

Department-Wide Social Media Uses

Third Party Application Privacy Impact Assessment

Department of State Privacy Coordinator Bureau of Administration Global Information Services Office of Information Programs and Services	Social Media Sites: Blog Twitter Tumblr Flicker Instagram Facebook Google+ YouTube
--	---

1) Purpose of the Department of State’s use of a third-party website or application. (Henceforth, third-party website or applications will be referred to as third party applications.)

(a) Give a general description of the third party application.

This Privacy Impact Assessment (PIA) covers all authorized third party social media websites and applications used by the Department of State (DoS) and the diplomatic missions of the United States. Social media technologies take on many different forms including blogs, forums, microblogs, and photo sharing. They are tools that allow for the creation, sharing or exchange of user-generated information, ideas, and pictures/videos in virtual communities and networks.

The social media websites and applications covered by this PIA do not solicit, collect, maintain, or disseminate sensitive personally identifiable information (PII) from individuals who interact with these authorized social media websites and applications. Public Diplomacy and Public Affairs is the primary account holder of DoS accounts on these social media web sites. As such, they will be responsible for ensuring that information posted to these websites is appropriate and approved for public dissemination.

(b) What is the specific purpose for using the third-party application and how does this purpose assist in accomplishing the Department’s mission?

The Department of State uses various third-party social media websites and applications to share information with the public and foreign audiences to promote the foreign policy of the United States and its U.S. diplomacy efforts. Social media is used to engage in dialogue, share information and media, and collaborate. Third-parties control and operate these non-governmental websites; however, DoS may use them as alternative channels to provide robust information and to engage with the public. DoS may also use these websites to make information and services widely available, while promoting transparency and accountability, as a service for those seeking information about, collaboration with, or services from DoS. In light of the vast capabilities of social media web services, DoS leverages these applications in

Department Wide Social Media Uses

order to enhance its ability to communicate with the public, as well as increase government transparency and promote public participation and collaboration through a more efficient, streamlined process of information dissemination to the public. DoS has created official accounts on the several social media web services listed on the title page. The official accounts on these social media web services will be used as a mechanism to provide mission-related information to the public.

(c) Is the use of the third-party application consistent with all applicable laws, regulations, and policies?

Yes, use of third party applications is consistent with all applicable laws, regulations, and policies.

(d) What federal authorities permit the collection of information for the intended purpose of this application?

5 U.S.C. 301, Management of Executive Agencies.

2) Personally Identifiable Information (PII) available through the use of the third-party application.

(a) What PII will be made available to the Department?

Although the DoS does not solicit, collect, maintain, or disseminate PII from visitors to these third-party social media websites or applications, it is possible for individuals to voluntarily make such information available to agencies. Typical examples of the types of PII that may become available to agencies include names of individuals and businesses, images from photos or videos, screen names, email addresses, etc.

In addition, many third-party social media websites or applications request PII at the time of registration. The process will vary across third-party social media websites or applications and often users can provide more than is required for registration. For example, users can provide such information as his or her interests, birthday, religious and political views, family members and relationship status, education, occupation and employment, photographs, contact information, and hometown. If the privacy setting on the third-party social media website or application is not restricted, such information may be made available to the Department.

Information provided to third-party social media websites or applications during registration is not collected or used by DoS. The Department does not ask individuals to post information on its websites or applications. Information that individuals voluntarily submit as part of the registration process is not the property of DoS and the Department will not solicit this information.

(b) What are the sources of the PII?

In addition to information provided to the third-party social media website or application during registration, other sources of PII may include screen names, information provided in comments, links, postings, and uploaded audio/video files.

Department Wide Social Media Uses

Other activities conducted on the third-party social media website or application, such as “friend-ing,” “following,” “liking,” joining a “group,” becoming a “fan,” and comparable functions, can also be a source of PII in the system.

(c) From which individuals is the information collected?

DoS does not solicit, collect, maintain, or disseminate personally identifiable information from these third-party social media websites or applications. However, PII that is voluntarily provided by an individual may be used by an agency to respond to inquiries, answer questions, or fulfill a request submitted by the individual.

(d) Does this collection of information require compliance with the Paperwork Reduction Act (PRA) and, if so, how will the Department comply with the statute?

No. Items collected by third party social media websites and applications that are not collecting information on behalf of the Federal government are not subject to the PRA.

3) Intended or expected use of PII

(a) How will the Department use the PII described in Section 2 above?

While DoS uses social media websites and applications as platforms for communicating their message to reach as many people as possible or to target specific audiences, the Department does not collect, maintain, or disseminate PII from individuals who interact with any DoS social media website or application.

