WRITTEN TESTIMONY

of

MARY ELLEN CALLAHAN
CHIEF PRIVACY OFFICER

and

RICHARD CHÁVEZ
DIRECTOR, OFFICE OF OPERATIONS COORDINATION AND PLANNING
U. S. DEPARTMENT OF HOMELAND SECURITY

Before

UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON HOMELAND SECURITY
SUBCOMMITTEE ON COUNTERTERRORISM AND INTELLIGENCE

Chairman Meehan, Ranking Member Speier, and Members of the subcommittee, we appreciate the opportunity to be here today to discuss the Department of Homeland Security's (DHS) use of social media, and the privacy protections the DHS Privacy Office has put into place.

Social media are web-based and mobile technologies that turn communication into an interactive dialogue in a variety of online fora. It may be appropriate for the government, including DHS, to use social media for a variety of reasons. The President has challenged his Administration to use technology and tools to create a more efficient, effective, and transparent government.[1] DHS recognizes that the use of social media by government actors must occur with appropriate privacy, civil rights, and civil liberties protections; whether DHS is disclosing its information

[1] President Barack Obama, Memorandum on *Transparency and Open Government* (January 21, 2009), available at http://www.gpoaccess.gov/presdocs/2009/DCPD200900010.pdf; OMB Memorandum M-10-06, *Open Government Directive* (December 8, 2009), available at http://www.whitehouse.gov/omb/assets/memoranda_2010/m10-06.pdf.

and press releases via social media platforms like Twitter and Facebook, reviewing news feeds for situational awareness, or researching identified, discrete targets for legitimate investigatory purposes. Accordingly, DHS has created Department-wide standards designed to protect privacy, civil rights, and civil liberties in each category of its use.

There are three general ways in which DHS utilizes social media, and each has associated privacy protections:

- External communications and outreach between the Department and the public;
- Awareness of breaking news of events or situations related to homeland security, known as "situational awareness;" and
- Operational use, when DHS has the appropriate authorities, such as law enforcement and investigations.

In each category, the Department has established and enforces standards that incorporate privacy protections *ex ante*, create uniform standards across the components and Department, and are transparent with regard to the scope of our activities.

External Communications and Outreach

Consistent with the President's 2009 Memorandum on Transparency and Open Government, the Office of Management and Budget's (OMB) Open Government Directive[2] and OMB's Memorandum M-10-23, Guidance for Agency Use of Third-Party Websites and Applications,[3] the Department uses the social networking medium to provide the public with robust information through many channels. For example, DHS currently has a presence on many of the major social

[2] *See supra* note 1.
[3] http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-23.pdf

networking platforms, including Facebook, Twitter, and YouTube. In addition, FEMA launched a FEMA app for smartphones that contains preparedness information for different types of disasters. Similarly, the Transportation Security Administration has MyTSA Mobile Application, which enables the traveling public access to relevant TSA travel information, such as types of items that may be carried through TSA security checkpoints, or estimated wait times.

In 2009, the Department established a Social Media Advisory Group, with representatives from the Privacy Office; Office of General Counsel; Chief Information Security Officer; Office of Records Management; and Office of Public Affairs to ensure that a variety of compliance issues including privacy, legal, security, and records management issues are addressed as DHS uses social media. This group governs and provides guidance on social media initiatives related to external communications and public outreach by reviewing recommendations from components and offices and evaluating Terms of Service agreements and Terms of Use policies. The group also developed a social media use plan, while working to ensure compliance issues are addressed and resolved before the first Department use of a particular application of social media.

