

Institute of Museum and Library Services



Adapted Privacy Impact Assessment

for

Use of Third-Party Websites and Applications to Communicate
with the Public

9 January 2024

Institute of Museum and Library Services Privacy Impact Assessment
IMLS-Wide/ Third-Party Social Media Web Services

Under the E-Government Act of 2002 (“E-Government Act”), the Institute of Museum and Library Services (“IMLS”) must perform a Privacy Impact Assessment (PIA) (i) before initiating a new electronic collection of information in identifiable form for 10 or more persons (excluding agencies, instrumentalities, or employees of the federal government); or (ii) before developing or procuring information technology systems or projects that collect, maintain, or disseminate information in identifiable form from or about members of the public.

Building upon the guidance contained in the E-Government Act, the Office of Management and Budget (“OMB”) issued OMB Memorandum M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications* which requires agencies to create an “adapted” PIA whenever they use a third-party website or application that makes personally identifiable information (PII) available to the agency.¹ Each adapted PIA should be posted on the agency’s official website and describe: (i) the specific purpose of the agency’s use of the third-party website or application; (ii) any PII that is likely to become available to the agency through public use of the third-party website or application; (iii) the agency’s intended or expected use of PII; (iv) with whom the agency will share PII; (v) whether and how the agency will maintain PII, and for how long; (vi) how the agency will secure PII that it uses or maintains; (vii) what other privacy risks exist and how the agency will mitigate those risks; and (viii) whether the agency’s activities will create or modify a “system of records” under the Privacy Act.

OMB Memorandum M-10-23 states that an agency may prepare one adapted PIA to cover multiple websites and applications that are functionally comparable, if the agency’s practices are substantially similar across the websites or applications. If the use of a website or application raises distinct privacy concerns, then the agency should prepare a PIA for each website or application.

¹ “Third-party websites or applications” is defined in OMB Memorandum M-10-23 as “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 at 8, *Guidance for Agency Use of Third-Party Websites and Applications* (June 24, 2010), available at https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/memoranda_2010/m10-23.pdf

Section 1. Description of IMLS' Use of Third-Party Websites and Applications.

Please provide a description of the third-party websites and applications that IMLS uses to communicate with the public.

Meta Platforms, Inc., doing business as Meta, and formerly named Facebook, Inc., and The Facebook, Inc., is an American multinational technology conglomerate based in Menlo Park, California. The company owns and operates Facebook, Instagram, Threads, and WhatsApp, among other products and services. IMLS currently uses the web-based platforms Facebook, Instagram, and Threads to communicate important updates about IMLS initiatives, available and awarded grants, and museum/library field information to the public who follow us on those platforms.

X (formerly Twitter Inc.) is an online social networking site based in San Francisco, CA. IMLS currently uses the web-based platform to communicate important updates about IMLS initiatives, available and awarded grants, and museum/library field information to the public who follow us.

LinkedIn is a business and employment-focused social media platform that works through websites and mobile apps based in Sunnyvale, CA and since December 2016, it has been a wholly owned subsidiary of Microsoft. IMLS currently uses the web-based platform to communicate, job openings, important updates about IMLS initiatives, available and awarded grants, and museum/library field information to the public who follow us on this platform.

YouTube is an online video sharing and social media platform headquartered in San Bruno, California. Accessible worldwide, since it launched in 2005, the site is owned by Google and is the second most visited website in the world, after Google Search. IMLS uses the platform to share recorded webinars about applying for grants, important interviews with the agency director or staff, and community impact videos highlighting National Medalists and grantees.

In your description, please be sure to address the following:

- a. *The specific purpose of the agency's use of the third-party website and/or application.*
- b. *Website and/or application location*
- c. *How information on the website and/or application is retrieved by the agency employee.*

Section 2. Information made available to IMLS through the use of third-party websites and applications.

2.1 Indicate below what PII is likely to become available to the agency through public use of the third-party website or application (check all that apply.)

