DHS MONITORING OF SOCIAL NETWORKING AND MEDIA: ENHANCING INTELLIGENCE GATHERING AND ENSURING PRIVACY

HEARING

BEFORE THE

SUBCOMMITTEE ON COUNTERTERRORISM AND INTELLIGENCE

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

FEBRUARY 16, 2012

Serial No. 112–68

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.gpo.gov/fdsys/

U.S. GOVERNMENT PRINTING OFFICE

76–514 PDF WASHINGTON : 2012

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

PETER T. KING, New York, *Chairman*

LAMAR SMITH, Texas
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
MICHAEL T. MCCAUL, Texas
GUS M. BILIRAKIS, Florida
PAUL C. BROUN, Georgia
CANDICE S. MILLER, Michigan
TIM WALBERG, Michigan
CHIP CRAVAACK, Minnesota
JOE WALSH, Illinois
PATRICK MEEHAN, Pennsylvania
BEN QUAYLE, Arizona
SCOTT RIGELL, Virginia
BILLY LONG, Missouri
JEFF DUNCAN, South Carolina
TOM MARINO, Pennsylvania
BLAKE FARENTHOLD, Texas
ROBERT L. TURNER, New York

BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
SHEILA JACKSON LEE, Texas
HENRY CUELLAR, Texas
YVETTE D. CLARKE, New York
LAURA RICHARDSON, California
DANNY K. DAVIS, Illinois
BRIAN HIGGINS, New York
JACKIE SPEIER, California
CEDRIC L. RICHMOND, Louisiana
HANSEN CLARKE, Michigan
WILLIAM R. KEATING, Massachusetts
KATHLEEN C. HOCHUL, New York
JANICE HAHN, California

MICHAEL J. RUSSELL, *Staff Director/Chief Counsel*
KERRY ANN WATKINS, *Senior Policy Director*
MICHAEL S. TWINCHEK, *Chief Clerk*
I. LANIER AVANT, *Minority Staff Director*

SUBCOMMITTEE ON COUNTERTERRORISM AND INTELLIGENCE

PATRICK MEEHAN, Pennsylvania, *Chairman*

PAUL C. BROUN, Georgia, *Vice Chair*
CHIP CRAVAACK, Minnesota
JOE WALSH, Illinois
BEN QUAYLE, Arizona
SCOTT RIGELL, Virginia
BILLY LONG, Missouri
PETER T. KING, New York *(Ex Officio)*

JACKIE SPEIER, California
LORETTA SANCHEZ, California
BRIAN HIGGINS, New York
KATHLEEN C. HOCHUL, New York
JANICE HAHN, California
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

KEVIN GUNDERSEN, *Staff Director*
ZACHARY HARRIS, *Subcommittee Clerk*
HOPE GOINS, *Minority Subcommittee Director*

CONTENTS

DHS MONITORING OF SOCIAL NETWORKING AND MEDIA: ENHANCING INTELLIGENCE GATHERING AND ENSURING PRIVACY

Thursday, February 16, 2012

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON COUNTERTERRORISM AND INTELLIGENCE,
Washington, DC.

The subcommittee met, pursuant to call, at 10:04 a.m., in Room 311, Cannon House Office Building, Hon. Patrick Meehan [Chairman of the subcommittee] presiding.

Present: Representatives Meehan, Cravaack, Quayle, Long, Speier, Thompson, and Hahn.

Mr. MEEHAN. Good morning. I get to do this, which indicates that the Committee on Homeland Security's Subcommittee on Counterterrorism and Intelligence will come to order.

The subcommittee is meeting today to hear testimony regarding tactics that are employed by the Department of Homeland Security to monitor social networking and media to enhance intelligence gathering, while at the same time protecting privacy. I would like to welcome everyone to today's hearing, and I look forward to hearing from today's witnesses on this very, very important issue.

Over the last year, this subcommittee has had hearings on a multitude of terror-related threats, particularly focusing on those that have influence on the homeland, including those posed by Hezbollah, AQAP, and Boko Haram, to be specific. A common theme that has emerged among many of these is the groups' use of social media and networking to recruit, to plan, to plot attacks against the homeland or U.S. interests abroad. I emphasize that a lot of this was focused on foreign-based websites on which this activity was presumed to be taking place.

In December, we held a hearing on the terrorists' use of social media. While there was disagreement among the witnesses on the effectiveness of that, we do know that terrorists use social media. All agreed that terrorist groups used these tools ultimately to their advantage.

However, the use of social media isn't confined to terrorists. It is also a criminal issue and represents an entirely new operating space for all sorts of bad actors. I saw it as a Federal prosecutor. Social media is now used by individuals who share pictures with family and friends, but it is also used by terrorists or other kinds of criminals operating everything from frauds to other kinds of bad acts.

I understand the importance of following leads wherever it may take investigators. So if there are leads on a social media or social network such as Twitter or Facebook, it may be appropriate to follow them, so long as the Government activity is consistent with the long-standing protections against improper intrusions into protected areas of personal privacy. Following leads means collecting intelligence, because, ultimately, no terrorism or criminal investigation can be effective without good intelligence. I understand and support intelligence collection within the rules of the law.

