Privacy Impact Assessment
for Third-Party Social Web Services

Office of Public Affairs

September 28, 2009

Contact Point
Tracy Russo
Office of Public Affairs
Department of Justice
(202) 514-2007

Reviewing Official
Vance Hitch
Chief Information Officer
Department of Justice
(202) 514-0507

Approving Official
Nancy C. Libin
Chief Privacy and Civil Liberties Officer
Department of Justice
(202) 307-0697

Introduction

Web 2.0 applications are web-based applications that can provide enhanced information sharing, collaboration, and decision-making by facilitating horizontal communication among multiple users. "Third-party social web services" are one type of Web 2.0 application that utilizes interactive, public websites to connect users with shared interests and/or common activities. Examples of well-known third-party social web services include Facebook, YouTube, MySpace, and Twitter. Facebook, which is based on personal connections, allows for a variety of types of content to be shared by users. In comparison, YouTube is a network that connects users based on shared video content, and Twitter allows users to publish and receive short messages, a process commonly referred to as "microblogging".

In light of the vast capabilities of third-party social web services, the Department of Justice ("Department" or "DOJ") developed a process to leverage these applications in order to enhance the Department's 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. As an initial step in this process, the Department has created official accounts on several third-party social web services, including Facebook, YouTube, MySpace, and Twitter. In the future, the Department may utilize other similar third-party social web services.

The Department's official accounts on these third-party social web services will be used as a mechanism to provide mission-related information to the public. The Department's Office of Public Affairs ("OPA") will be the primary account holder of the Department's accounts on these third-party social websites. As such, OPA will be responsible for ensuring that information posted to these websites is appropriate and approved for public dissemination. Additionally, the Department has created a Web 2.0 policy working group to review issues pertaining to the Department's use of Web 2.0 applications and third-party social web services in order to ensure that the Department's uses are in accordance with applicable laws, policies, and regulations.

Because the accounts that the Department will open on these third-party websites are not a part of the Department's internal information systems nor will they be operated by a contractor of the Department, the Department does not and will not collect information from individuals when individuals interact with the Department's social web accounts. While it may appear that information posted by third parties on the Department's accounts is the Department's information, such third-party postings are technically and factually under the dominion of the third-party social websites. Further, although individual third-party social websites may require individuals to register with the site in order to access various accounts, the Department does not collect, maintain, or disseminate information provided by individuals to these social websites. Any information that users provide to register on third-party social websites is voluntarily contributed and is not maintained by any Department of Justice entity. Although the Department does not collect, maintain, or disseminate an individual's personally identifiable information ("PII") in relation to the Department's accounts on third-party social web services, the Department completed this Privacy Impact Assessment in order to identify any potential privacy issues and provide transparency to the public regarding the Department's accounts on such third-party social websites.

Section 1.0
The System and the Information Collected and Stored within the System.

The following questions are intended to define the scope of the information in the system, specifically the nature of the information and the sources from which it is obtained.

1.1 What information is to be collected?

The Department does not collect, maintain, or disseminate PII from individuals who interact with the Department's accounts on third-party social websites.[1] Although some social websites, such as YouTube, Facebook, MySpace, and Twitter, may request information, such as a name, email address, and birth date, at the time of registration, the Department does not collect, maintain, or disseminate this information. In addition, the Department does not collect, maintain, or disseminate PII from individuals who interact with the Department's account.

The Department will use third-party social websites to disseminate mission-related information that OPA has collected and approved for public dissemination. The Department does not own, manage, or control the applications used on third-party social websites. Prior to its dissemination, Departmental information may be captured and maintained in Department-controlled information systems.

1.2 From whom is the information collected?

The Department does not collect, maintain, or disseminate PII from individuals who interact with the Department's accounts on the third-party social websites. Although social websites may collect PII from individuals, the Department does not collect, maintain, or disseminate this information.

Section 2.0
The Purpose of the System and the Information Collected and Stored within the System.

The following questions are intended to delineate clearly the purpose for which information is collected in the system.

2.1 Why is the information being collected?

The Department does not collect, maintain, or disseminate PII from individuals who interact with the Department's social web accounts.