DHS also established Department-wide standards for use of social media for communications and outreach purposes through the creation, and development of, two Privacy Impact Assessments (PIAs). The PIAs address two types of uses of social media within the communications/outreach category: 1) interactive platforms where the Department has official identities, using those profiles to provide information about the Department and its services, while having the ability to interact with members of the public such as allowing them to post comments on the official Department page or profile;[4] and 2) unidirectional social media

[4] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia-dhs_socialnetworkinginteractions.pdf

applications encompassing a range of applications, often referred to as applets or widgets, that allow users to view relevant, real-time content from predetermined sources, such as podcasts, Short Message Service (SMS) texting, audio and video streams, and Really Simple Syndication (RSS) feeds.[5]

The PIAs analyze the Department's use of social media and networking for communications purposes, if and how these interactions and applications could result in the Department receiving personally identifiable information (PII), and the privacy protections in place. The PIAs describe the information the Department may have access to, how it will use the information, what information is retained and shared, and how individuals can gain access to and correct their information. For example, official DHS accounts across social media and networking websites and applications must be identified by the component or Department seal as well as an anonymous, but easily identifiable user name account displaying a DHS presence, such as "DHS John Q. Employee." Both the communications and outreach PIAs also include periodically-updated appendices that identify the specific Department-approved profiles and applications. In addition, the PIAs contain provisions that Department-approved profiles are subject to Privacy Compliance Reviews by the DHS Privacy Office.

Situational Awareness

The Office of Operations Coordination and Planning (OPS), National Operations Center (NOC), has a statutory responsibility (Section 515 of the Homeland Security Act (6 U.S.C. §

[5] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_dhswide_unidirectionalsocialmedia.pdf

321d(b)(1))) to provide situational awareness and establish a common operating picture for the federal government, and for state, local, tribal governments as appropriate, in the event of a natural disaster, act of terrorism, or other man-made disaster, and (2) ensure that critical terrorism and disaster-related information reaches government decision-makers. Traditional media sources, and more recently social media sources, such as Twitter, Facebook, and a vast number of blogs, provide public reports on breaking events with a potential nexus to homeland security. By examining open source traditional and social media information, comparing it with many other sources of information, and including it where appropriate into NOC reports, the NOC can provide a more comprehensive picture of breaking or evolving events. To fulfill its statutory responsibility to provide situational awareness and to access the potential value of the public information within the social media realm, in 2010, the NOC launched the first of three pilots using social media monitoring related to specific natural disasters and international events.

Beginning with the pilots, the reason the NOC utilizes social media tools is to identify breaking or evolving incidents and events to provide timely situational awareness and establish a more complete common operating picture. The NOC views information from a variety of sources to include open source reporting and a variety of public and government sources. The NOC synthesizes these reports for inclusion in a single comprehensive report. These reports are then disseminated to DHS components, interagency partners, and state, local, tribal, territorial, and private sector partners with access to the NOC's common operating picture. The content of the reports may be related to standing critical information requirements, emerging events potentially affecting the homeland, or special events such as the Super Bowl or the United Nations General Assembly.

Prior to implementing each social media pilot, the Privacy Office and the Office of Operations Coordination and Planning developed detailed standards and procedures associated with reviewing information on social media web sites. These standards and procedures are documented through a series of pilot-specific PIAs.[6]

The NOC pilots occurred during the 2010 Haiti earthquake response, the 2010 Winter Olympics in Vancouver, British Columbia; and the response to the April 2010, Deep Water Horizon Gulf Coast oil spill. For each of these pilots, the NOC utilized internet-based platforms to provide situational awareness and develop a common operating picture directly related to the response, recovery, and rebuilding efforts in Haiti by reviewing information on publicly-available online fora, blogs, public websites, and message boards.

Following the three discrete social media monitoring pilots by the NOC, the Privacy Office did a thorough (and public) Privacy Compliance Review of the NOC's implementation of the PIAs' privacy protections.[7] The Privacy Office's review found that the NOC's social media monitoring activities did not collect PII, did not monitor or track individuals' comments, and complied with the stated privacy parameters set forth in the underlying PIAs.

Given the positive assessment of the three pilots, OPS and the Privacy Office designed a holistic set of privacy protections to be implemented whenever information made available through social media is being reviewed for situational awareness and establishing a common operating

---

[6] The NOC and the Privacy Office developed three PIAs in the pilot stage of the NOC Media Monitoring Initiative: *Haiti Social Media Disaster Monitoring Initiative*, January 21, 2010, available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ops_haiti.pdf; *2010 Winter Olympics Social Media Event Monitoring Initiative* February 10, 2010, available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ops_2010winterolympics.pdf; and April 2010 *BP Oil Spill Response Social Media Event Monitoring Initiative*, April 29, 2010, available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ops_bpoilspill.pdf.

