

ELECTRONIC PRIVACY INFORMATION CENTER

Workshop Comments of the Electronic Privacy Information Center
Privacy Office of the Department of Homeland Security

Government 2.0 Workshop: Privacy and Best Practices

Docket No. DHS-2009-0020

E-mail: privacyworkshop@dhs.gov

Subject: Government 2.0

Workshop Comment" and the Docket Number (DHS-2009-0020)

June 1, 2009

Introduction

By notice published in the Federal Register on April 17, 2009, the Department of Homeland Security's (DHS) Privacy Office announced it seeks public comment to develop best practices to guide federal government agencies' use of social media. The agency requests comments on "any issue of fact, law, or policy related to the privacy issues posed by Government use of social media." The agency plans to "develop a comprehensive record regarding Government use of social media." The agency also will conduct a public workshop on Government 2.0: Privacy and Best Practices.¹ Pursuant to this notice the Electronic Privacy Information Center submits the following comments to the Department of Homeland Security's Privacy Office on topics: 2) What are the benefits; 5) What are the privacy issues; and 8) What should be the elements of privacy best practices of the Federal Register notice DHA-2009-0020.

The Electronic Privacy Information Center (EPIC) is a public interest research center in Washington, D.C. It was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values. EPIC has a long-standing interest in privacy and technology issues.² EPIC has a specialized area of expertise regarding digital communication technologies and privacy policy.³ The government's use of social media present new challenges to its role to be transparent to citizens, protect privacy rights, and sustain US democratic values.

Background

Social networking Web sites, such as MySpace, Facebook, and Friendster have become established forums for informally keeping in contact with old acquaintances and meeting new ones. Users can create their own Web page and post details about themselves: where they went

¹ Public Workshop: Government 2.0: Privacy and Best Practices, 74 Fed. Reg.17876 (Apr. 17, 2009), available at <http://edocket.access.gpo.gov/2009/E9-8868.htm>.

² Available at <http://www.epic.org/>.

³ Available at <http://www.epic.org/privacy/default.html>.

to school, their favorite movie titles, and their relationship status. They can link to friends on the same site, whose photos, names, and perhaps a brief description, will also appear on the Web page. While these Web sites are useful tools for exchanging information, there has been growing concerns over breaches in privacy caused by these social networking services.⁴

In 2007, the Pew Research Center reported over 55% of teens 12-17 had online profiles hosted by social networking service providers.⁵ In January of this year, the Pew Research Center's survey report revealed that 30% of adults 35-44 had online profiles with social networking services.⁶ The numbers of adults with personal online profiles with social networking sites has tripled in four years from 8% in 2005 to 35% in 2009.⁷ Adults make up a larger percentage of the population than youth, which means their share of social network profiles translates into a larger number than total youth profiles.

Primary Privacy Issue Regarding Government Use of Social Media

Government support of protections for developing technologies has a checkered past. In August 1945, at the end of World War II, the National Security Agency (NSA) approached heads of telecommunication companies to conduct intercepts of communications. Within weeks, "despite the fear of prosecution and the warnings of their legal advisers," the NSA had agreements with Western Union, RCA, Global, ITT World Communications to intercept and collect telegraph traffic.⁸ Initially Western Union limited access to communications from only one country and insisted that its employees "operate the [microfilm] camera and to the actual handling of the messages." RCA, Global, and ITT World Communications also "gave the NSA access to the "great bulk" of their telegrams.⁹

During the social and political transformative period of the 1960s government agencies engaged in wiretapping and surveillance of civil rights, cultural, and youth leaders due often to First Amendment protected activity. Between 1956 and 1971, the FBI conducted the domestic Counter Intelligence Program known as CONINTELPRO.¹⁰ The objective was to investigate and disrupt dissident US political organizations.

⁴ See <http://epic.org/privacy/socialnet/default.html>

⁵ See Amanda Lenhart & Mary Madden, *Social Networking Websites and Teens*, Pew Research Center Publications, January 7, 2007, <http://pewresearch.org/pubs/118/social-networking-websites-and-teens>.

⁶ See Sharon Jayson, *Older adults among newer members on social networking sites*, USA Today, Jan. 14, 2009 http://www.usatoday.com/tech/hotsites/2009-01-14-social-networking_N.htm.

