Privacy Best Practices for Social Media

July 2013

Table of Contents

1. Overview

"Social media," also known as "Web 2.0" or "Gov 2.0," are web-based tools, websites, applications, and media that connect users and allow them to engage in dialogue, share information, collaborate, and interact. Social media websites are oriented primarily to create a rich and engaging user experience. In social media, users add value to the content and data online; their interactions with the information (e.g., both collectively and individually) can significantly alter the experiences of subsequent users.

Websites like Twitter, Facebook, YouTube, Flickr, and others make it easy to reach large numbers of people. The Internet may be used to reach millions of people just by posting a blog, sharing a video, or by tweeting an observation or question on Twitter. YouTube is now the second largest search engine (after Google) in the world. Social media allows anyone who uses information to also create it. Hence, this makes social media an ideal platform for sharing information, starting conversations, and exchanging knowledge within and outside government. Billions of pieces of content (e.g., web links, news stories, blog posts, notes, photo albums) are shared each month on Facebook and other social media sites. These venues serve as a space where content is both discovered and shared.

One of the Federal Government's most important missions is to provide citizens, customers, and partners with easy access to government information and services. As society increasingly relies on social media as a primary source for information, it is clear that these platforms have an important role to play in the Federal Government's communication strategy, including its move toward a digital, open government.[1] Social media allows an agency to post messages in places where people regularly interact, and ensures it reaches interested audiences – including audiences known to the agency as well as those that are unknown. In addition, social media enhances the Federal Government's situational awareness by enabling agencies to learn about problems and issues being discussed by different audiences, and allowing agencies to react, respond, and assist the public more efficiently and effectively. Government agencies also may use social media to fulfill their operational missions, for example, detecting and preventing benefit fraud and abuse.

This paper addresses various ways the Federal Government can use social media for information sharing, situational awareness, and to support agency operations, and the key considerations for each.[2] The paper also explains privacy best practices for establishing a social media program, from

---

[1] Social media use ties into the Federal CIO's Digital Government Strategy and the need to deliver better Government services to the public at lower costs. The Government needs to be prepared to "deliver and receive digital information and services anytime, anywhere and on any device." http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government-strategy.pdf. Social media also will help agencies meet the goals of transparency, participation, and collaboration set forth in the Administration's Open Government Directive. http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-06.pdf.

[2] This paper is a snap shot and does not reflect all of the social media tools that are available. It provides information on privacy best practices associated with the use of social media and does not specifically focus on technology. As the technology continues to evolve, privacy best practices will need to evolve with it, and this paper will be updated as necessary. This paper is not meant to authorize or prohibit and specific use of social media. The intent of this paper is to provide privacy best practices for agencies to consider when deciding whether or not to use social media. All uses of social media must be consistent with the agency's legal authorities. In addition, although this paper focuses exclusively on the privacy best practices associated with the use of social media, there are other considerations that should be

pulling together an intra-agency team of experts to establishing internal social media polices and ensuring transparency of social media uses through published privacy notices and documentation. The privacy best practices also cover specific technological issues, including web measurement and customization technologies, URL shortening technologies, and cybersecurity risks. When used properly, social media can be an incredibly powerful set of tools, precisely because these tools connect an agency directly to diverse audiences and opinions.[3] As described below, appropriate technical, administrative, and physical controls to protect data privacy and security can promote transparency, participation, and trust in the use of social media to communicate and interact with the public.[4]

2. Types of Use of Social Media

Before implementing any use of social media, an agency needs to understand its mission, and how different uses of social media can advance that mission. There are various ways agencies within the Federal Government can use social media in order to more effectively fulfill their mission. Each different use of social media raises different considerations and requires different operational policies, privacy documentation, and notices to the public, as explained below.

The main uses of social media to date include:

a. Using social media to communicate and share information with the public. Pursuant to President Obama's January 2009 memorandum promoting increased Government transparency, public participation, and collaboration,[5] agencies throughout the Federal Government accelerated their efforts to identify new opportunities to interact with the public, become more transparent, describe and promote agency activities, seek comment, and disseminate timely information. Social media websites and social networking services are well-suited to enable such interaction and information sharing. There are two main categories of social media applications/tools that an agency can use to share information with the public:

    i. Interactive applications allow an agency to engage in dialogue and collaborate with members of the public. These applications can be broken down into categories based on the mode or method used to disseminate information:

        1) Applications used to disseminate video and image content. These include, but are not limited to, the use of third party social media providers such as YouTube, Flickr, and Picasa.