In addition to following leads, social media provides a forum for the Government to have situational awareness of breaking events—something I know you spend a great deal of time—terrorist attacks, natural disasters—where the Department of Homeland Security is responsible for providing real-time situational awareness and information sharing across the Federal Government and down to the State and local enforcement level, to first responders as well, in the event of a terror attack or a natural disaster. For example, my good friend on the committee, Mr. Long, who experienced tornadoes in his district, may have an appreciation of the need for real-time communication, sort of the virtual 9–1–1.

But, conversely, the Government can use tools to communicate with people about disasters to enhance situational awareness among the citizenry. In these cases, intelligence collection and dissemination is a win-win for the Government and the people.

But a few weeks ago, it was reported that the Department of Homeland Security has instituted a program, and I quote: "to produce short reports about threats and hazards using publicly available information." As I said, I support that. However, in what I view as something that we have to determine whether it crosses the line, these reports also revealed that DHS has tasked analysts with collecting intelligence on any media reports, "that reflect adversely on the U.S. Government and the Department of Homeland Security, including both positive and negative reports on FEMA, CBP, ICE, among others."

In one example, DHS used multiple social networking blogs, including Facebook and Twitter, three different blogs, and reader comments in newspapers to capture the reaction of residents to a possible plan to bring Guantanamo detainees to a local prison in Standish, Minnesota.

In my view, collecting and analyzing, disseminating private citizens' comments could have a chilling effect on individuals' privacy rights and people's freedom of speech and dissent against their Government. I fully recognize that if an individual willingly uses Facebook, Twitter, or the comments section of a newspaper website, they, in effect, forfeit their right to an expectation of privacy. However, other private individuals reading your Facebook status updates is different than the Department of Homeland Security reading them, analyzing them, and possibly disseminating and collecting them for future purposes. My guess is that the average American has no problem with other private individuals reading their voluntary on-line writings and postings in open forums but may feel a bit of unease knowing the Federal Government may be doing the same.

I fully recognize these are very complex and nuanced issues, and that is why we are holding today's hearing. I look forward to hearing from today's witnesses on how they are collecting intelligence to keep us safe and aware, yet also ensuring personal individual privacy.

The Chair now recognizes the Ranking Minority Member of the subcommittee, the gentlewoman from California, Ms. Speier, for any comments that she may have.

Ms. SPEIER. Thank you, Mr. Chairman. I would like to associate my comments with yours. I think that they were outstanding and really place a good frame on the discussion we are going to have today.

I would also like to thank the witnesses who will be testifying today.

You know, the explosion in the use of social media has changed communication as we know it. With just the touch of a button, millions of people can post and receive information through Twitter, Facebook, blogs, and text messaging in an instant. In just the short time that we have been sitting here in this hearing, there have been over 3 million comments that have been posted to Facebook and a half a million tweets that have been sent.

Over the past year, we have seen the impact of using social media first-hand. Last year, the Arab Spring was driven by potesters who organized and communicated largely via social media. We have also seen the power of social media here in the United States over the past few months as protesters organize via Twitter and Facebook for the Occupy Wall Street movements throughout the country. We have seen bills before Congress stopped in their tracks by the power of social media.

This growing universe of social networking presents great challenges and opportunities to the mission at the Department of Homeland Security as it works to keep our Nation safe. Through this hearing, we hope to learn how the Department of Homeland Security is harnessing the power of social media. Is it possible that DHS could use social media to communicate emergency recovery and response information to the general public? Can this information be generated quickly? How would such technology have improved the response to disasters like Hurricane Katrina? What about the case of a man-made disaster or a mass evacuation like we saw last year in the nuclear meltdown in Japan? Could Twitter and instant messaging be used to let people know where to evacuate and what to avoid?

The vast amounts of publicly available data also present a potentially great resource for open-source information collection. In 2010, we saw alert citizens report suspicious activities in Times Square that led to the arrest of Faisal Shahzad. Could similar public reporting be done using social media? How can DHS fully exploit the benefits and opportunities of social media without impeding on the civil rights and civil liberties of those who choose to use social media? Can DHS actively and effectively monitor social media in an open and above-board way without being accused of spying on lawful activities?

Last month, the press reported widely on a case where a couple from England was prevented from entering the United States be-

cause of a tweet. Was this an overreaction? Could or should a mere tweet or posting prevent a person from boarding a plane or entering the United States?

I am looking forward to learning from the witnesses exactly how DHS uses social media and what DHS is doing to make sure that in its use of social media it is not being perceived as being a Big Brother. I want to learn from the witnesses what privacy protections are in place with regard to DHS's using social media and how the individual components are being trained on these protections.

Further, I am very interested to find out today how the Department can even handle the sheer volume of open-source postings that may be found on any of the various social networking websites. Further, if the Department begins to use social media as open-source tools, as the Office of Intelligence and Analysis Under Secretary has indicated, how will its analysts be trained to continue to respect the civil liberties of those that choose to use social media?

Social media could possibly be an integral tool in recognizing and preventing emerging threats. However, there has to be some specific systems in place that can manage this information while continuing to respect civil rights and civil liberties. I look forward to hearing what steps are being taken in this area.

I yield back.

Mr. MEEHAN. Thank you, Ranking Member Speier, for your observations, which I, as well, share.

