INTERIM PRIVACY IMPACT ASSESSMENT FOR THIRD-PARTY SOCIAL MEDIA WEBSITES AND APPLICATIONS

Introduction

The Privacy and Civil Liberties Oversight Board ("PCLOB") uses various third-party social media websites and applications, such as Twitter and LinkedIn, to share information about the agency's activities with the public. The PCLOB's purpose in using social media is to communicate its activities to the public, not to collect or use personal information from social media users. While we do not actively collect any personal information, the nature of maintaining social media accounts means that the agency sometimes does have access to personally identifiable information ("PII"). Although PCLOB does not actively collect this data, the PCLOB does receive notifications from social media platforms when users contact the agency directly or mention it online. These notifications may be considered federal records. In such instances, the PCLOB will retain the information for the minimum amount of time required by our agency's records schedule. The PCLOB will not use any personal information for any purpose other than responding to a user's request. This privacy impact assessment explains the ways in which the agency might acquire PII and outlines PCLOB practices for handling this information.

Background

The term "third-party websites and applications" refers to web-based technologies that are not exclusively operated or controlled by a government entity, or to web-based technologies that involve significant participation of a nongovernment entity. They are typically referred to as "social media." These technologies are often located on a ".com" website or other location that is not part of an official government domain. These third-party websites and applications are typically referred to as social media, Web 2.0, or Gov 2.0.

The PCLOB uses multiple social media websites or applications that may include, but are not limited to, Twitter and LinkedIn. The PCLOB's Public Affairs Officer or another authorized individual administers these official social media websites or applications. This Privacy Impact Assessment (PIA) covers all authorized third-party social media websites and applications used by the PCLOB that are functionally comparable and share substantially similar practices across their websites and/or applications. The Appendices provide more specific information about the websites and applications that the PCLOB uses. The Appendices will be updated if the PCLOB intends to use additional third-party platforms.

Although these sites may contain official information from the PCLOB, they are not authoritative sources of official agency information. Use of these third-party sites does not constitute an endorsement by the PCLOB or any of its employees of sponsors, information, or products presented on these external sites. It is also important to note that the privacy protections provided on the PCLOB website may not be available on third-party social media sites and applications, which are governed by their own privacy policies. In this PIA, the PCLOB details privacy issues relevant to its use of third party social media websites and applications. To obtain

information about third-party privacy policy and practices, please reference the relevant third party's privacy policy.

Section 1 – Specific Purpose of the Agency's Use of a 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?

The PCLOB uses third-party social media websites and applications to share information with the public. Our use of these social websites and applications helps to inform the public of our activities.

1.2 Is the agency's use of the third-party website or application consistent with all applicable laws, regulations, or policies?

The PCLOB's use of social media websites and applications is consistent with relevant laws and guidance, including the Privacy Act of 1974 and the E-Government Act of 2002. The PCLOB also draws on executive branch guidance, such as OMB memoranda, where applicable. The agency's use of these websites or applications helps to further our statutory obligations to inform the public of our activities, as appropriate, and in a manner consistent with the protection of classified information. See 42 USC 2000ee(f)(2).

When the PCLOB uses the websites or applications covered under this PIA, it does not actively seek PII and may only use the minimum amount of PII it receives from a user necessary to fulfill a user's request. PII may not be retrieved by personal identifier, and thus a Privacy Act System of Records Notice is not required.

Section 2 – Is Any PII Likely to Become Available to the Agency?

2.1 What PII may be made available to the PCLOB?

The PCLOB does not actively seek PII or use information provided to third-party social media websites or applications, nor does the PCLOB solicit such information. Any information that individuals voluntarily submit during the registration process is not the PCLOB's property.

Although the PCLOB 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 the PCLOB. In registering for social media accounts, users often make publicly available information that might include their names, images from photos or videos, screen names or handles, and email addresses. The PCLOB will not actively collect any of this information.

In addition, many third-party social media websites or applications request PII from users at the time of registration. The process varies across third-party social media websites or applications, and users sometimes provide more information than is required for registration. For example, users may provide information about birthday, address, contact information, family members and

relationship status, education, occupation and employment, and hometown. If users' privacy settings on third-party social media websites or applications are not restricted, such information may be visible to the PCLOB.

2.2 What PII is collected, maintained, or disseminated?

The PCLOB does not solicit, actively seek, or disseminate PII from these third-party social media websites or applications. However, users may voluntarily provide PII when communicating with official PCLOB accounts and PII may be made available to PCLOB by the social network provider.