---

taken into account when standing up a social media program, such as Section 508 of the Rehabilitation Act of 1973 and the Paperwork Reduction Act.

[3] US General Services Administration, web page "Chapter 2. What is Social Media?," http://www.gsa.gov/portal/content/250041.

[4] This document is intended to complement other guidance and recommendations prepared by this Subcommittee for ensuring data privacy and security in the Federal mobile and digital space. *See, e.g.*, *Recommendations for Standardized Implementation of Digital Privacy Controls* (Federal CIO Council, Dec. 2012), https://cio.gov/wp-content/uploads/downloads/2012/12/Standardized_Digital_Privacy_Controls.pdf.

[5] See Open Government Directive, supra note 1.

2) Blogs, microblogs, or other applications that permit entries of commentary. These include blog tools such as Twitter, Google Blogger, and Wordpress.

3) Social networking applications that facilitate two-way (bi-directional) interaction and networking with the public. These include third party social media providers such as Facebook, MySpace, LinkedIn, and GovLoop.

Any time an agency allows the public to comment or interact with the agency through social media, it should implement a commenting policy, consider how such interaction will be managed as "records" under the Federal Records Act, and if retained, whether the Privacy Act of 1974, as amended, applies, as discussed below. It is also important to clearly inform users whether the interaction on the social media website will be free-flowing or moderated, and if the postings will be in real-time or possibly involve a delay.

ii. Unidirectional or "push" applications are used for the purpose of one-way (non-interactive) dissemination of information to the public. These include applications such as widgets/RSS Feeds and audio/video files.

It is important to note that these types of applications can either be hosted by a third party or on an agency's domain or server. If hosted on a third party domain/server, the responsible organizations within the agency should assess the third party's Privacy Policy and Terms of Service and work with legal counsel to make sure they understand the implications before the agency agrees to use that application.

b. Using social media to enhance situational awareness. Note: In this discussion, the term "situational awareness" means viewing social media content made available to the public, and is not intended to include obtaining access to private networks or interacting on social media sites. Monitoring social media sites to enhance situational awareness means gathering mission-related information from a variety of sources, including "crowdsourcing," and then communicating that information to agency leadership to inform decision making and responsiveness. Agencies with national security, emergency response/management, and disaster recovery responsibilities may benefit most from this use of social media. Using social media to enhance situational awareness can be done by monitoring publicly available online forums, blogs, public websites, and message boards to gather information related to specific search terms (excluding individual members of the public unless there is an operational need and proper authority), events, or issues.

Through the use of publicly available search engines and content aggregators, an agency can monitor activities on social media websites for information that the agency can use to provide situational awareness. When monitoring publicly available sites, an agency should extract only the pertinent, authorized information that is needed to fulfill the business or mission need. The agency should limit its information gathering to facts surrounding the event (what is happening), rather than who is either involved or reporting the information, unless the agency has specific legal authority to collect information on individuals. Personally Identifiable Information (PII) may be collected only in very limited situations, and only when specifically authorized. For example, even though reporting should focus on what instead of whom, in certain circumstances it may lend credibility if the names of key government or political officials who are associated with the particular event or activity are

identified. An agency should develop a policy outlining specific guidelines on when collecting PII may be legal and appropriate based on the agency's authorities, and who will be allowed access to the PII.[6]

Uses of social media to enhance situational awareness should be approved by senior leadership of the agency/organization, including, but not limited to, privacy officials and legal counsel. To ensure transparency and provide notice on potential collection, detailed information of the agency's practices must be discussed in a publicly available Privacy Impact Assessment (PIA). Also, if the agency decides to collect and retrieve PII, the agency must be sure to follow the applicable provisions of the Privacy Act of 1974, as amended[7] and publish or update its applicable System of Records Notice (SORN) to cover the information collection.[8] Even when the agency is not maintaining or retrieving PII, situational awareness activities may still need to comply with other applicable laws. Agencies should also ensure that the program is in compliance with its policies by conducting periodic program or privacy compliance reviews.

