



Adapted Privacy Impact Assessment

Steller

January 29, 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?

Steller is a web-based privately owned third party social media application that is open to members of the public. Steller is a content sharing platform where images and information posted is widely disseminated. Steller users can create stories, which may include a series of images and text, and can search, share, and comment on the stories within the Steller community.

Steller has a large community of outdoor adventurers, and by becoming a member and using the platform, the Department of the Interior (DOI) will have the ability to promote visits to DOI-managed public lands and recreational sites. DOI will utilize the application to collaborate and share information online with the Steller community to facilitate dialogue, improve customer service, and encourage public participation and collaboration.

Steller users can create content by uploading photos, videos, and text to the Steller application, and by commenting on other users' posts and stories. The content can be viewed (but not downloaded) through the application by other users. DOI will embed the Steller stories it creates on government websites that support DOI-managed public lands for easy viewing of content generated by the community to promote these lands. In addition, Steller would allow parks, refuges and other public land locations to create free flower, animal and trail guides to better serve visitors at national parks and other public lands.

The Department does not actively seek PII through the use of the Steller application, and will only receive minimal amount of PII in order to fulfill a user's request. For example, when a Steller user sends a question to DOI asking about a photo that DOI has uploaded, DOI will be able to view the user name of the individual asking the question.

- 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 collect, maintain, or disseminate PII from Steller users; however, PII is available through interactions with Steller users on the official DOI Steller account and DOI will be able to view any PII that users make available to the Steller community.

Steller users are required to provide an email address, password, and a username in order for them to register as a user of the application, and may also associate a profile image with their user account. When a Steller user likes or comments on a story or post, the user's username, first and/or last name, profile image, and comments will become available to the Steller community and will be visible to DOI. Clicking on a username will lead to other images, stories, or posts associated with the user.

Steller users also have the option of creating Steller accounts using their Facebook or Twitter accounts, in which case, Steller 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. Steller users can control or limit the personal information shared with other users by choosing the private account setting, which would allow the user to approve the individuals who follow their stories. This would limit the exposure or sharing of personal information for the Steller user. Unless the private account setting is turned on, DOI would be able to see the usernames, and any other information users voluntarily provide, such as their names, profile photo, biography, and website.

DOI receives notifications when a Steller user tags DOI's official Steller account, comments on a story, or likes a story, and would be able to see the username, image, or comments shared with DOI. If Steller users tag DOI in their stories or comment on a DOI Steller 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 Steller, or by utilizing their private account setting.

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



Steller users are subject to the Steller privacy policy and terms of service regarding use of their data and how information may be handled and shared.

2.2 What are the sources of the PII?

All PII is voluntarily provided by users when they create an account with Steller, create stories, follow, share or otherwise interact with the Steller 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?

PII is generally not requested, collected or maintained through the use of Steller by DOI. However, if a Steller user or member of the public interacts with DOI through its official Steller account, including commenting on a DOI photo, requests information, or submits feedback through Steller, 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 Steller application where possible and will not collect or maintain the PII.

Any DOI bureau or office that collects PII or uses Steller 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 Steller 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 Steller is to promote travel to public lands and provide better services to visitors to public lands, develop community engagement, and increase government transparency. DOI does not collect, maintain or disseminate PII from individuals who interact with DOI utilizing the Steller 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 Steller, may be used to notify the appropriate agency officials or law enforcement organizations.

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

DOI may share other Steller users' stories with DOI followers to highlight travel to public lands and increase engagement with the Steller community. In addition, if a Steller user or member of the public interacts with DOI through its official Steller account -- including commenting on DOI stories, requesting information, or submitting feedback through Steller -- 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?

Steller is a third-party social media application and a smartphone mobile application. DOI does not collect, maintain, or share PII with other agencies, and is not responsible for how Steller 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 Steller community may be viewed by all members of the public.

DOI does not generally collect, maintain, or share PII available through interactions with Steller users. When a Steller user or member of the public interacts with DOI through its official Steller account by following or commenting on DOI stories, requesting information, or submitting feedback through Steller, 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 Steller, and may be used to notify the appropriate agency officials or law enforcement organizations.

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

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

DOI entered into Terms of Service with Steller, which include the use of advertisements, endorsements, and system security, to address issues related to DOI's official use of the Steller application. 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.

SECTION 5: Maintenance and Retention of PII

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

Generally, PII is not collected or maintained from interactions or use of the Steller application. 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. Records published through Steller 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. 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?

Generally, PII is not collected or maintained through the Steller application. 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 Steller users, except in 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 DOI policy. This information may include username, name, profile photo, images, contents of postings, and other personal information available to DOI through Steller, and may be used to notify the appropriate agency officials or law enforcement organizations. 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?

Steller is a third-party website that is independently operated and controls access to user data within its system. Steller users control access to their own PII via system settings and through discretion with respect to the personal information users provide. Accordingly, users will likely avoid disclosing particularly sensitive PII, which could be used by itself or with other available information to commit fraud or identity theft, or for other harmful or unlawful purposes. However, 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 Steller manages information.

Another privacy risk is third-party advertising and tracking. Steller 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 has no control over how Steller 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 Steller. 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(s) to users on DOI’s data posted in the application.

Another risk is accounts or third party content that misrepresent agency authority or affiliation. Certain accounts or pages on the third-party social media website may not be officially authorized by, or affiliated with DOI, even if they use official insignia or otherwise 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 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.

Finally, 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 of the use of Steller. 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 posted the Privacy Notice below on its official Steller page:

DOI Privacy Notice

The Department of the Interior (DOI) uses Steller, a non-government third party social networking application, to share information, promote public participation, and enhance communication with the public. Your use of the Steller application to communicate with DOI is voluntary, and through your interaction with DOI your personal information may become available. Generally, personal information is not actively collected by DOI; however, if you request information or submit feedback from interaction with DOI through use of Steller, your profile name, image, contact information, and other information may be used to communicate with you or provide the requested information. You should know that any comments, images or videos posted on DOI's official Steller page may be viewed by any Steller user. You are subject to Steller's privacy policy and terms of use during your interactions with DOI on Steller. DOI will not share the information provided with third parties for promotional purposes. Please review the DOI Privacy Policy for how information is handled:
<https://www.doi.gov/privacy>.

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 personally identifiable information that becomes available through interaction on the DOI official website. 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 social media 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?



No, DOI does not collect, maintain or disseminate PII from its use of Steller. Any DOI bureau or office that creates a system of records from use of Steller 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.

DOI does not collect, maintain or disseminate PII from its use of Steller. Any DOI bureau or office that creates a system of records from use of Steller 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>.