Department of Justice

Adapted Privacy Impact Assessment
for
Use of Third-Party Social Media Tools to Communicate with the Public

Issued by:
[Wyn Hornbuckle,
Deputy Director, Office of Public Affairs (PAO),
PAO Senior Component Official for Privacy]

Approved by: Peter A. Winn, Acting Chief Privacy and Civil Liberties Officer, Department of Justice

Date approved: [July 25, 2017]

(May 2015 DOJ PIA Form)

EXECUTIVE SUMMARY

In accordance with the President's Memorandum on Transparency and Open Government, issued on January 21, 2009,[1] and the Office of Management and Budget (OMB) Memorandum M-10-06, *Open Government Directive*, issued on December 8, 2009,[2] the United States Department of Justice (DOJ or "Department") is permitted to utilize third-party social websites and applications ("social media tools"),[3] such as YouTube, Facebook, LinkedIn, Twitter, and Instagram, as a mechanism to provide mission-related information to the public. The Department is pleased to participate in open, un-moderated forums offered by social media tools in order to increase government transparency, promote public participation, and encourage collaboration with the Department.

In accordance with OMB Memorandum M-10-23, an "adapted" Privacy Impact Assessment (PIA) is required whenever an agency's use of a third-party website or application makes personally identifiable information (PII) available to the agency.[4] In general, each adapted PIA should be posted on the agency's official website and should include: (1) the specific purpose of the agency's use of the social media tools; (2) how the agency will use PII that becomes available through the use of the social media tools; (3) who at the agency will have access to PII; (4) with whom PII will be shared outside the agency; (5) whether and how the agency will maintain PII, and for how long; (6) how the agency will secure PII that it uses or maintains; and (7) what other privacy risks exist and how the agency will mitigate those risks. Based on the changing landscape of the Department's use of social media tools to communicate with the public, the Department-wide adapted PIA for Third-Party Social Media Web Services is being revised.[5]

---

[1] This Memorandum can be found at: https://obamawhitehouse.archives.gov/the-press-office/transparency-and-open-government.

[2] This Memorandum can be found at: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2010/m10-06.pdf.

[3] The terms "third-party websites or applications" and "social media tools" refer to "web-based technologies that are not exclusively operated or controlled by a government entity, or web-based technologies that involve significant participation of a nongovernment entity. Often these technologies are located on a '.com' website or other location that is not part of an official government domain. However, third-party applications can also be embedded or incorporated on an agency's official website." *See* OMB Memorandum M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications* (June 25, 2010) [hereinafter OMB Memorandum M-10-23] (citations omitted), https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2010/m10-23.pdf.

[4] The term "make PII available" includes "any agency action that causes PII to become available or accessible to the agency, whether or not the agency solicits or collects it. In general, an individual can make PII available to an agency when he or she provides, submits, communicates, links, posts, or associates PII while using the website or application. 'Associate' can include activities commonly referred to as 'friend-ing,' 'following,' 'liking,' joining a 'group,' becoming a 'fan,' and comparable functions." *See* OMB Memorandum M-10-23 at 8.

[5] This adapted PIA is limited to the Department's use of social media tools to communicate with the public. The personal use of social media by Department employees; use of social media during the course of civil or criminal investigations or litigation; and use of social media for exclusively internal communications are not addressed by this adapted PIA. In narrow circumstances, the Department's law enforcement and national security responsibilities may require the use of social media tools for operational purposes, in accordance with law and Department policies. Such operational uses are not addressed by this adapted PIA. *See* CIO Council, *Privacy Best Practices for Social Media Use* (2013), https://cio.gov/wp-content/uploads/downloads/2013/07/Privacy-Best-Practices-for-Social-Media.pdf.

Section 1: Description of the Department's Use of Third-Party Social Media Tools to Communicate with the Public

The Department uses social media tools to enhance the user experience, promote access to information, and provide ease of navigation throughout DOJ websites. Additionally, the Department is pleased to participate in open, un-moderated forums offered by social media tools to increase government transparency, promote public participation, and encourage collaboration with the Department.