⁷ See Amanda Lenhart, *Social Networks Grow: Friending Mom and Dad*, Pew Research Center Publications, January 14, 2009, <http://pewresearch.org/pubs/1079/social-networks-grow>.

⁸ See JAMES BAMFORD, *THE PUZZLE PALACE* 304-305 (Penguin Books 1983).

⁹ WHITFIELD DIFFIE & SUSAN LANDAU, *PRIVACY ON THE LINE* 158 (MIT Press 2007).

¹⁰ Available at <http://www.answers.com/topic/cointelpro>.

Last year's amendment of the Foreign Intelligence Surveillance Act (FISA)¹¹ specifically awarded retroactive immunity to telecommunication companies from prosecution for involvement in warrantless domestic wire-tapping¹² operations. This demonstrates a questionably close connection between communications providers and the government, which provides protection to companies when the government violates the privacy of communication services consumers.

There is a risk that this history is about to be repeated. The GSA, on behalf of a coalition of US government agencies,¹³ recently concluded nine months of negotiations with social media service providers including: YouTube, vimeo, blip.tv and Flickr.¹⁴ The GSA did not see any need to alter the terms and conditions set out by the social media site Twitter.com, as it believed that they already aligned with federal requirements. The GSA is also negotiating several "Memoranda of Understanding"¹⁵ with social networking sites, such as Facebook and Myspace.¹⁶

There is "a disconnect between users' perception of privacy and the privacy framework that is actually in place."¹⁷ EPIC's submission of a FOIA request for documents regarding the negotiated agreements between federal government agencies and social media service providers is of public interest and should be disclosed. Two draft agreements (Flickr¹⁸ and blip.tv¹⁹) are available online, as well as the general guidelines created by the FWMC to assist government agencies seeking to establish agreements with social media sites.

EPIC is seeking disclosure of the agreements negotiated by the GSA, which have not been made public. Social networking applications make it easy for users to share information about themselves with others. Many online services relay information about online associations as users create new relationships. While government agencies may use social networking, cloud

¹¹ Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801-1871 (2004), *available at* <http://uscode.house.gov/download/pls/50C36.txt>.

¹² James Risén & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, *available at* <http://www.nytimes.com/2005/12/16/politics/16program.html>.

¹³ Federal Web Managers Council, *Web Content Mangers Forum: Terms of Service: FAQs*, https://forum.webcontent.gov/?page=TOS_FAQs (last visited May 26, 2009).

¹⁴ Jill R. Aitoro, *GSA signs deals for agencies to use for social networking sites*, Nextgov, March 25, 2009, *available at* http://www.nextgov.com/nextgov/ng_20090325_5490.php?zone=ngtoday.

¹⁵ *Id.*, defining Memoranda of Understanding as "efforts to put down on paper the expectations of the parties...cover[ing] free services only and [they] can't be used to negotiate premium services that require a fee."

¹⁶ *Id.*

¹⁷ ELECTRONIC PRIVACY INFORMATION CENTER, *PRIVACY & HUMAN RIGHTS: AN INTERNATIONAL SURVEY OF PRIVACY LAWS AND DEVELOPMENTS* 115 (Electronic Privacy Information Center and Privacy International 2007).

¹⁸ *Available at* https://forum.webcontent.gov/resource/resmgr/Docs/Flickr_TOS_Agreement_Amended.doc.

¹⁹ *Available at* https://forum.webcontent.gov/resource/resmgr/Docs/Blip_tv_Terms_of_Use_Agree.doc.

computing, and Internet services to create greater transparency on their activities, it remains unclear if there are data collection, use, and sharing limitations.

Challenges and Opportunities Regarding Federal Government Use of Social Media

A. What are the benefits, to the public and to Government, of Government's use of social media?

Social Media presents a great opportunity for the government to provide vital, timely, and accurate information to the public on a wide range of matters as well as engage citizens in a deliberative process that directly affect their interests or lives.

Discussions around US civic engagement, have too often been limited solely to the very important function of voting in public elections. Voting is an essential component of self-governance, but it is not the only option available to citizens for communicating with Federal government agencies. The lack of citizen literacy regarding their right to speak directly to government agencies to help shape the policy development process could be effectively addressed through the use of social media. Broad public access to Internet technology creates an opportunity to breach another hedge between citizens and full participation in the process of self-governance.

