharing or disclosing any sensitive PII when interacting with DOI. Users should also review Medium's privacy policy and Terms of Use to ensure an understanding and determine how they wish to use the Medium application.

Another privacy risk is third-party advertising and tracking. Medium displays third party advertising in accordance with its normal course of business. If the user clicks on the



advertisement or reads the communication to learn about the advertised product or service, the user's profile information or other PII may be shared by the website operator with the advertiser. The user's actions may also initiate tracking technology (e.g., "cookies," "web bugs," "beacons"), enabling the website operator or advertiser to create or develop a history or profile of the user's activities. The tracking data can be used to target specific types of advertisements to the user, i.e., behavioral advertising, or it can be used or shared for other marketing or non-marketing purposes. Users can avoid or minimize these risks by regularly deleting "cookies" through their browser settings, not clicking on advertisements or not visiting advertisers' sites. Users may also opt-out of some tracking technologies all together. This data is not shared with DOI, and DOI does not have access to information within the application, and does not control how Medium manages information or its privacy or security procedures.

Risks also include spam, unsolicited communications, spyware, and other threats. Users may receive spam or other unsolicited or fraudulent communications as a result of their interactions on Medium. To avoid harm, users should be wary of responding to such communications, particularly those that may solicit the user's personal information, which can be used for fraudulent or other undesirable purposes. Users should also avoid accepting or viewing unknown or unsolicited links, applications, or other content that may be sent or forwarded in such communications. These unsolicited links and applications can contain unwanted tracking technology as well as computer viruses or other malicious payloads that can pose a variety of risks to the user. Where possible, DOI will also provide warnings about these risks in a notice to users on DOI's official page.

There is a risk that third-party accounts or content may misrepresent agency authority or affiliation. Certain third-party accounts, social media websites, or content may not be officially authorized by, or affiliated with DOI, even where they appear to represent DOI or the Federal government. Interacting with such unauthorized accounts or pages may expose users to the privacy or security risks described above. DOI will make every reasonable effort to label or identify its official account or page in ways that would help users distinguish it from any unauthorized accounts or pages. DOI will also inform the website operator about any unofficial accounts or pages purporting to represent DOI, seek their removal, and warn users about such accounts or pages.

If DOI posts an external link that leads to a third-party website or any other location that is not part of an official government domain, DOI will provide notice explaining that visitors are being directed to a non-government website that may have different privacy policies (and risks) from those of DOI's official pages or website.

DOI will examine the third-party website's privacy policy to evaluate the risks and determine that the site is appropriate for DOI's use prior to using the third-party social media application. DOI will monitor any changes to the website's privacy policies and periodically reassess the risks to the extent practicable.



DOI will establish and maintain procedures to identify, evaluate, and address any new additional privacy requirements that may result from new statutes, regulations, or policies. DOI will evaluate the privacy risks of any new changes to the application before continuing to utilize it. DOI monitors research or trends in privacy protection technologies or policies that may facilitate new approaches to avoiding or mitigating privacy risks and better protecting PII.

- 7.2 Does the agency provide appropriate notice to individuals informing them of privacy risks associated with the use of the third-party website or application?

This privacy impact assessment provides notice to the public on the privacy implications for use of Medium. Additionally, DOI provides notice of privacy practices through its privacy policy, published system of records notice and privacy impact assessments, which are available on the DOI Privacy Program website at <https://www.doi.gov/privacy/privacy-program>. Where possible, DOI also posts a Privacy Notice on its official social media pages to inform users on how DOI handles information that becomes available through user interactions and directs users to DOI's Privacy Policy.

DOI's Privacy Policy at <https://www.doi.gov/privacy> provides information on the DOI Privacy Program and privacy related policies, notices and activities, and contains information on DOI's social media policy and how DOI handles PII that becomes available through interaction with DOI. The Privacy Policy also informs the public that DOI has no control over access restrictions or privacy procedures on third-party websites, and that individuals are subject to third-party social media website privacy and security policies. DOI's linking policy informs the public that they are subject to third-party privacy policies when they leave a DOI official website to link to third-party web sites.

SECTION 8: Creation or Modification of a System of Records

- 8.1 Will the agency's activities create or modify a "system of records" under the Privacy Act of 1974?

The Department does not collect, maintain or disseminate PII from Medium users, and is not creating a system of records from use of Medium. Any DOI bureau or office that uses Medium in a way that creates a system of records will complete a separate PIA for that specific use and collection of information, and must maintain the records in accordance with DOI-08, Social Networks system of records notice or other applicable system of records notice. DOI Privacy Act notices are available for viewing at the DOI Privacy Program website: <https://www.doi.gov/privacy/privacy-program>.

- 8.2 Provide the name and identifier for the Privacy Act system of records.



Medium Adapted Privacy Impact Assessment

The Department does not collect, maintain or disseminate PII from Medium users, and is not creating a system of records from use of Medium. Any DOI bureau or office that uses Medium in a way that creates a system of records will complete a separate PIA for that specific use and collection of information, and must maintain the records in accordance with DOI-08, Social Networks system of records notice or other applicable system of records notice. DOI Privacy Act notices are available for viewing at the DOI Privacy Program website: <https://www.doi.gov/privacy/privacy-program>.