Communicating and sharing information with the public involves the posting of information or some level of interaction between the agency and the public, while situational awareness is limited to viewing publicly available information. As noted earlier, while situational awareness may involve analyzing information posted by specific individuals, its focus is on assembling or aggregating data and monitoring or identifying patterns, trends or events, and not on monitoring individuals. Thus, when using social media to enhance situational awareness, the agency should not:

i. Post information collected about specific individuals;

ii. Actively seek to connect with other internal or external personal users;

iii. Accept other internal or external personal users' invitations to connect; or

iv. Interact on social media websites.

c. Using social media as an operational tool. An agency may use social media as an operational tool to collect publicly available information for a variety of purposes, where permitted by the agency's legal authorities and mission. For example:

i. Investigatory purposes: Investigating an individual or company in a criminal, civil, or administrative context to prevent fraud or other illegal activities (including undercover investigations when an agency has legal authority to engage in such investigations).

---

[6] Whenever an agency expects to capture a record from social media that will be maintained in a "system of records," the agency should carefully consider the Privacy Act of 1974, as amended, e.g., whether the information is relevant and necessary, and whether the record may describe how an individual exercises First Amendment rights. 5 U.S.C. §§ 552a (e)(1), (e)(7).

[7] For example, the Privacy Act of 1974, as amended, generally prohibits Federal agencies from collecting and maintaining information about individuals except as relevant and necessary to accomplish a legally authorized purpose.

[8] *See also Recommendations for Standardized Implementation of Digital Privacy Controls*, supra note 4, for a discussion and checklist of other laws and policies requiring notice of PII collection or maintenance in agency digital services and programs.

ii. Evaluation purposes: Making a benefit or eligibility determination about an individual (member of the public).

iii. Employment purposes (existing employees): Making a personnel determination about an employee.

iv. Hiring purposes (prospective employees): Conducting a background investigation on, or adjudicating the security clearance of, a prospective employee. To the extent possible, an agency must ensure that notice is provided prior to accessing or collecting information, that consent is obtained, and that the individual is involved in the process. (Note: Special consideration should be taken when using publicly available information, and agencies should not require an applicant to provide access to his/her social media accounts).

v. Intelligence purposes: Conducting authorized intelligence activities in accordance with the provisions of Executive Order 12333, as amended.

Due to its sensitivity, operational uses of social media should be approved and documented by senior agency leadership, including, but not limited to, privacy officials and General Counsel.9 Agencies must develop specific operational use policies and procedures, as well as PIAs/SORNs, where appropriate, to cover operational use. Program and privacy compliance reviews should be conducted on a routine basis to ensure the agency is in compliance with its policies and other documentation.

It is important that the agency be transparent about uses of social media, especially those that involve viewing publicly available information. By being transparent about what type of information the agency is collecting and how it is collecting it, the agency can help minimize the public's concern that the Government is monitoring individual speech and actions on social media.

Before engaging in any use of social media, an agency should first evaluate the various ways that it would like to use social media, and then develop and implement appropriate policies and procedures to govern that use, including the development or revision of PIAs and SORNs, as necessary, to cover the collection of information. All PIAs and SORNs must be approved by the Senior Agency Official for Privacy (SAOP) as required by OMB Memorandum M-10-23, *Guidance for Agency Use of Third Party Websites and Applications,* June 25, 2010.

At a minimum, an agency needs to ensure it has the proper authorities for all proposed use of social media, and that clear guidelines exist which outline how and when information can be collected about or from members of the public. Training and Rules of Behavior should be developed and followed by all employees and contractors engaging in the use of social media for official purposes.[10] Agencies can help mitigate the risk of inappropriate collection or misuse of PII by ensuring that all personnel are trained appropriately on guidelines and held accountable.

---

[9] For example, agency officials must consider whether the non-consensual collection or use of information about an individual from social media for employment or hiring purposes is authorized by the Privacy Act of 1974, as amended, Federal personnel laws governing prohibited personnel practices, and Federal policy currently under review on the permissible scope of background investigations for security clearances and employment suitability determinations.

