EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

June 25, 2010

M-10-23

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Peter R. Orszag
Director

SUBJECT: Guidance for Agency Use of Third-Party Websites and Applications

This Memorandum requires Federal agencies to take specific steps to protect individual privacy whenever they use third-party websites and applications to engage with the public.

In the *Memorandum on Transparency and Open Government*, issued on January 21, 2009, the President called for the establishment of "a system of transparency, public participation, and collaboration."[1] The President emphasized that "[k]nowledge is widely dispersed in society, and public officials benefit from having access to that dispersed knowledge." Following the President's memorandum, the Office of Management and Budget (OMB) issued the *Open Government Directive*, which required a series of concrete steps to implement the system of transparency, participation, and collaboration.[2]

On April 7, 2010, OMB issued several guidance documents responding to the *Open Government Directive*. One such guidance — the most relevant to this Memorandum — is *Social Media, Web-Based Interactive Technologies, and the Paperwork Reduction Act*.[3] That memorandum focuses on the requirements of the Paperwork Reduction Act (PRA)[4] in connection with social media and web-based interactive technologies; it explains that without triggering the PRA, agencies may use such media and technologies to promote open government in many ways.

---

[1] President Barack Obama, Memorandum on Transparency and Open Government (Jan. 21, 2009), *available at* http://www.gpoaccess.gov/presdocs/2009/DCPD200900010.pdf

[2] OMB Memorandum M-10-06, *Open Government Directive* (Dec. 8, 2009), *available at* http://www.whitehouse.gov/omb/assets/memoranda_2010/m10-06.pdf

[3] *Available at* http://www.whitehouse.gov/omb/assets/inforeg/SocialMediaGuidance_04072010.pdf

[4] 44 U.S.C. § 3501.

Like the April 7, 2010 guidance and OMB's *Guidance for Online Use of Web Measurement and Customization Technologies*,[5] this Memorandum recognizes that open government increasingly relies on Federal agency uses of new technologies, such as social media networks and web 2.0 applications. Such uses offer important opportunities for promoting the goals of transparency, public participation, and collaboration. However, increased use of these technologies also requires greater vigilance by Federal agencies to protect individual privacy.

The purpose of this Memorandum is to help Federal agencies to protect privacy, consistent with law, whenever they use web-based technologies to increase openness in government. As explained below, the Memorandum builds on OMB's existing guidance; it calls for transparent privacy policies, individual notice, and a careful analysis of the privacy implications whenever Federal agencies choose to use third-party technologies to engage with the public.[6]

1. Scope.

This Memorandum applies to any Federal agency use of third-party websites or applications to engage with the public for the purpose of implementing the principles of the *Open Government Directive*.[7] The guidance also applies when an agency relies on a contractor (or other non-Federal entity) to operate a third-party website or application to engage with the public on the agency's behalf. Whenever an agency uses web measurement and customization technologies, the agency should refer to OMB's memorandum providing *Guidance for Online Use of Web Measurement and Customization Technologies*.

2. Existing Requirements.

Compliance with Existing Requirements. Agencies are reminded of their obligation to comply with applicable privacy laws (including the Privacy Act of 1974[8]) and OMB guidance, as well as to consult established privacy principles.[9] In addition, agencies should coordinate with their Senior Agency Official for Privacy (SAOP).

---

[5] OMB Memorandum M-10-22, *Guidance for Online Use of Web Measurement and Customization Technologies* (June 25, 2010), *available at* http://www.whitehouse.gov/omb/assets/memoranda_2010/m10-22.pdf

[6] Definitions are provided in the Appendix to this Memorandum.

[7] This guidance does not apply to internal agency activities (such as on intranets, applications, or interactions that do not involve the public) or to activities that are part of authorized law enforcement, national security, or intelligence activities.

[8] 5 U.S.C. § 552a.