As explained in Section 2.1, users provide PII to social media websites and applications at the time of registration.

2.3 What are the sources of PII in the system?

The PCLOB does not have access to the information that social media websites/applications collect when users register. Authorized PCLOB account users do have access to information that users post to their public profiles, which could include name (real or pseudonym), handle or username, location, and any additional information that users post in a biography or profile. Users might also send unsolicited private messages to PCLOB accounts that contain PII. In addition, the PCLOB receives notifications about user messages or actions from the social media website or application. These notifications will be maintained in accordance with the agency's records retention schedule.

2.4 Do the PCLOB's activities trigger the Paperwork Reduction (PRA) and, if so, how will the agency, comply with the statute?

The PCLOB's use of social media websites and applications as outlined in Section 1.1 is not a web-based interactive technology that would trigger the PRA. See OMB memorandum on *Social Media, Web-Based Interactive Technologies, and the Paperwork Reduction Act*.

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

3.1 Generally, how will the PCLOB use the PII described in Section 2.0?

While the PCLOB uses social media websites and applications as platforms for communicating its message, the agency does not actively seek, maintain, or disseminate PII from individuals who interact with any social media website or application. If an individual contacts the PCLOB through a social media website or application, the PCLOB may use that person's screen name or handle, email address, or other user-provided information to respond to specific comments or questions.

3.2 What are specific examples of the agency's use of PII?

- Jane Doe submits a private message via Twitter (Direct Message) in response to a PCLOB Tweet. The PCLOB Public Affairs Officer or other authorized user may respond privately to Jane by addressing her by her Twitter handle.
- John Doe submits a private LinkedIn message with a specific inquiry. A PCLOB representative may respond with a private message answering the question or directing John to another resource.

Section 4: How Will the PCLOB Share or Disclose PII?

4.1 With which entities or persons inside or outside the agency will PII be shared, and for what purpose will PII be disclosed?

The PCLOB will shared information internally only for the purpose of responding to a request. In addition, the agency may be required to share PII in response to lawful requests for information. In doing so, the PCLOB will protect elements of personal information to the greatest extent permitted.

4.2 What safeguards prevent expansion of uses beyond those authorized by law and described in this PIA?

Only approved staff members have the account access required to manage the PCLOB's social media websites and applications. Any staff members with access must comply with applicable PCLOB rules. PCLOB registers its social media accounts using official PCLOB email accounts. Administrators may not use personal accounts to manage PCLOB social media accounts.

Members of the public do not have to be registered users of social media accounts to view PCLOB content on official social media accounts. Social media accounts are third-party sites, and PCLOB social media accounts generally contain comparable information that is available on the PCLOB's website and other resources.

Section 5: How will the PCLOB Maintain and Retain PII?

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

If a user submits PII in a request or inquiry to the PCLOB through a social media website or application, the PCLOB may use the PII provided by the user to fulfill the specific request. In doing so, the agency will use as little personal information as possible. As part of its notification settings on social media websites or applications, the PCLOB receives email notifications of messages from users or mentions of PCLOB that may contain PII. The PCLOB will not use this information except if necessary to respond to the user, and will not disseminate this information. In accordance with the PCLOB's records schedule, established by the National Archives and Records Administration (NARA), these emails are retained for three years before they are deleted.

5.2 Was the retention period established to minimize privacy risk?

Yes. The retention period is intended to ensure compliance with the agency's records obligations while minimizing privacy risks to personal information.

Section 6: How does the PCLOB Secure PII?

As mentioned above, only approved staff members have the account access required to manage the PCLOB's social media websites and applications. Any staff members with access must comply with applicable rules. The PCLOB's social media accounts are registered using official PCLOB email accounts. Administrators are not permitted to use personal accounts to manage PCLOB social media accounts.

Section 7: Identification and Mitigation of Other Privacy Risks

7.1 What other privacy risks exist, and how will the PCLOB mitigate those risks?

Disclosure of PII/BII 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 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, the PCLOB will monitor postings to its authorized social media websites and applications to the extent practicable and will delete such posts of which the PCLOB becomes aware.

Despite such efforts, the information may remain available elsewhere on the website, and others may have already viewed or copied the information. Additionally, the PCLOB does not request or collect any sensitive personal information, nor does it conduct any official transactions on social media applications. Where possible, the PCLOB will provide 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 application or website.

