DHS Privacy Office

Government 2.0: Privacy and Best Practices

Report on the DHS Privacy Office Public Workshop

June 22 and 23, 2009

November 2009

Homeland Security

Table of Contents

Executive Summary

This report summarizes the *Government 2.0 Privacy and Best Practices* public workshop conducted by the Department of Homeland Security (DHS) Privacy Office on June 22-23, 2009. The workshop brought together leading academic, private sector, and public sector experts to help federal agencies explore best practices for the use of social media technologies to further President Obama's Transparency and Open Government Initiative.[1] The DHS Privacy Office also invited interested parties to submit written comments on government use of social media. The comments and workshop transcript are posted on the DHS Privacy Office website.[2] The workshop consisted of five panels and began with opening remarks by Vivek Kundra, the newly appointed federal Chief Information Officer. During the first panel, federal representatives showcased their social media activities and discussed the ways in which their organizations engage the public using social media technologies. The term "Government 2.0" is a variation on the term "Web 2.0," a term coined by O'Reilly Media in 2003 that referred to a second generation of the World Wide Web as an enabling platform for Web-based communities of interest, collaboration, and hosted services.[3] Web 2.0 supports many different applications, including the social media technologies – blogs, social networking, video sharing, wikis, etc. – discussed at this workshop to promote public interaction and collaboration. While the panelists cited many benefits of using social media, they also shared challenges their organizations may have encountered and lessons learned through their experiences. The panelists emphasized the need for comprehensive and clear policies regarding the government's use of social media and underscored the importance of obtaining input from all stakeholders across the organization (*e.g.*, privacy, legal, IT security, and records) to identify and address the inevitable issues that surface when the government uses these technologies.

The second panel, which consisted of representatives from privacy and civil liberties advocacy groups, government, and academia, explored the ways in which the government's use of social media impacts, or could potentially impact, the privacy of individuals. The panelists expressed support for the government's experimentation with social media to enhance transparency, but cautioned that the government has a responsibility to implement strong privacy protections when using such technologies. Specifically, the panel recommended that government agencies abide by the Fair Information Practice Principles (FIPPs) when engaging the public through social media, especially the principles of purpose specification, use limitation, individual participation, and data minimization. In addition, the panel called upon government to proactively educate the public about how to protect their privacy when interacting with the government through social media.

---

[1] *Transparency and Open Government Memorandum for the Heads of Executive Departments and Agencies* (Transparency and Open Government Memorandum), 74 Fed. Reg. 4685 (Jan. 21, 2009), *available at* http://edocket.access.gpo.gov/2009/pdf/E9-1777.pdf.

[2] The workshop transcript and comments are available at http://www.dhs.gov/xinfoshare/committees/editorial_0699.shtm. The DHS Privacy Office received comments from The Honorable Bennie G. Thompson, Chairman, Homeland Security Committee, as well as several members of the public.

[3] Webster's New World Telecom Dictionary, http://www.yourdictionary.com/telecom/web-2-0.

The third panel, comprised of security and technology experts, addressed the question of how to facilitate the secure use of Web 2.0 technologies within the federal government in a way that ensures security is an enabler supporting the deployment of social media and cloud computing initiatives. The panelists noted that government social media websites could be rich targets for attack by adversaries because they may contain a great deal of sensitive data. Therefore, the panelists agreed it is important for the government to have security measures in place to prevent such a threat. The panel also recommended that federal agencies employ a risk-based approach when making information security decisions regarding social media, suggesting agencies tailor such policies to the particular mission and data being exposed instead of applying a blanket policy for an entire agency or program. The panel concluded with a discussion of cloud computing, in which the panelists explored the legal and security issues associated with protecting data in the cloud.

The fourth panel discussed the numerous legal issues raised by government's use of social media and the application of various laws, acts, and regulations to such use. This panel agreed that agency engagement with the public via social media should be encouraged, but cautioned that government use of social media raises significant and complex issues. The panel explored in detail many of the privacy, ethical, and legal issues of using social media and discussed the ways in which government may take steps to address them in a privacy protective manner. The workshop concluded with a panel discussion of privacy best practices for government use of social media that used the FIPPs as a framework for developing a roadmap to guide the government's use of social media while also protecting privacy.

In summary, the workshop highlighted the unique opportunities social media provide for government to engage and communicate with the public. Panelists agreed, however, that the government's use of social media raises complex legal, policy, and privacy issues that government must address as it expands its use of these new tools. To that end, panelists recommended each agency have a process in place for considering potential uses of social media and resolving the attendant issues before new tools are launched – a process that should include input from agency legal, policy, communications, procurement, privacy, technology, and security officials. In addition, these policies should reflect the well-established FIPPs that provide a framework to protect privacy and provide appropriate safeguards. Panelists also noted the need for the Obama Administration to provide guidance on the use of tracking cookies and social media generally. In the absence of an over-arching federal social media policy, panelists agreed that agencies must rely on agency stakeholders and experts to develop social media policies that include appropriate privacy safeguards.

Panel 1: How Is Government Using Social Media?

The first panel of the workshop presented an overview and examples of the government's use of social media, the experience of selecting and using collaboration tools, and how the unique nature of these tools assists government agencies in achieving their missions. The panel included representatives from the Defense Department (DoD), the Department of State (State Department), the Federal Emergency Management Agency (FEMA), the National Academy of Public Administration (NAPA), the Transportation Security Administration (TSA), and the Environmental Protection Agency (EPA).

The Return to an Era of Collaboration

Representing DoD, the opening panelist began by explaining that the core challenge of adopting social media is not the tools themselves, but rather generational and cultural differences that affect the use of those tools. The panelist posited that the current generation has more in common with the culture of the 1800s than with that of the immediate past, because the nineteenth century was characterized by participation – people living in small communities, collaborating and participating in each others' lives to meet each others' needs, and by necessity, living relatively transparent lives.

According to the panelist, the broadcast era then followed in the twentieth century and, fueled by technology, enabled communication to reach beyond local communities. "Big media" reigned during the broadcast era. Radio, television, and newspapers reached across great distances and created a new kind of distance between individuals living in communities. The panelist further suggested that these broadcast media were one-way rather than interactive and participatory; and as a result, people who grew up in the broadcast era are accustomed to publishing and receiving information in large-scale, one-directional ways.

As the DoD panelist explained, the foundational technology that gave rise to the broadcast era continued to develop and, rather than simply extending the reach of "big media's" approach to communication, today has created dramatically new capabilities for individuals. In fact, these new social media tools have enabled a return to the nineteenth century's approach to social interactions and made close, collaborative, and participatory communications possible again – this time at the pace and scale of the twenty-first century global society.

With the unique combination of 21st century technical capability and 19th century cultures of community, today's individuals have essentially the same presence and opportunities for engagement as large transnational corporations. The true challenge of social media, the panelist opined, is to shift the one-way broadcast model to a multi-directional collaboration model of sharing and discussion and, ultimately, ubiquitous cultural participation. The challenge facing those in the broadcast era generation is to accept the value of the new collaborative approach, even as they struggle to understand it and participate in it.

The Defense Department's Use of Social Media

The panelist then presented an example of the DoD's use of both traditional broadcast era communication mechanisms and new social media collaboration tools. The DoD launched its Bloggers Roundtable program in January 2007 because the information that it believed should be

available to the American public was not being covered by traditional news media. This program uses traditional communications such as conference calls to reach social media communicators (bloggers) supported by a variety of secondary tools such as podcasts (downloadable media files available by subscription), RSS Feeds (subscription-based alerts of new website content), and professional transcription services. DOD has experienced a secondary benefit from using this combination of tools to send out its messages, *i.e.,* the bloggers are more apt to share accurate information with others and expand the reach of DoD's message.

The first panelist concluded by recommending the following principles to guide federal agencies wishing to communicate through social media:

- Pick the approach that best meets the mission need;
- Do not assume that using social media is the best approach;
- Learn about the technology and culture before using social media;
- Identify the unique value your agency can contribute to a topic through the use of social media and collaboration tools;
- Allow users to police social media environments as much as possible;
- Commit to collaboration and plan to actively participate in communication with the public through the chosen social media;
- Build trust among the participants; and
- Follow public affairs guidelines when using social media.

The State Department's Use of Social Media

The second panelist presented a case study of the State Department's use of social media to support its mission of public diplomacy. The panelist explained that the State Department's public diplomacy mission to inform, influence, and engage foreign publics on U.S. values and policies has been in place for 60 years. To achieve this mission, the State Department built libraries oversees and established people-to-people exchanges, which are still the preferred methods of sharing the American experience with foreign nationals. According to the panelist, social media present the perfect digital complement to direct personal exchanges and provide an opportunity to amplify traditional programs.

The State Department has undertaken several key forays into social media, including engaging Arabic-speaking bloggers, creating a presence on Facebook, using Twitter, conducting two global video contests, and establishing a social network. The State Department has also created mobile games and has begun using Second Life, an online virtual gaming environment.[4] The panelist showcased a State Department video contest initiated to encourage individual participation by prompting anyone in the world to complete the phrase "Democracy is_____." The State Department made the videos available on America.gov, thereby prompting further online discussion and participation. It also used social media technologies to expand the reach of

[4] Second Life is a virtual world developed by Linden Labs that enables people to create avatars (*i.e.,* computer representations of themselves), who can socialize with other users, conduct business, own property, and attend educational functions. The State Department has used Second Life to conduct public diplomacy and discussions with groups around the globe in this virtual world.

major public diplomacy initiatives such as the President's June 2009 "New Beginnings" speech in Cairo, Egypt, which enabled individuals to sign up to receive text messages of the speech. The speech was translated into Farsi, Arabic, and Urdu, thereby reaching much of the Middle East and places as far away as Pakistan.

The panelist explained that as the State Department began preparing to create its new social media site, its leadership examined the privacy, records management, legal, and diplomatic security implications of using these new tools prior to launching its social media site and is continuing to develop internal policies and guidelines for its use of social media.

