



One Hundred Eleventh Congress
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515

June 1, 2009

Department of Homeland Security
Office of the Chief Privacy Officer
Attn: Martha K. Landesberg
Associate Director for Privacy Policy and Education
Privacy Office
Washington, DC 20528

Re: Government 2.0 Privacy and Best Practices
DHS Docket 2009-0020

Dear Ms. Landesberg:

On June 22-23, 2009, the Department of Homeland Security Privacy Office will host a public workshop, *Government 2.0: Privacy and Best Practices*. This workshop will bring together leading academic, private-sector, and public-sector experts to discuss the privacy issues posed by Government use of social media. This workshop is designed to develop ideas to help Federal agencies engage the public through social media in a privacy-protective manner and explore best practices agencies can use to implement President Obama's January 21, 2009, Transparency and Open Government Memorandum.

As Chairman of the U.S. House of Representatives' Committee on Homeland Security, I support the government's use of social media. However, certain practices need be implemented to protect the integrity of the privacy rights of individuals.

I. Advantages of Social Media

Increased use of technology to promote participatory democracy has long been a goal of the Federal Government. Over eight years ago, the E-Government Act of 2002 called for the promotion of the use of the Internet and other information technologies to provide increased opportunities for citizen participation in Government. Additionally, the Act promoted the use of the Internet and emerging technologies within and across Government agencies to provide citizen-centric Government information and services.

The advancement of technological innovation has made these laudable goals easily achievable.

The advent of social media outlets provide the general public with new avenues of discovering, reading, and sharing news, information and other forms of content.

People use a variety of social media outlets such as blogs, social networking, multimedia and collaboration, and entertainment. The popular social networking site, Facebook, has over 300 million users, and the popular microblogging tool, Twitter, has users that send over 3 million tweets a day. With an increasing number of people relying on this form of technology as a primary information gathering resource, short message services (SMS) messages, microblogging, social networking and other media can be exceptional information sharing resources.

In the last decade, as more people come to rely upon social media outlets, their use has supplemented and in some cases replaced traditional media outlets in disseminating news and information.

The Committee on Homeland Security uses its website as an information portal for postings of webcasts of its hearings and meetings as well as disseminating information about natural disasters and incidents of national significance.

Clearly, social media outlets allow the government to simultaneously disseminate useful information to hundreds of thousands of people. Internet portals and SMS allow multiple agencies to reach large numbers of people.

Given the Department's responsibility to provide a coordinated, comprehensive federal response in the event of a terrorist attack, natural disaster or other large-scale emergency, the use of social media during catastrophic events can be an invaluable tool for saving lives, preparing the public, and disseminating necessary information.

For instance, prior to a natural disaster such as a hurricane or a flood, state and local officials can use SMS to convey evacuation warnings and notices to people living in affected areas. Following such an event, SMS or microblogs can be used to direct people to FEMA, the federal entity tasked with disaster relief.

Rapid deployment of accurate information combined with the ability of the average citizen to interact with public officials will ultimately increase accountability and trust in government. For instance, constituents of elected officials who use the popular microblogging tool Twitter, are able to follow government action in real time. This allows constituents an opportunity to read legislation online, comment, and provide feedback.

II. Privacy Concerns

The Federal government's use of this format is a part of a commonsense approach to facilitate greater public discourse on matters of importance. However, proper safeguards must be implemented to ensure that the Government's use of social media outlets complies with the Privacy Act and related legal protections.

The government must make sure that it is responsible when using social media. The government must not only ensure the accuracy of the posted information but also, the government must exercise necessary internal controls to make sure that the privacy of users that interact with the government through social media is protected.

In considering the use of social media outlets, the Department must consider the parameters of privacy policies. As a practical matter, visitors should be made aware that social media are not secure portals and do not have cryptic protocols that provide security and data integrity.

While these risks may be well understood, other risks to privacy interests can be more subtle. It is not impractical to assume that the government could gather information from people with whom it connects on blogs and social networking sites. Because social networking sites, blogs, and microblogs do not have the same privacy policies as government sites, government must develop sufficient guidelines and provide appropriate and clear notice of any information gathering activities which could be used to create a profile or engage in data mining. Moreover, if information gathering activities should occur, Constitutionally clear protocols must be developed to direct such activities.

As the Department of Homeland Security seeks to expand its use of social media it must develop guidelines to ensure proper compliance with the letter and the spirit of the Privacy Act. Specifically, the Department must promulgate a Privacy Impact Assessment (PIA) of each social media outlet to evaluate possible privacy risks and methods to mitigate those risks prior to engaging in the activity. Moreover, the Department must periodically reassess the PIA to assure that changes in technology have not altered the risk calculation.

Although an expectation of privacy in personal information placed on social media networks may not be reasonable, there is a reasonable expectation that the information will not be used to engage in data mining or otherwise target individuals who are exercising constitutionally protected rights.

Finally, the use of social media must not replace traditional methods of information distribution. While many citizens embrace the use of this new technology, the Federal government must not enact policies that exacerbate the digital divide.

Social media can be very useful for the government. When used appropriately, social media can provide the government an efficient and effective way to communicate with people. However, the government must make sure that social media is used as e an

information sharing mechanism, not an information gathering method. If the government uses social media properly, people can remain informed with ease and have confidence that their government is constantly working to meet their needs.

Sincerely,

A handwritten signature in black ink, appearing to read "Ben Ray Lujan". The signature is written in a cursive style with a large initial "B" and "L".

Chairman
Committee on Homeland Security