[1] Of course, information posted by the public on these third-party social websites is information that is in the public domain, and to the extent that any content posted indicates a violation or potential violation of law (e.g., a threat of criminal action or harm to national security), the Department will take appropriate action, as would be taken with any other such information in the public domain.

2.2 What specific legal authorities, arrangements, and/or agreements authorize the collection of information?

Not applicable. The Department does not collect, maintain, or disseminate PII from individuals who interact with the Department's social web accounts.

2.3 Privacy Impact Analysis: Given the amount and type of information collected, as well as the purpose, discuss what privacy risks were identified and how they were mitigated.

Not applicable. The Department does not collect, maintain, or disseminate PII from individuals who interact with the Department's social web accounts.

With regard to information collected to be posted to third-party social websites, OPA is the primary account holder for these websites, and as such, will ensure that information disseminated via such websites is vetted and approved for public dissemination in accordance with applicable laws, regulations, and policies. Accordingly, any privacy risks concerning unauthorized disclosure of personally identifiable information via third-party social websites by the Department should be mitigated.

Section 3.0
Uses of the System and the Information.

The following questions are intended to clearly delineate the intended uses of the information in the system.

3.1 Describe all uses of the information.

The Department does not collect, maintain, or disseminate PII from individuals who interact with the Department's social web accounts. Rather, the Department's accounts on third-party social websites are for the purpose of disseminating mission-related information to the public.

3.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern? (Sometimes referred to as "data mining".)

No. The Department does not collect, maintain, or disseminate PII from individuals who interact with the Department's social web accounts.

3.3 How will the information collected from individuals or derived from the system, including the system itself, be checked for accuracy?

The Department does not collect, maintain, or disseminate PII from individuals who interact with the Department's social web accounts.

With regard to the information disseminated on the third-party social websites, OPA will check the accuracy of that information during the review, editorial, and disclosure approval process.

3.4 What is the retention period for the data in the system? Has the applicable retention schedule been approved by the National Archives and Records Administration (NARA)?

Although the Department does not collect, maintain, or disseminate PII from individuals who interact with the Department's social web accounts, the Department does disseminate information regarding the Department's activities, which may be of interest to the public, through the Department's social web accounts. In accordance with the Federal Records Act, the Department is currently developing a records retention schedule for Departmental records that are posted to third-party social websites.

3.5 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

The Department does not collect, maintain, or disseminate PII from individuals who interact with the Department's social web accounts. Because the Department's accounts on these third-party social websites are created in order to disseminate mission-related information to the public, OPA will follow current internal policies and procedures for disseminating such information to the public and ensure that disclosures are in accordance with applicable laws, regulations, and policies before the Department uses these accounts as a mechanism for public disclosure of information.

After information is posted to the Department's accounts on these third-party social websites, the privacy and security policies of the public websites control the information as posted to those sites.

Section 4.0
Internal Sharing and Disclosure of Information within the System.

The following questions are intended to define the scope of sharing both within the Department of Justice and with other recipients.

4.1 With which internal components of the Department is the information shared?

The Department does not collect, maintain, or disseminate PII from individuals who interact with the Department's social web accounts. Thus, information is not shared with internal Department components.

4.2 For each recipient component or office, what information is shared and for what purpose?

Not applicable. The Department does not collect, maintain, or disseminate PII from individuals who interact with the Department's social web accounts.

4.3 How is the information transmitted or disclosed?

Not applicable. The Department does not collect, maintain, or disseminate PII from individuals who interact with the Department's social web accounts.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

Not applicable. The Department does not collect, maintain, or disseminate PII from individuals who interact with the Department's social web accounts.

Section 5.0
External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DOJ which includes foreign, Federal, state and local government, and the private sector.

5.1 With which external (non-DOJ) recipient(s) is the information shared?

The Department has created accounts on the aforementioned third-party social websites for the purpose of disseminating mission-related information to the public. Therefore, the Department will share mission-related information that has been vetted and approved for official dissemination to anyone who may have the capabilities to access the posts via the third-party social websites.