[10] Agencies should also consider incorporating guidance on the personal use of social media to help employees and contractors avoid inadvertently appearing to speak on behalf of the agency, or violating privacy, confidentiality, ethical, criminal, or other restrictions on disclosure of PII or other information.

3. Establishing a Social Media Program

Before using social media for any purpose, whether the websites or applications are hosted by the agency or a third party, a federal agency should first understand its mission and how it seeks to use social media to further that mission. The agency should establish a social media policy or program, and engage key offices throughout the development and use of social media. A clear owner for each social media websites should be established to ensure accountability, and that all responsibilities associated with the social media program are being fulfilled. Key agency offices involved in the development and ongoing use of social media may include (this list is not exhaustive, and the office's names, may vary among federal agencies):

- Privacy Office;
- Office of the Chief Information Officer;
- Information Security Office;
- Chief Security Office;
- Office of Procurement (Acquisitions);
- Office of General Counsel;
- Chief (Designated Agency) Ethics Officer;
- Office of Public Affairs;
- Records Management Office;
- Office of the Chief Human Capital Officer (including the Labor Relations Office); and
- Program/Mission Office.

Throughout the process of standing up a social media program, key agency offices should be involved when and where necessary. For example, when negotiating extended or additional terms of service with a social media website, the agency should involve its Office of Procurement and Office of General Counsel, when appropriate.[11] Likewise, while creating privacy policies specific to the particular social media website or determining whether the agency should engage the public on the social media website, the agency's Privacy Office should be involved.

Irrespective of whether the agency has determined which social media website(s) to utilize, federal agency policies should be broad enough to encompass all types of social media and should be forward looking. At a minimum, these policies should include information about appropriate access, acceptable use, use of third party websites, use of embedded applications, and agency branding. Policies should include the inherent risks of social media and provide a mitigation assessment for each risk.

As an agency is developing policies for the use of social media, the agency should also engage its Privacy Office to develop (or update) relevant or necessary privacy compliance documentation including PIAs, SORNs, and Privacy Threshold Analyses (PTA), as appropriate. Completing privacy compliance documentation and posting that documentation on the agency's public-facing website

[11] See Appendix B, References, and Appendix C, Additional Resources, for information on Terms of Service (TOS) and M-13-10, *Antideficiency Act Implications of Certain Online Terms of Service Agreements*, April 4, 2013.

provides transparency to the public as to how the agency uses social media, with which agencies it will share information collected, and how the information collected is protected and retained. Moreover, OMB Memorandum M-10-23 requires PIAs be completed whenever an agency uses a third party website or application that makes PII available to the agency.[12]

In addition to an agency's Privacy Policy on its public-facing website, each agency should also establish and post an appropriate Privacy Policy or Notice on the social media website or application, whenever feasible. The Privacy Policy or Notice should explain that the social media website or application is not controlled or operated by the agency, indicate if and how the agency will maintain, use, or share PII provided on the social media website or application, make clear that any PII provided on the social media website or application may also be provided to the agency or that website or application, and direct individuals to the agency's official website. Additionally, the main page of the social media website or application and the social media Privacy Policy or Notice should also contain a clear and conspicuous link to the agency's Privacy Policy found on its main website as required in OMB Memorandum M-10-23.

When an agency establishes an official agency presence on a social media website or application, it is essential that the agency prominently display its agency seal and name on each individual webpage so that an individual reviewing the webpage will be informed that it is an official website associated with a federal agency. If an agency has a third party hosted social media website (e.g., an agency's Facebook page), and it provides links on that social media website to any non-government websites (e.g., a non-profit organization's website), the agency must ascertain whether the non-government website can display an affiliation to that federal agency by posting its seal or name as an affiliated entity.

Finally, federal agencies should be cognizant of the use of embedded applications by certain social media websites. These embedded applications may not only collect PII from individuals who have posted or accessed the social media website, but can potentially contain malicious coding. If an agency decides to use a third party application or website that uses embedded applications, then the agency must disclose this information and describe this use in the agency's main Privacy Policy, along with the social media website Privacy Policy or Notice.