The Department uses third-party social media tools to disseminate mission-related information that DOJ components have approved for public dissemination. Social media tools can provide enhanced information sharing, collaboration, and decision-making by facilitating horizontal communication among multiple users. In light of the vast capabilities of third-party social media tools, the Department 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. The Department currently maintains official DOJ accounts on several third-party social media tools (e.g., Facebook, YouTube, Instagram, and Twitter).[6]

The Department of Justice Public Affairs Office (PAO) is responsible for working with DOJ components to align and coordinate the Department's public message and use of social media. DOJ components must obtain approval from the Social Media Working Group (SMWG) before using social media tools to communicate with the public, in accordance with processes described in DOJ policy. Per DOJ policy, the SMWG includes the Department's PAO, the Office of Privacy and Civil Liberties (OPCL), the Office of Records Management Policy (ORMP), the Departmental Ethics Office (DEO), the Justice Management Division's (JMD) Office of General Counsel (OGC), and other relevant DOJ components. The SMWG reviews various issues, including privacy and records management issues, in order to ensure that the Department's uses are in accordance with applicable laws, policies, and regulations.

To gain this approval, DOJ components are required to submit a completed social media project request form to the SMWG. The SMWG will review the project request form to ensure that the proposed use of social media aligns with the Department's broader public relations strategy and contains a valid proposal for such use. The SMWG will contact the component via email to either approve or deny the request. After the SMWG's review and approval of the project request form, DOJ components must complete the social media records management questionnaire form and an initial privacy assessment. The Department has also issued a number of Directives that formalize the Department's policy on the use of social media to communicate with the public.

[6] An inventory of authorized DOJ accounts can be found at: https://www.justice.gov/social.

Section 2: Information Likely to be Made Available to the Department Through The use of Third-Party Social Media Tools.

2.1 Indicate below what information is collected, maintained, or disseminated.

Registration Information Provided to Social Media Tools: Users of social media tools may be required to submit certain PII to the social networking website or application service at the time of registration. Users voluntarily submit additional or optional information to further identify or categorize themselves if they so choose. The Department does not collect, maintain, or disseminate this registration information when users create accounts on social media tools.[7] Users' registration information and activity on social media tools are governed by the security and privacy policies of the social networking website or application service. Users may wish to review the privacy policies of these services before using them to understand how and when those websites collect, use, and share the information users make available by using their services. The privacy policies for third-party websites commonly used by the Department can be found on the DOJ website privacy policy.[8]

PII Made Available to the Department: The creation and use of official Department accounts may cause PII to become available or accessible to the Department. Such information may become available when a user provides, submits, communicates, links, posts, or associates information with official Department of Justice accounts (e.g., through "liking," "friend-ing," responding to tweets, or commenting on content provided by the Department). In certain circumstances, DOJ Capstone Officials,[9] which include DOJ Senior Leadership, Heads of Components, and their direct reports, may "share," "retweet," "friend," "follow," or respond publicly to content made available on official Department of Justice accounts. To the extent that the Department's "share," "retweet," "friend-ing," "follow," or public response constitutes the creation of a record under the Federal Records Act,[10] the Department may maintain and archive such interaction, as explained in Section 3. Additionally, the Department may collect, maintain, or disseminate information made available to the Department on official Department accounts for a specific law enforcement purpose (e.g., activity that indicates a violation or potential violation of law, a threat of physical harm, or harm to national security), or when required by law, consistent with the Privacy Act of 1974 ("Privacy Act").[11] The Department will not otherwise collect, maintain, or disseminate personal information made available on official Department of Justice accounts.

Dissemination of PII through Authorized Department of Justice Accounts: All information disseminated by the Department through the use of social media tools will be carried out in accordance with Department policy. The use of social media tools will be consistent with the Department's

---

[7] Note that information a user provides, submits, or links to, posts or comments on, or associates with official Department of Justice accounts, including information that may have been provided during the registration process, such as the user's name, may be collected, maintained, or disseminated, consistent with the practices described in this adapted PIA.
[8] The Department's privacy policy can be viewed at: https://www.justice.gov/doj/privacy-policy.
[9] For more information on the Capstone Approach, *see* National Archives and Records Administration (NARA), *White Paper on The Capstone Approach and Capstone GRS* (April 2015), https://www.archives.gov/files/records-mgmt/email-management/final-capstone-white-paper.pdf.
[10] 44 U.S.C. § 3101 *et seq.* (2012).
[11] 5 U.S.C. 552a (2012).

privacy policy, including its policy on "Visiting Official Department of Justice Pages on Third-Party Websites." Additionally, the Department will ensure that all postings on these accounts containing individuals' names or other PII are consistent with Department policy, including but not limited to, the United States Attorneys' Manual (USAM) 1-7.000 Media Relations.[12]