The Federal Emergency Management Agency's Use of Social Media

FEMA provided the next case study. According to the FEMA representative, FEMA's experience with social media began in 2007 with its interest in sharing video content through the YouTube website. FEMA's social media strategy began with a legal analysis and expanded to privacy, records retention, IT security, branding, and management issues. To address these issues, FEMA created a FEMA-wide policy working group that brought together stakeholders from program offices, records management, IT and IT security, legal, external affairs, and the policy office. FEMA's YouTube channel went live in May 2008. Since that time, FEMA has also begun using other third-party Web 2.0 services including Twitter, Google Books, Facebook, and My Space. To complement its use of third-party products, FEMA launched a multimedia site on FEMA.gov that allows users to watch and embed videos without persistent cookies.[5]

According to the panelist, FEMA was the first federal agency to enter into an agreement with YouTube. FEMA's use of social media, the panelist explained, enables it to quickly and directly fulfill its public mission to inform the public by providing alerts about the location and nature of disasters, and by making shelter and disaster recovery information and other resources available on the FEMA sites. FEMA is interested in using these same social media tools to work more directly and dynamically with its state and local partners. This would enable collaboration and information sharing with both the internal FEMA audience and the external public audience. A key advantage of the new collaborative tools is FEMA's ability to interact with state and local partners during a disaster. FEMA intends to extend this same level of interaction to non-government organizations such as the American Red Cross.

The FEMA panelist recommended the following strategic approach for government agencies using social media:

- Identify a mission need and specific authority;
- Assemble all stakeholders including privacy, legal, IT security, and records management to identify issues the agency must address in order to use social media technologies; and
- Develop a plan to address all issues identified by stakeholders, preferably documenting them in official standard operating procedures.

The panelist also discussed a number of challenges in controlling the official messages that an

[5] Persistent cookies are small files that remain on a user's hard drive until they are erased or expire, in contrast to session cookies, which disappear after a user closes the current internet session. Persistent cookies are often used to collect information about a user (*e.g.*, web surfing behavior, user preferences, etc.). http://www.webopedia.com/TERM/P/persistent_cookie.html.

agency distributes through social media. The panelist identified three significant challenges: (1) having an effective mechanism to identify official spokespersons within an agency; (2) having clear internal guidance on what agency information may and may not be shared; and (3) having a structured approach to the development of social media projects. Another panelist added the challenge of educating agency personnel who represent the agency through social media about the legal and policy rules that apply to their use of these tools.

The FEMA panelist highlighted the importance of branding social media sites so that the public is clear about which sites and services are official and thus trustworthy. The panelist also stressed the importance of maintaining control over the authoritative source of information. FEMA uses its official government website as the source of FEMA information and uses social media sites strategically to drive the audience to the FEMA.gov website for official information.

The National Academy of Public Administration's Use of Social Media

The NAPA representative began by discussing how difficult it can be to locate government services online when they are posted using the government's organizational structure. Individuals often have to know how an agency is organized to find a particular service. According to the NAPA panelist, a better approach is to present the services in a user-driven, intuitive manner. The panelist also described the challenge of working through the legal, regulatory, and policy issues that must be addressed before a new model for online government services can be implemented. The panelist noted that these challenges are not technology challenges, and that, in fact, social media can be used to identify new opportunities to improve the availability and delivery of government services.

NAPA's online Collaboration Project is a prime example of the ability to involve the public directly in collaboration with the government.[6] The NAPA panelist explained how the website provides a forum for participants to post actual case studies of real government agency challenges. The online collaboration areas on NAPA's website allow individuals to describe a business problem they want to solve, an approach to address the problem, the lessons to be learned, and ultimately to share any results of the process with the other participants in the case study collaboration area.

The panelist emphasized that the true challenge in offering online collaboration services is to foster a meaningful discussion by maintaining momentum and value. One way to foster a robust level of dialogue and produce actionable results from brainstorming sessions, the panelist said, is to specifically identify relevant experts and representatives from diverse perspectives to participate directly in the discussion to keep it moving in a productive direction. Thus, according to the panelist, the ongoing management challenge in social media engagements ultimately can move away from managing the technology toward managing the collaboration itself.

The panelist noted that NAPA has found that the public can also moderate a discussion and keep it focused. As an example, the panelist highlighted NAPA's online dialogue about health IT and privacy, which produced a set of proposed principles that were developed during the online

[6] http://www.collaborationproject.org. Participants in the Collaboration project can dialogue about different laws and policies as well as government operations to find better ways to craft online government services. Topics covered have included: procurement law, compliance with Section 508 of the Rehabilitation Act of 1973, privacy, security, and data authenticity.

discussion.[7] The unique value offered by such use of online social media, the panelist stated, is the individuals' ability to participate directly in the discussion of important government policy issues.[8]

The Transportation Security Administration's Use of Social Media

The TSA panelist discussed the value of government-sponsored blogs. According to the panelist, one of the key advantages of blogging is the ability to illustrate the human side of an agency's workforce, for example, the challenges TSA screeners face when interacting with travelers in pressured situations. The TSA blog provides an alternative avenue for TSA to provide general explanations and additional context about issues that arise during the passenger screening process. It also provides a forum for TSA to describe the rationale for the agency's policies and practices. The panelist noted that the TSA blog's tone is informal and encourages conversation. The blog provides additional background information about TSA activities and thus a greater level of transparency. The blog also creates another channel for providing direct and quick clarification regarding issues of public concern. Other panelists added that, in their experience, blogs provide an opportunity for agencies to make real, direct, meaningful improvements in their services in response to public concerns.

At this point, panelists discussed the critical question of whether to moderate comments on government blogs and social media sites, and if so, how to moderate them. They discussed the importance of posting clear policies on agency social media sites describing the standards agencies use to determine which comments they will and will not post. The TSA panelist explained, for example, that TSA will not post comments that include abusive language, personal attacks, personal information, or spam.[9] The panelist also noted that senior management is actively involved in the review process for comments submitted by the public. In a subsequent panel, panelists discussed the First Amendment implications of government's moderating public comments on government websites.

The TSA panelist offered the following suggestions for operating a successful blog:

- Find an internal champion within the agency who can drive resolution of issues and the development of policy;
- Identify as agency spokespersons individuals whose temperaments are compatible with the informative and informal nature of the blogging culture;
- Develop standard operating procedures to formalize the process for facilitating, managing, and contributing to the agency blog; and

---

[7] Information about NAPA's activities is *available at* www.napawash.org.

[8] From July to October 2009, NAPA hosted the DHS National Dialogue on the Quadrennial Homeland Security Review (QHSR), This National Dialogue tool enabled the DHS stakeholder community to participate in a dynamic, interactive discussion about the QHSR and directly inform the work of the DHS study groups developing the Department's strategic direction over the next four years. The QHSR is scheduled to be delivered to Congress in a final report by December 31, 2009. More information on the QHSR process is available at www.dhs.gov/qhsr.

[9] The TSA panelist then discussed the benefit of TSA's "Delete-O-Meter" as a demonstration of transparency regarding how few posts are actually blocked. TSA's Delete-O-Meter lists the number of posts to the TSA blog (www.tsa.gov/blog) that were deleted. TSA provides a written explanation of this meter along with the rules that TSA applies to determine if a particular post would be deleted on a page dedicated to the Delete-O-Meter: http://www.tsa.gov/blog/2008/02/welcome-to-delete-o-meter.html.

- Maintain public awareness of the blog to continue the momentum and value of the online dialogue.

The TSA panelist also discussed the value of using these social media tools internally, and specifically mentioned TSA's "Idea Factory," an intranet forum that empowers TSA employees in the field to propose improvements to TSA procedures. Ideas suggested via the Idea Factory are voted upon and discussed across the agency, thereby promoting a richer dialogue that provides greater diversity of actionable proposals for policies and procedures. This intranet forum is now being expanded across DHS.

The TSA panelist also noted the cross-over value of using Twitter along with an agency's blog. TSA uses Twitter to notify the public of new blog posts. TSA also uses these quick announcements as another venue for direct dialogue with the public, where individuals may ask, for example, whether they can carry specific items on board their flights and receive immediate answers from TSA, thereby also informing all who are following the discussion.

The Environmental Protection Agency's Use of Social Media

The EPA has found that social media can play a unique role in extending agencies' public education efforts. The EPA panelist spoke specifically of EPA's use of social media to educate the public about the dangers of radon. EPA launched an online video contest called "Radon: Test, Fix, Save a Life," the first online video contest in the federal government. According to the panelist, EPA asked citizens to submit their own video public service announcements on radon and launched the "Radon Leaders Saving Lives" campaign, a joint effort with EPA's state and local partners, to greatly reduce radon-induced lung cancer deaths. To promote better collaboration and communication, EPA also launched RadonLeaders.org, which provides discussion forums, blogs, a calendar, and many additional resources. The panelist noted the lengthy internal planning required to develop a social media strategy that supports these social media initiatives and the need to comply with applicable administrative, technical, and legal requirements.

The EPA panelist also discussed "crowd sourcing" – directly engaging the public in the development of services and information (such as educational videos) that the government has traditionally developed itself. Crowd sourcing can reinvigorate both web content and the public's interest. It can also resolve the challenges presented by traditional broadcast methods of public education, which are being overshadowed by the large number of television and radio channels and by individuals' use of technologies such as digital video recorders which enable individuals to select the content they want to view.

As the panel concluded, the representatives collectively discussed the advantages of delivering content online through emerging social media avenues – specifically, as one panelist suggested, the fact that the act of searching for information instead of passively receiving it makes that information more meaningful. In addition, several panelists supported the view that the significance of information is heightened when someone else recommends it – a defining characteristic of the social media environment. The panel demonstrated how federal agencies are experimenting with these new tools and creating initiatives to increase public participation in government.

Panel 2: How Does Government 2.0 Impact Privacy?