[7] http://www.dhs.gov/xlibrary/assets/privacy/privacy-privcomrev-ops-olympicsandhaiti.pdf. Three Privacy Compliance Reviews have been completed and published by the Privacy Office, available at: http://www.dhs.gov/files/publications/gc_1284657535855.shtm.

picture. In June 2010, the Department released its *Publicly Available Social Media Monitoring and Situational Awareness Initiative* PIA, incorporating these protections.[8] This PIA describes how the NOC uses Internet-based platforms that provide a variety of ways to review information accessible on publicly-available online fora, blogs, public websites, and message boards. Through the use of publicly-available search engines and content aggregators, the NOC reviews information accessible on certain heavily-trafficked social media sites for information that the NOC can use to provide situational awareness and establish a common operating picture, all without monitoring or tracking individuals' comments or relying on the collection of PII, with very narrow exceptions, discussed below.

The NOC does not: 1) actively seek PII except for the narrow exceptions; 2) post any information on social media sites; 3) actively seek to connect with internal/external social media users; 4) accept internal/external personal users' invitations to connect; or 5) interact on social media sites. The NOC is, however, permitted to establish user names (consistent with the criteria established in the communications and outreach PIAs) and passwords to form profiles and follow relevant government, media, and subject matter experts on social media sites as described in the June 2010 PIA; and to use search tools under established criteria and search terms that support situational awareness and establishing a common operating picture.

As part of the publication of the June 2010 PIA, the Privacy Office mandates Privacy Compliance Reviews every six months. After conducting the second Privacy Compliance Review, the Privacy Office determined that this PIA should be updated to allow for the collection and dissemination of PII in a very limited number of situations in order to respond to the evolving operational needs of the NOC. After January 2011, this PII on the following

[8] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ops_publiclyavailablesocialmedia.pdf.

categories of individuals may be collected when it lends credibility to the report or facilitates coordination with federal, state, local, tribal, territorial, and foreign governments, or international law enforcement partners:

1) U.S. and foreign individuals *in extremis*, i.e., in situations involving potential life or death circumstances;

2) Senior U.S. and foreign government officials who make public statements or provide public updates;

3) U.S. and foreign government spokespersons who make public statements or provide public updates;

4) U.S. and foreign private sector officials and spokespersons who make public statements or provide public updates;

5) Names of anchors, newscasters, or on-scene reporters who are known or identified as reporters in their posts or articles, or who use traditional and/or social media in real time to provide their audience situational awareness and information;

6) Current and former public officials who are victims of incidents or activities related to homeland security; and

7) Terrorists, drug cartel leaders, or other persons known to have been involved in major crimes of homeland security interest, (e.g., mass shooters such as those at Virginia Tech or Ft. Hood) who are killed or found dead.[9]

For this narrow category of individuals, DHS may only collect the full name, affiliation, position or title, and publicly-available user ID, when it lends credibility to the report. DHS determined

[9] The most recent PIA update (authorizing these narrow PII categories collection) was finalized January 6, 2011, and is available at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ops_publiclyavailablesocialmedia_update.pdf.

that this information improves the efficacy and effectiveness of the social media monitoring initiative without an unwarranted invasion of privacy of individuals in each of these categories. For this narrow category of individuals the PII is only stored in the narrative report in which it is used, and is not tracked for any other reason. DHS published a System of Records Notice[10] that describes the creation of these seven exceptions for the collection of PII and narrowly tailored, how much information can be collected, and how the information can be used. Furthermore, the Privacy Office is commencing its semi-annual Privacy Compliance Review in late February to ensure that the NOC continues to adhere to the privacy protections identified in the PIA.