We are also pleased to have in attendance the Ranking Member of the committee. The gentleman from Mississippi, Mr. Thompson, is with us. As is the custom of the subcommittee where there are moments when we are graced with the presence of those Ranking and senior members, we give to them the opportunity to make an opening statement if they wish. So, at this minute, the Chair would recognize Mr. Thompson for any comments that he might have.

Mr. THOMPSON. Thank you very much, Mr. Chairman, for your gracious introduction. I would like to thank you and the Ranking Member for holding this hearing today. I would also like to thank the witnesses for their testimony also.

Social media outlets provide the general public with new avenues of discovering, reading, and sharing news, information, and other forms of content. With an increasing number of people relying on this form of technology as a primary information-gathering resource, social media has supplemented, and in some cases replaced, traditional media outlets as a source of news and information.

Social media allows DHS to quickly and efficiently disseminate accurate and useful information to hundreds of thousands of people simultaneously. 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. After a disaster, the same means can be used to direct people to FEMA. Both the Majority and Minority of this committee have a Twitter page.

I think we all agree that social media outlets are useful. However, usefulness alone is not the only criteria we value. Rapid deployment of accurate information, combined with the ability of the average citizen to interact with public officials, will ultimately in-

crease DHS's trust and accountability. To ensure that accountability and trust are embraced as a value, DHS must employ proper safeguards, including guidelines on information-gathering activities and a clear policy on creating a profile or data-mining. If information-gathering activities should occur, clear protocols that adhere to the Constitution and the Privacy Act must be developed to direct such activities. The public must be confident that interacting with DHS on a website or blog or Facebook will not result in surveillance or a compromise of Constitutionally-protected rights.

Further, the use of social media must not replace traditional methods of information distribution. When used appropriately, social media is an efficient and effective way to communicate with people. If used improperly by a Federal agency, public trust and confidence will be compromised or forever destroyed.

Given the high stakes involved, DHS cannot afford to make a mistake. I trust that in your efforts to navigate the Department's journey in the world of social media, you will work closely with the committee and keep us informed of your activities. We look forward to being your GPS.

With that, I yield back.

Mr. MEEHAN. Thank you, Mr. Chairman, for that sense of direction.

We will stop it there. Other Members of the committee are reminded that opening statements may be submitted for the record.

We are pleased to have a distinguished panel of witnesses before us today on this very, very important topic.

The first is Ms. Mary Ellen Callahan. She was appointed the chief privacy officer and the chief Freedom of Information Act officer by Department of Homeland Security Secretary Napolitano in March 2009.

Created by Congress in 2002, the Department's privacy officer is the first statutorily mandated privacy office in any Federal agency, whose mission is to preserve and enhance privacy protections for all individuals, to promote the transparency of Homeland Security operations, and to serve as the leader in the Federal privacy community. Ms. Callahan is responsible for evaluating Department-wide programs, systems, and technologies, and rulemaking for potential privacy impacts, and for providing mitigation strategies to reduce any privacy impact.

Prior to joining the Department, Ms. Callahan was a partner with the law firm of Hogan & Hartson, where she specialized in privacy and data security law. She serves as vice chair of the American Bar Association's Privacy and Information Security Committee of the Antitrust Division. Now as chief privacy officer, she co-chairs both the CIO Council's Privacy Committee and the Information-Sharing Environment Privacy Guidelines Committee.

Thank you for being here today, Ms. Callahan.

I would also like to recognize Mr. Richard Chávez, who is the director of Office of Operations Coordination and Planning at the Department of Homeland Security.

He provides counsel directly to the Secretary of Homeland Security on a wide range of operational issues, to include prevention, protection, mitigation, response and recovery operations, continuity of operations, and planning. He leads an office of approximately

550 people who are responsible for monitoring the security of the United States on a daily basis and providing National situational awareness and developing the National common operating picture.

His office provides vital decision support information to the Federal interagency, Governors, homeland security advisors, law enforcement, private-sector, and critical infrastructure operators in all States and territories and more than 50 urban major areas Nation-wide.

Mr. Chávez has over 30 years of Government experience, serving with DHS and the Department of Defense as an Air Force officer and a senior civilian in the Office of the Under Secretary of Defense for Policy.

Before I recognize you for your comments, I have before me on the table a report from the Electronic Privacy Information Center. I ask unanimous consent to insert in the record a statement from EPIC.

Hearing no objection, so ordered.

[The information follows:]

STATEMENT OF MARC ROTENBERG, PRESIDENT, AND GINGER MCCALL, STAFF COUNSEL, THE ELECTRONIC PRIVACY INFORMATION CENTER (EPIC)

Thank you, Mr. Chairman, for the invitation to submit this statement for the record for this hearing on "DHS Monitoring of Social Networking and Media: Enhancing Intelligence Gathering and Ensuring Privacy" to be held on February 16, 2012 before the House Subcommittee on Counterterrorism and Intelligence. We ask that this statement be included in the hearing record.

EPIC thanks you and Members of the subcommittee for your attention to this important issue. The DHS monitoring of social networks and media organizations is entirely without legal basis and threatens important free speech and expression rights. Your decision to hold this hearing will help protect important American rights.