4. Interacting with the Public

It is imperative that agencies are transparent about their use of social media to avoid concerns about over-collection of information or unauthorized surveillance of these websites, especially when an agency is using a third party hosted social media website. Agencies should only engage in the use of social media in a manner that protects privacy and respects the intent of users.

a. Disseminating information:

   Generally, social media websites and applications are privately owned by third parties. Each social networking website and application provides its own privacy policy, and while users are typically required to submit some PII during the registration process, as a best practice agencies should not solicit or collect this PII. Additionally, to the extent feasible, the agency should post a Privacy Notice on its page on the social media website or

[12] http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-23.pdf.

application. If an agency posts a link that leads to a social media website or application, 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 redirected to a non-government website that may have a different privacy policy than that of the agency's official website as required by OMB Memorandum M-10-23.

If an agency decides to allow comments, viewpoints, and opinions on its social media websites or applications (regardless of whether the sites/applications are agency or third party hosted), the agency must respect the public's First Amendment rights. [13] However, an agency should monitor and, generally speaking, may remove public comments that are political or endorse a political candidate, target specific individuals or groups, are abusive, contain sensitive PII, or are similarly unacceptable. In consultation with legal counsel, agencies should develop and post a comment policy and/or a "Rules of Use" policy covering the social media websites or applications where the agency has a presence and has allowed the public to post to the website or application. It is recommended that agencies display a statement that indicates third party comments do not reflect the views of the agency.

b. Collecting information:

The agency should collect only the minimum information necessary for the proper performance of official agency functions. Additionally, official government accounts across social media websites and applications should be identified by the agency or Department seal (when possible or appropriate), and should provide a way for a visitor to link back to the agency's or Department's own website, if necessary, to obtain official Government information.

When an agency uses social media websites and applications, the agency:

i. Should consider carefully whether to actively seek PII, and should use only the minimum amount of PII, which it receives, to accomplish a purpose required by statute, executive order, or regulation;

ii. Should not search social media websites or applications for or by PII unless authorized to do so, and legal requirements and representations in PIAs and SORNs have been complied with;

iii. Should not "friend," "follow," or "like" public users proactively; however, an agency may accept friend requests from public users[14] (exceptions can be made for "friending" other U.S. federal, state, local, and tribal government agencies, professional associations, or other organization as appropriate based on your agency's policies); and

[13] The Privacy Act of 1974, as amended, prohibits agencies from maintaining records that describe how any individual exercises rights guaranteed by the First Amendment, unless certain exceptions apply. 5 U.S.C. § 552a(e)(7).

[14] A statement should be included in the PIA and on the social media account page to inform users that the acceptance of friend requests does not indicate endorsement. Agencies should also have policies that address "friending," "following," and "liking" users.

iv. Should adopt user names and profiles that are easily identifiable as agency accounts, as well as establish secure passwords so that accounts can only be accessed by administrators.

5. Information Sharing and Retention

When using social media to interact with the public or collect information, it is important to have agency policies in place that provide guidance on the sharing and retention of such information.

a. Sharing with other parties (federal or non-federal): Information gathered by one agency should only be shared with another federal, state, or local agency, or other organization when the following criteria are met:

   i. The sharing of the information is within the agency's existing authorities;

   ii. The sharing is appropriate and consistent with the Routine Uses listed in the applicable SORN(s), or conducted through an interagency agreement (e.g., memorandum of understanding);

   iii. The receiving agency or organization is authorized to receive the information and even then, only the minimum data (or data elements) should be shared to fulfill the authorized mission or business need; and

   iv. The receiving agency agrees to protect the information and retain it only as long as necessary; and to re-disseminate the information only in accordance with the criteria listed above.

b. Retention: If PII is posted on a social media website or application, or sent to an agency in connection with the transaction of public business, it may become a federal record.[15] In these cases, the agency is required to maintain a copy per the appropriate records retention policies. Agencies should develop record retention schedules specifically to cover information collected through social media that outline what information should be retained and for how long. An agency should retain only the minimum amount of PII that is necessary for the proper performance of official agency functions. An agency should also ensure that retention policies and schedules are clearly described in, and are consistent with, applicable PIAs and SORNs.