2.2 Indicate sources of the information in the system. (Check all that apply.)

Directly from individual about whom the information pertains					
In person		Hard copy: mail/fax		Online	X
Telephone		Email			
Other (specify):					

Government sources					
Within the Component		Other DOJ components		Other federal entities	
State, local, tribal		Foreign			
Other (specify):					

Non-government sources					
Members of the public	X	Public media, internet	X	Private sector	
Commercial data brokers					

The creation and use of official Department accounts may cause PII to become available or accessible to the Department. Such information may become available when a user provides, submits, communicates, links, posts, or associates information with official Department of Justice accounts (e.g., through "liking," "friend-ing," responding to tweets, or commenting on content provided by the Department). In certain circumstances, DOJ Capstone Officials, which include DOJ Senior Leadership, Heads of Components, and their direct reports, may "share," "retweet," "friend," "follow," or respond publicly to content made available on official Department of Justice accounts. To the extent that the Department's "share," "retweet," "friend-ing," "follow," or public response constitutes the creation of a record under the Federal Records Act, the Department may maintain and archive such interaction. Additionally, the Department may collect, maintain, or disseminate information made available to the Department on official Department of Justice accounts for a specific law enforcement purpose (e.g., activity that indicates a violation or potential violation of law, a threat of physical harm, or harm to national security), or when required by law, consistent with the Privacy Act. The Department will not otherwise collect, maintain, or disseminate personal information made available on official Department of Justice accounts.

Additionally, the Department may disseminate PII through the use of social media tools. Any information disseminated through these tools will be vetted through the appropriate Department approvals processes before being posted publicly. DOJ components will ensure that posting of PII by the Department is consistent with the Department's policies, including the USAM 1-7.000 Media Relations. Components will ensure that all postings of pictures or photos is done in accordance with

[12] The USAM can be found at: https://www.justice.gov/usam/united-states-attorneys-manual.

Department guidance on positing photos to Department websites.

2.3 Analysis: Now that you have identified the information collected and the sources of the information, please identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Please describe the choices that the component made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

Risks to individual privacy exist any time PII is made available to the Department. First, when an individual interacts with the Department using social media tools, he or she may post PII publicly in comments or replies or share PII with the Department through direct messaging. These interactions may expose the Department to PII of social media users. In order to mitigate this risk, the Department will limit the collection, maintenance, and dissemination of PII made available on official Department of Justice accounts to the limit circumstances described above.

A second risk associated with the Department's use of social media tools is that the Department may inappropriately disseminate PII when posting content to social media pages. The Department will mitigate this risk of disseminating PII by following the Department privacy policy and all policies and guidance regarding public disclosures and media relations when posting information, images, or videos to social media pages, including but not limited to, the USAM 1-7.000 Media Relations. The Department's SMWG will also provide training, awareness, and assistance to DOJ components operating authorized DOJ accounts.

Finally, risks may also arise when authorized DOJ accounts "friend," "follow," or respond to other social media accounts (e.g., "like," retweet, or share content posted by other users). To mitigate this risk, each component must ensure that its accounts only follow and share/retweet content in accordance with Federal law and Department policies and procedures. DOJ components are strongly encouraged to discuss potential issues related to following accounts and sharing/retweeting content with their Senior Component Official for Privacy, Ethics Official, and/or OGC, as necessary.

Section 3: The Department's Intended or Expected Use of PII

3.1 Generally, how will the Department use the PII described in Section 2?

The creation and use of official DOJ accounts may cause PII to become available or accessible to the Department, as described above. In certain circumstances, DOJ Capstone Officials, which include DOJ Senior Leadership, Heads of Components, and their direct reports, may "share," "retweet," "friend," "follow," or respond publicly to content made available on official Department of Justice accounts. To the extent that the Department's "share," "retweet," "friend-ing," "follow," or public response constitutes the creation of a record under the Federal Records Act, the Department may

maintain and archive such interaction. Additionally, the Department may collect, maintain, or disseminate information made available to the Department on official Department of Justice accounts for a specific law enforcement purpose (e.g., activity that indicates a violation or potential violation of law, a threat of physical harm, or harm to national security), or when required by law, consistent with the Privacy Act. The Department will not otherwise collect, maintain, or disseminate personal information made available on official Department of Justice accounts.

3.2 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration (NARA), if available.)

The Department of Justice has created accounts on several social networking sites in order to provide information to the public. When interacting with an authorized DOJ account, users are not required to provide any information to the Department of Justice. Any registration information users may have provided to the social networking service, described above, is neither accessible nor maintained by any Department of Justice entity. Authorized DOJ accounts are generally used to send out alerts about speeches, press briefings, and other information that will "point" or "redirect" followers to the DOJ website.