The Electronic Privacy Information Center (EPIC) is a non-partisan, public interest research organization established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC works to promote Government accountability and transparency particularly with respect to activities that implicate Constitutional rights and fundamental freedoms. EPIC has been analyzing law enforcement monitoring of social networks and on-line media for several years. In early 2011, EPIC submitted comments to the Department of Homeland Security on the agency's proposal to undertake monitoring of social network and news organizations.[1] EPIC has also pursued several Freedom of Information requests to obtain relevant documents so that the Members of your committee and the public would have the opportunity to meaningful assess the agency's activities.

I. EPIC OBTAINED DOCUMENTS THAT REVEAL THAT THE DHS IS MONITORING SOCIAL NETWORK AND MEDIA ORGANIZATIONS FOR DISSENT AND CRITICISM OF THE AGENCY

In April 12, 2011, EPIC submitted a Freedom of Information Act ("FOIA") request to the Department of Homeland Security ("DHS") seeking agency records detailing the media monitoring program. The request sought the following documents:

- All contracts, proposals, and communications between the Federal Government and third parties, including, but not limited to, H.B. Gary Federal, Palantir Technologies, and/or Berico Technologies, and/or parent or subsidiary companies, that include provisions concerning the capability of social media monitoring technology to capture, store, aggregate, analyze, and/or match personally-identifiable information.
- All contracts, proposals, and communications between DHS and any States, localities, Tribes, territories, and foreign governments, and/or their agencies or subsidiaries, and/or any corporate entities, including but not limited to H.B.

[1] EPIC, Comments of the Electronic Privacy Information Center to the Department of Homeland Security "Systems of Records Notice" DHS–2011–0003, March 3, 2011, available at: *http://epic.org/privacy/socialmedia/Comments%20on%20DHS-2011-0003-1.pdf*.

Gary Federal, Palantir Technologies, and/or Berico Technologies, regarding the implementation of any social media monitoring initiative.
- All documents used by DHS for internal training of staff and personnel regarding social media monitoring, including any correspondence and communications between DHS, internal staff and personnel, and/or privacy officers, regarding the receipt, use, and/or implementation of training and evaluation documents.
- All documents detailing the technical specifications of social media monitoring software and analytic tools, including any security measures to protect records of collected information and analysis.
- All documents concerning data breaches of records generated by social media monitoring technology.[2]

When the agency failed to comply with FOIA's deadlines, EPIC filed suit on December 23, 2011. As a result of this lawsuit, DHS disclosed to EPIC 285 pages of documents, including statements of work, contracts, and other agency records related to social network and media monitoring.[3]

These documents reveal that the agency had paid over $11 million to an outside company, General Dynamics, to engage in monitoring of social networks and media organizations and to prepare summary reports for DHS.[4] According to DHS documents, General Dynamics will "Monitor public social communications on the internet," including the public comment sections of NYT, LA Times, Huff Po, Drudge, Wired's tech blogs, ABC News.[5] DHS also requested monitoring of Wikipedia pages for changes[6] and announced its plans to set up social network profiles to monitor social network users.[7]

DHS required General Dynamics to monitor not just "potential threats and hazards," "potential impact on DHS capability" to accomplish its homeland security mission, and "events with operational value," but also paid the company to "Identify[] reports that reflect adversely on the U.S. Government, DHS, or prevent, protect, respond or recovery Government activities."[8]

Within the documents, DHS clearly stated its intention to "capture public reaction to major Government proposals."[9] DHS instructed the media monitoring company to generate summaries of media "reports on DHS, Components, and other Federal Agencies: Positive and negative reports on FEMA, CIA, CBP, ICE, etc. as well as organizations outside the DHS."[10]

In one DHS-authored document, titled "Social Networking/Media Capability Analyst Handbook" the agency presented examples of good summary reports and flawed summary reports. One report held up as an exemplar was titled "Residents Voice Opposition Over Possible Plan to Bring Guantanamo Detainees to Local Prison-Standish MI."[11] This report summarizes dissent on blogs and social networking cites, quoting commenters who took issue with the Obama administration's plan to transfer detainees to the Standish Prison.

These documents clearly show an agency program that aims to document legitimate on-line dissent and criticism. The agency has not established any legal basis for this program.

News media reports indicate that the Department of Homeland Security is not the only agency engaging in this sort of monitoring. Recent news stories confirm that

---

[2] EPIC FOIA Request, Apr. 12, 2011, available at: *http://epic.org/privacy/socialnet/EPIC-FOIA-DHS-Social-Media-Monitoring-04-12-11.pdf;* see also Olivia Katrandjian, *DHS Creates Accounts Solely to Monitor Social Networks,* ABC News, Dec. 28, 2011, available at: *http://abcnews.go.com/US/dhs-creates-fake-accounts-monitor-social-networks/story?id=15247533#.TzvuuONSQ3o.*

[3] DHS Social Media Monitoring Documents, available at: *http://epic.org/foia/epic-v-dhs-mediamonitoring/EPIC-FOIA-DHS-Media-Monitoring-12-2012.pdf;* see e.g. Charlie Savage, *Federal Contractor Monitored Social Network Sites,* The New York Times, Jan. 13, 2012, available at: *http://www.nytimes.com/2012/01/14/us/federal-security-program-monitored-public-opinion.html;* Jaikumar Vijayan, *DHS Media Monitoring Could Chill Public Dissent, EPIC Warns,* Computerworld Jan. 16, 2012, available at: *http://www.computerworld.com/s/article/9223441/DHS_media_monitoring_could_chill_public_dissent_EPIC_warns;* Ellen Nakashima, *DHS Monitoring of Social Media Concerns Civil Liberties Advocates,* Washington Post, Jan. 13, 2012, available at: *http://www.washingtonpost.com/world/national-security/dhs-monitoring-of-social-media-worries-civil-liberties-advocates/2012/01/13/gIQANPO7wP_story.html.*

[4] EPIC, DHS Social Media Monitoring Documents at 1.