6. Web Measurement and Customization Technologies

Web measurement and customization technologies are used to remember a user's online interactions with a website or online application in order to conduct measurement and analysis of usage, or to customize the user's experience.[16]

---

[15] National Archives and Records Administration (NARA), Bulletin 2011-02, *Guidance on Managing Records in Web 2.0/Social Media Platforms*, October 20, 2011, http://www.archives.gov/records-mgmt/bulletins/2011/2011-02.html.

[16] Executive Office of the President, Office of Management and Budget, M-10-22, http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-22.pdf.

For example, persistent cookies are used for customization so that a user's preferences on a web page are remembered each time he or she visits. Web analytics provide a myriad of information, including the volume of traffic visiting a web page or how many visitors clicked on an item, to assist the web developer in customizing web content with the information users want to see the most. Information is provided at an aggregated level so that no PII is available. Web analytics help to keep content interesting and relevant to the user. Apps.gov provides information on vendors that provide this type of service.

If an agency uses a third party platform to host its social media website, it is important that the agency offer an alternative location (e.g., the agency's .gov website) where the same information can be found. In doing so, the user has the option to access the information without being tracked by the third party that is hosting the agency's social media website. Also, the agency should include information regarding web measurement and customization technologies in its website's Privacy Policy.

7. Use of Third Party Websites

In many instances, federal agencies use third party websites, including social media websites, to provide and collect information from individuals. Before an agency uses these websites to interact with the public, the agency should first review the website's Privacy Policy for potential risks (e.g., maintaining data posted by individuals, selling data posted on the website), and determine if it is appropriate to use the third party website. If the agency chooses to use the third party website, it is incumbent upon the agency to periodically review the website's Privacy Policy for any changes, and if found, determine if these changes give rise to a change in the agency's posted Privacy Notice or Privacy Policy.

Many third party websites, particularly social media websites, allow users to comment either directly to the website or to postings on the website. In many instances, users looking for assistance may provide their PII not realizing the risks involved. Agencies must determine before and during the use of third party social media websites whether to allow individuals to post to those websites, and if so, if monitoring of comments is appropriate. If the agency decides to monitor comments, this fact should be included in the social media Privacy Policy or Notice, and the agency should be prepared to respond to any public reaction that may occur if it decides to delete particular comments made on the third party website.

8. Universal Resource Locator (URL) Shortening Technology

Federal agencies should weigh the risks before implementing any URL shortening technology on public or third party websites, in emails, or in other electronic communications. URL shortening technology allows federal agencies to substantially shorten the length of any URL, while still being able to direct an individual to the requested website or webpage. URL shortening technology is especially useful for federal agencies that use Twitter, which limits the number of characters in any given message, to direct the public to pertinent websites easily. Risks that federal agencies should address include the potential compromise of the shortened URL and redirecting of individuals to illegitimate websites, which could lead to the dissemination of misinformation about the agency, to cyber attacks mentioned in Section 9, or to identity theft.

If a federal agency employs or redirects individuals to a third party website that uses URL shortening technologies, the agency should provide clear and prominent notice to individuals before redirecting them to that website. This notice can be included on an "exit" page, "pop-up," or in the electronic communication to the individual. Additionally, the third party website must have clear and prominent notices on their website advising of the use of this technology.

If an agency wants to implement URL shortening technology, the U.S. General Services Administration (GSA) has a URL shortener that creates short, trustworthy .gov URLs, along with a tracking mechanism so that an agency can measure the impact and use of the shortened URL. The service, which requires registration, shortens only government URLs including .gov, .mil, and .fed.us. For additional information, or to register for the service, visit https://go.usa.gov/.