Identifying numbers (IN)			
a. Social Security Number (full or truncated form) *	<input type="checkbox"/>	b. Driver's License	<input type="checkbox"/>
d. Taxpayer ID	<input type="checkbox"/>	e. Passport	<input type="checkbox"/>
g. Employer/ Employee ID	<input type="checkbox"/>	h. Credit Card	<input type="checkbox"/>
j. File/ Grant ID	<input type="checkbox"/>		<input type="checkbox"/>
k. Other identifying numbers:			
* Explanation for the need to collect, maintain, or disseminate the Social Security Number:			

General Personal Data (GPD)**			
a. Name	<input checked="" type="checkbox"/>	b. Maiden Name	<input type="checkbox"/>
d. Date of Birth	<input type="checkbox"/>	e. Home Address	<input type="checkbox"/>
g. Gender	<input checked="" type="checkbox"/>	h. Personal Telephone Number	<input type="checkbox"/>
j. Marital Status	<input type="checkbox"/>	k. Race/ Ethnicity	<input type="checkbox"/>
i. Other general personal data: ** Information available to the extent each user shares/makes public in their profile**			

Work-related data**			
a. Occupation	<input checked="" type="checkbox"/>	b. Job Title	<input checked="" type="checkbox"/>
d. Work Address	<input type="checkbox"/>	e. Work Telephone Number	<input type="checkbox"/>
g. Employment History	<input checked="" type="checkbox"/>	h. Procurement/ Contracting Records	<input type="checkbox"/>
j. Other work-related data: **Information available to the extent each user shares/makes public in their profile**			

System Administration/ Audit Data			
a. IP Address	<input type="checkbox"/>	b. User ID/ Username	<input checked="" type="checkbox"/>
d. Queries Run	<input type="checkbox"/>	e. ID of Files Accessed	<input type="checkbox"/>
Other system administration/audit data:			

2.2 Indicate sources of the information in the website and/or application and explain how the information is received.

Information in the site’s user profile is uploaded by the individual user and details can vary widely from each individual. IMLS does not directly receive PII data of users we are engaged with on social media platforms.

IMLS has the capability to see the names of people who engage with our content which is the most basic information “received” by the agency.

The individual platforms collect cookies. Cookies help administrators provide, protect, and improve the products, such as by personalizing content, tailoring and measuring ads, and providing a safer experience. The cookies can include session cookies, which are deleted when users close the browser, and persistent cookies, which stay in a browser until they expire, or users delete them. IMLS does not have access to this data.

2.3 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. (Please mention the retention schedule approved by National Archives and Records Administration (NARA) for these records.)

While IMLS has access to user data on these platforms, the agency does not consolidate or collect “follower” lists or data as the information can change daily and is not relevant to IMLS business. Therefore, this information is not reflected in the OC retention schedule for NARA.

Section 3. Intended or Expected Use of PII

3.1 Indicate the intended or expected use of the PII described in Section 2. (E.g., for administrative purposes, to improve our services, etc.)

IMLS can use analytics data assessed by individual platforms that track content engagement by age and/or gender. This data does not connect us to the individual profiles. It does inform the type of content we develop for the public depending on if we are connecting with the intended audience.

3.2 Indicate whether the website and/or application collects only the minimum amount required to achieve the purpose stated in response to Question 3.1?

The platform asks for the minimum required PII to develop those analytics. It is still up to the user how much information they disclose, or if it is truthful. Users who are logged in and interact with IMLS's social media pages, at a minimum, make their names available to the agency. For LinkedIn, and potentially the other platforms, other information voluntarily disclosed may become visible to the agency. However, the agency does not use these social media platforms to solicit, collect, maintain, or disseminate PII.

Section 4. Information Security and Safeguards

4.1 Does this website and/or application connect, obtain, or share PII with any other IMLS systems or projects?

Yes? Explain.	
No, this website and/or application does not connect with, obtain, nor share PII with any other IMLS system or project.	X

4.2 Does this website and/or application connect, obtain, or share PII with any external (non-IMLS) systems, websites, applications, people, or projects?

<p>Yes? Explain. (Please also describe the type of PII shared, the purpose for sharing it, the name of the information sharing agreement, and how the PII will be shared.)</p>	<p>Users may opt to link an account with another social media company or service. This is all done at the discretion of the user. IMLS may link their social media profiles with another social media company within that social media's universe. For instance, the agency's Instagram account may be connected with their Threads account, both companies are owned by the same parent company.</p>
<p>No, this website and/or application does not connect with, obtain, nor share PII with any other external system, website, application, people, or project.</p>	

4.3 Identify who will have access to the website and/or application and the PII made available through it.

Members of the public	X
IMLS employees/ contractors	
Other (explain)	

4.4 Does the website and/or application maintain an audit or access log?

<p>Yes? Explain. (Including what information is compiled in the log)</p>	<p>The individual platforms collect cookies. Cookies help administrators provide, protect and improve the products, such as by personalizing content, tailoring and measuring ads, and providing a safer experience. The cookies can include session cookies, which are deleted when users close the browser, and persistent cookies, which stay in a browser until they expire or users delete them. IMLS does not have access to this data.</p>
<p>No, this website and/or application does not compile an audit or access log.</p>	

4.5 What administrative, technical, and physical safeguards are in place to protect the PII in the website and/or application?