The workshop's second panel explored how government's use of social media impacts, or could potentially impact, the privacy of individuals. The panelists included representatives of privacy and civil liberties advocacy groups, government, and academia. Panelists discussed the privacy issues posed by government's use of social media on both government-controlled and third-party websites, and offered guidance on how government can address these issues.

The panel began with a discussion of citizens' expectations about their interactions with government through social media and, in particular, their expectations about how the government uses the information they provide about themselves on social networking sites. One panelist analogized individuals' assumptions about their interactions with government in these settings to using a one-way mirror. People value the transparency into government activities that social media can provide and want to be able to see what the government is doing. At the same time, however, people do not want or expect that government will peer into their personal lives. According to the panelist, there is a presumption of openness for government-to-citizen communications, but a presumption of privacy when individuals communicate with the government. Panelists generally agreed that government agencies should take this distinction into account as they engage the public through social media activities.

Several panelists expressed the view that individual privacy could be either enhanced or diminished by government's use of social media, depending upon whether and how government agencies collect or use personal information disclosed by individuals in interactive settings. Privacy is least affected when agencies use social media solely to disseminate information to the public or to make their core functions, *e.g.*, providing services and benefits, more efficient and user-friendly. Privacy concerns are heightened, however, when government agencies participate in interactive settings, for example, through government pages on social networking sites that are designed to enable the sharing of virtually unlimited personal information – and where personal information is, in fact, shared extensively. When an individual "friends" the government on a social networking site, that individual is giving the government access to all the personal information that his or her other friends know. As one panelist suggested, social networking sites are premised on equality among participants; but the government cannot be an ordinary participant or a "friend." For that reason, in this panelist's view, social networking is not an appropriate technology for government agencies' interactions with citizens. Panelists agreed that privacy could be compromised if there are not clear limits on how the government uses personal information to which it has access in social networking environments. Indeed, there was general agreement among the panelists that government agencies should not collect personal information posted by individuals on government-sponsored blogs or government web pages on social networking sites without a compelling reason at a minimum, or if at all.

Panelists also discussed the privacy implications of government's use of third-party commercial providers to gather personal information for traditional government functions on their websites (*e.g.*, applications for employment or benefits, identity verification, etc.). As one panelist noted, individuals expect that only the government makes use of personal information provided through these functions and may not understand that the information they provide is actually collected and stored on third-party servers. Panelists agreed that service providers should be prohibited

from using personal information gathered on behalf of government agencies for their own purposes, such as tracking individuals' online activities or marketing to them.

Panelists raised similar concerns with regard to some government agencies' practice of allowing third parties to serve content on government websites. In these panelists' view, there must be restrictions on how third parties use personal information they gather through cookies or other tracking technologies deployed in the process of serving content on government websites to ensure individuals' privacy is not compromised. Panelists noted that there is considerable confusion as to whose privacy policy applies when a third party serves content on a government agency website, and they agreed that agencies should be transparent to the public about the role third parties play on their websites. Several panelists noted that uncertainty about who has access to personal information provided through government use of social media could diminish individuals' willingness to express their views and otherwise interact with the government.

Panelists offered several suggestions for addressing the potential privacy impacts of government use of social media. There was consensus that, in keeping with President Obama's Transparency and Open Government Initiative, government agencies should be transparent in their interactions with individuals through social media and have clear website privacy policies. There was also general agreement that the legal structure underpinning government's collection of personal information should be strengthened. One panelist urged that Congress amend the Privacy Act of 1974 to reach government web pages on third-party websites, even though the government does not control those sites.

Panelists also agreed that clear rules are needed for government's interactions with the public through social media. Government agencies should abide by the well-established FIPPs when engaging the public in using social media – particularly the purpose specification, use limitation, individual participation, and data minimization principles. As one panelist recommended, agencies should limit the personal information they collect through social media to that which is absolutely necessary, and should provide strong opportunities for individuals to exercise choice about how agencies use the personal information they submit. If agencies wish to solicit feedback about information they have provided through social media, the panelist opined, they should do so without collecting personal information. Another panelist urged government agencies to use their web pages on social networking sites solely for the purpose of "pushing" information out to the public, and to steer citizens to their official agency websites to submit comments or provide personal information.

Panelists expressed support for the government's experimentation with social media to enhance transparency, but cautioned that the government has a responsibility to take the lead in implementing privacy protections in interactive environments. One panelist argued that, given the government's ongoing interest in having web pages on social networking sites and in allowing third parties to provide content through social media on their sites, government agencies should use the contracting process to require third parties to implement rigorous privacy standards in their Terms of Service (TOS) and online Terms of Use.

As the panel came to an end, several panelists called upon government agencies to be proactive in educating the public about how to protect their privacy in interactions with the government

through social media. Public education on the benefits and risks of using social media, one panelist argued, is an inevitable aspect of government's role.

Panel 3: What Security Issues Are Raised by Government 2.0?

The workshop's third panel addressed the question of how to facilitate the secure use of Web 2.0 technologies within the federal government in a way that ensures security is supportive of the deployment of new technologies. The discussion focused on social media and cloud computing. Panelists included security and technology experts from federal agencies, the private sector, and academia.

Threats Against the Federal Government

By way of introduction, panelists discussed the threats the federal government faces when it uses social media, threats that differ in kind from those individuals face when using social media from their personal computers. Social media applications rely on user-generated content that can be added and viewed from anywhere in the world; however, as the panelists pointed out, these feature-rich applications also expose websites to new vulnerabilities for attack.

Panelists also mentioned the significant threat arising from our adversaries' efforts to collect data, and noted that social media websites may be a rich target with lots of sensitive data aggregated on one social network. Panelists stated that both good personal security practices and good federal agency security policies are essential to combating this threat. In addition, panelists urged federal agencies to engage with social media networks to reduce the likelihood that social media networks will be targeted for their valuable aggregated data. Panelists also noted that sensitive information can be placed on social media networks and shared so quickly that it can be difficult for government to respond effectively to remove it. Even if, however, the government tries to withdraw or close off social media access, it may not be able to address these new, emerging threats. According to these panelists, there is a need to maintain collaboration among federal agencies and monitor the current social media environment from a security perspective.

Benefits of Using Social Media

Panelists suggested that expanding social networks can foster a number of security benefits such as enabling the government to inform the public about new vulnerabilities or threats. This information can be shared in real-time, and users can respond to protect themselves. A Web 2.0 platform can enable better security decision making and, in this way, panelists agreed, using Web 2.0 technologies may actually enhance security.

One panelist noted that using Web 2.0 applications through a "Software as a Service" (SAAS) model ensures that end users will always have the latest software version, eliminating the need to download a patch to maintain the software. In the panelist's view, if federal agencies deploy and host their own Web 2.0 applications, such as an internal social networking capability, they will have better visibility and control over users and data on their websites. This would enable

websites to conduct real-time monitoring, response, and intelligence-gathering about security threats.

Panelists next discussed how the government can ensure the reliability of information as the government increasingly engages in Web 2.0 technologies. Panelists agreed that an authoritative government information source is necessary and mentioned Data.gov as a good example of how to provide government information to the public in an effective manner. Panelists noted the benefits of the Web 2.0 "Wikipedia Effect" (also known as crowd sourcing, discussed earlier), whereby so many individuals see data that, if inaccuracies exist, they are noticed and corrected. Panelists also suggested that tagging information can help to identify authoritative data and its origin.

Secure Social Media Use

Panelists also discussed federal agencies' differing approaches to providing or blocking access to social networking platforms. One panelist commented that the security in place for most federal agencies' Web 2.0 applications fits the castle-and-moat paradigm of security; the moat is dry and the front door is open. As the panelist explained, our nation's adversaries do not need to use sophisticated attacks when baseline federal information security is poor. Panelists agreed that federal agencies must employ a risk-based approach when making information security decisions regarding social media. They suggested that agencies consider the particular mission and the data being exposed, rather than applying a blanket policy for an entire agency or program, and make information sharing and social media decisions based on the sensitivity and potential impact of disclosing government data.

One panelist compared information systems to a battleship taking on water. A ship is meant to continue operating during a fight, to take on water but still stay afloat. Information systems should operate in a similar manner, the panelist opined, so they remain functional and protect their data even when under attack. Coordinated policies throughout federal information systems would make this possible, the panelist argued, but the requisite coordination does not yet fully exist. The level of employee access to social media provided by federal agencies varies widely. Though there may be good reasons to block some sites at some agencies, panelists agreed that agencies fail to communicate with each other about how they make these decisions and do not always apply the same criteria. One panelist speculated that the problem, perhaps, is not so much a lack of communication, though communication is not optimal, but rather a lack of coordinated policies and procedures. When agency Security Operations Centers and Network Operations Centers are monitoring incoming traffic, they make decisions based on the operational information they see. An outdated policy may say to block one site but not another, based solely upon whether a site was launched before or after the policy was created. Panelists agreed that more relevant policies and more flexible procedures are needed to address personal and professional use of social media as well as monitoring capabilities.

Panelists also discussed the issue of government employees' personal use of social media in ways that could compromise government security. Several panelists opined that users will find work-arounds to gain access to social networks if federal agencies choose to block those networks. In these panelists' view, federal policy and training on use of internet resources has not changed, though usage and behavioral norms are different on social media websites. In their

view, it is necessary to identify new best practices that enable federal employees to secure their personal and professional personas as they use social networking. Some panelists recommended keeping two online personae, one personal and one professional. Other panelists expressed the view that most government managers are even unaware that their employees are engaging in social media. How many government accounting departments, one panelist asked, truly know how many of their interns are updating their Facebook status throughout the day?