9. Cybersecurity Risks Associated with the Use of Social Media

According to the CIO Council's *Guidelines for Secure Use of Social Media by Federal Departments and Agencies*,[17] social media technologies such as wikis, blogs, and social networks are especially vulnerable to the following methods and techniques of cyber attacks:

a. Spear Phishing: Spear phishing targets a specific user or group of users, and attempts to deceive the user into performing an action that launches an attack, such as opening a document or clicking a link. Spear phishers rely on knowing a personal piece of information about their target, such as an event, interest, travel plans, or current issues. Sometimes this information is gathered by hacking into a targeted network, but more often it is easier to look up the target on a social media network. Spear phishers use social media as an alternative way to send phishing messages as the social media platform bypasses traditional email security controls such as antivirus protection. Social media websites can be used as a propagation mechanism to trick users into opening a document or clicking a link.

b. Social Engineering: Social engineering relies on exploiting the human element of trust. The first step in any social engineering attack is to collect information about the attacker's target. Social media websites can reveal many details of personal information, including resumes, home addresses, phone numbers, birth dates, employment information, work locations, family members, education, hobbies, interests, and photos. Social media websites may share more personal information than users expect or need to, and attackers are earnestly using social media to learn personal information about an individual. By expressing interest in similar topics, the attacker builds a trust relationship with the victim. This positions the attacker to influence the victim's friends and co-workers, or even to collect sufficient information about the victim to fraudulently pose as him or her.

c. Web Application Attacks: Social media websites are attractive to attackers who are looking to slip in malicious code or to link to off-site content that contains malware (short for malicious software) because malicious content is easy to disguise as valid content on social media websites. There is also a risk that developers of user-generated games and applications on some websites can have code approved and then inject malicious code at a

[17] *Guidelines for Secure Use of Social Media by Federal Departments and Agencies,* Version 1.0, Federal CIO Council, September 2009.

later time. If an attacker hijacks the account of a federal user or a federal account, there is an elevated risk that unauthorized posts, tweets, or messages may be seen by the public as official messages, or may be used to spread malware by encouraging users to click links or download unwanted applications (i.e., "web application attacks") or malware.

Another common risk associated with the use of social media is the accidental or unintended release of sensitive, For Official Use Only (FOUO), or classified information. This can be caused by an exfiltration of the information by a hacker or by an employee who may not be aware that the information should not be disclosed publicly.

All of the risks mentioned above can be mitigated by implementing both technical and non-technical security controls, including role-based training for employees who are responsible for managing social media accounts on behalf of the agency and through strong language in contracts with third parties.

10. Summary

Social media websites have become a valuable tool for federal agencies to leverage in order to engage customers, understand and address issues being raised by the public, and advance operational missions. Social media is a critical tool for agencies to use as they move toward a digital, open government. To ensure a successful experience and to adequately protect PII, it is important for an agency to bring together the appropriate stakeholders before setting up a website or application. The offices listed in section 3, *Establishing a Social Media Program*, should be involved from the beginning and participate throughout the entire process of developing a policy for the use of social media. In addition, privacy documentation, such as PIAs, should be developed to maintain transparency along with strong Terms of Service Agreements with third party vendors. Reaching out to agency partners and benchmarking privacy best practices will help to ensure the process for implementing privacy protections for social media will go more smoothly. This paper is one resource to help agencies take advantage of the benefits a vibrant social media program can offer.

Appendix A: Definitions

***Cookies*:** a cookie is used to identify and customize web pages for a user. There are two kinds of cookies: session cookies and persistent cookies. A session cookie is a line of text that is stored temporarily in a computer's random access memory (RAM), is never written to a drive, and is destroyed as soon as the user closes his/her browser. A persistent cookie is saved to a file on the hard drive and is called up the next time a user visits that website. This lets the website remember what the user was interested in the last time he or she visited.

Crowdsourcing: soliciting data related to a specific topic, idea, or issue from a large population of public users, traditionally an online community, who have knowledge of that topic, idea, or issue.

***Malicious Code*:** a term used to describe any code in any part of a software system or script that is intended to cause undesired effects, security breaches, or damage to a system. Malicious code describes a broad category of system security terms that includes attack scripts, viruses, worms, Trojan horses, backdoors, and malicious active content.

***Malware*:** software programs designed by hackers to damage or do other unwanted actions to a computer system to gather sensitive information or gain access to private computer systems.

***Personally Identifiable Information (PII)*:** per OMB M-10-23, the term "PII," as defined in OMB M-07-16, 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.

