

Mapping the boundaries of social media use in government: organizational, professional and personal

Download pdf >>

The boundaries between interests and uses of social media appear relatively straightforward on paper, however, in practice, social media use by professionals in the workplace is often guided by different interests at different times. This blurring of boundaries between interests and uses of social media by employees from organizational to professional to personal presents a set of challenges to government organizations, among others. As more and more government entities enter the world of social media, questions about employee access, acceptable use, employee conduct, and account management surface.

The use of social media in government is often treated generically, frequently described as an 'organization' being the user. A closer look reveals that this understanding of users and uses is insufficient because it overlooks the subtle shifting of boundaries between individuals' and agencies' interests in using social media. The nature of social media platforms enables individuals to engage simultaneously in activities online that are personal, professional, and organizational. The shifting boundaries between users' roles and interests have implications for organizations designing social media policies and developing social media strategies.

This issue brief guides decision makers in developing policies on the use of social media in their organizations. This brief defines three types of social media use and highlights the need for policies that guide the management of the boundaries between these uses.

A shared understanding of the issues associated with the blurring lines within an organization can provide a foundation for making more informed choices about how to structure employee access to social media sites and the policies needed to manage an organization's social media presence and employee behavior.

In researching existing social media policy development, we analyzed 26 publicly available government social media policies and guidance documents and interviews with 32 government professionals to help formulate our guidance document – Designing social media policy for government: Eight essential elements from which this issue brief highlights the first of the eight essential elements – Employee Access.

Three Functional Uses of Social Media

THREE USES

- **Organizational use**—Official organizational use implies that an employee's use of social media is for the express purpose of communicating an organization's broad interests, or specific programmatic and policy interests.
- **Professional use**—Professional use implies that an employee's use of social media is for the purpose of furthering their specific job responsibilities or professional duties through an externally focused site.
- **Personal use**—Using social media for personal interests has nothing to do with an employee's job duties for the organization.

Organizational Use

Official organizational use refers to employee use of social media to communicate on behalf of the organization through an official organizational social media account. Employees acting in an official capacity are not communicating on behalf of themselves as individuals, but rather on behalf of their organization or their department. For example, the United States Environmental Protection Agency (EPA) has a dedicated YouTube channel. Employees charged with maintaining this account are doing so on behalf of the EPA as part of their regular job duties. Another example of official use is when a government employee is asked to run a contest on IdeaScale on behalf of the organization, program area, or policy area. Not all official uses of social media are citizen facing, internal blogs or wikis for collaboration among project teams are also considered official use.

Professional Use

Professional use refers to an employee use of social media for the purpose of fulfilling professional goals and improving their professional skills by accessing networks of other professionals through social media sites. Unlike in official organizational use, the sites employees are using are not maintained or monitored by the organization

and employees are using their personal accounts to access these sites. For example, almost 30,000 government employees are members of the social media site GovLoop.com. The site is designed to foster engagement between professionals by creating various communities of practice for sharing knowledge and enhancing ability to collaborate with professionals from other organizations.

Personal Use

Personal use refers to employee use of social media for personal interests, such as conducting personal business that is not connected to an employee's organization or job responsibilities. For example, an employee may want to check on the status of friends on their personal Facebook page, send out a personal Tweet, or watch the latest viral video on YouTube.

Blurring boundaries: some challenges

On paper, the boundaries between interests and uses appear relatively straightforward. In practice, however, they are fluid and difficult to manage as employees can use social media tools simultaneously for organizational, professional, and personal interests. In addition, the social media environment does not easily accommodate an 'organization' as a user, and does not readily distinguish a "personal" persona and a "professional" persona. The blurring boundaries create challenges for organizations looking to develop policies and guidelines for managing social media use.

"The issue is that the lines are unclear. You can certainly have two Facebook accounts, but the people at the working level don't see the distinction."

#State-level government professional

Governments that allow access to social media sites, whether for organizational, professional, or personal interests, face new challenges in managing such engagement.

Linked-up professional and personal personas

In the physical world, time and distance separate what we do and say at work, and what we do and say outside of work. The physical distance creates a way to manage your personal and professional life. In the social media world, a basic building block is a person's individual persona. This persona is tied directly to a personal email and personal profile. Social media sites use many different ways to construct individuals' social networks, often tracking an individual's connections by events, organizations, or interests or linking individuals through pictures, friends, or geography. These connections are made by social media sites, whether they are personal or professional, and whether you, as a user, intended to make the connection or the connection was made for you. Thus, a situation can arise where a personally or professionally inappropriate posting of a friend is inadvertently connected with the professional persona of an individual who then faces possible job related repercussions.