Cloud Computing

The panel concluded with a discussion of cloud computing.[10] There was general agreement that, despite the trend toward storing data "in the cloud," data centers will not disappear. It is still necessary for government agencies to implement strong security, to certify and accredit systems, and to follow National Institute of Standards and Technology (NIST) guidance[11] to put controls in place and mitigate risk. Panelists agreed that agencies must change standard contract language to require visibility into service provider capabilities, update TOS agreements, and improve security controls and asset management to demonstrate strong data security. Even though the locus for processing of information is shifting, government agencies and contractors need to know what information they have, where that information is stored, who is using that information, and who has access to it. In addition, panelists agreed, government agencies must use the new tools securely. While the panelists acknowledged that cloud computing may have security weaknesses, they said processes can be instituted to make it more secure. Currently, many outsourced and contracted web services store or process government data and applications. As panelists pointed out, this is a jurisdictional issue with both legal and security implications that raises the question: is protecting data in the cloud the government's responsibility as the data owner, or the cloud's responsibility as the service provider?

Other panelists argued that the way government agencies create agreements and construct information systems may change, relying less on contracts and more on handshakes to create a "spontaneous cloud," or spontaneous web services, pulling together whatever web services are necessary to complete a particular task. This model would be less regimented and formalized than the way agencies do things today, offering more flexible and rapidly deployable capabilities. Panelists also discussed how the different services available, including Infrastructure as a Service (IAAS), Platform as a Service (PAAS), and SAAS, vary in terms of security considerations. Panelists commented that cloud computing is really about distributing computing resources and activities. The process of discovering where data resides will require a set of tools different from those available today.

---

[10] The NIST working definition of cloud computing is "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (*e.g.*, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." *Draft NIST Working Definition of Cloud Computing*, NIST Information Technology Laboratory, Aug. 21, 2009 *available at* http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc.

[11] *See Managing Risk from Information Systems*, NIST SP 800-39, Apr. 3, 2008. *See also Recommended Security Controls for Federal Information Systems and Organizations*, NIST SP 800-53 Rev. 3 CNTL. No. AC-20, Aug. 2009.

Panel 4: What Legal Issues Are Raised by Government 2.0?

Panelists on the workshop's fourth panel represented federal agencies and academia. They acknowledged that President Obama's Transparency and Open Government Memorandum,[12] which directs federal agencies to harness new technologies (*e.g.*, social networking tools) to engage the public, has been the driving force behind the recent increase in government use of social media. Panelists stated that agency engagement with the public via social media should be encouraged, but cautioned that government use of social media raises significant and complex legal issues. Nonetheless, panelists agreed that these issues should not be perceived as barriers to government use of social media.

Panelists discussed the following issues raised by government use of social media:

- The implications of the Rehabilitation Act of 1973;[13]
- The implications of the Federal Acquisition Regulation (FAR), which governs federal agency procurement of goods and services;[14]
- Legal issues raised by social media providers' Licensing Agreements and Terms of Service;
- Ethical issues;
- Records management issues;
- The applicability of the Privacy Act of 1974, as amended;[15]
- The implications of other federal laws and policy, including the Freedom of Information Act (FOIA),[16] the Paperwork Reduction Act (PRA),[17] the Federal Advisory Committee Act (FACA),[18] the E-Government Act of 2002 (E-Government Act),[19] and the Office of Management and Budget (OMB) prohibition against federal agency use of persistent cookies and other web tracking technologies;[20] and
- First Amendment issues.[21]

To begin the panel, one member presented an overview of the legal issues raised by government use of social media and provided an introductory description of the legal topics that the panelists would discuss.

---

[12] 74 Fed. Reg. 4685 (Jan. 21, 2009).
[13] 29 U.S.C. § 794(d).
[14] 48 C.F.R. chs. 1-99 (2009). The FAR codifies uniform policies for the acquisition of supplies and services by federal executive agencies.
[15] 5 U.S.C. § 552a (1974), as amended.
[16] 5 U.S.C. § 552 (2006), amended by OPEN Government Act of 2007, Pub. L. No. 110-175, 121Stat. 2524.
[17] 44 U.S.C. § 3501 et. seq.
[18] 5 U.S.C. App. 2 and its implementing regulations at 41 C.F.R. § 102- 3.
[19] Pub. L. 107-347 (2002).
[20] *See* OMB, Executive Office of the President, OMB Memorandum No. 03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, Attachment A § III (D)(2)(a)(v)(1) (a)-(b) (prohibiting federal agency use of persistent cookies and other web tracking technologies except that agency heads may approve the use of persistent tracking technology for a compelling need).
[21] The First Amendment provides that "Congress shall make no law . . . abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances." U.S. Const. amend. I.

The Rehabilitation Act of 1973

The first panelist discussed whether Section 508 of the Rehabilitation Act of 1973 applies to government use of social media. Section 508 requires that the government make its electronic and information technology accessible to its employees with disabilities. It also requires that individuals with disabilities who are seeking information or services from a federal agency have access to and use of information comparable to that provided to the general public, unless an undue burden would be imposed on the agency. The panelist observed that it is yet unclear whether Section 508 applies to third-party social media websites. The panelist reported that some government agencies are currently using social media provider websites that do not comply with Section 508, but that the issue is as yet unsettled and requires the government to issue further clarification of the rules. The U.S. General Services Administration's (GSA) *Social Media Handbook* advises that GSA employees and contractors using non-accessible non-federal sites to also make the information available in alternative formats for individuals with disabilities.[22]

Procurement/Federal Acquisition Regulation

The next legal issue discussed was the application of the FAR to social media. One of the panelists stated that the FAR does not apply to government acquisition of social media services because most of the services are free, and the FAR only applies to the acquisition of services by contract with appropriated funds. The panelist stated that the FAR was enacted to ensure that the government conducts business with integrity, impartiality, fairness, and openness.[23] Accordingly, the panelist queried whether government procurement processes (which are well-defined and require that executive agencies meet certain requirements when acquiring software, supplies, and other services with appropriated funds) should also apply to government use of social media tools.

The panelist suggested that the government could acquire Web 2.0 technologies in several ways. First, the government could use the "traditional procurement process," which, the panelist stated, is administratively burdensome and may hinder the government's ability to procure Web 2.0 technologies in a timely fashion. Second, the government could choose to adopt an "open use" model, which would permit the government to obtain Web 2.0 technologies in the same manner that the private sector obtains the technologies (*i.e.*, without the administrative constraints that hamper the government's efforts to procure technologies). The panelist argued that the disadvantage of this model is that there is a risk that the government could be viewed as choosing favorites among social media providers, and that the government could be locked into a licensing agreement with a social media company that does not benefit the government. Third, the government could adopt a "conditional use" model, which would allow the government to develop policies and procedures to govern its acquisition of Web 2.0 technologies. In the panelist's view, the "conditional use" model would be the best option for the government, as the policies and procedures developed would mitigate any appearance of favoritism in the choice of

---

[22] GSA Order CIO P 2106.2, *Social Media Handbook*, July 17, 2009, http://www.gsa.gov/graphics/staffoffices/socialmediahandbook.pdf, pages 9-10.
[23] *See* 48 C.F.R. § 1.102-2(c)(1)(2009).

social media and would provide the flexibility the government needs to acquire Web 2.0 technologies in a timely fashion.

Licensing Agreements/Terms of Service

The panelists then discussed the clauses included in most social media service providers' licensing agreements and TOS that may create complications with the government as end user, as well as the potential endorsement issues raised by government use of social media. One panelist identified indemnification, choice of law, and confidentiality clauses, as well as clauses that permit providers to use a government seal for commercial purposes, as provisions that could create unique problems for government entities. Most social media provider licensing agreements and TOS include indemnification clauses that require users to compensate social media providers for any losses incurred as a result of the actions of the user. The panelist noted that the government is prohibited by the Anti-Deficiency Act from agreeing to open-ended indemnification clauses, and that the open-ended nature of the providers' clauses could obligate the government to expend funds in excess of the amount available in the agency's fiscal year appropriation, thus violating the Anti-Deficiency Act.[24] The panelist advised that the only way to pursue a tort claim against the federal government, however, is to initiate a claim under the Federal Tort Claims Act (FTCA),[25] which authorizes tort suits to be brought against the government. Thus, the panelist recommended that the provision be amended in negotiations with social media companies to invoke the FTCA so that individuals are provided a venue to sue the government, which would otherwise be unavailable to them.

The panelist also noted that social media licensing agreements and TOS usually include choice of law clauses that require that disputes be settled in state courts, and opined that subjecting the federal government to such clauses may violate the Supremacy Clause of the Constitution.[26] The panelist stated that the government cannot agree to a clause that limits jurisdiction to state courts because the Supremacy Clause of the Constitution mandates that suits brought against the government be initiated in federal court. The choice of law clauses may also implicate the doctrine of sovereign immunity, which prohibits individuals from suing the federal government without its consent and is derived from the Eleventh Amendment.[27] That panelist recommended that federal agencies revise choice of law clauses to permit the initiation of law suits in federal court pursuant to any applicable federal statute.

The panelist stated that confidentiality clauses included in many social media provider licensing agreements and TOS provide that the agreements are confidential, to protect the social media provider's trade secrets. The panelist noted, however, that the government cannot agree to such provisions because it is required to disclose non-exempt information to requesters pursuant to

---

[24] The Act prohibits the Government from "making or authorizing expenditure from, or creating or authorizing an obligation under, any appropriation or fund in excess of the amount available in [an] appropriation or fund unless authorized by law." 31 U.S.C. § 1341 (a)(1)(A).

[25] 28 U.S.C. § 1346(b).

[26] U.S. Const. art. VI.

[27] The Eleventh Amendment provides that "the Judicial power of the United States shall not be construed to extend to any suit in law or equity, commenced or prosecuted against one of the United States by Citizens of another State, or by Citizens or Subjects of any Foreign State." U.S. Const. amend. XI.

FOIA.[28] The panelist recommended that government agencies should consider revising these clauses to state that information will be reviewed and released in accordance with FOIA.

The panelist further explained that many social media licensing agreements and TOS include clauses that allow social media providers to use government content (*e.g.*, an agency's official seal) for commercial purposes. The panelist noted, however, that the government cannot agree to such terms, because it is prohibited from endorsing commercial products.[29] The panelist argued that allowing social media companies to use government content or the seal in this manner could be interpreted as an endorsement of particular social media providers. The panelist noted that social media providers are allowed to say that the government uses the service, but that providers may not represent or imply that the government endorses a particular social media provider. The panelist also cautioned government agencies against linking to third-party social media websites, because doing so could be perceived as an endorsement of those sites.