[5] EPIC, DHS Social Media Monitoring Documents at 127, 135, 148, 193.

[6] EPIC, DHS Social Media Monitoring Documents at 124, 191.

[7] EPIC, DHS Social Media Monitoring Documents at 128.

[8] Attachment 1; EPIC, DHS Social Media Monitoring Documents at 51, 195.

[9] EPIC, DHS Social Media Monitoring Documents at 116.

[10] EPIC, DHS Social Media Monitoring Documents at 183, 198.

[11] EPIC, DHS Social Media Monitoring Documents at 118.

the Federal Bureau of Investigation has also been developing a similar social network and media monitoring program.[12]

II. THERE IS NO LEGAL BASIS FOR THE DHS' SOCIAL NETWORK AND MEDIA MONITORING PROGRAM

The agency has demonstrated no legal basis for its social network and media monitoring program, which threatens important free speech and expression rights.

Law enforcement agency monitoring of on-line criticism and dissent chills legitimate criticism of the Government, and implicates the First Amendment. Freedom of Speech and Expression are at the core of civil liberties and have been strongly protected by the Constitution and the U.S. courts.[13] Government programs that threaten important First Amendment rights are immediately suspect and should only be undertaken where the Government can demonstrate a compelling interest that cannot be satisfied in other way.[14] Government programs that note and record on-line comments, dissent, and criticism for the purpose of subsequent investigation send a chilling message to on-line commenters, bloggers, and journalists—"You are being watched." This is truly what George Orwell described in 1984.

As EPIC has stated in prior comments to DHS, the agency's social network and media monitoring program would also violate the Privacy Act.[15] The Privacy Act requires agencies to:

"establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."[16]

The DHS program, as described in the agency's own documents, would involve collecting information, including Personally Identifiable Information ("PII"). While the agency acknowledges that PII are covered under the Privacy Act and seeks to limit some collection, the documents obtained by EPIC also reveal that there are several exceptions to the "no PII" rule, including allowances for collection of PII of anchors, newscasters, or on-scene reporters who . . . use traditional and/or social media.[17] This would allow the agency to build files on bloggers and internet activists, in violation of the Privacy Act.

The Privacy Act imposes limitations on the dissemination of personal information collected by an agency. As EPIC has noted in its comments the DHS, the agency's social network and media monitoring program permits the collection and disclosure of information that contravenes the text and purpose of the Privacy Act.[18] DHS has indicated that it plans to regularly relay the records to Federal, State, local, Tribal, territorial, foreign, or international government partners.[19] The DHS Chief Privacy Officer ("CPO") has stated that the records would be transferred both by "email and telephone" to contacts inside and outside of the agency.[20] The CPO has also stated

---

[12] Marcus Wohlson, *FBI Seeks Digital Tool to Mine Entire Universe of Social Media,* Chicago Sun Times, Associated Press, Feb. 12, 2012, available at: *http://www.usatoday.com/USCP/PNI/Nation/World/2012-0213-PNI0213wir-FBI-social-media__ST__U.htm*.

[13] See e.g. *United States* v. *Stevens,* 130 S. Ct. 1577, 1585, 176 L. Ed. 2d 435 (2010) (holding that the "First Amendment itself reflects a judgment by the American people that the benefits of its restrictions on the Government outweigh the costs").

[14] See e.g. *NAACP* v. *Button,* 83 S.Ct. 328 (1963); *Citizens United* v. *Fed. Election Comm'n,* 130 S. Ct. 876 (2010).

[15] EPIC, Comments of the Electronic Privacy Information Center to the Department of Homeland Security "Systems of Records Notice" DHS–2011–0003, March 3, 2011, available at: *http://epic.org/privacy/socialmedia/Comments%20on%20DHS-2011-0003-1.pdf*.

[16] 5 U.S.C. § 552a(e)(10) (2010).

[17] DHS Social Media Monitoring Documents at 107.

[18] EPIC, Comments of the Electronic Privacy Information Center to the Department of Homeland Security "Systems of Records Notice" DHS–2011–0003, March 3, 2011, available at: *http://epic.org/privacy/socialmedia/Comments%20on%20DHS-2011-0003-1.pdf*.

[19] EPIC, Comments of the Electronic Privacy Information Center to the Department of Homeland Security "Systems of Records Notice" DHS–2011–0003, March 3, 2011, available at: *http://epic.org/privacy/socialmedia/Comments%20on%20DHS-2011-0003-1.pdf;* DHS Social Media Monitoring Documents at 139, 207.