The linked-up nature of personal and professional personas in the social media environment is further complicated by the old adage of "nothing goes away on the Internet." The digital traces accumulating on the Internet, and in some cases, in perpetuity, raise issues not only for an individual but also for their employer. One can imagine a scenario where in 2008 a passionate graduate student expresses an opinion about a sensitive public policy issue on a social media site, and in 2016, that comment is linked back to his or her professional persona. However, now, the student is a brand new employee of a government organization, which is now publicly linked to this proclamation via their employee's social media account.

Coordinating organizational messages

Most government agencies currently operate within a centralized communication structure, often presenting an "official organizational message" that is put out through the communications department. As more professionals, in roles other than communication staff, use social media, it becomes more difficult to maintain a consistent "official" message. The potential for the public to perceive the opinions and postings created by employees as an organization's official position or message increases. While agencies can easily control messages posted on their official social media sites, the ability to control messages posted by employees on other public social media sites the organization does not maintain is limited.

Monitoring employee use

When an organization allows access to social media sites, one aspect of managing employee use can require organizations to rely on employees to determine and maintain an appropriate balance between personal and professional activities. Traditional website monitoring, such as tracking employee site access, blocking sites, or

tracking how long employees spend on certain sites, is less effective for monitoring social media. Employees have more leeway on social media sites to multi-task and engage in professional and personal activities simultaneously. For example, a government professional might devote some work time to networking on GovLoop.com by sharing programmatic ideas and experiences with peers in the Acquisition 2.0 group, but may simultaneously be contributing a favorite recipe to the GovLoop.com GovGourmet group. Relinquishing control and giving responsibility to employees requires trust, which can be difficult to establish.

These are just a few of the challenges stemming from the blurring boundaries between the three types of use. Agencies that are mindful of these challenges can design policies and guidelines that encourage responsible use of social media sites.

Managing the boundaries

The challenges raised by the use of social media are numerous and continue to evolve. Despite the uncertainty of how these challenges will play out in the future, agencies are actively working through the issues. The next sections describe approaches as found in our research, organizations are taking to address various areas of social media policy and guidance, such as access, acceptable use, employee conduct, and managing organizational social media accounts. Addressing these areas within the policy is an important first step in managing employee use of social media in government.

Access policies: taking a holistic view of use

An access policy refers to the type of access employees have to social media sites while at work using government equipment. From our research, governments currently limit access by controlling the number and types of employees who can request access or by designating the types of social media sites that are accessible. In most cases, organizations grant access only to those with responsibility for maintaining an official organizational social media account.

As social media use by citizens and governments becomes more prevalent, organizations will need to expand access considerations to include professional and personal uses. Each approach to access, whether restrictive or open, has a set of benefits and potential risks. Some of the benefits of controlling access to social media sites are that it minimizes the potential security and legal risks that may accompany use. In addition, the organization does not have to expend valuable resources on managing use or training. Some of the costs of tightly controlling access include dampening employee morale and creativity, and decreasing the ability to attract new employees. Another important cost is that employees are unable to take advantage of social media to engage with other professionals to exchange information, create new knowledge, and solve problems.

Ultimately the decision about employee access has to be made by each individual organization based on their unique context. When decisions about access are being made, it is important to consider these issues across all types of social media use.

Acceptable use: setting expectations for personal and professional use

From our interviews we learned for many, once access was granted, there was a concern that there would be a decrease in employee productivity as a result of wasted time on social media sites. One way to alleviate this concern is through the use of an acceptable use policy that will delineate how employees are expected to use social media tools while at work. These policies address issues such as time of use, type of use, purposes of use, and types of equipment.

Based on the interviews with organizations who currently had social media policies, most reference existing acceptable use policies when determining acceptable use of social media. They treated personal use of social media as just one more media type, similar to blogs, newspapers, or radio.

What we found that was missing from acceptable use policies for social media are acceptable use guidelines for organizational and professional interests. Many of the professionals interviewed felt that these uses were better addressed by individual supervisory channels, rather than an organizational-wide policy. However, as use of social media becomes more ubiquitous in government workspace, governments will be faced with more nuanced questions about professional use, such as, Can I use my professional email to create accounts on social media sites, and if so, which ones? Or, are the rules for commenting the same for all social media sites and for all employees within the organization? Are there time limits on using social media for professional networking purposes?