Ethics

According to one panelist, ethics is a subset of all of the legal issues raised by the panelists. The panelist stated that government use of social media represents a new way for the government to conduct business, and that the rules that currently govern the government's use of Web 2.0 technologies may be insufficient. The panelist opined that while many existing ethics rules are applicable, new rules may also have to be developed. Ethical rules, suggested the panelist, should focus on individual employees, as well as employees acting in their official capacities, and the panelist urged that guidance be developed to govern employees acting in both their official and personal capacities when using social media websites.

Records Management

One of the panelists, a representative of the National Archives and Records Administration (NARA), discussed records management issues associated with government use of social media, focusing on the question of whether records posted on social media websites are federal records pursuant to the Federal Records Act.[30] The panelist noted the breadth of the Act's definition of "record," and opined that if the government is conducting official business on social media websites, the definition is likely broad enough to encompass the government's activities on those sites. The panelist opined that many federal agencies engaging the public via Web 2.0

---

[28] FOIA provides that individuals have the right to request federal agency records unless the records (or portions of them) are protected from public disclosure by one of nine exemptions. *See* 5 U.S.C. § 552 (2006), amended by the OPEN Government Act of 2007, Pub. L. No. 110-175, 121Stat. 2524.

[29] *See e.g.*, 41 C.F.R. § 102-173.95 (2009) (providing that "[a] .Gov Internet domain cannot be used to imply in any manner that the government endorses or favors a specific commercial product, commodity, or service . . . [cannot] post ads directly on government sites as the .gov guidelines state, and [government space] cannot be used to advertise for private individuals, firms, or corporations.").

[30] The Act provides that "records" include "all books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them." 44 U.S.C. § 3301.

technologies have not yet addressed whether the records they post on social media websites are federal records and whether those records must be preserved. The panelist also opined that many of the records posted or created on government sponsored pages on social media websites may qualify as "temporary federal records" that must be retained for a specified duration of time identified in an agency's records retention schedule.[31] NARA has updated its earlier guidance to assist agencies with making these decisions.[32]

The Privacy Act of 1974

The next panelist discussed whether the Privacy Act applies to government use of social media. The Privacy Act establishes a code of fair information practices that govern the collection, maintenance, use, and dissemination of personally identifiable information (PII) about individuals that is maintained by federal agencies in systems of records. The panelist argued that the key issue is whether or not the agency maintains "control" over the data posted or created on social media websites, and opined that in many instances the government does not maintain such control. The panelist argued that even though many privacy advocates have recommended that the Privacy Act be amended to reflect advances in technology (*i.e.*, the development of Web 2.0 technologies), the Act in its existing form provides a viable analytical framework for evaluating whether an agency exercises "control" over records created or posted on social media websites.[33]

The panelist identified three categories of government use of Web 2.0 technologies. The first category applies to government-owned and government-controlled Web 2.0 technologies. The panelist opined that the Privacy Act applies to the government's use of such technologies to the extent that the government retrieves information by name or personal identifier. The second category applies to Web 2.0 technologies that are controlled by the government, but are owned by private entities. The panelist suggested that subsection (m) of the Privacy Act would apply to Web 2.0 technologies used in these circumstances, if the government retrieves information by name or personal identifier.[34] The third category includes privately-owned and privately-controlled Web 2.0 technologies. In the panelist's view, the Privacy Act does not apply to government use of privately-owned and operated Web 2.0 technologies because in this instance,

---

[31] Pursuant to 44 U.S.C. § 3303, all federal records must be scheduled according to an agency schedule or a General Records Schedule (GRS), which provides disposition authority for temporary administrative records common to several or all federal agencies. All records schedules must be approved by NARA and must identify records as "temporary" or "permanent" records. Accordingly, records schedules provide instructions for the disposition of "temporary" and "permanent" federal records.

[32] *See NARA Guidance on Managing Web Records* (Jan. 2005) *available at* http://www.archives.gov/records-mgmt/pdf/managing-web-records-index.pdf; *see also NARA Implications of Recent Web Technologies for NARA Web Guidance* (Sep. 16, 2009) *available at* http://www.archives.gov/records-mgmt/initiatives/web-tech.html.

[33] The panelist noted that the scope of the Act's coverage is dependent upon whether the records are considered to be within a "system of records," and that whether a record is considered to be within a "system of records" is dependent upon whether the agency exercises "control" over the record. The panelist advised that it is useful to examine the Privacy Act's definition of a "system of records," which provides that "a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some number, symbol, or other identifying particular assigned to the individual," because the definition articulates a "control" test. 5 U.S.C. § 552a(a)(5).

[34] Subsection (m) of the Privacy Act provides that "[w]hen an agency provides by a contract for the operation by or on behalf of an agency of a system of records to accomplish an agency function, the agency shall, consistent with its authority, cause the requirements of [the Privacy Act] to be applied to such system." 5 U.S.C. § 552a(m)(1).

the government does not exercise "control" over the records as defined by the Privacy Act. The panelist cautioned, however, that the Privacy Act *may* apply to government activities on privately owned and operated social media websites if the government collects information and incorporates the information into agency files. The panelist advised federal agencies to ensure that they do not disclose Privacy Act protected materials on social media websites unless one of the Act's exceptions authorizes the disclosure.[35] Finally, the panelist advised that agencies should be careful not to collect information about an individual's exercise of his or her First Amendment rights, unless doing so is related to an authorized law enforcement activity.[36]

The Freedom of Information Act, Paperwork Reduction Act, the Federal Advisory Committee Act, the E-Government Act, and Web-Tracking Technologies

The panelists discussed the implications for government use of social media in light of FOIA, the Paperwork Reduction Act (PRA), the Federal Advisory Committee Act (FACA), the E-Government Act, and OMB's prohibition against federal agency use of "persistent cookies" and other web tracking technologies.[37] One panelist noted that courts construing FOIA's definition of "agency records" focus on the element of control, not unlike the Privacy Act analysis discussed earlier in the panel. The panelist stated that courts apply a four-part test when determining whether an agency exercises "control" over a record. They examine the following: (a) who created the record and the intent of the record creator; (b) whether the agency intended to relinquish control; (c) the agency's ability to use or dispose of the records; and (d) the extent to which the records are integrated into the agency's files.[38] The panelist opined that the test is instructive and provides a useful framework for determining whether an agency exercises "control" over records created or posted on social media websites.

The panelist also suggested that the PRA, which applies to governmental solicitation of information from ten or more persons,[39] may apply to many activities the government conducts on social media sites because the government often allows users to submit comments. The panelist advised that agencies should also be cognizant of FACA when engaging the public via social media tools and that government activity on social media websites may trigger FACA. FACA applies to groups established by a federal official that provide advice to federal agencies and members of the general public.[40]

---

[35] *See* 5 U.S.C. § 552a(b).
[36] *See* 5 U.S.C. § 552(e)(7).
[37] *See* § 208 of the E-Government Act of 2002, Pub. L. 107-347, and the accompanying guidelines issued by the OMB on September 26, 2003. Section 208 mandates that Federal agencies prepare Privacy Impact Assessments (PIAs) prior to developing or procuring Information Technology systems which collect, maintain, or disseminate information in identifiable form from or about members of the public.
[38] *See Burka v. HHS*, 87 F.3d 508, 151 (D.C. Cir. 1996) (quoting *Tax Analysts v. DOJ*, 845 F.2d 1060, 1069 (D.C. Cir. 1988)).
[39] Among other things, the Act requires that agencies seek public comments on proposed collections of information by publishing notices in the Federal Register for a period of 60 days, and certify to OMB that the agency has taken steps to reduce the burden of the collection on small businesses, local governments, etc. 44 U.S.C. § 3501 *et. seq*.
[40] 5 U.S.C. App. 3 (1972), as amended.

The panelist also discussed OMB's prohibition against federal agency use of persistent cookies and other web tracking technologies on federal agency websites.[41] The panelist inquired about the extent to which tracking technologies are being used on government sponsored web pages on social media websites, and questioned whether OMB's prohibition extends to government activity on those sites. The panelist opined that, as an alternative to using social media websites that use persistent cookies and other web tracking technologies, government agencies could choose to create social networking platforms that conform to governmental privacy and security requirements. Finally, the panelist raised the issue of whether the E-Government Act applies to the government's use of social media. The E-Government Act mandates that federal agencies conduct Privacy Impact Assessments (PIAs) when procuring information technology systems that collect PII.[42] The panelist stated that PIAs provide an opportunity for agencies to examine the privacy and security risks associated with the government's use of social media, but did not express a conclusion as to whether government use of social media activities qualifies as an IT procurement pursuant to the E-Government Act. Some federal agencies such as DHS, however, perform PIAs to evaluate new information collections or other activities that raise privacy issues. The DHS Privacy Office is planning to conduct PIAs for DHS's use of the various types of social media to provide greater transparency in this area.

The First Amendment

The legal issues panel concluded with a discussion about the First Amendment implications of government use of social media. One panelist discussed the applicability of the First Amendment generally, the government's attempt to control speech on government websites and government-sponsored pages on privately-owned social media websites, anonymous speech on government websites, and whether government employees maintain First Amendment rights.