The problem presented to citizens is the complexity and opaque nature of filing agency complaints and comments. Providing tools and training through social media on how citizens can participate in agency decision-making by filing agency complaints and comments presents another means of raising the civic participation quotient in ways that improve the custodial role of federal government agency and create great transparency for citizens on government operations.

Civic engagement in public policy making can be encouraged by social networking initiatives when federal agencies seek to change or adopt new rules based on federal statutes.²⁰ A major hurdle in engaging popular participation in agency rulemaking is the lack of sophistication on the part of federal agency in the best methods for engaging the public through Internet communication technology.

EPIC's experience in launching a public campaign on the opportunity to submit comments to the Department of Homeland Security regarding its request for input on the rule for the "Minimum Standards for Driver's Licenses and Identification Cards Acceptable to Federal Agencies for Official Purposes," engaged over 60 organizations resulting in over 12,000 comments being submitted to the agency. The volume could have been much higher, but the submission process initially only allowed access to the process through the <http://regulations.gov> portal, which required the submitter to input the assigned docket number; the other option was to submit the comment by fax.

²⁰ The Privacy Coalition & EPIC, *Stop REAL ID! Submit Comments to the Department of Homeland Security by May 8th*, 2007, <http://privacycoalition.org/stoprealid/>.

Because of the tech savvy resources and grassroots organizational skills of Consumer Action, ACLU, Liberty Coalition and many other organizations participating in the campaign, the volume of submissions by the close of the comment period had overwhelmed the fax lines. The agency added an e-mail option for the final hours of the campaign.

An additional benefit to government's mastery of web 2.0 services is the occasional public need to have immediate access to accurate, reliable, and urgent information when new health and safety threats emerge. The recent reports of an H1N1 flu virus meant that the Federal government was in sole possession of knowledge regarding an emerging health threat. The reaction to the situation was an example of what is needed to abate and mitigate emerging threats posed by heretofore-unknown highly communicable diseases. Janet Napolitano, Secretary of the Department of Homeland Security, used every means available to her to organize the agency's response and coordinate federal agencies. She also coordinated communication with local, state, and international governments. Most important in the government's efforts was the level of transparency provided to the public on the evolving nature of the threat. Through official reports the public kept pace with developments until many of the key aspects of the illness could be assessed. Later, the ability of the government to communicate the status of the threat allowed a less vigilant stance on the part of the public, while federal, state, and local officials continue to address long-term issues related to H1N1. Managing communication in a constantly changing news environment makes web 2.0 a valuable asset for informing the public during emergencies.

Recommendations:

- Do not track users on government sponsored web sites or information portals.
- Apply Privacy Act protection to all data collected by the government and government contractors.
- Prohibit commercialization of information on users who visit government sponsored social media resources.
- Apply meaningful rules for public participation in official comment across all platforms.
- Promote open government and protect privacy.

B. What privacy issues are raised by Government use of social media? What are the privacy impacts of Government use of social media? Are there privacy issues that are unique to Government use of social media?

Several agencies have engaged social media in a variety of ways. For example, the FBI has created a widget for displaying the most wanted list,²¹ the Department of Defense has established a video uploading site for use by troops,²² and the State Department is using Facebook inform users about its work. While social media may be employed as a useful tool for distributing information to people in an efficient and immediate manner, there are privacy issues raised by the structure of many of the social media web sites. There are more than 274 million

²¹ See <http://www.fbi.gov/widgets.htm>.

²² See <http://www.trooptube.tv>.

users registered with the top six social networking sites, making social media an invaluable tool for distributing information.²³

Under Government 2.0, federal agencies have increasingly moved to the world of social media to capitalize on this means of communication.²⁴ As part of the new Administration's "Open Government Initiative"²⁵ the White House collaborated with YouTube.com to broadcast official government videos.²⁶ In addition to displaying the videos on YouTube.com, the official White House web site²⁷ also provided embedded versions of the videos, originating from YouTube as the host site.²⁸ Because the default YouTube embedded code includes the use of persistent cookies,²⁹ YouTube was initially able to track personal information of every visitor who loaded a page containing video content on the White House web site. Use of persistent cookie technology is explicitly prohibited from government use by "long-standing federal rules."³⁰

As a result of the embedding code, YouTube was able to collect personal information related to users of an official government web site. After public objections, the Administration arranged for YouTube to remove persistent cookies from every video on the White House website, although possibly not on the YouTube site itself. The exploit of user access to government-sponsored content came from the service provider.