5.2 What information is shared and for what purpose?

As stated above, the Department intends to share mission-related information that has been vetted and approved for dissemination to the public.

5.3 How is the information transmitted or disclosed?

The mission-related information will be transmitted or disclosed via the Department's accounts on these third-party social websites.

5.4 Are there any agreements concerning the security and privacy of the data once it is shared?

No. Information will be vetted and approved for dissemination to the public. Because the purpose behind the Department's presence on the third-party social websites is to transmit information to the public, agreements concerning the security and privacy of data would not be necessary.

5.5 What type of training is required for users from agencies outside DOJ prior to receiving access to the information?

As the information posted to these third-party social websites is intended for public dissemination, no training for users of outside agencies is required.

5.6 Are there any provisions in place for auditing the recipients' use of the information?

As the information posted to these third-party social websites is intended for public dissemination, auditing the recipients' use of the information is unnecessary.

5.7 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

As stated above, the Department will use its accounts on third-party social web services as an additional mechanism for disseminating vetted and approved mission-related information to the public. OPA will ensure that information disseminated via these websites has been approved for public dissemination. Through this vetting process, OPA conducts a review of any potential privacy risks before disclosing information that may personally identify an individual pursuant to applicable laws, polices, and regulations. Accordingly, risks associated with unauthorized disclosure of personally identifiable information should be mitigated.

Section 6.0
Notice

The following questions are directed at notice to the individual of the scope of information collected, the opportunity to consent to uses of said information, and the opportunity to decline to provide information.

6.1 Was any form of notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice.) If notice was not provided, why not?

With regard to the Department's accounts on third-party social websites, the Department does not collect, maintain, or disseminate any information from individuals who interact with the Department's third-party social web accounts. The Department provides notice on its third-party social website accounts explicitly stating that these accounts are not part of the Department's government-operated website.

With regard to notice to individuals who provide information to the Department that may be disseminated via the Department's accounts on third-party social websites, the Department provides notice to such individuals and obtains consent when necessary and applicable, in accordance with law, regulations, and policies.

6.2 Do individuals have an opportunity and/or right to decline to provide information?

The Department does not collect, maintain, or disseminate PII from individuals who interact with the Department's social web accounts. If an individual chooses to provide information to the social website through registration or other interaction with the site, such actions are between the individual and the third-party social websites.

With regard to information provided to be disseminated via the Department's accounts on the public websites, the Department provides an opportunity to decline to provide information when practicable and as required by law.

6.3 Do individuals have an opportunity to consent to particular uses of the information, and if so, what is the procedure by which an individual would provide such consent?

The Department does not collect, maintain, or disseminate PII from individuals who interact with the Department's third-party social website accounts.

With regard to information provided to be disseminated via the Department's accounts on the public websites, the Department obtains consent when practicable and as required by law from individuals who provide such information.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

The primary privacy risk associated with the Department's use of third-party social websites is unauthorized disclosure of personally identifiable information. Because the Department has a procedure for vetting and approving the content prior to posting on the websites, this privacy risk should be mitigated. Additionally, notice is given to and consent is obtained from individuals who provide information to be posted to the Department's accounts.

A secondary privacy risk is that individuals who interact with the Department via these accounts may believe that they are submitting information to the Department when posting information on these accounts. To prevent any misunderstanding, the Department will provide notice on its accounts to ensure that the public is aware that it is not interacting with a Department-operated website.

Section 7.0
Individual Access and Redress

The following questions concern an individual's ability to ensure the accuracy of the information collected about him/her.

7.1 What are the procedures which allow individuals the opportunity to seek access to or redress of their own information?

The Department does not collect, maintain, or disseminate PII from individuals who interact with the Department's social web accounts. If an individual desires to seek access to or redress of information provided by the Department for disclosure to the public through the third-party social website, the individual should contact OPA. With regard to other information that may appear on the Department's accounts on the third-party social websites that was not posted by the Department, the individual should follow the procedures established by the site for such actions.

7.2 How are individuals notified of the procedures for seeking access to or amendment of their information?

The Department does not collect, maintain, or disseminate PII from individuals who interact with the Department's social web accounts. With regard to Department information that is posted to third-party social web accounts, OPA, which approves all information posted, has published its contact information and procedures on its webpage.