Operational Use

There may be situations where particular programs within the Department or its components may need to access material on social media or individual profiles in support of authorized missions. Given the breadth of the Department's mission, and the fact that access, collection, and use of social media and other publicly-available information is governed by specific legal authorities, rather than Department-wide standards, the Department has taken a different approach in embedding privacy protections into Department use of social media for operational purposes, with authority-based requirements implemented through policy and Management Directives. For example, components of DHS such as U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, Federal Protective Service, Federal Air Marshals Service, U.S. Coast Guard, and U.S. Secret Service have the authority to engage in law enforcement activities which may include the use of online and Internet materials. Other DHS offices and components may be authorized to utilize social media for specific law enforcement purposes such as investigating

[10] http://edocket.access.gpo.gov/2011/2011-2198.htm.

fraud. The Office of Intelligence and Analysis also has some overt collection authorities for intelligence purposes which may include the use of online and Internet materials.

DHS has established objective criteria by which those investigatory components can access publicly-available information. DHS components cannot review individuals' information unless they have appropriate underlying authority and supervisory approval. Moreover, Office of Operations Coordination and Planning and Office of Intelligence and Analysis have additional specific policies on the use of social media for operational purposes. One of DHS' responsibilities is to confirm our work is being done under the appropriate legal framework for federal law enforcement activities. However, with increased access to individuals' personal information posted on the Internet and social media sites, these DHS components have been reminded that they must also be conscious of privacy considerations.

At DHS, we work every day to strike a balance between our need to use open source Internet and social media information for all purposes, but particularly law enforcement and investigatory purposes to further our mission, while protecting First Amendment rights, Fourth Amendment rights, and privacy.

In 1999, the Department of Justice issued guidelines for federal law enforcement agents that outline online investigative principles that are applicable, but do not explicitly reference, social media. In 2011, the Office of the Director of National Intelligence issued guidelines that outline how intelligence community professionals should use technology, including social media. Both guidelines address the following topics: obtaining information from publicly-available media under the same conditions that apply to obtaining information from other sources generally open to the public; passively observing and logging real-time electronic communications on media

open to the public under the same circumstances in which these activities could be undertaken when attending a public meeting; and retaining the contents of a stored electronic message, such as online traffic, if that information would have been retained had it been written on paper. Moreover, federal law enforcement agents communicating online with witnesses, subjects, or victims must disclose their affiliation with law enforcement when DHS guidelines would require such disclosure if the communication were taking place in person or over the telephone — they may communicate online under a non-identifying name or fictitious identity if DHS guidelines and procedures would authorize such communications in the physical world.[11] Finally, federal law enforcement agents may not access restricted online sources absent legal authority permitting entry into a private space. Until a Department-wide Management Directive on using social media for operational purposes is finalized, the Secretary has instructed all components to adhere to the DOJ or ODNI guidelines as appropriate.

In light of the varying authorities and responsibilities within the Department, instead of having a Privacy Impact Assessment with general standards (such as for communications and situational awareness purposes), the Department is developing a Management Directive for Privacy Protections in Operational Use of Social Media. The Management Directive will be enforceable throughout the Department, and will identify the authorities, restrictions, and privacy oversight related to use of social media for operational purposes. The Management Directive will also provide instructions on how to embed privacy protections into the operational use of social media and each investigation performed by Department personnel. The Privacy Office has

[11] *See, e.g., Online Investigative Principles for Federal Law Enforcement Agents* (Department of Justice, 1999) and *Civil Liberties and Privacy Guidance for Intelligence Community Professionals: Properly Obtaining and Using Publicly Available Information* (Office of the Director of National Intelligence, 2011).

already investigated one component's use of social media for investigatory purposes; its conclusions are informing the Management Directive.

Consistent with the Department's approach to embed privacy protections throughout the lifecycle of Department activities, the Privacy Office will conduct a Privacy Compliance Review or assessment of the Department's adherence to the social media Management Directive approximately six months after the Directive is implemented.

Conclusion

In light of the scope and availability of information including PII found in social media venues, the Privacy Office intends to continue to monitor the Department's use of social media in all three categories—communications and outreach, situational awareness, and operational use—to ensure privacy protections are built-in and followed.

#####