There are many statutory provisions in place that do apply to privacy protection of users of social media that also have implications on the Government 2.0 initiatives:

²³ *Supra*, note 17.

²⁴ See Federal Web Managers Council, *Social Media and Web 2.0 in Government*, April 23, 2009, http://www.usa.gov/webcontent/technology/other_tech.shtml.

²⁵ Memoranda from Barack Obama, President of the United States, on Transparency and Open Government (January 21, 2009) *available at* http://www.whitehouse.gov/the_press_office/TransparencyandOpenGovernment/.

²⁶ Andrew Bleeker, Your Weekly Address from the President-elect, Nov. 15, 2008, http://change.gov/newsroom/entry/your_weekly_address_from_the_president_elect/.

²⁷ *Available at* <http://www.whitehouse.gov>.

²⁸ *Supra*, note 26.

²⁹ "Cookies are text files that have unique identifiers associated with them and are used to store and retrieve information that allow Web sites to recognize returning users, track on-line purchases, or maintain and serve customized Web pages. Cookies may be classified as either "session" or "persistent." Session cookies expire when the user exits the browser, while persistent cookies can remain on the user's computer for a specified length of time." U.S. GEN. ACCOUNTING OFFICE, INTERNET PRIVACY: IMPLEMENTATION OF FEDERAL GUIDANCE FOR AGENCY USE OF "COOKIES" 1 (U.S. Gen. Accounting Office 2001) *available at* www.gao.gov/cgi-bin/getrpt?GAO-01-424.

³⁰ Memorandum from Joshua B. Bolton, Director, Office of Management and Budget on Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (Sept. 26, 2003) *available at* http://www.whitehouse.gov/omb/memoranda_m03-22/.

Enforce the Privacy Act of 1974³¹

The Privacy Act is a very important, technology-neutral law that helps ensure accountability and transparency when personal information is collected by government agencies. The goal is not to limit the use of technology; it is to help ensure that new technology is used in a way to protect democratic values.³²

Privacy rights have been consistently recognized in United States legislation and case law.³³ The Privacy Act of 1974 regulates the collection and retention of personal information by state agencies.³⁴ The language of §552a establishes a government agency may, “maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the president.”³⁵

This provision could affect agencies’ use of social networking services as outlined below, and provide important protection of user privacy. Social media, such as YouTube, Facebook, LinkedIn, and Twitter, offer exciting new opportunities for public participation in government. At the same time, these services collect detailed personal information from users, including viewing habits, IP addresses, and location. Americans should not lose Privacy Act protections simply because the federal government acquires personal information indirectly through third-party vendors.

Office of Management and Budget (OMB)

The OMB develops and promotes a federal government-wide management agenda that includes information technology.³⁶ The OMB regulations on government web sites state “as a first priority, you must post privacy policies to your Department or Agency’s principal web site, ... add privacy policies to any other known, major entry points to your sites as well as at any web page where you collect substantial personal information from the public. Each policy must clearly and concisely inform visitors to the site what information the agency collects about individuals, why the agency collects it, and how the agency will use it.”³⁷ In addition, Government agencies are directed to acquire an OMB control number and act in accordance with the Paperwork Reduction Act³⁸ as well as subsequent OMB regulations and draft guidelines.³⁹

³¹ 5 U.S.C. § 552a.

³² See <http://opengov.ideascale.com/akira/dtd/3540-4049>.

³³ See, e.g., Fair Credit Reporting Act as Amended 2009 (15 U.S.C. § 1681 et seq.); Video Privacy Protection Act of 1988 (18 U.S.C. § 2710); Video Voyeurism Prevention Act of 2004 (18 U.S.C. § 1801).

³⁴ *Supra*, note 32.

³⁵ *Supra*, note 31.

³⁶ See <http://www.whitehouse.gov/omb/management/>

³⁷ Memorandum from Jacob J. Lew, Director, Office of Management and Budget on Privacy Policies on Federal Web Sites (June 2, 1999) *available at* http://www.whitehouse.gov/omb/memoranda_m99-18/.

³⁸ Paperwork Reduction Act of 1980 (44 U.S.C. § 3501 et seq.).