[20] Department of Homeland Security, Privacy Impact Assessment for the Office of Operations Coordination and Planning Publicly Available Social Media Monitoring and Situational Awareness Initiative, 8, Jan. 6, 2011.

that "[n]o procedures are in place" to determine which users may access this system of records.[21]

DHS' program also fails to comply with Privacy Act requirements that agencies make "reasonable efforts to assure that records are accurate, complete, timely, and relevant for agency purposes" prior to their dissemination outside of the Federal Government. DHS has readily admitted that its social media monitoring initiative explicitly relies on unverified sources of information to construct the records that DHS will then disseminate to State, local, Tribal, territorial, foreign, or international government partners. As the DHS CPO has stated, "[u]sers may accidentally or purposefully generate inaccurate or erroneous information. There is no mechanism for correcting this."[22] The agency unlawfully shifts responsibility for verifying the agency's information onto the social media users the agency plans to follow: "the community is largely self-governing and erroneous information is normally expunged or debated rather quickly by others within the community with more accurate and/or truthful information."[23]

As EPIC has previously stated in comments to DHS, the collection of information about individuals obtained from social networks and the monitoring of media organizations falls outside of the agency's statutory authority. The agency has failed to cite any statutory provision that would indicate that Congress gave the DHS authority to engage in intelligence collection, let alone to violate the Constitutional rights of individuals using the internet to express criticisms of the agency or the U.S. Government. In fact, the one statutory provision cited by the agency only allows the DHS Secretary to "access, receive, and analyze law enforcement information, intelligence information, and other information from agencies of the Federal Government, State and local government agencies and private sector entities." (Emphasis added). It does not authorize the agency to initiate a program to gather or collect that information itself. The only relevant provision that does mention gathering narrows the term to "incident management decision making."

Hence, DHS' monitoring and gathering of social network and media information is not within the agency's delegated duties. DHS monitoring of stories or individuals that "report adversely" on the agency (or the Government more broadly) is even further outside of its delegated duties. The agency has failed to establish any legal basis for this program.[24]

III. EPIC'S RECOMMENDATIONS

The problems described above are significant and far-reaching. An agency that was established to help protect the United States against future foreign attacks is now deploying its significant resources to monitor political opposition and the work of journalists within the United States. It has no legal basis to do so, and in pursuing the monitoring of social networks and media organizations for activities that "reflect adversely" on the agency and the U.S. Government, it has transformed its purpose from protecting the American public to protecting simply itself.

---

[21] Department of Homeland Security, Privacy Impact Assessment for the Office of Operations Coordination and Planning Publicly Available Social Media Monitoring and Situational Awareness Initiative, 10, June 22, 2010, DHS Social Media Monitoring Documents at 156, 145.

[22] DHS Social Media Monitoring Documents at 156, 145.

[23] DHS Social Media Monitoring Documents at 156, 145.

[24] The Attorney General has established elaborate Guidelines for domestic investigations. The Attorney General Guidelines for Domestic FBI Investigations, available at *www.justice.gov/ag/readingroom/guidelines.pdf*. While EPIC does not necessarily endorse the standards set out in the DIOG, we note that they require at a minimum a predicate that justifies a Federal investigation. Expressing criticism of the Government or a particular Federal agency alone can simply never be the basis for a Federal investigation under the Attorney General Guidelines.

> Circumstances Warranting Investigation
>
> A predicated investigation may be initiated on the basis of any of the following circumstances:
>
> a. An activity constituting a Federal crime or a threat to the National security has or may have occurred, is or may be occurring, or will or may occur and the investigation may obtain information relating to the activity or the involvement or role of an individual, group, or organization in such activity.
>
> b. An individual, group, organization, entity, information, property, or activity is or may be a target of attack, victimization, acquisition, infiltration, or recruitment in connection with criminal activity in violation of Federal law or a threat to the National security and the investigation may obtain information that would help to protect against such activity or threat.
>
> c. The investigation may obtain foreign intelligence that is responsive to a foreign intelligence requirement.

Id. at 21. See, generally, EPIC, "The Attorney General Guidelines," available at *http://epic.org/privacy/fbi/*

We specifically recommend that the subcommittee take the following steps to address the immediate risks to Constitutional liberty:

- Require that the DHS immediately and permanently cease the practice of monitoring social networks and media organizations for the purpose of identifying political and journalistic activities that "reflect adversely" on the agency or the Federal Government.
- Require that the DHS suspend the social network and media organization monitoring program until safeguards are put into place which will ensure oversight, including annual reporting requirements.
- Require that other agencies, including the Federal Bureau of Investigation, which have developed or are in the process of developing similar programs provide publicly available, annual reports to Congress that set out in the detail the legal standard for this activity and describe how Constitutional rights will be safeguarded.

IV. CONCLUSION

EPIC respectfully requests that the subcommittee take the steps outlined in this statement, including requiring the immediate and permanent end to DHS' practice of monitoring for dissent; adopting guidelines for greater oversight of the DHS' social network and media monitoring program, and imposing the same oversight requirements on similar social network and media monitoring programs at other agencies.

Thank you for your consideration of our views. We would be pleased to provide any further information the Committee requests.

Mr. MEEHAN. Now, for all panelists, I know you gave us some detailed testimony in written form. If you could do your best to summarize your submitted testimony, we would appreciate that.

I now welcome back Ms. Callahan and recognize her first for her testimony.

Thank you.

STATEMENT OF MARY ELLEN CALLAHAN, CHIEF PRIVACY OFFICER, DEPARTMENT OF HOMELAND SECURITY

Ms. CALLAHAN. Thank you very much, sir.