Finally, the PCLOB aims whenever possible to post information on its social media websites and applications that is already public information on its official website. As a result, members of the public generally do not need to visit the agency's social media web pages or accounts to find comparable information.

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 PCLOB on the website. The social media provider displays this advertising content, which is not endorsed by the PCLOB or another U.S. government entity. 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,” “image renderings”), 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 altogether.

Spam, unsolicited communications, spyware, other threats
Users may also receive spam or other unsolicited or fraudulent communications as a result of their interactions with the PCLOB 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 also should avoid accepting or viewing unknown or unsolicited links, applications, or other content that may be sent or forwarded in such communications. These unsolicited links and applications can contain unwanted tracking technology as well as computer viruses or other malicious payloads that can pose a variety of risks to the user. Where possible, the PCLOB will also provide warnings about these risks in a notice to users on the third-party social media website.

Accounts or pages that misrepresent agency authority or affiliation
Certain accounts or pages on the third-party social media website may not be officially authorized by, or affiliated with the PCLOB, even if they use official insignia or otherwise appear to represent the PCLOB or the federal government. Interacting with such unauthorized accounts or pages may expose users to the privacy or security risks described above. The PCLOB will make reasonable efforts to label or identify its account or page in ways that would help users distinguish it from any unauthorized accounts or pages. The PCLOB will also inform the website operator about any unofficial accounts or pages purporting to represent the PCLOB, seek their removal, and warn users about such accounts or pages.

External links and embedded third-party applications
PCLOB social media accounts will not link to third-party websites that are not part of an official government domain except to provide information about activities undertaken by Board Members or PCLOB employees. In doing so, the PCLOB is not providing a PCLOB or U.S. government endorsement of the non-government website or entity. If the PCLOB incorporates or embeds a third-party social media application, separate from any applications that may be incorporated or embedded by the website operator itself, the PCLOB will disclose and explain the nature or extent, if any, of the third-party’s involvement in the PCLOB’s use of the social media application(s). The PCLOB will also describe the use of these social media application(s) in its own privacy policy.

Monitoring future requirements and future technology
In addition to the measures described above, the PCLOB will identify, evaluate, and address any new additional privacy requirements that may result from new statutes, regulations, or policies. Second, the PCLOB will evaluate the privacy risks of any new technologies before deciding whether to adopt them. Third, the PCLOB will monitor research or trends in privacy protection

technologies or policies that may facilitate new approaches to avoiding or mitigating privacy risks and better protecting PII.

Section 8: Creation or Modification of a System of Records

Will the PCLOB's activities create or modify a "system of records" under the Privacy Act (5 U.S.C. § 552a) of 1974?

No. The PCLOB does not retain or search for PII or usernames/handles/screennames in a manner that would require the PCLOB to create or modify a system of records under the Privacy Act of 1974.

APPENDIX A: TWITTER

Specific questions or issues are addressed only where necessary to supplement the information provided in the main body of this PIA.

Section 1 – Specific Purpose of the Agency's Use of a Third-Party Website or Application

The PCLOB uses Twitter, a microblogging website (i.e., a blog consisting of short posts or messages limited to 140 characters), to disseminate information to the public.

The PCLOB's Twitter profile is public, which means that anyone – including visitors who are not registered Twitter users – can visit the account and read the agency's tweets. However, only registered users can post tweets on Twitter. The PCLOB does not permit public posts on its Twitter account. Tweets from other users do not show up in the PCLOB's home streams unless retweeted by the PCLOB's account.

Tweets/Retweets
The PCLOB uses tweets to inform the public about PCLOB-related information or resources, which may include information pertaining to the activities of individual Board Members. These tweets appear in reverse chronological order on the PCLOB's profile page. Additionally, any Twitter users who "follow" a PCLOB account will receive agency tweets in their Twitter "stream" or "timeline." In turn, users may share the PCLOB's resources with their network of Twitter followers (generally done by sending out the same tweet and giving credit to the PCLOB's original tweet, called a "retweet") and others can do the same. The PCLOB does not retweet non-government accounts, nor does it endorse the views of non-government accounts or account holders.

Follows/Following
Anyone can follow the PCLOB Twitter account, as it is not private and does not require permission to follow. The @PCLOB_GOV account will only follow other government agencies and their leadership.

Mentions
If a registered user posts a tweet that includes a PCLOB account handle, this is called a mention. The tweet will appear in the user's profile and home stream as well as the timelines of all followers of that user. Additionally, that tweet will show up in the notifications/mentions stream of the PCLOB account.