***Phishing*:** the use of fraudulent email, websites, or text messaging to trick people into divulging personal information such as credit card data, Social Security numbers, and other information which can then be used for identity theft, extortion, or other crimes.

***Privacy Impact Assessment (PIA)*:** is an analysis of how information is handled by (i) ensuring handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) determining the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system, and (iii) examining and evaluating protections and alternative processes for handling information to mitigate potential privacy risks.

***Privacy Threshold Analysis (PTA)*:** a document that serves as the determination by a privacy office as to whether a system or website has privacy implications and if additional compliance documentation is required (i.e., PIA or SORN).

***Social Media*:** websites, applications, and web-based tools that allow the creation and exchange of user-generated content. Through social media, people or groups can engage in dialogue, interact, and create, organize, edit, comment on, combine, and share content.

***System of Record Notice (SORN)*:** statement providing public notice of the existence of a group of records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifier assigned to the individual. The Privacy Act requires each agency to publish notice of its systems of records in the Federal Register.

Appendix B: References

Guidance documents that should be reviewed include the following:

NARA Guidance on Managing Web Records, January 2005. This guidance assists agency officials with managing web records properly. http://www.archives.gov/records-mgmt/pdf/managing-web-records-index.pdf

CIO Council, *Guidelines for Secure Use of Social Media by Federal Departments and Agencies*, Version 1.0, September 2009. This document is intended as guidance for any federal agency that uses social media services to collaborate and communicate among employees, partners, other federal agencies, and the public. https://cio.gov/wp-content/uploads/downloads/2012/09/Guidelines_for_Secure_Use_Social_Media_v01-0.pdf

OMB Memorandum, *Social Media, Web-Based Interactive Technologies, and the Paperwork Reduction Act*, April 7, 2010. OMB's Open Government Directive, this memorandum responds to that requirement by the goal of promoting flexible and open interactions between federal agencies and the public. http://www.whitehouse.gov/sites/default/files/omb/assets/inforeg/SocialMediaGuidance_04072010.pdf

OMB Memorandum M-10-22, *Guidance for Online Use of Web Measurement and Customization Technologies*, June 25, 2010. This memorandum establishes new procedures and provides updated guidance and requirements for agency use of web measurement and customization technologies. http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-22.pdf

OMB Memorandum M-10-23, *Guidance for Agency Use of Third Party Websites and Applications*, June 25, 2010. 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. http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-23.pdf

OMB Memorandum M-13-10, *Antideficiency Act Implications of Certain Online Terms of Service Agreements*, April 4, 2013. This memorandum recognizes that internet-based social media products and services are among the tools that Federal agencies are using to promote openness, transparency, and citizen engagement. This memorandum explains that when choosing which social medial tools to adopt it is important for agencies to exercise diligence in reviewing the set of terms of that governs access to and use of these products and services. http://www.whitehouse.gov/sites/default/files/omb/memoranda/2013/m-13-10.pdf

Appendix C: Additional Resources

HowTo.gov: using Social Media in Government: http://www.howto.gov/social-media/using-social-media

Social Media Metrics for Federal Agencies: http://www.howto.gov/social-media/using-social-media/metrics-for-federal-agencies

Social Media Registry: this project is a GSA database that allows the public to verify the URLs of a federal agency's social media pages. Public users will be able to copy-and-paste the URL into the database and learn whether the URL matches a URL that has been registered by the agency (http://www.usa.gov/Contact/verify-social-media.shtml). Agencies are encouraged to register all of their social media URLs and should identify a point of contact, who will receive email updates. Agencies should contact GSA at Socialmediaregistry@gsa.gov if they have a large number of social media URL and would like to enter them in bulk.

GSA has negotiated Terms of Service Agreements with several social media providers. These agreements can be found at http://www.howto.gov/web-content/resources/tools/terms-of-service-agreements/negotiated-terms-of-service-agreements. To find out an agency point of contact, go to http://www.howto.gov/web-content/resources/tools/terms-of-service-agreements/agency-points-of-contact.

Terms of Service model agreement template: http://www.howto.gov/sites/default/files/model-amendment-to-tos-for-g.pdf.

Apps.Gov (https://www.apps.gov): a service provided by GSA that allows agencies to purchase business solutions.