Good morning. Chairman Meehan, Ranking Member Speier, Ranking Member Thompson, and Members of the committee, thank you for this opportunity to discuss the Department of Homeland Security's uses of social media and the privacy protections my office has embedded into all of these uses.

As described in our written testimony, communications and social media provide important benefits to the American public and to the Department. With that said, as the Chairman and the Ranking Member acknowledged, there is a great deal of personal information that, although publicly available, is not necessary for the Department to see or use.

Let me be clear: DHS recognizes the use of social media by Government actors must occur with appropriate privacy, civil rights, and civil liberties protections. For this reason, DHS has created Department-wide standards designed to protect privacy in each category of its use.

There are essentially three uses of social media by the Department of Homeland Security: First, external communications and outreach between the Department and the public; second, awareness of breaking news and events and situations related to homeland security, known as situational awareness; and third, when DHS has the appropriate authorities to use social media for operational use such as law enforcement and investigations. In each category, the Department has established standards that are de-

signed to incorporate privacy protections ex ante, to create uniform standards across the components and Department, and to be transparent about the scope of our activities.

The Department utilizes the opportunity social networking presents to provide the public with robust information. For example, DHS has a presence on many of the major social networking platforms. FEMA, of course, is well-known for utilizing social media effectively for education and in emergencies.

DHS established Department-wide standards for use of social media for communications and outreach purposes through the development and publication of two Privacy Impact Assessments, known as PIAs. All DHS profiles and communications via social media must adhere to these PIAs.

As my colleague Mr. Chávez will describe, the Office of Operations Coordination and Planning has a statutory responsibility to provide situational awareness and establish a common operating picture for the Federal Government. The Privacy Office and Operations work together closely and develop detailed standards and procedures associated with reviewing social media, launched three pilots, and then did a privacy compliance review of those pilots. Together, the National Operations Center and the Privacy Office designed a holistic set of privacy protections to be implemented whenever social media is being reviewed for situational awareness, and then memorialized them in a publicly available PIA in June 2010.

Several months later, as part of a mandated privacy compliance review, my office determined that the PIA should be updated to allow for the collection and dissemination of personally identifiable information in a very limited number of situations. After January 2011, limited personally identifiable information on a few categories of individuals may be collected only when it lends credibility to the report or facilitates coordination. The categories are essentially: Public figures who make public statements or are part of an event; or people who are in potential life-or-death circumstances.

The first weekend that personally identifiable information was allowed to be collected and disseminated was the weekend that Congresswoman Giffords was shot in Arizona. Learning immediately who was the impacted Member of Congress was very useful for the Department, for the Federal Government, and facilitated rapid coordination.

There may also 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 such as law enforcement. Given the breadth of the Department's mission and the fact that access, collection, and use of social media or other publicly available information is governed by specific legal authorities rather than Department-wide standards, the Department takes a different approach to embedding privacy protections into this type of social media, implementing privacy protections through a policy and management directive.

The Department is finalizing a management directive for privacy protections in the operational use of social media, which will systematize the previous component policies, be enforceable throughout the Department, and will identify the authorities, restrictions,

and privacy oversight related to the use of social media for operational purposes. The directive will also provide instructions on how to embed privacy protections into the operational use of social media and in each investigation performed by Departmental personnel. Essentially, the standard is, if you can't do it off-line, you can't do it on-line.

In light of the scope and availability of information, including personal information, found in social media, the Privacy Office intends to continue to monitor the Department's use of social media in all three categories. The Department has established a comprehensive compliance regime. It is every employee's responsibility to adhere to those standards, and the Privacy Office will seek to confirm that compliance in order to protect the public's trust in the Department's use of social media.

Thank you, sir.

[The joint statement of Ms. Callahan and Mr. Chávez follows:]

JOINT PREPARED STATEMENT OF MARY ELLEN CALLAHAN AND RICHARD CHÁVEZ

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 on-line 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 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 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

[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.*

[2] See supra note 1.

[3] *http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda__2010/m10-23.pdf.*

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 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. § 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

[4] *http://www.dhs.gov/xlibrary/assets/privacy/privacy__pia-dhs__socialnetworkinginteractions.pdf.*

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

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 websites. 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, Deepwater 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 on-line 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 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 on-line 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 6 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 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:

---

[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.*

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

(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 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 on-line and internet materials. Other DHS offices and components may be authorized to utilize social media for specific law enforcement purposes such as investigating fraud. The Office of Intelligence and Analysis also has some overt collection authorities for intelligence purposes which may include the use of on-line 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.

---

[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.*

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

In 1999, the Department of Justice issued guidelines for Federal law enforcement agents that outline on-line 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 on-line traffic, if that information would have been retained had it been written on paper. Moreover, Federal law enforcement agents communicating on-line 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 on-line 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 on-line 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 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 life cycle 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 6 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.

Mr. MEEHAN. Thank you, Ms. Callahan.

Now I recognize Mr. Chávez for his testimony.

STATEMENT OF RICHARD CHÁVEZ, DIRECTOR, OFFICE OF OPERATIONS COORDINATION AND PLANNING, DEPARTMENT OF HOMELAND SECURITY

Mr. CHÁVEZ. Good morning, Chairman Meehan, Ranking Member Speier, and Members of the subcommittee. I also would like to thank you for inviting me here today to talk to you about the National Operations Center use of social media monitoring to provide real-time or near-real-time situational awareness of potential occurring events or incidents that may impact the safety, security, and resilience of the homeland.

