



Adapted Privacy Impact Assessment

Schemer

May 15, 2012

Contact

Departmental Privacy Office
U.S. Department of the Interior
1849 C Street NW
Mail Stop 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 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?

Schemer is a social media application owned and operated by Google Inc. that is used for sharing and discovering activities for individuals to do (referred to as "schemes"), including events to attend and places to visit. Schemer is available both through the Internet and through mobile applications for Android and iOS operating systems. Users can list things they want to do, share their list items with other users and mark items as done. When a user posts a scheme, other users can post comments on the scheme.

Schemer will provide the Department of the Interior (DOI) with the opportunity to promote various events and locations, such as national parks, festivals, and special events as well as disseminating information to the public, enhancing communication, fostering and sharing ideas, promoting public participation and collaboration, and increasing government transparency.

The primary account holder is the Department of the Interior Office of Communications, which will be responsible for ensuring official information posted on the Department's Schemer page by Department officials or employees is appropriate and approved for public dissemination. DOI bureaus and offices are also responsible for ensuring official information posted on bureau or office Schemer pages is appropriate and approved for public dissemination in accordance with applicable laws, regulations, and DOI privacy, security and social media policies.

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 for the use of the third-party website or application?

Presidential Memorandum on Transparency and Open Government, January 21, 2009; OMB M-10-06, Open Government Directive, December 8, 2009; OMB M-10-23, Guidance for Agency Use of Third-Party Websites and Applications, June 25, 2010; the Paperwork Reduction Act, 44 U.S.C. 3501; the Clinger-Cohen Act of 1996, 40 U.S.C. 1401; OMB Circular A-130; 210 Departmental Manual 18; 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?

In order to join Schemer, a user must be a member of Google+, and provide a username and password, which is used to log in to Schemer. Profile information for the user is automatically pulled from Google+. Users must establish and edit their profiles through Google+; separate Schemer profiles cannot be set up. The Department holds an official DOI Google+ account and has completed a separate Google+ Adapted Privacy Impact Assessment for its use of the Google+ application. The Google+ Adapted Privacy Impact Assessment addresses how DOI handles the personal information made available through the use of Google+ and associated privacy considerations; therefore, the Google+ privacy assessment is not reiterated here, but may be viewed at: http://www.doi.gov/ocio/information_assurance/privacy/ppia.cfm.

Schemer users are required to provide some additional information to augment their Google+ profile data, including a “home base”, which is either the user’s full address or city and state of residence. Users can also add other preferred locations in addition to their home base. The home base and other locations are not visible to other users, but are utilized to match users with local schemes. In addition, Schemer users can identify their interests by checking off various subjects from a list, from items such as “natural wonders”, “street food” and “running”. These interests are visible to other users, and are also used by Schemer to match users with potentially interesting schemes.

Schemer users can communicate by posting and commenting on various schemes. Schemer also provides links to users’ Google+ profiles, which allows users to engage in further communication through Google+. Through these interactions with users on DOI’s official Schemer page and from comments posted by Schemer users, personally identifiable information (PII) may become available to DOI, including name, profile photo, contents of comments, Google+ profile information, geographic location for mobile application users, or other personal information provided by the user.

The Department does not request, collect or share PII from the use of Schemer. However, there may be unusual circumstances where there is 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 name, profile photo, content of comments, Google+ profile information, geographic location for mobile application users, or other personal information provided by the user, and may be used to notify the appropriate agency officials or law enforcement organizations.

The use of Schemer is governed by Google’s universal Terms of Service and Privacy Policy. Pursuant to the Terms of Service and Privacy Policy, information provided by users of one Google service, including PII, may be combined or integrated into other Google services. As a result, PII provided by a user in another Google service, such as Google+, could become available to DOI through Schemer. Google users can set their own privacy settings and exhibit control over some of the personal information tied to the user’s Google account and whom that information is shared with. In general, DOI is likely to have access to users’ Google+ profile information through the use of Schemer, including name, profile picture, and any other personal information provided by the user.



2.2 What are the sources of the PII?

Sources of information are Schemer users world-wide, including members of the general public and Federal employees, and may include other government agencies and private organizations.

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

PII may become available to DOI through interactions with users on Schemer; however, DOI does not request or collect PII from users of Schemer. If a Schemer user interacts with DOI by commenting on any of the schemes posted by DOI, their name, profile photo, content of comments, Google+ profile information, or other personal information provided by the user may become available to DOI and may be used to interact with the user, or to provide any requested information or service. There may be unusual circumstances where there is 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 name, profile photo, content of comments, Google+ profile information, geographic location for mobile application users, or other personal information provided by the user, and may be used to notify the appropriate agency officials or law enforcement organizations.

Any DOI bureau or office that uses Schemer in a way that creates a system of records must complete a separate PIA for the specific use and collection of information, and must maintain the records in accordance with DOI-08, Social Networks system of records notice. DOI Privacy Act system of records notices may be viewed at: http://www.doi.gov/ocio/information_assurance/privacy/privacy-act-notices-9-06-06.cfm.

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 Schemer to survey the public or in any manner that would trigger the requirements of the Paperwork Reduction Act.