Only approved staff members from the agency have access to the social media pages. Each staff member with access completes regular security, privacy, and ethics training and additionally must comply with the agency's policies for managing accounts and data. IMLS's social media pages are registered as business accounts and are not administered by any employee's personal accounts.

4.6 What are the privacy risks associated with the website and/or application and how are those risks mitigated? (E.g., automated privacy controls, privacy training, etc.) Please include a description of the technology used to protect PII in the website and/or application.

Social accounts are frequently the target of malicious hacking and identity theft. There are reporting mechanisms for fake accounts, violations of community standards, as well as system firewalls and other physical privacy controls. IMLS staff undergoes federally required annual training on ethics and privacy.

Section 5. Notice and Consent

5.1 Indicate how individuals will be notified that their PII is being collected, maintained, or disseminated. (Check the box or expand on the response that applies.)

<p>Yes, notice is provided through a systems and records notice (SORN) that was published in the Federal Register and is discussed in the next section.</p>	
<p>Yes, notice is provided through a Privacy Act statement, PIA, privacy policy, or privacy notice. The Privacy Act statement, privacy policy, PIA, and/or the privacy notice can be found at (provide text of the notice if a link isn't available):</p>	<p>Meta privacy policy https://www.facebook.com/privacy/policy/ X, formerly Twitter privacy policy https://twitter.com/en/privacy LI privacy policy https://www.linkedin.com/legal/privacy-policy YouTube privacy policy</p>

	https://www.youtube.com/howyoutubeworks/our-commitments/protecting-user-data/ We also post the agency’s privacy policy on all our social media profiles. IMLS’s privacy policy can be found at https://imls.gov/privacyterms .
Yes, notice is provided by other means:	
No, notice is not provided. Please explain why:	

5.2 Please describe whether individuals are given the opportunity to consent to uses of their PII, decline to provide PII, or opt-out of the website and/or application. Specify how below.

Consent	Yes, individuals have the opportunity to consent to uses of their PII:	X	
	No, individuals do not have the opportunity to consent to uses of their PII.		
Decline	Yes, individuals have the opportunity to decline to provide their PII:	X	
	No, individuals do not have the opportunity to decline to provide their PII.		
Opt-out of	Yes, individuals have the opportunity to opt-out of the website and/or application:	X	
	No, individuals do not have the opt-out of the website and/or application.		

Section 6. Privacy Act

6.1 Is a 'system of records' being created under the Privacy Act?

The Privacy Act of 1974 defines a 'system of records' as, "a group of any records from which information is retrieved by the name of the individual or some identifying number, symbol, or other identifying particular assigned to the individual." ²

Yes, a 'system of records' is created by this website and/or application.	
No, a 'system of records' is not created by this website and/or application.	X

6.2 If you answered 'yes' to the previous question, please include a link to the 'system of records' notice for this website and/or application. Or please indicate that we will need to create a new 'systems of records' notice for this website and/or application.

² See, *The Privacy Act of 1974*, §552a (5). <https://www.govinfo.gov/content/pkg/USCODE-2018-title5/pdf/USCODE-2018-title5-partI-chap5-subchapII-sec552a.pdf>.

Section 7. Assessment Analysis

Social media platforms like Meta, X, LinkedIn, and YouTube are PaaS (Platform as a Service). IMLS does not use any of these websites to solicit, collect, maintain, or disseminate PII from members of the public. Due to this, the privacy impact of the agency's use of these platforms are low. The agency limits the number of employees that have administrative access to manage the social media profiles of the agency. The employees that do have administrative access are trained on privacy, security, and ethics annually. The employees are trained to avoid inadvertent collection or disclosure of non-public information and the pages are monitored to ensure adherence to these policies and guidelines.