Although important, of greater significance are protections provided to users through the technology-neutral Privacy Act.

Administrative Procedure Act (APA)

There are laws that are designed to ensure “meaningful” public participation in the decisions of government. These laws provide for public notice and opportunities for the public to express their views on the decisions that government makes. They also require that decisions be made openly and transparently, and they allow courts to decide when agencies have unfairly disregarded the opinions of the public.

The APA regulates the procedures for commenting on existing and proposed rules and states that, “Each agency shall give an interested person the right to petition for the issuance, amendment, or repeal of a rule.” The Act outlines specific channels that must be employed by agencies to receive comments. This requirement raises issues with agency use of social media sites to encourage comments and discussion, which would effectively avoid the regulations enforced by the APA.

While EPIC recognizes the positive and progressive nature of President Obama’s Memorandum on Open Government,⁴⁰ the most appropriate use of social media is to encourage commenting and then to direct individuals to the official sites and regulated channels. Public participation is the cornerstone of American democracy. When citizens take the time to participate in government, their views should be valued. A process for public comment should be open to all, easily accessible, established without favoritism, and ensure the systematic collection of the public’s views.

Recommendations:

- Agency use of social media sites should be limited to providing information and directing users to official sites for the provision of benefits or services.
- Social media sites are not suitable forums for issue discussions outside of the purview of the relevant regulations.
- Laws that help ensure meaningful public participation in decisions by government should apply to all new technology platforms.

C. What should be the elements of privacy best practices for Government use of social media? The Privacy Office requests that, where possible, comments include references to literature, technical standards and/or other resources that would support implementation of the best practices identified.

³⁹ OFFICE OF MANAGEMENT AND BUDGET, STANDARDS AND GUIDELINES FOR STATISTICAL SURVEYS (Office of Management and Budget 2004).

⁴⁰ *Supra*, note 26.

Americans should not lose Privacy Act protections simply because the federal government acquires personal information indirectly through third-party vendors. Social media sites collect a variety of information from users, including viewing habits, IP addresses, and location. If collected directly by the Federal Government, this information would be subject to the provisions of the Privacy Act.

The Privacy Act helps ensure accountability and transparency when personal information is collected by government agencies. The goal is not to limit the use of technology; it is to help ensure that new technology is used in a way to protect democratic values.

Once a person becomes a first tier contact to the government on a social media site certain information relating to second tier contacts also becomes available to the agency administrator.⁴¹ While a person may associate themselves with a government body in order to take advantage of the information and services provided, they may unknowingly be providing the government with personal information that they do not wish to disclose.

A primary risk posed by such social media web sites is that the government may use the guise of a profile providing useful information to gain access and harvest individual's personal information for purposes which may not be obvious to the user. This two-way data flow exposes people to government scrutiny in situations where they would not expect to be observed.

There are several types of social media sites, each of which raise differing privacy issues, some of which overlap:

Media Sharing

Web sites that provide a service for uploading images and videos, such as Flickr and YouTube, raise a number of privacy issues. Firstly, there is the issue of copyright infringement, likeness and incriminating content. If agencies, or their employees are allowed to upload images in an official capacity, there must be stringent safeguards to ensure that content is not uploaded that breaches individuals' rights.

Second, the majority of these sites allow for persons to comment on, or discuss hosted material. There is a risk that agencies may use this forum to gather comments and the identity of the author. By using social media sites to gather such information agencies should not escape regulatory obligations established by APA, OMB, and the Privacy Act. If the content actively encourages suggestions it may constitute a survey and be in breach of the OMB regulations.

Recommendations:

⁴¹ In this document "first tier" is being used to describe a "friend," of a group or a profile on a site such as Myspace, Facebook and Twitter. "Second Tier" is being used to describe persons connected to first tier contacts through the same site, but with no connection to the original group or profile.

- Agencies should not share access to information related to users who engage in social media relationships with another agency.
- Agencies should not solicit social media users who opt-in to relationships with the agency to join another agency's cause or promote relationships with another agency's social media efforts.
- Recognize that all agencies will not have equal success in the social networking world, some will be less popular, while others may gain a great deal of social media interest.
- Information made available through social networking or web 2.0 media should also be available on agency web sites.

News and Interactive

Blogs and virtual worlds combine aspects of media uploading sites and social networking sites. These forms of media require strict regulation if they are to be utilized by government agencies as they can encompass all the privacy issues outlined above in the other forms of social media.