[9] Since 1973, a series of government reports — both general and agency-specific — have established Fair Information Practices that set forth many accepted principles of information privacy. *See, e.g.*, U.S. Dep't of Health, Educ., and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens* (1973), *available at* http://aspe.hhs.gov/DATACNCL/1973privacy/tocprefacemembers.htm

Modifications to Existing Guidance. This Memorandum modifies the following OMB memoranda:

- OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*

- OMB Memorandum M-99-18, *Privacy Policies on Federal Web Sites*

3. General Requirements.

Subject to the requirements set forth below, agencies may use third-party websites and applications to engage openly with the public. These websites and applications offer new tools that will help people to connect with their government, promoting the goals of transparency, participation, and collaboration. At the same time, agencies should comply with the requirements in this Memorandum to ensure that privacy is fully protected.

Agencies should also provide individuals with alternatives to third-party websites and applications. People should be able to obtain comparable information and services through an agency's official website or other official means. For example, members of the public should be able to learn about the agency's activities and to communicate with the agency without having to join a third-party social media website. In addition, if an agency uses a third-party service to solicit feedback, the agency should provide an alternative government email address where users can also send feedback.

When using a third-party website or application, agencies should adhere to the following general requirements:

a. **Third-Party Privacy Policies**. Before an agency uses any third-party website or application to engage with the public, the agency should examine the third party's privacy policy to evaluate the risks and determine whether the website or application is appropriate for the agency's use. In addition, the agency should monitor any changes to the third party's privacy policy and periodically reassess the risks.

b. **External Links.** If an agency posts a link that leads to a third-party website or any other location that is not part of an official government domain, the agency should 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.

c. **Embedded Applications.** If an agency incorporates or embeds a third-party application on its website or any other official government domain, the agency should take the necessary steps to disclose the third party's involvement and describe the agency's activities in its Privacy Policy, as specified in this Memorandum.

d. **Agency Branding.** In general, when an agency uses a third-party website or application that is not part of an official government domain, the agency should apply appropriate branding to distinguish the agency's activities from those of nongovernment actors. For example, to the extent practicable, an agency should add its seal or emblem to its profile page on a social media website to indicate that it is an official agency presence.

e. **Information Collection.** If information is collected through an agency's use of a third-party website or application, the agency should collect only the information "necessary for the proper performance of agency functions and which has practical utility."[10] If personally identifiable information (PII) is collected, the agency should collect only the minimum necessary to accomplish a purpose required by statute, regulation, or executive order.

4. Requirements for Privacy Assessment and Public Notice.

a. **Privacy Impact Assessments (PIAs).** While OMB Memorandum M-03-22[11] provides broad guidance on the PIA process, an agency's use of third-party websites and applications raises new questions. For that reason, OMB is modifying its existing guidance to require an adapted PIA, described below, for an agency's use of such websites and applications.

The adapted PIA is required whenever an agency's use of a third-party website or application makes PII available to the agency. Each adapted PIA should be tailored to address the specific functions of the website or application, but adapted PIAs need not be more elaborate than the agency's other PIAs. In general, each PIA should be posted on the agency's official website.

The PIA should 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;

[10] OMB Circular A-130, *available at* http://www.whitehouse.gov/omb/Circulars_a130_a130trans4/

[11] OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (Sept. 26, 2003), *available at* http://www.whitehouse.gov/omb/memoranda_m03-22/

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.[12]

In general, an agency's use of a third-party website or application should be covered in a single, separate PIA. However, an agency may prepare one PIA to cover multiple websites or applications that are functionally comparable, as long as the agency's practices are substantially similar across each website and application. If an agency's use of a website or application raises distinct privacy risks, the agency should prepare a PIA that is exclusive to that website or application.

An agency should work with its SAOP to determine how many PIAs are needed, to identify when updates to PIAs are necessary, and to ensure full compliance with OMB policies. OMB is available to provide further guidance on the PIA process and to direct agencies to model PIAs and other resources that may be useful.

b. **Agency Privacy Policies.** OMB Memoranda M-99-18[13] and M-03-22 establish requirements for agency Privacy Policies. Agencies should continue to comply with existing guidance and should also update their Privacy Policy to describe their use of third-party websites and applications, including:

i. the specific purpose of the agency's use of the third-party websites or applications;

ii. how the agency will use PII that becomes available through the use of the third-party websites or applications;

iii. who at the agency will have access to PII;

iv. with whom PII will be shared outside the agency;

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; and

[12] *See* 5 U.S.C. § 552a(5).