The panelist noted that the government is prohibited from restricting or regulating speech, except in very limited circumstances. The panelist stated that the imposition of restrictions on certain types of speech (*i.e.*, banning racist or hate language) on government social media websites implicates the First Amendment, but cautioned that this area of law is unsettled. According to the panelist, courts asked to determine whether the government's regulation of speech on social media sites violates the First Amendment will likely follow traditional First Amendment analysis, determining, as an initial matter, whether the regulation is taking place in either a "traditional public forum," a "limited public forum," or a "non public forum."[43] The panelist opined that a serious argument could be made that government activity on social media websites can be equated to a traditional public forum, but concluded that courts may likely find that the government's activities on social media websites are comparable to "limited public forums." In that case, the panelist stated, to survive a First Amendment challenge the government would have to demonstrate that its restrictions on speech were necessary, and that they were narrowly tailored to achieve a compelling need. The panelist opined that the government may be able to

---

[41] *See OMB Memorandum No. 03-22*, Attachment A § III (D)(2)(a)(v)(1) (a)-(b).
[42] *See* Pub. L. 107-347 (2002).
[43] *See Perry Education Association v. Perry Local Educators' Association*, 460 U.S. 37 (1983) (recognizing that there are three categories of public forums: "traditional public forums," "limited public forums," and "non public forums)."

limit speech to specific topics on social media websites, but that any further restrictions on speech may be unconstitutional. Accordingly, the panelist noted that governmental attempts to limit offensive, indecent, and hate speech on social media websites may be deemed unconstitutional. The panelist also discussed anonymous speech on government websites and social media web pages. The Supreme Court has held that the First Amendment protects anonymous speech, and opined that the government cannot mandate that individuals disclose their identities in order to express opinions on social media websites.[44] Thus, the panelist argued that providing PII should be voluntary on government social media websites.

Finally, the panelist addressed whether government employees have First Amendment rights. The panelist stated that government employees have First Amendment rights if they are speaking in their personal capacities, but noted that the Supreme Court recently limited the First Amendment rights of government employees speaking in an official capacity.[45] The panelist argued that employees speaking in a personal capacity may not have First Amendment rights if the speech harms the employer, and suggested that the government's rights may outweigh the employee's rights under those circumstances.

Panel 5: What Are the Privacy Best Practices for Government 2.0?

The final workshop panel applied the FIPPs as a framework for developing a roadmap to guide the government's use of social media while protecting privacy. Rooted in the tenets of the Privacy Act of 1974 and mirrored in the laws of many states, as well as many foreign nations and international organizations, the FIPPs provide a framework for identifying and addressing privacy concerns and protections. The panelists represented federal agencies, privacy and open government advocacy groups, and academia. They generally agreed that the eight principles – Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability and Auditing – can serve as a basis for privacy protection in the Web 2.0 world.

Transparency Principle

The government should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII.

The discussion began with the recognition that the government is not just any user of social media. The government bears greater responsibility to the public and carries more clout than other users. Panelists noted that there are several areas of transparency, not only the traditional

---

[44] *See e.g.*, *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334 (1995) (recognizing the tradition of protecting anonymous speech and finding that an Ohio statute which prohibited the distribution of anonymous campaign literature violated the First Amendment).

[45] *See e.g.*, *Garcetti vs. Ceballos*, 547 U.S. 410, 425 (2006) (finding that the "First Amendment [does not] shield from discipline the expressions employees make pursuant to their professional duties [and that] the Court's precedents do not support the existence of a constitutional cause of action behind every statement a public employee makes in the course of doing his or her job.").

focus on notice provided in a privacy policy that describes the website's information practices, but also transparency about process, especially when the government is engaging the public through social media and seeking feedback on issues. The government must explain why it is engaging the public using social media, how it will use the information the public submits, and how the public can influence outcomes related to the issues discussed.

Panelists argued that where agencies find that a social media service provider is unwilling to provide all of the protections in its TOS that the government is seeking on behalf of the public, the government has the option of binding itself publicly and telling the public that it will not do certain things. For example, even if the social media provider collects certain information or has certain optional applications that the public uses, the government can bind itself not to ask the public for certain information or to seek information held by the provider. Panelists noted that it is within the government's control to determine what information it collects and what it discloses. Even when the government uses a social media provider, it can control both of these activities, bind and limit itself, and make its policies transparent.

Panelists recommended that the government be creative when determining how to provide transparency. One panelist suggested that the privacy policy be described in the information section of the TOS and in a prominent place that is relevant to users. Another panelist suggested using an "interstitial" or "bumper"[46] to inform visitors when they are leaving a federal web page to go to a non-federal web page. This pop-up box could also be used to inform visitors about what privacy policy applies and provide a link to the policy. This example of "just-in-time" notice could also be provided where an agency invites visitors to post comments or provide responses to questions. According to the panelists, providing an interstitial or just-in-time notice may be particularly important when an agency's policy includes provisions that visitors would not expect. Panelists generally agreed that the conventional link to the privacy policy at the bottom of a web page alone is insufficient.

Panelists suggested that technology could offer another method of giving notice. The privacy provisions of the E-Government Act require federal websites to have both a "human readable" privacy policy and a machine readable technology that automatically alerts users about whether website privacy practices match the users' personal privacy preferences. One panelist explained that P3P, the Platform for Privacy Preferences Project, a protocol developed by the World Wide Web Consortium, is currently the only industry standard for a machine-readable privacy policy,[47] and described the "Privacy Bird," a software tool developed at AT&T Corporation and later maintained at Carnegie Mellon University's (CMU) CyLab, as an example of the type of P3P tool that the government might consider using. The Privacy Bird was designed to allow users to set their privacy preferences on their browsers and then have the tool review every website

---

[46] Interstitials and bumpers are web pages displayed to users before they are directed to an expected page (*e.g.*, displaying a web page informing a user that he will be redirected to another site several seconds before directly linking him to the other site). http://www.webopedia.com/TERM/I/interstitial.html.

[47] P3P allows websites to state their intended use of information they collect from visitors in a computer-readable format using Extensible Markup Language, or XML. P3P-enabled browsers automatically fetch and read P3P privacy policies on websites and can check privacy policies against the user's preferences or against other legal or regulatory guidelines. P3P client software can be built into a web browser, plug-ins, or other software. Thus, users do not need to read the privacy policies at every site they visit. http://www.w3.org/P3P/.

visited to determine whether the user's privacy preferences are met and, if not, to alert the user to the differences.

OMB Memorandum 03-22, *Guidelines for Implementing the Privacy Provisions of the E-Government Act of 2002*, requires federal websites to adopt machine readable technology that alerts users automatically about whether site privacy practices match their personal privacy preferences. One of the panelists, who had helped develop P3P, stated that the failure of P3P to gain traction is due more to the fact that websites and browsers did not adopt it than to rejection by the public.[48] The public is generally unfamiliar with these tools and the implementations were relatively difficult to use. According to the panelist, CMU is now experimenting with a "nutritional label" for privacy and enhancements to the Privacy Bird.

The discussion then turned to the transparency issue of what privacy policy applies when government content is hosted by a social media provider – is it the government's privacy policy or the provider's policy? This, in turn, raised several questions: Who owns the data? Does the Privacy Act apply? Who is administering the data? One panelist suggested that the answers may depend upon, among other issues, whether the services being performed are an inherently governmental function, whether the government is contracting for the performance of that function, and whether the administration of data includes PII. When the government contracts with a contractor to serve as the government's agent in performing a governmental function, panelists stated, that agent is governed by the policies of the Privacy Act if PII is involved, and the Privacy Act's requirements should be included in the government's contract for such services. The more difficult question is whether no-fee services and TOS agreements for such services should include privacy and other federal requirements. According to the panelists, the challenge is that these social media providers operate to make a profit, which generally means serving advertisements and collecting tracking information, both of which are not practices that are generally appropriate for government web pages.

Panelists suggested that there are at least two approaches the government could take to ensure that federal protections are implemented by social media providers. First, the White House and GSA could negotiate terms on behalf of the entire federal government that provide the types of privacy protections the public expects when engaging with the government. Providers would likely be more willing to accept government-wide terms than to negotiate with individual agencies. Panelists pointed to the White House negotiations with Google regarding YouTube as evidence that social media providers may be willing to make accommodations to obtain government business. One panelist suggested that the Federal CIO Council, in conjunction with the GSA, develop recommended language to address privacy and other legal issues and negotiate TOS agreements with providers that reflect federal government interests. The panelist also suggested another approach: Congress could pass a technology-neutral statute that requires companies to provide certain protections for privacy, accessibility for disabled persons, or other protections.

---

[48] The panelist further stated that P3P failed because (1) websites did not adopt it, (2) browser makers did not feel the need to include it because the websites were not adopting it, and (3) mainstream consumers were not looking for the tools because the tools were not in the browsers. Therefore, there was not enough pressure to implement P3P or enough use of P3P even to gauge whether users would like it.

The panelists agreed that transparency requires government agencies to be clear in their privacy policies about the information they are collecting from users and about what information they will disclose. That will require providing meaningful notice, but even more importantly, panelists stated, privacy protections must be secured either by negotiating protective TOS or seeking legislation to protect privacy.

Individual Participation Principle

The government should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for its collection, use, dissemination, and maintenance. The government should also provide mechanisms for appropriate access, correction, and redress regarding its use of PII.

One panelist stated that the individual participation principle usually comes down to a question of whether data collection should occur on an opt-in or opt-out basis, but that this question may not always be the best way to frame the principle. Another panelist suggested that the choice model should depend on the particular use of the information. For example, visitors could be given an opt-out choice regarding an agency's use of persistent cookies for web analytics, *i.e.*, to help the agency assess and improve its website content. When used in this way, the panelist stated, persistent cookies do not raise privacy concerns. Social media providers whose services government agencies use to collect this information for web analytics would be required not to use this information for any other purpose as a means to protect privacy.

For all other uses of persistent cookies, panelists agreed, opt-in choice should be implemented. This is already being done in many instances, *e.g.*, when websites provide a "remember me" check box that is unchecked and allows visitors to actively check it in instances where visitors are asked to fill in a form, use shopping carts, comment on blogs, take distance learning sessions, or log-in to a website. Panelists noted that there are some situations, however, where visitors really do not have a choice – for example, with regard to logging their IP addresses. As panelists noted, there is no way technically to prevent logging visitors; and in fact, site managers need to have such information in order to perform security forensics in the event of an attack on their sites. The issue in that instance, according to the panelists, is how much information is needed to perform those functional tasks, not whether the visitor should be given choice.