7.3 If no opportunity to seek amendment is provided, are any other redress alternatives available to the individual?

The Department does not collect, maintain, or disseminate PII from individuals who interact with the Department's social web accounts. With regard to Department information that is posted to third-party social web accounts, OPA, which approves all information posted, has published its contact information and procedures, to the extent applicable, on its webpage.

7.4 Privacy Impact Analysis: Discuss any opportunities or procedures by which an individual can contest information contained in this system or actions taken as a result of agency reliance on information in the system.

The Department does not collect, maintain, or disseminate PII from individuals who interact with the Department's third-party social web accounts. Nor does the Department intend to rely on information that has been posted by the public on the Department's third-party social web accounts. With regard to Department information that is posted to third-party social web accounts, OPA, which approves all information posted, has published its contact information and procedures on its webpage. With regard to other information that may appear on the Department's accounts on the third-party social websites and that was not posted by the Department, the individual should follow the procedures established by the site for such actions.

Section 8.0
Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 Which user group(s) will have access to the system?

The Department does not own or control access to the third-party social websites. If an individual desires to seek information about a social website's technical access and security, the individual should direct those inquiries to the social website administrator.

8.2 Will contractors to the Department have access to the system? If so, please submit a copy of the contract describing their role with this PIA.

Not Applicable.

8.3 Does the system use "roles" to assign privileges to users of the system?

Not Applicable.

With regard to information posted to the Department's accounts, OPA holds the accounts and will post information to them on behalf of the Department.

8.4 What procedures are in place to determine which users may access the system and are they documented?

Not Applicable.

Currently, OPA is the Department's account holder on the third-party social websites, and as such, has sole access to the accounts on these public websites. The Department has established a Web 2.0 policy working group to discuss issues that may arise with the Department's presence on these websites.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

Not Applicable.

8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?

Not Applicable.

8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

Not Applicable.

Because OPA will post information to the Department's accounts of these third-party social websites, OPA is provided training with regard to public dissemination of information by the Department. Additionally, the Department's Web 2.0 policy working group, of which OPA is a part, will continue to review issues as they arise with the Department's presence on these websites.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

Not Applicable.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

Not Applicable. The Department does not own or control access to the third-party social websites.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 Were competing technologies evaluated to assess and compare their ability to effectively achieve system goals?

The Department does not own or control access to the third-party social websites. If an individual desires to seek information about a social website's use of technology, the individual should direct those inquiries to the social website administrator.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

Not Applicable.

9.3 What design choices were made to enhance privacy?

Not Applicable.

Conclusion

The Department of Justice created accounts on several third-party social websites, including YouTube, Facebook, MySpace, and Twitter, as a mechanism to provide mission-related information to the public. Because the accounts that the Department will open on these websites are not a part of the Department's internal information systems nor will they be operated by a contractor of the Department, the Department does not and will not collect information from individuals when individuals interact with the Department's social web accounts. No personally identifiable information is requested by the Department when the user interacts with a Department account. Although individuals may voluntarily contribute their information to the third-party social websites with the intent to share the information with others on the website, the Department does not collect, maintain, or disseminate this information. Moreover, individuals who visit and interact with Department of Justice accounts are usually familiar with third-party social websites and are already registered members of the websites before they interact with a Department account; thus, these individuals are aware of the voluntary nature of participation in these sites. Finally, OPA has established procedures for properly vetting and approving the public dissemination of information via the Department's accounts on these websites. As such, the risks associated with unauthorized disclosure of personally identifiable information via these websites should be mitigated.

Responsible Official

_____/s/_____ Date 9/28/09

Tracy Russo
New Media Specialist

Office of Public Affairs
Department of Justice

Reviewing Official

_____/s/_____ Date 9/28/09

Vance Hitch
Chief Information Officer

Office of the Chief Information Officer
Department of Justice

Approving Official

_____/s/_____ Date 9/28/09

Nancy C. Libin
Chief Privacy and Civil Liberties Officer

Office of the Deputy Attorney General
Department of Justice