In addition, Widgets⁴² provide a separate problem because the extent of their purpose may not be obvious. Widgets can be programmed to secretly gather information from a person's computer without that user's knowledge.

Recommendations:

- Restrictions on the uploading of content are required and agencies using social networking to gauge public sentiment, for polling, or refinement of messaging campaigns should disclose the purpose of the outreach and restrict use of information.
- Official comments for agency rule making purposes should be restricted solely to official agency sites.
- During official comment period, social media should be used to direct users to the appropriate official web services for posting comments.
- Agencies that deploy applications or tools for public use, which can include widgets or other special purpose code should not track or collect information on users.
- Any applications or code developed by a federal government agency or own its behalf must be associated with the agency at all times and must limit its life on a users computer to 60 days.

Persistent Cookies

OMB policy prohibits federal web sites from employing persistent cookies to track visitors' Internet activity. "Particular privacy threats exists when providers of web technology or information services can track the activities of users over time and across different web sites.

⁴² A widgets is defined as a "small program[] that can be displayed on portal pages, computer desktops, dashboards, and other objects." DEBORAH MORLEY & CHARLES S. PARKER, UNDERSTANDING COMPUTERS TODAY AND TOMORROW 357 (Marie Lee ed., Course Technology, Cengage Learning 2009).

These concerns are especially great where individuals who have come to government web sites may be tracked, which can involve third party host, such as in the case of the White House use of YouTube.

Recommendations:

- Federal Agencies should not adopt the more casual practices regarding cookies that social networking services use. Government is government—its relationship with citizens is not equaled by any other social networking context.
- Federal agencies using third party web media services should be prohibited from using cookies to track activities of users.⁴³
- Agreements between federal agencies and web 2.0 service providers should prohibit them from deploying cookies that track user activity on agency web sites or social media services.

Additional Steps to Address Privacy and Web 2.0

Certification Schemes for Government Social Media Pages

The most important element to consider in the government move to social media is a technology-neutral certification scheme to prevent consumer confusion on government social media pages. Policy should promote a uniform system where every social media source displays an official agency seal and requires an affirmative viewer response, acknowledging awareness of the nature of the content.

This certification system should model itself after methods already in place to signal to a viewer that they are leaving an official government site.⁴⁴ However, EPIC recommends that, in the place of a pop-up screen, the seal should be placed directly on the page in order to reduce confusion as viewers travel back and forth between government and private social sites.

Implementation and enforcement of this system are no substitute for affirmative privacy protections provided by federal statutes or regulations. DHS's goal of protecting Americans from abuse should not extend to an ability to dictate other uses of social networking services what they can and cannot do with personal pages.⁴⁵

Recommendations:

- Federal government agencies should develop a model certification system for the

⁴³ See Memorandum from Jacob J. Lew, Director, Office of Management and Budget on Privacy Policies and Data Collection on Federal Websites (June 2, 1999) *available at* <http://www.whitehouse.gov/omb/memoranda/m00-13.html>.

⁴⁴ An example of this system is available at <http://www.whitehouse.gov/>, by clicking on one of the links under “Stay Connected.”

⁴⁵ Homeland Security Council, *National Strategy for Homeland Security 1* (October, 2007) *Available at* http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf.

- provision of official government information and web 2.0 services;
- Create a Federal e-government uniform transition screen distinguished by the host agency's seal to inform users when enter a government sponsored web 2.0 environment
 - Develop a standard protocol to inform users as they transitioning from a web 2.0 environment to the official web site
 - Maintain department staff training modules on what the role of government in social networking ought to be.

A One-Way Flow of Data and Information

EPIC recommends that government limit its use of social media to education and information purposes. In his January 2009 Memorandum on Transparency and Open Government, President Barack Obama stated that his administration would “take appropriate action, consistent with law and policy, to rapidly disclose information in forms that the public can readily find and use.”⁴⁶

By establishing a one-way flow of data and information the Administration would be able to broadcast important topics and headlines while remaining compliant with basic statutory and common law procedures for open government. In order to implement the one-way data flow system, EPIC recommend a system that strictly distinguishes between citizen discussion boards and informal suggestion boxes, as compared to formal comments directed to federal government resource compliant with open government laws.