Purpose Specification Principle

The government should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the information is intended to be used.

The panel discussion about the purpose specification principle focused on the need for government agencies to carefully consider what data they will collect and share with other organizations. Key issues identified include: (1) what limits, if any, there are on how government can use information publicly posted on social media websites, whether on a government or third-party domain; and (2) whether information posted by individuals on government websites for one purpose can be used by the government for unrelated purposes. One panelist suggested that the answer to these questions turns on the user's expectation, and

that the government should document the purpose for which it will use the information and make that purpose transparent to the user. Panelists reminded the audience that since the tragedy of September 11, 2001, there has been a presumption in favor of information sharing by the government. Yet, panelists noted, there is a possible conflict here between the purpose specification principle and pressure to support the sharing of user data. The use of PII posted on social media websites for intelligence and law enforcement, some argued, may raise questions as to whether such uses fall within visitors' expectations. The panelists argued that the government should, in keeping with the transparency principle, always disclose its information collection and sharing policies.

A related concern is the nature of the undertaking and the kind of information being collected. Some information is more sensitive than others; so for example, providing visitors with the option of using screen names rather than their email addresses when posting comments can achieve the same purpose in many instances while protecting visitors' privacy.

Data Minimization Principle

The government should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).

Panelists noted that social media by their very nature are designed to encourage information sharing; thus, it is not clear how the data minimization principle plays out in this communication-rich environment. Web 2.0 is viewed as providing data empowerment – using publicly generated content and fostering communities that heretofore have been impossible to create. Therefore, panelists asserted, data minimization may seem to be in conflict with social media. In addition, once this information is online, it is almost impossible to remove completely. Privacy advocates once argued that data minimization was more efficient than collecting unlimited data because data storage was expensive; but, as panelists pointed out, data storage is no longer expensive. Moreover, panelists stated, it can be difficult and costly for websites to delete data. The panelists asserted, however, that concern about data breaches may pressure some social media providers to reduce their collection of sensitive PII (*e.g.*, social security numbers, medical information, credit card numbers, etc.), as breach notification can be costly.

In some instances, panelists stated, minimization of PII may not be difficult to implement. For example, an agency could ask website visitors to register using a valid email address, which the website would retain, but give visitors the opportunity to select a screen name so that their privacy can be protected when posting comments on the site. Other examples include admonishing visitors to refrain from including PII in their blog responses or moderating public comments to remove PII.

According to the panelists, data minimization may be more desirable for the government because collecting PII brings with it the panoply of legal requirements discussed earlier in the workshop. At a minimum, collecting PII would require agencies to conduct a PIA and create policies and procedures to mitigate privacy and security concerns. The panelists stated that in situations where the data collected are not under government control, such as when the government uses third-party social media sites, questions arise as to whether privacy and security impacts must

still be addressed. Panelists argued that government should conduct privacy and security assessments when considering the use of third-party social media to ensure consistency with federal protections.

With regard to data retention, panelists noted that some social media providers have been reducing the periods for which they retain PII. Security considerations, however, may be in conflict with such data retention policies, panelists explained, because security managers want to retain site logs for longer periods to investigate intrusions, malware, and other patterns of attacks. The security expert on the panel observed that the more incoming traffic data is stored for investigative purposes, the more difficult data minimization becomes.

Use Limitation Principle

The government should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the agency should be for a purpose compatible with the purpose(s) for which the PII was collected.

Panelists agreed that the government should not use data for purposes beyond those for which the data was provided. Some panelists pointed out, however, that there are instances in which information collected for one purpose may have value that was not recognized at the time the agency collected it. The use of data for such secondary purposes may or may not be an issue depending on the sensitivity of the information which, as panelists noted, may also impact the need for data minimization. Panelists observed that some types of data are not sensitive, and the sharing of that information may actually promote the public interest. Social media provide a number of fora for people to share their information, and some panelists argued that aggregation of that information could bring a level of situational awareness that government should be able to use. Just as private sector companies can learn about their customers by monitoring social media activities, these panelists said, the government can learn about its users. One panelist cited Virtual Alabama,[49] in which Alabama's Department of Homeland Security partners with the U.S. Space & Rocket Center to use Google Earth Enterprise to collect, display, evaluate, and share data online with state, county, and municipal governments, emergency responder teams, and the criminal justice system. This is an example of how data that was once housed in silos can be taken together and "mashed up" – integrated by software to produce a new result or service hosted online. Where the data are sensitive, however, using it for secondary purposes could generate concerns. Some panelists stated, for example, that medical information should only be used for the purpose for which it was collected.

Panelists noted that de-identification of data has been the traditional answer to privacy concerns posed by information sharing, but that new tools are enabling re-identification of de-identified data. This is particularly an issue for statistical agencies. The proliferation of publicly available information, coupled with the improvement of search capabilities, makes it difficult to say that de-identification is sufficient to protect privacy. Reporting aggregated data generally does not pose a privacy concern, but panelists asserted that even such new Obama Administration efforts

[49] Information about Virtual Alabama is *available at* http://www.dhs.alabama.gov/virtual_alabama/home.aspx?sm=g_a.

as the Data.gov website must be monitored to ensure that the data sets published there do not pose privacy risks.

The panelists also argued that when the government takes PII from a social media website and integrates it with its system of record, that information becomes subject to the Privacy Act and E-Government Act and must meet their notice and PIA requirements. Use limitations apply to such collections, although agencies may apply discretionary exemptions for law enforcement and intelligence uses.

The panelists also discussed limiting the right of social media providers to track visitors to government web content posted on providers' websites. One of the panelists argued that the government should use its leverage when negotiating TOS agreements to protect visitors using social media websites from social media providers' tracking without individual consent. According to the panelist, the onus is on the White House, GSA, and the federal agencies that are promoting the Web 2.0 initiative to obtain that protection. Panelists discussed the first steps GSA has taken to negotiate provisions that would make it possible for government agencies to enter into agreements with social media providers, as providers' standard TOS agreements often included provisions that were legally unacceptable to the government. Panelists opined, however, that in negotiating these provisions GSA did not initially consider a number of other requirements, including privacy.

According to these panelists, the government now must establish a mechanism for identifying government-wide requirements for the use of social media. The challenge, panelists stated, is that the fundamental business model for social media firms is advertising, which conflicts with traditional government practice. One panelist suggested that the government examine whether it can negotiate terms with social media websites that are compatible with current advertising models before launching into building its own social media platforms. Another panelist noted the need for the government to target educational efforts regarding social media to young people, who, the panelist opined, do not have a good understanding of the risks to their own privacy and security posed by sharing personal information in social media environments.

Data Quality and Integrity Principle

The government should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.

Panelists stated that the goal of social media should be to provide as much accurate information as possible, and that social media are useless if the information being disseminated is incorrect. As panelists pointed out, the goal of social media is not simply the proliferation of data, but rather access to the right data at the right time. One panelist noted that one social media provider is contemplating authenticating speakers as an alternative to advertising, demonstrating that data quality and integrity can be an important principle in social media while also serving as an alternative revenue model to advertising.

Security Principle

The government should protect PII through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

Panelists discussed the need for the government to protect PII on social media websites used for official government services. Different use cases, however, require different approaches to security. The security expert on the panel divided social media into four use cases: (1) inward sharing (*e.g.*, using internal collaborative resources, internal to the organization like Intellipedia); (2) inbound sharing (*e.g.*, where internal users gather information using external services, such as an online poll); (3) outward sharing, also known as inter-institutional sharing (*e.g.*, when the government makes data feeds available to the rest of the world, such as through Data.gov and Recovery.gov, and the outside world has a high level of visibility into government); and (4) outbound sharing (*e.g.*, when the outside world provides information using different information feeds and those are captured by internal data sources, including federal social media websites). Each of the four use cases has a different security profile. According to the panelist, blogging on a .gov website uses a government information system that falls under the Federal Information Security Management Act of 2002 (FISMA)[50] security requirements. The panelist argued, however, that when a government employee accesses an external social media website there are no assurances of security controls.

Panelists stated that education is key to ensuring that the government workforce is aware of the risks associated with social media. Social media are resulting in a blending of professional and personal use by government employees, which can increase security risks. When a federal employee identifies himself on a social media site as a federal employee, he establishes a federal footprint that may be an "attack surface"[51] that can be exploited. Panelists urged federal agencies to establish policies that provide guidance on how to securely use social media websites, including developing acceptable use policies and conducting training to ensure awareness of these policies.[52]

Accountability and Auditing Principle

The government should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

---

[50] *See* Title 44 U.S.C. Chapter 35, Subchapter III, "Information Security" [The Federal Information Security Management Act of 2002 as amended].

[51] The panelist described an "attack surface" as the size of entity's Internet footprint, and suggested that the bigger the footprint the more vulnerable the entity is to attack. For example, if an individual were to disclose through social media that they are an employee or contractor of a federal agency, then an attacker could use additional avenues such as the person's home computer or email account as a means of penetrating the government's information systems.

[52] IBM filed a comment to the workshop that included an example of an employees' acceptable use policy.

Panelists agreed that government agencies must have strong program management and oversight for their use of social media. Accountability, panelists noted, requires transparency up front about a program's goals, information being collected, and how it will be used. This due diligence is particularly important, according to the panelists, when agencies use third parties such as social media providers to conduct activities on behalf of the government. Panelists also urged agencies to identify very clear performance measures and to revisit them as technology and circumstances, and therefore the privacy landscape, continue to evolve.

Several panelists stated that government use of social media has presented particular accountability challenges because the government is not using the traditional procurement process to obtain social media services. As discussed above in the summary of the workshop's panel on legal issues, many of the social media providers' services are free and do not meet the federal procurement requirements, and their TOS agreements do not provide for the due diligence process required by traditional government contracting. One panelist suggested, however, that the government experiment with social media before establishing government-wide procurement standards. Another panelist stated that the government is already working to identify qualified providers that can be used by agencies to build government-wide infrastructure for social media. One panelist expressed the view that GSA could be the incubator for developing a centralized platform of applications, service agreements, tools, and methodologies for government-wide use, thereby standardizing terms and conditions and policies as the government moves toward becoming a platform for social media.