Employee conduct: navigating the personal and the professional

Most organizations that were interviewed have some type of employee conduct guidelines that delineate expectations about employees' behavior when representing the organization. These guidelines outline how employees are expected to behave and the potential repercussions for misconduct. Conduct guidelines are fairly standard, often telling employees to stay away from the use of indecent language, disparaging comments about people based on their race, religion, gender, or sexual orientations, or restrictions on posting confidential and privileged information.

While the issue of appropriate conduct at work or when acting in an official capacity is relatively straightforward, questions of acceptable conduct on social media sites are less clear. The blurry boundaries between personal and professional social media personas and the public nature of the social media world, makes it difficult for governments to draw a clear line around employee conduct. Out of the reviewed policies that addressed the question of conduct, the majority simply referenced existing employee conduct guidelines in respect to employee's official use of social media. What was rarely addressed was the question of employee conduct while using social media for personal and professional social media use.

Some agencies, such as the Environmental Protection Agency and the US Air Force, provide employees with additional guidance and support in regards to their conduct on social media sites. The agencies created flow charts for dealing with a range of citizen comments on social media sites. The charts describe a chain of events and suggested reactions for employees to use when they come across a negative, inaccurate, or derogatory statement directed at the organization. Other agencies are instructing employees to post disclaimers about the content of the information on their personal or professional posts. The disclaimers are designed to distance employee comments from an official organizational position.

From our interviews with government professionals, it became clear that while they worry about employees' personal communication, they are unsure to what degree they can dictate what is permissible in such situations. Some managers expressed questions about personal privacy or infringing on First Amendment rights. At the moment, definitive answers to these questions are not available, and agencies are only beginning to experience and deal with these issues. Determining the balance between protecting employees' rights and safeguarding the organization's message and reputation is something agencies will have to consider. As organizations move forward, they will have to pay attention to their unique context and consider the issues through the lens of all three uses of social media tools.

Account management: protecting the integrity of your organization's social media presence

Of the professionals interviewed during our study, many professionals felt establishing authentic organization accounts and processes for maintaining them as important. They saw protecting legitimate accounts as key to being seen as a trustworthy source of information to citizens and stakeholders. Account management practices encompass the creation, maintenance, and cancellation of social media accounts. From our research, the following describe some of the steps agencies are taking to manage and safeguard official organization social media accounts:

Establish an account opening protocol

Social media's widespread availability and relatively low barriers to use make it easy to establish accounts. These factors also enable situations where accounts can be opened on behalf of agencies or by professionals without organizational approval or consideration of enterprise-wide social media strategies.

To address this issue of easy account setup, many organizations are creating procedures for opening social media accounts. The procedures we heard about vary widely, from an informal chat with an organization executive to the submission of a full business case requiring multiple layers of approval.

Maintain a list of existing official organizational accounts

Over time, agencies may establish numerous social media accounts. These accounts are an organizational asset and require appropriate management to ensure access during emergency situations and adequate maintenance.

As a form of control we learned that some organizations we interviewed required the IT department or individual units to maintain a list of all social media accounts and the associated communal log-on names and passwords. The goal is to ensure all accounts are maintained appropriately. Maintaining such lists enables agencies to retain control of access to accounts in cases where the responsible employees are out of the office, on vacation, or leave the organization.

Maintain a list of employees with privileges to official organization accounts

It is likely that one or multiple employees have knowledge of official social media account usernames and passwords. Agencies or units are taking steps to ensure the security and integrity of these accounts. For example, if an employee with privileges to the accounts leaves an organization, the password, and in some cases, username should be changed.

Follow standard password security guidelines

Just as email, social media accounts are vulnerable to attacks from various sources. Following standard password security guidelines is key to maintaining the integrity of organization's social media accounts. Choosing secure passwords and changing them frequently is necessary to participation in the web 2.0 world.

Moving Forward

Technologies will continue to change more quickly than policies, management practices, and employee skill sets. The boundaries between personal, professional and organizational use of social media are likely to keep shifting in unexpected ways as a result of the constants changes in how people are interacting on-line. Designing and continually updating organization's social media policies and guidelines helps governments manage the implications of such environment. How social media can best be used by government, professionals, and individual citizens is still very much an open question. New policy instruments are part of the resource set necessary to assist governments in their efforts to balance the opportunities with challenges

For further guidance, download CTG's [Designing social media policy for government: Eight essential elements](#) or inquire about our social media training, [Managing Social Media: A Training Class for Government](#).

Natalie Helbig, Program Associate

Jana Hrdinová, Program Associate