Encouraging Use of Proper Political Channels

“The United States is founded on democratic principles that recognize the importance of informed public debate concerning government activities.”⁴⁷ It is not necessary that the government be a party to these debates – in fact, a strong point can be made that the absence of a government presence encourages more robust deliberations.⁴⁸

Discussion boards, including suggestion boxes, should be defined by a user-to-user interface, and should have content that is protected from use in any official government action. However, the President has stated that the “executive departments and agencies should...solicit feedback to identify information of greatest use to the public.”⁴⁹ EPIC would recommend that the best way for the government to attain official feedback is through links that connect to their official website.

⁴⁶ *Supra*, note 25.

⁴⁷ Brief for National Security Archive, et al. as Amici Curiae Supporting Plaintiffs-Appellees, *Ashcroft v. Doe*, No. 05-0570-cv at 3 (2nd Cir. 2005), *available at* http://www.epic.org/open_gov/nsl/secretcy_amicus.pdf.

⁴⁸ “Without the opportunity to discuss politics in private...the finished positions that appear in public might never be formulated.” *Supra*, note 9 at 143.

⁴⁹ *Supra*, note 25.

Official government sites allow citizens to leave commentary with guaranteed privacy safeguards. Statutory mandates for official actions, such as those in the APA, relating to notice rulemaking, and the Paperwork Reduction Act, controlling government-conducted surveys, spell out detailed compliance standards. The provisions of these sections are largely written in technologically neutral terms, allowing great flexibility in extension of their provisions between many different media, as well as between different Internet social media formats. This standard leads EPIC to recommend these provisions be explicitly upheld and enforced in relation to Internet sources.

Used in the manner discussed above, discussion boards and suggestion boxes would satisfy Administration objectives for “public engagement [to] enhance the Government’s effectiveness and improve the quality of its decisions,”⁵⁰ while established procedures and safeguards could control comments on official government actions and decisions.

Recognition of the “Social Media Culture” and Prohibitions on Use of Personal Information

Government entities should recognize the unique culture of social media communities. Personal statements and information posted on social networks is often more extensive and specific than the information a user would typically announce to the public, let alone the government. In social media environments the general expectation is that the user has control of their information.⁵¹

EPIC also takes issue with the use and archiving of private information obtained by agencies from users of these sites. On many social media sites, government agencies would not only have access to the personal information of “first tier” contacts, but also to that of “second tier” contacts.

The Privacy Act prevents the retention of any personal information unless it is for a specific agency purpose, which the individual must be notified of.⁵² It is unclear how these rules will be held to apply in situations regarding government sponsored pages on private social media sites. EPIC’s recommends a one-way communication model would promote these restrictions by preventing any access of government to this information in the first instance. However, the government may still obtain some information naturally by the action of creating a connection. To handle this data “leak,” EPIC recommends that the Privacy Act be explicitly held to apply to any website involved with official government sources, preventing government use or storage of information from all contact tiers.

However, to meet open government obligations agency sites should be public and therefore viewable by members as well as non-members of social networking services. The information provided should also be available on the agency’s web site and through other means

⁵⁰ *Id.*

⁵¹ *See supra*, note 17.

⁵² *Supra*, note 32.

of public access. Agency and non-agency official web pages and content should be achievable by Internet archiving services.⁵³

Recommendations:

- Agencies should have a separate status on social networking services they are not individuals, nonprofits, or commercial enterprises.
- The social media contact of users who elect to participate in social networking activities with government agencies should have a firewall around their network of contacts.
- Users who elect to engage in social media activities with government agencies should not be required to share personal information about them.

Maintaining the Restrictions on Persistent Cookies

“The history of the last five years shows that attacks on privacy are not an anomaly...when the government has the power to invade privacy, abuses occur.”⁵⁴ To combat this there needs to be additional safeguards added to government-hosted pages on social media and networks. Traditionally these limits have been utilized through the prohibition of persistent cookies by any government agency, following from official OMB policies.⁵⁵

The cookie incident between YouTube and the White House⁵⁶ demonstrates how agreements can be reached with non-government entities in order to ensure statutory compliance. If persistent cookies can be removed from YouTube videos embedded on the White House site, EPIC advises the use of the same policy approach to prohibit the use of persistent cookies from all government social media pages. These efforts will be key preserving the privacy of all connections, and to ensure the use of these pages in concert with the EPIC proposal to restrict government social media pages to informational and educational purposes.