Panelists stated that employee training is a core element of accountability and that training employees on how to properly handle PII in the context of social media is a central step in protecting privacy. Panelists also argued that before entering into TOS agreements with providers, government must conduct due diligence to assure that potential providers protect individual privacy.

One of the panelists observed that the FIPPs are an "ecosystem," meaning principles that should be considered as a whole, with each principle integral to the others. As applied to government use of social media, the panelist said, the FIPPs can only direct government in the right direction; they cannot resolve every issue. According to the panelist, the FIPPS do, however, ensure that privacy is front and center of decision making and not eroded by the sheer momentum of government's initiative to make use of new means of engaging with the public.

Conclusion

The *Government 2.0 Privacy and Best Practices Workshop* identified the broad range of legal and policy issues facing federal agencies scrambling to fulfill the Obama Administration's call for greater transparency and public participation in government. This workshop brought together experts to share best practices and help guide agencies to develop policies and practices that can support the government's use of social media in a privacy sensitive manner. The legal and policy issues are complex, but not insurmountable, if the various legal, policy, and communication experts and stakeholders are brought together and participate in a process to address the issues *before* engaging in social media activities. Moreover, the FIPPs can provide

an analytical framework for government to protect the privacy of the public, but application of each of the principles to the various social media tools will require recognition that privacy protection is a priority and not an afterthought. And finally, public education is needed to ensure individuals understand the privacy risks associated with using social media and the steps they can take to protect their privacy. The DHS Privacy Office offers this workshop report as a roadmap to help inform government agencies and the public on how the government can protect privacy while using social media to enhance open government.

Appendices

Social Media Resources

CIO Council, Information Security and Identity Management Committee (ISIMC), Network and Infrastructure Security Subcommittee (NISSC), Web 2.0 Security Working Group (W20SWG), *Guidelines for Secure Use of Social Media by Federal Departments and Agencies*, Sept. 2009, *available at* http://www.cio.gov/Library/documents_details.cfm?id=Guidelines%20for%20Secure%20Use%20of%20Social%20Media%20by%20Federal%20Departments%20and%20Agencies,%20v1.0&structure=Information%20Technology&category=Best%20Practices.

Department of Defense, *Operations Security (OPSEC) and Internet Safety*, *available at* http://www.au.af.mil/au/awc/awcgate/dod/blogbrochure.pdf.

Federal Knowledge Management Initiative, *Report and Recommendations on Web 2.0 and Social Software*, Apr. 2009, *available at* http://wiki.nasa.gov/cm/wiki/?id=7733.

Federal Web Managers Council, *A Practical Guide to Help You Manage Your Agency's Website*, *available at* http://www.webcontent.gov.

Federal Web Managers Council, *Social Media and the Federal Government: Perceived and Real Barriers and Potential Solutions*, Dec. 23, 2008, *available at* http://www.usa.gov/webcontent/documents/SocialMediaFed%20Govt_BarriersPotentialSolutions.pdf.

General Services Administration, *Social Media and Web 2.0 in Government*, Jan. 2009, *available at* http://www.usa.gov/webcontent/technology/other_tech.shtml

General Services Administration, Order CIO 2106.1, *Social Media Policy*, July 17, 2009, *available at* http://www.gsa.gov/graphics/staffoffices/socialmediapolicy.pdf

General Services Administration, **O**rder CIO P 2106.2, *Social Media Handbook*, July 17, 2009, *available at* http://www.gsa.gov/graphics/staffoffices/socialmediahandbook.pdf

Department of Health and Human Services, G*eneral Guidance for Utilization of New and/or Social Media*, *available at* http://www.dhhs.gov/web/policies/webstandards/socialmedia.html

Office of Management and Budget, P*olicies for Federal Agency Public Websites (OMB M-05-04)*, Dec. 17, 2004, *available at* http://www.usa.gov/webcontent/reqs_bestpractices/omb_policies.shtml.

Government 2.0 Privacy and Best Practices Workshop Agenda

AGENDA

Government 2.0: Privacy and Best Practices

The Washington Court Hotel, Atrium Ballroom
525 New Jersey Ave. NW, Washington, DC
June 22 - 23, 2009

Workshop, Day One	***8:30 a.m. – 4:30 p.m.***
Welcome	**8:30 a.m. – 8:45 a.m.**
Mary Ellen Callahan, Chief Privacy Officer, DHS	
Opening Remarks	**8:45 a.m. – 9:15 a.m.**
Vivek Kundra, Federal Chief Information Officer, The White House	
Panel 1: How is Government using social media?	**9:15 a.m. – 12:00 p.m.**
Moderator: Peter Sand, Director of Technology and Intelligence, DHS Privacy Office	**Break from 10:30-10:45**
Panelists will demonstrate Federal agencies' use of social media. They will present the benefits to their agencies and the public of using social media and discuss the challenges faced in leveraging these technologies for transparency. They will also discuss the policies they have adopted to address privacy and other Federal requirements.	
Panelists	
Jeremy Ames, New Media Specialist, U.S. Environmental Protection Agency	
Jodi Cramer, General Attorney, Office of the Chief Counsel, General Law Division, Federal Emergency Management Agency, DHS	
Curtis "Bob" Burns, Program Analyst, Office of Strategic Communications and Public Affairs, Transportation Security Administration, DHS	

Victor E. Riche, Managing Director, Office of Information Technology, Bureau of International Information Programs & Bureau of Educational & Cultural Affairs, U.S. Department of State

Maxine Teller, Principal of MiXT Media Strategies, Senior New Media Strategist, Emerging Media Directorate, Defense Media Activity, U.S. Department of Defense

Lena Trudeau, Vice President, National Academy of Public Administration

Lunch (on your own) ***12:00 p.m. – 1:30 p.m.***

Panel 2: How does Government 2.0 impact privacy?

Moderator: Martha K. Landesberg, Associate Director of Privacy Policy, DHS Privacy Office

Panelists will discuss the privacy impacts associated with Government use of social media and whether and how the Privacy Act applies. They will also consider how the Government can provide adequate notice of its uses of the information collected through social media and whether there should be any limitations on its uses. The panelists will discuss the privacy implications of the use of third-party technology on Government websites or web pages.

Panelists

Jonathan Cantor, Executive Director for Privacy and Disclosure, Social Security Administration

Danielle Citron, Professor, University of Maryland School of Law

Lillie Coney, Associate Director, Electronic Privacy Information Center

Tim Jones, Activism and Technology Manager, Electronic Frontier Foundation

Jay Stanley, Public Education Director, Technology and Liberty Program, American Civil Liberties Union

Heather West, Policy Analyst, Center for Democracy and Technology

Break **2:45 p.m. – 3:00 p.m.**

Panel 3: What security issues are raised by Government 2.0?	**3:00 p.m. – 4:15 p.m.**

Moderator: Earl Crane, Chief Information Security Architect, DHS Office of the Chief Information Security Officer

Panelists will discuss the security risks and mitigations specific to Government use of social media. They will discuss the security risks posed by Government hosted social media activities and by Government use of third-party service providers. They will also consider security concerns, including the risks of social engineering, for Government employees.

Panelists

Brian Burns, Deputy Chief Information Officer for Emerging Technology, U.S. Department of the Navy

Dan Chenok, Senior Vice President and General Manager, Pragmatics

Mark Drapeau, Associate Research Fellow, Center for Technology and National Security Policy, National Defense University, Department of Defense

Edward *W.* Felten, Professor of Computer Science and Public Affairs, Princeton University

Adjournment, Day One	**4:15 p.m.**

Workshop continues on Tuesday, June 23, 2009	***8:30 a.m. – 12:30 p.m.***

Workshop, Day Two	***8:30 a.m. – 12:30 p.m.***

Opening Remarks	

Panel 4: What legal issues are raised by Government 2.0?	**8:45 a.m. – 10:45 a.m.**

Moderator: Rosalind Kennedy, Associate Director of Technology and Intelligence Policy, DHS Privacy Office

Panelists will examine the application of the broad array of

current laws, regulations, and policies that apply to the Government's use of social media and whether additional protections are needed.

Panelists

Laurence Brewer, Director, Life Cycle Management Division, U.S. National Archives and Records Administration

Robert Coyle, Legal Advisor for Ethics, Office of General Counsel, DHS

Jodi Cramer, General Attorney, Office of the Chief Counsel, General Law Division, Federal Emergency Management Agency, DHS

Aden Fine, Senior Staff Attorney, National Legal Department, American Civil Liberties Union

Kirsten J. Moncada, Director, Office of Privacy and Civil Liberties, U.S. Department of Justice

Peter Swire, C. William O'Neill Professor of Law, Moritz College of Law, Ohio State University

Alex Tang, Senior Attorney, Office of General Counsel, Federal Trade Commission

Break **10:45 a.m. – 11:00 a.m.**

Panel 5: What are the privacy best practices for Government 2.0? **11:00 a.m. – 12:30 p.m.**

Moderator: Toby Milgrom Levin, Senior Advisor and Director of Privacy Policy, DHS Privacy Office

Panelists will discuss what should be the best practices for Government use of social media in light of the legal, privacy, and security issues discussed earlier in the workshop. They will explore how the Fair Information Practice Principles can be embedded in social media policies.

Panelists

Earl Crane, Chief Information Security Architect, DHS Office of the Chief Information Security Officer

Ari Schwartz, Vice President and Chief Operating Officer, Center for Democracy and Technology

Peter Swire, C. William O'Neill Professor of Law, Moritz

College of Law, Ohio State University

David Temoshok, Director, Identity Policy and Management, Office of Governmentwide Policy, U.S. General Services Administration

Lena Trudeau, Vice President, National Academy of Public Administration

Closing remarks	**12:30 p.m.**