If a user posts a tweet that starts with a mention of the PCLOB's Twitter account (@PCLOB_GOV), it will only appear in the home streams of users who follow both that user and the PCLOB account. However, all public tweets are searchable by the public on Twitter's website or other third party sites linked to Twitter. Thus, anyone can search for mentions of PCLOB Twitter accounts.

Public tweets may also be picked up by other search engines, aggregator sites, or applications outside of Twitter. The PCLOB cannot delete tweets sent by other users even if they mention a

PCLOB account, but the PCLOB can block Twitter users or other messages that are deemed as harassing toward the PCLOB. Additionally, the PCLOB can report "spam"-style Twitter accounts, and Twitter can investigate and delete the account if necessary.

Section 2 – Is Any PII Likely to Become Available to the Agency?

2.1 What PII will be made available to the PCLOB?

Twitter requires users to provide their first name, last name, a valid email address, and a password, with the option to provide additional information in their biography when they register an account. Even though some of this information may be accessible to the PCLOB, depending on a Twitter user's privacy settings (users can protect their tweets by using a private account setting), the PCLOB does not intend to collect, disseminate, or maintain any of the information provided to Twitter.

Section 7: Identification and Mitigation of Other Privacy Risks

Users interested in more information about Twitter's privacy policy can review it online.

APPENDIX B: LINKEDIN

Specific questions or issues are addressed only where necessary to supplement the information provided in the main body of this PIA.

Section 1: Specific Purpose

1.1 What is the specific purpose of the agency's use of LinkedIn, and how does that use fit with the agency's broader mission?

LinkedIn is a popular professional networking website. Registered users can create personal profile pages to post resumes, apply for jobs, search other profiles, and post and read other status/news updates. In addition, users can network with other LinkedIn users by "connecting" their LinkedIn profiles, which can be located by using the site's search function by allowing LinkedIn to search one's personal email contacts for matching LinkedIn accounts and profiles.

LinkedIn also hosts "company pages" for a variety of entities, including government agencies. The PCLOB maintains the official agency LinkedIn company page using a PCLOB-approved LinkedIn account administered by authorized PCLOB staff members. The official PCLOB LinkedIn page permits the Agency to reach users who may not be regular visitors to PCLOB websites and may include links to PCLOB job postings on government websites, and relevant PCLOB news and resources. It also contains general information consistent with the LinkedIn company page format, including company type, size, industry, logo, location, etc.

Company pages have some public information, including a basic company overview, but users must be registered and logged in to LinkedIn to view all company content. All registered users can interact with the PCLOB company page. To register for a LinkedIn account, users must provide a first and last name, email, and a password. Users may choose to provide additional information about themselves, such as current and previous job experience, education, interests, links to other social media accounts, etc. Users can select additional settings to make their LinkedIn profiles partially or completely private. Some, but not all, LinkedIn content and services may be accessible to viewers who do not register or log onto LinkedIn. Additionally, some services are free while others require fees.

For company pages, LinkedIn offers analytic tools that permit page managers to assess the effectiveness of their page through aggregate data, such as number of page views, page visitor demographics, and number of unique visitors.

The PCLOB LinkedIn account will use InMail, which enables the receipt of direct messages, but will not make personal connections with other LinkedIn users from its official account and will not use other current or future LinkedIn functionality except as specified in this PIA. The PCLOB will manage its LinkedIn account through www.LinkedIn.com only, not through a mobile app.

Section 2: Is Any PII Likely to Become Available to the Agency?

2.1 What PII will be made available to the PCLOB?

While the PCLOB may post links to job openings at the agency, the PCLOB will not collect personal information, including resumes or job applications, through LinkedIn. The PCLOB will not collect comments, names of individuals, or other PII from individuals who communicate with the agency on LinkedIn.

2.2 What are the Sources of PII?

Sources of PII potentially include information that LinkedIn users make publicly available in their profiles, including their full name, personal information, and links to documents or resources, as well as content that users post in identifiable form, such as comments on the PCLOB's posts. As noted above, the PCLOB does not intend to collect or copy user profiles of individuals who communicate with the agency on LinkedIn and does not intend to retain records of those user communications in identifiable form except when required for Federal records retention purposes.

Section 7: Identification and Mitigation of Other Privacy Risks

Users interested in more information about LinkedIn's privacy policy can review it online.