(b) Provide specific examples of how the PII may be used.

DoS may use a person’s screen name, email address, or other information provided by the user to respond to specific comments or questions directed to or about agency activities, or to fulfill a request. In such situation, only the minimum required information that is needed to appropriately respond is used.

4) Sharing or disclosing PII

(a) With what entities or persons inside or outside the Department will the PII be shared and for what purpose will the PII be disclosed?

DoS does not share PII that is made available through its third-party websites internally or with outside entities.

(b) How will the PII be transmitted or disclosed to internal or external entities or persons?

DoS does not transmit PII that is made available through its third-party websites internally or with outside entities.

(c) What safeguards will be in place to prevent uses other than those legally authorized and described in this PIA? Only approved workforce members from the Department have access to manage official Department websites and

Department Wide Social Media Uses

applications. 5 FAM 792 codifies the Department's official use of social media. Each workforce member with access must comply with the FAM.

5) Maintenance and retention of PII

(a) How will the Department maintain the PII and for what time period?

DoS does not collect, maintain, or disseminate PII from individuals who interact with any of its websites or applications that are covered by this PIA. If a user submits PII in a request or an inquiry to an agency through the agency's website, the agency may use the PII provided by the user to fulfill the specific request. Although the PII may be maintained by the third-party website or application, it is not maintained by the agency.

(b) Is there a records disposition schedule covering this collection? If so, what is the retention period?

DoS does not collect, maintain, or disseminate PII that is made available on any of its websites or applications covered by this PIA, therefore, a records disposition schedule is not required.

6) Securing PII

(a) Will the Department's privacy and security officials collaborate to develop methods for securing PII?

DoS has established that no PII from the Department's websites or applications covered by this PIA will be collected, maintained, or disseminated.

When interacting with DoS or others on a third-party website or application, PII that users share or disclose may become available to other users or any individuals with access to the website. In order to mitigate the risks of disclosure of sensitive PII, to the extent possible, the agency may choose to delete or hide comments or other user interactions when a user's sensitive information is included.

(b) Describe how a user will access the third party application.

Users can access many sites without registering and simply viewing the third-party website or application as a visitor. For example, a Facebook account is not required to view the Department's page on this website.

7) Identifying and mitigating other privacy risks

What other privacy risks exist and how will the Department mitigate those risks?

Disclosure of PII by users: When interacting on a social media website (e.g., posting comments), PII that users share or disclose will ordinarily become available to other users or anyone else with access to the site. Most users will likely avoid disclosing particularly sensitive or confidential PII (e.g., Social Security or credit

Department Wide Social Media Uses

card number), 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 those risks, where possible, DoS provides appropriate notice to users on the third-party social media website itself, warning them to avoid sharing or disclosing any sensitive PII when interacting with the agency on the website. Users should also review the privacy policies of any third-party social media providers to determine if they wish to utilize that social media.

Third-party advertising and tracking: A third-party website operator may display advertising or other special communications on behalf of other businesses, organizations, or itself when a user interacts with the Department on the website. If the user clicks on the advertisement or reads the communication to learn about the advertised product or service, the user's 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.

Individuals falsely claiming to be Official pages: A malicious individual may set up a third-party social media website and claim for it to be an official Department webpage. To negate these false sites, all Department third-party social media websites have standard branding. This branding allows the public to know that this is an official Department website, and that they can trust the information that is on it.

Spam, unsolicited communications, spyware, and other threats: Users may also receive spam or other unsolicited or fraudulent communications as a result of their interactions with the Department on third-party social media websites. 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.

8) Creating or modifying a system of records

Department Wide Social Media Uses

- (a) Is there an existing system of records to cover this collection of records as required under the Privacy Act of 1974?**

Since DoS does not collect, maintain, or disseminate PII from individuals who interact with any of its websites or applications that are covered by this PIA and information cannot be retrieved by a personal identifier there is no requirement for a Privacy Act System of Records Notice.

- (b) If “yes” to the question above, which system of records notice (SORN) covers this collection?**

If DoS did collect, maintain, or disseminate PII from individuals and retrieved this information by a personal identifier then the applicable notice would be State-79, Digital Outreach and Communications.

If there is no existing Department SORN to cover this collection, one must be created. Please contact SornTeam@state.gov for guidance.

- (c) Is notice provided to the record subjects, other than through the SORN (e.g., through a Privacy Act statement or privacy notice)?**

The Department provides notice about its third-party website and application use in the Privacy Policy appearing on www.state.gov.