[13] OMB Memorandum M-99-18, *Privacy Policies on Federal Web Sites* (June 2, 1999), *available at* http://www.whitehouse.gov/omb/memoranda_m99-18/

vii. what other privacy risks exist and how the agency will mitigate those risks.

An agency should also, when feasible, provide links to the relevant privacy policies of the third-party websites and applications being used.

c. **Agency Privacy Notices.** To the extent feasible, an agency should post a Privacy Notice, described below, on the third-party website or application itself. The Privacy Notice should:

i. explain that the website or application is not a government website or application, that it is controlled or operated by a third party, and that the agency's Privacy Policy does not apply to the third party;

ii. indicate whether and how the agency will maintain, use, or share PII that becomes available through the use of the third-party website or application;

iii. explain that by using the website or application to communicate with the agency, individuals may be providing nongovernment third parties access to PII;

iv. direct individuals to the agency's official website; and

v. direct individuals to the agency's Privacy Policy as described above.

An agency should take all practical steps to ensure that its Privacy Notice is conspicuous, salient, clearly labeled, written in plain language, and prominently displayed at all locations where the public might make PII available to the agency.

5. Role of the Senior Agency Official for Privacy (SAOP).

When agencies are evaluating whether to use third-party websites or applications, they should consult with their SAOP. OMB Memorandum M-05-08 provides that an agency's SAOP shall have a "central policy-making role" and shall have "overall responsibility and accountability for ensuring the agency's implementation of information privacy protections."[14] Agencies should confer with their SAOP at the earliest possible stage of their planning process, and consult with the SAOP through implementation and post-implementation review.

[14] OMB Memorandum M-05-08, *Designation of Senior Agency Officials for Privacy* (Feb. 11, 2005), available at http://www.whitehouse.gov/omb/assets/omb/memoranda/fy2005/m05-08.pdf

6. OMB Assistance.

When additional assistance is needed, an agency is encouraged to consult the appropriate Office of Information and Regulatory Affairs (OIRA) desk officer for clarification and guidance. For questions specifically about this Memorandum, agencies may contact OMB at privacy-oira@omb.eop.gov.

Appendix

Definitions

Third-party websites or applications. The term "third-party websites or applications" refers 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.[15] However, third-party applications can also be embedded or incorporated on an agency's official website.

Personally Identifiable Information (PII). The term "PII," as defined in OMB Memorandum M-07-16[16] refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available — in any medium and from any source — that, when combined with other available information, could be used to identify an individual.

Make PII Available. 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.

Privacy Impact Assessment (PIA). The term "PIA," which is now subject to the modifications in this Memorandum, was defined in OMB Memorandum M-03-22[17] as:

> [A]n analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate

---

[15] *See* OMB Memorandum M-05-04, *Policies for Federal Agency Public Websites* (Dec. 17, 2004) (identifying ".gov," ".mil," and "Fed.us" as appropriate government domains), *available at* http://www.whitehouse.gov/OMB/memoranda/fy2005/m05-04.pdf

[16] OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 22, 2007), *available at* http://www.whitehouse.gov/OMB/memoranda/fy2007/m07-16.pdf

[17] OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (Sept. 26, 2003), *available at* http://www.whitehouse.gov/omb/memoranda_m03-22/

protections and alternative processes for handling information to mitigate potential privacy risks.

Privacy Policy. The term "Privacy Policy" is described in OMB Memorandum M-99-18,[18] and is further explained in OMB Memorandum M-03-22. When the term is used in this Memorandum, it refers to a single, centrally located statement that is accessible from an agency's official homepage. The Privacy Policy should be a consolidated explanation of the agency's general privacy-related practices that pertain to its official website and its other online activities.

Privacy Notice. While a Privacy Policy is a statement about an agency's general practices, the term "Privacy Notice" refers to a brief description of how the agency's Privacy Policy will apply in a specific situation. Because the Privacy Notice should serve to notify individuals before they engage with an agency, a Privacy Notice should be provided on the specific webpage or application where individuals have the opportunity to make PII available to the agency.

[18] OMB Memorandum M-99-18, *Privacy Policies on Federal Web Sites* (June 2, 1999), *available at* http://www.whitehouse.gov/omb/memoranda_m99-18/