In certain circumstances, the Department may collect content posted on social media tools that will be retained and disposed of in accordance with guidelines approved by NARA. For instance, Department of Justice Capstone Officials, which include DOJ Senior Leadership, Heads of Components, and their direct reports, may "share," "retweet," "friend," "follow," or respond publicly to content made available on official Department of Justice accounts. To the extent that the Department's "share," "retweet," "friend-ing," "follow," or public response constitutes the creation of a record under the Federal Records Act, the interaction must be retained as required by applicable records retention schedules. Once Capstone Official records have met their relevant Department of Justice retention period, they will be transferred to NARA for possible public release under NARA's authority. Capstone Official records, which may include content posted on Official DOJ Capstone Official accounts, are retained under approved Records Retention Schedules.

3.3 Analysis: Describe any potential threats to privacy as a result of the component's use of the information, and controls that the component has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

There are associated privacy risks any time PII is made available to, or used by the Department. An individual interacting with the Department using social media tools may post PII publicly in comments or replies, or share PII with the Department through direct messaging. These interactions may expose the Department to PII of social media users, and such information may be appropriately used by the Department. In order to mitigate risks associated with such use, the Department will limit the collection, maintenance, or dissemination of PII made available on official Department of Justice

accounts to the circumstances described above.

Additionally, there is the risk that the Department's use of social media tools may inappropriately disseminate PII when posting content to social media pages. The Department will mitigate this risk by following the Department's privacy policy and all policies and guidance regarding public disclosures and media relations when posting information, images, or videos to social media pages, including but not limited to, the USAM 1-7.000 Media Relations. The Department's SMWG will also provide training, awareness, and assistance to DOJ components operating authorized DOJ accounts. Accordingly, risks associated with unauthorized disclosure of PII should be mitigated.

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information in the system and how the information will be shared, such as on a case-by-case basis, bulk transfer, or direct access.

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Within the component	X			
DOJ components	X			See above.
Federal entities	X			See above.
State, local, tribal gov't entities				
Public	X			All information disseminated by the Department through the use of social media tools will be carried out in accordance with Department policy.
Private sector				
Foreign governments				
Foreign entities				
Other (specify):	X			See above.

4.2 Analysis: Disclosure or sharing of information necessarily increases risks to privacy. Describe controls that the component has put into place in order to prevent or mitigate threats to privacy in connection with the disclosure of information. (For example: measures taken to reduce the risk of unauthorized disclosure, data breach, or receipt by an unauthorized recipient; terms in applicable MOUs, contracts, or agreements that address safeguards to be implemented by the recipient to ensure appropriate use of the information – training, access controls, and security measures; etc.)

In certain circumstances DOJ Capstone Officials, which include DOJ Senior Leadership, Heads of Components, and their direct reports, may "share," "retweet," "friend," "follow," or respond publicly to content made available on official Department of Justice accounts. To the extent that the Department's "share," "retweet," "friend-ing," "follow," or public response constitutes the creation of a record under the Federal Records Act, the Department may maintain and archive such interaction. Additionally, the Department may collect, maintain, or disseminate information made available to the Department on official Department of Justice accounts for a specific law enforcement purpose (e.g., activity that indicates a violation or potential violation of law, a threat of physical harm, or harm to national security), or when required by law, consistent with the Privacy Act. To the extent that PII is collected or maintained from individuals who interact with the Department's social web accounts, the Department will safeguard the information, as detailed in Section 6.

Section 5: Notice, Consent, and Redress

5.1 Indicate whether individuals will be notified if their information is collected, maintained, or disseminated by the system. (Check all that apply.)

X	Yes, notice is provided pursuant to a system of records notice published in the *Federal Register*. See Section 7, below	
X	Yes, notice is provided by other means.	Specify how: The Department will set-up official accounts, approved by PAO and the SMWG, which clearly establish that the accounts are managed by DOJ. For example, the Department will use the DOJ seal on the social networking websites or applications. The Department also manages a privacy policy that informs visitors of the Department's use of pages on third-party social media tools. To the extent feasible, the Department will post the DOJ privacy policy on the social networking website or application itself. If an agency posts a link that leads to a social networking or application website, the agency will provide an alert to the visitor, such as a statement adjacent to the link or a "pop-up," explaining that visitors are being directed to a nongovernment website that may have different privacy policies from those of the agency's official website. Users should also consult the privacy policies of the third-party social media tools they subscribe to for more information.
	No, notice is not provided.	Specify why not:

5.2 Indicate whether and how individuals have the opportunity to decline to provide information.

X	Yes, individuals have the opportunity to decline to provide information.	Specify how: PII made available to authorized DOJ accounts for the purpose of communicating with the public is voluntarily contributed and in the public domain. Individuals are not required to interact with authorized DOJ accounts.
	No, individuals do not have the opportunity to decline to provide information.	Specify why not:

5.3 Indicate whether and how individuals have the opportunity to consent to particular uses of the information.

	Yes, individuals have an opportunity to consent to particular uses of the information.	Specify how:
X	No, individuals do not have the opportunity to consent to particular uses of the information.	Specify why not: Consent to particular uses of information is not necessary because the Department generally does not collect, maintain, or disseminate personal information users make available on official Department of Justice accounts. However, information posted by the public on these third-party social websites is information that is in the public domain and voluntarily posted, at the poster's discretion. In order to post content to third-party websites, the individuals have consented to the third-party websites' policy. In certain circumstances, Department of Justice Capstone Officials, which include DOJ Senior Leadership, Heads of Components, and their direct reports, may "share," "retweet," "friend," "follow," or respond publicly to content made available on official Department of Justice accounts. To the extent that the Department's "share," "retweet," "friend-ing," "follow," or public response constitutes the creation of a record under the Federal Records Act, the Department may maintain and archive such interaction.

5.4 Analysis: Clear and conspicuous notice and the opportunity to consent to the collection and use of individuals' information provides transparency and allows individuals to understand how their information will be handled. Describe how notice for the system was crafted with these principles in mind, or if notice is not provided, explain why not. If individuals are not provided the opportunity to consent to collection or use of the information, explain why not.

The Department provides individuals with notice of its social media policy both through the DOJ website privacy policy and through privacy notices provided on the social media tool. The Department-wide Privacy Policy has a full section dedicated to informing individuals of the Department's use of social media websites when communicating with the public. DOJ components are required to comply with DOJ policy when they use social media tools to communicate with the public.

Additionally, the Department's pages on third-party websites will include clear indications of their association with the Department and, to the extent feasible, provide specific privacy notices to users. These privacy notices will, to the extent feasible, explain that the third-party website is not a government website and that Department's website privacy policy does not apply to the social media tool. It will also indicate the Department's use and sharing of PII that is made available, explain that PII may be made available to third parties when using social media to communicate with the Department, direct individuals to the component's website, and direct individuals to the Department's website privacy policy.

Section 6: Information Security

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

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, to ensure that the Department's use of social media complies with federal laws, executive orders, regulations, and policies, and to apply standards consistently across the entire Department, the SMWG will meet to ensure that all documents related to social networking websites and applications are cleared to ensure compliance issues are considered and coordinated before implementation.

A secondary privacy risk is that individuals who interact with the Department through 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.

Another risk to PII is unauthorized access to Department social media accounts. To mitigate this risk, the Department has designated PAO as the primary holder of the Department's social media

accounts. PAO will ensure that accounts are only accessed and used in accordance with Department policy.

Section 7: Privacy Act

7.1 Indicate whether a system of records is being created, or has been created, in accordance with the Privacy Act, 5 U.S.C. § 552a. (Check the applicable block below and add the supplementary information requested.)

X	Yes, and this system is covered by an existing system of records notice. Provide the system name and number, as well as the Federal Register citation(s) for the most recent complete notice and any subsequent notices reflecting amendment to the system: See response below.
	Yes, and a system of records notice is in development.
	No, a system of records is not being created.

7.2 Analysis: Describe how information in the system about United States citizens and/or lawfully admitted permanent resident aliens is or will be retrieved.

Generally, the Department does not collect, maintain, or disseminate PII from individuals who interact with authorized Department of Justice accounts. Therefore, PII is not nor can it be retrieved by a personal identifier of United States citizens and/or lawfully admitted permanent resident aliens.

In certain, limited circumstances, the Department may collect information made available on authorized DOJ accounts, as described above in Section 2. Consistent with Department policy, such information may only be collected, maintained, or disseminated consistent with the Privacy Act. As such, should information constitute a record maintained as a system of records, it must be covered by an applicable Privacy Act System of Records Notices or DOJ will be prohibited from collecting such information until an applicable Privacy Act System of Records Notices is published.