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 uses Schemer to promote various events and locations, such as national parks, festivals, and special events, as well as to disseminate information to the public, enhance communication, promote public participation and collaboration, and increase government transparency. User interactions with DOI on Schemer may include name, profile photo, comments, Google+ profile information, or other personal information provided by the user. This information may be used to interact or communicate with users or to provide any requested information or service. Also, in cases where there is evidence of criminal activity, a threat to the government or the public, or an employee violation of DOI policy, the information provided, including name, profile photo, contents of comments, Google+ profile information, geographic location for mobile application



users, or other personal information, 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.

If a user interacts with DOI, requests information or submits feedback through Schemer, their name, profile photo, contents of comments, or other user provided personal information, may be used to interact with the user or to provide additional information on DOI programs or services. Also, there may be cases where there is evidence of criminal activity, a threat to the government or the public, or an employee violation of DOI policy. This information may include name, profile photo, contents of comments, Google+ profile information, geographic location for mobile application users, or other user provided personal information, and may be used to notify the appropriate agency officials or law enforcement organizations.

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?

Schemer is a third party social networking application used by individuals and organizations world-wide, including Federal, Tribal, State and local agencies who may have access to the data posted by users in Schemer. DOI does not collect PII or share PII with these other agencies and is not responsible for how they may access or use Schemer data. However, there may be cases where there is evidence of criminal activity, a threat to the government, a threat to the public, or an employee violation of DOI policy. These incidents may include name, profile photo, contents of comments, Google+ profile information, geographic location for mobile application users, or other personal information provided by the user, 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?

Official mission related information posted on Schemer by DOI is reviewed and approved for public dissemination prior to posting so any privacy risks for the unauthorized disclosure of personal data by the Department is mitigated. DOI does not control the content on Schemer, except for official DOI postings.

Schemer users are subject to Google's Privacy Policy and Terms of Service, and must exercise user discretion regarding the information provided and their privacy settings. However, the provision of information and user consent applies only to terms of use for Google applications. DOI has no control over access restrictions or procedures for Google's services, or over content posted in Schemer and the personal information provided by users. Google is responsible for protecting its users' privacy and the security of the data in the application. Schemer users can control access to their own PII, generally via privacy settings. There could potentially be millions of users of Google's services who have access to information posted on Schemer, including the general public, Federal employees, private organizations, and Federal, State, Tribal and local agencies.



SECTION 5: Maintenance and Retention of PII

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

DOI does not collect or maintain PII from Schemer users. Retention periods for official postings vary as records are maintained in accordance with the applicable records schedule for each specific type of record maintained by the Department. Records published through Schemer represent public informational releases by the Department, and must be assessed on a case-by-case basis depending on the individual/entity 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, tearing, 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 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 Schemer users. In unusual cases there may be 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 name, profile photo, contents of comments, Google+ profile information, geographic location for mobile application users, or other personal information provided by the user, 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 2.51 and applicable DOI privacy and security policies.



Access to DOI's network is restricted to authorized users with password 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 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?

The official information posted by DOI has been reviewed and approved for public dissemination so any privacy risk of unauthorized disclosure of personal data by the Department is mitigated. Except for official postings, DOI has no control over the information or user content posted in Schemer. DOI does not have any control over personal information posted by individual Schemer users, including members of general public and Federal employees. DOI systems do not share data with the Schemer application.

Schemer is a Google service and is an independently operated third party application that controls access to user data within its systems. Schemer users can control access to their own PII, generally via system settings. DOI has the same access as any other user, and DOI cannot prevent or ensure that users do not disclose PII on DOI's Schemer site.

Schemer's mobile applications present concerns related to geolocation functions and geospatial privacy concerns. Users who create posts indicating that they are at a specific location are potentially creating a public record of their geographic location. The utilization of Schemer's mobile application can create a real time identification of a user's location. Users have the option not to use the Schemer mobile application.

DOI cannot guarantee a specific level of privacy protection or security for third party applications. Users concerned about privacy, including location-based privacy matters, may take various steps, including adjusting profile settings, to prevent access to their PII, but DOI makes no representation about the effectiveness of the settings options offered by Google. Schemer users are advised to review Google's Terms of Service and Privacy Policy prior to use.

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

DOI's Privacy Policy informs the public on how DOI handles PII 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 those 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. The DOI Privacy Policy may be viewed at <http://www.doi.gov/privacy.cfm>.



DOI has posted a Privacy Notice on its official Google+ profile which is visible by Schemer users, and which informs users that Google+ is a non-government third party application. It also informs users on how DOI handles PII that becomes available through user interaction, and directs users to the DOI Privacy Policy for information handling practices.

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 Schemer. Any DOI bureau or office that creates a system of records from use of Schemer 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, which may be viewed at http://www.doi.gov/ocio/information_assurance/privacy/privacy-act-notices-9-06-06.cfm.

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

DOI does not collect, maintain or disseminate PII obtained from the use of Schemer. Any DOI bureau or office that creates a system of records from use of Schemer will complete a separate PIA for that specific use and must maintain the records in accordance with DOI-08, Social Networks system of records notice which may be viewed at http://www.doi.gov/ocio/information_assurance/privacy/privacy-act-notices-9-06-06.cfm.