Applying Government Terms of Use to Agency-Sponsored Social Media Pages

The dissemination of personal information from government hosted social media network sites should be restricted by the Terms of Use between these private sites and the official government pages, since “in many cases the user content uploaded onto a social networking site becomes the property of that site.”⁵⁷ Private companies that act as federal contractors in any other area must comply with heightened standards in order to conduct government business.⁵⁸

Recommendations:

⁵³ See <http://www.archive.org/index.php>.

⁵⁴ *Supra*, note 9 at 169.

⁵⁵ *Supra*, note 30.

⁵⁶ See *discussion, supra*, pg 6.

⁵⁷ *Supra*, note 17 at 116.

⁵⁸ See, e.g., 5 U.S.C. § 552, applying to all government contractors following the Open Government Act of 2007, § 9.

- Agencies must differentiate themselves by requiring the social media sites to comply with heightened Privacy Terms for government-sponsored pages.
- Third party social media sites that host government content should further be required to comply with the policies set out by OMB regarding clear and concise posting of privacy policies at all web site points of entry.⁵⁹

Transparency on Government's Efforts to Engage Social Media

The dissemination of media directly from government sites to private citizens, that may use embedded video, widgets, or other applications that are hosted by a third party. Special considerations occur when the government hosts their own content. As a result, heightened access requirements for downloadable third party hosted social media are the only acceptable method to allow for compliance with privacy statutes and regulations without applying a complete bar to government involvement in this genre of networking.

In relation to widgets, EPIC acknowledges that the natural function of widgets is to both send and receive information from the accessing individual, which essentially contradicts the one-way communication model that we have suggested. In response, EPIC recommends that should the government elect to deploy widgets it should be done with complete transparency. Further, access to information, benefits, or services should not be dependent on acceptance of widgets nor other software application or device. Users should be allowed to accept or reject the widget through a message that makes clear to users that rejection does not mean the user will not access to information, benefits or services.

When the information hosted by the government consists of visual media, such as TroopTube.tv,⁶⁰ further problems arise in the privacy realm. In order to encourage the use of these sites as communication outlets, and address privacy concerns, EPIC recommends the implementation of a "walled garden approach."⁶¹ For sites such as TroopTube, this application would require a valid and verifiable access ID, already possessed by both soldiers and family members, which, once entered, would grant universal access to the content on the site.⁶² EPIC allows that this may restrict the scope of the site, but notes that the restriction would primarily apply to those outside the government's target audience.

Need for Increased Oversight

In order to ensure compliance with the recommendations EPIC has put forth, EPIC suggests an increased emphasis on regulatory oversight of agencies engaged in social media activities. A November 2008 statistic shows that active, independent government web sites

⁵⁹ *Supra*, note 38.

⁶⁰ *Supra*, note 22.

⁶¹ For general discussion of the "walled garden" approach *see, e.g.* <http://news.bbc.co.uk/2/hi/technology/6944653.stm>.

⁶² *Id.*

number over 24,000, while the network of web professionals employed numbers only 1,500, a number reached by calculating all employees from federal, state, and local levels.⁶³

An increased number of web professionals is required in order to appropriately monitor compliance with the statutory requirements of privacy and transparency, including avoiding the use of persistent cookies, storage of personal information, or use of informal commentary to guide formal political processes. To implement this oversight, EPIC recommends an initial evaluation of the ratio of web specialists to government web sites, including the number of government-sponsored pages on social media networks.

Conclusion

Privacy protection is vital to the successful integration of government into the world of social media, and EPIC hopes that DHS will take these recommendations into consideration in deciding the future of Government 2.0. EPIC is willing and able to contribute to the further development of policy that encourages the appropriate government use of social media, while guarding the right to privacy so essential to our way of life.

Respectfully submitted,

Lillie Coney
Associate Director
EPIC
1718 Connecticut Avenue, NW
Suite 200
Washington, DC 20009

Amie Stepanovich
Law Clerk
EPIC

Colin Irwin
Law Clerk
EPIC

⁶³ Federal Web Managers Council, *Putting Citizens First: Transforming Online Government* (November, 2008) available at www.usa.gov/webcontent/documents/Federal_Web_Managers_WhitePaper.pdf.