[11] See, e.g., On-line 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).

As stated in Section 515 of the Homeland Security Act, as amended, the National Operations Center is the principal operations center for the Department of Homeland Security and shall provide situational awareness and a common operating picture for the entire Federal Government and for State, local, and Tribal governments as appropriate in the event of a natural disaster, act of terrorism, or other man-made disaster, and ensure that critical terrorism and disaster-related information reaches Government decision-makers.

In order to fulfill these statutory responsibilities, the National Operations Center, also known as the NOC, gathers reports from multiple sources, to include open-source media reporting. Media reporting is often the first indication of a potential incident. For this reason, the NOC utilizes and incorporates media reporting into its incident reports. The primary focus of our reporting is on what is happening, and not who is reporting the event.

As previously stated, the NOC gathers reports from a variety of sources and synthesizes them into one single comprehensive incident report that is distributed again to the DHS leadership, DHS components, and other Federal, State, local, Tribal, territorial, and non-governmental and private-sector partners for action as appropriate.

The after-action assessments relating to the Government's response during Hurricane Katrina highlighted the importance of real- and near-real-time information from media reporting to enable a more timely response during a dynamic catastrophic event. In 2006, following Hurricane Katrina, the NOC began assessing the incorporation of media reporting for major media networks into incident reports to provide responders with real-time information. To date, incorporating media reporting into the NOC's incident reports has enabled our partners to have greater awareness during events and incidents.

Here is a real-world example of how the NOC incorporates media reporting. In early January 2012, the media in Charlotte, North Carolina, was first on scene reporting damage after severe weather erupted across multiple counties near Charlotte. The media reports were combined with reporting from State and local sources. The end result, again, was a more timely incident report that provided specific and comprehensive information to our partners, enabling them to make informed decisions.

The NOC incorporates media reporting into incidents across the full spectrum of Homeland Security operations: Prevent and protect, respond and recover.

Another real-world example of how NOC incorporates media reporting into its incident reports also occurred in early January 2012. The incident occurred in Austin, Texas. The media in Austin posted incident information about evacuation of a high school after a suspicious device was seen in a vehicle on campus. The media reported that, according to county sheriff's office spokesmen, sheriff's deputies were responding to an explosive device in a car. Through additional Government reporting, the NOC learned that the scene was secured and that no explosive device was found by law enforcement officials.

Again, I would like to emphasize that it is the "what," not the "who," that is relevant for NOC reporting purposes. The NOC adheres to strict enforcement of privacy guidelines with regard to media reports. The NOC, in coordination with the DHS Office of Privacy, evaluates processes and incident reports on a recurring basis to ensure our privacy guidelines are being complied with.

Again, thank you for the opportunity to speak with you today, and I am happy to answer any questions you may have.

Mr. MEEHAN. Well, thank you for your testimony, Mr. Chávez.

As I said in my opening statement, I am concerned about some of the news reports and materials related to DHS monitoring of social media and the networks. So I will now recognize myself for a few minutes of questioning.

The testimony has been revealing in the sense of giving us the overall perspective. I think all of us appreciate the ability for the Governmental entities to broadcast through the various pieces so people know about what you are doing.

Mr. Chávez, you talked a lot about, sort of, media monitoring. There is an expectation on the part of many of those who are reporters and otherwise, they know they are putting their product out so that it can be reviewed. So I think we can go past those kinds of things.

We also appreciate, as I said in my opening statement, about the opportunity to avail ourselves in real time of breaking information that can be communicated in certain ways that are now available so that there is the ability to keep those that need to make the decisions up on the latest information.

But you are sensitive—we are here today because where we are trying to find is where that line is where the public citizen—it is not just the expectation of privacy, because we know they are communicating in public fora or even quasi-public fora. But we are talking now about monitoring on-line information in blogs, in websites, in message boards. Some of these have, you know, the indicia of, sort of, quasi-privacy communities, so to speak.

So my real question for you is to help us understand what you are doing to assure that individual communication is not leading to individuals being identified by the Government and what you are doing to assure that we are not creating a chilling effect so that somebody in a community who is concerned about a particular issue will be more reluctant to write a letter to the editor, to post something on a blog.

I will close my opening comments—and I know you have come prepared to answer these, but we are all very concerned about a couple of the circumstances that have happened. Most specifically, what looks as if it is a directive within the contract you have with a private contractor who is employed to help you disseminate or gather information. It is identifying media reports that reflect adversely on the U.S. Government, DHS, or prevent, protect, respond, or recovery activities. So, in effect, we are asking somebody to go out and let us know what people are saying that is negative about us. This appears to be what was asked for in the contract with General Dynamics.

So I would like you to tell me what it is that we are doing to assure that private commentary is not being misused and what we

can do to assure that the activities of monitoring are not going to create some kind of a chilling effect on individuals' willingness and readiness, not only to comment, but, frankly, to make comments which may be critical of the Government.

Ms. Callahan.

Ms. CALLAHAN. Thank you, sir.

With regard to the privacy protections that the Department has implemented specifically with regard to situational awareness, to be very clear, as Mr. Chávez said, it is the "what," not the "who," that is being identified and that we are concerned with.

As you are aware, my office not only mandated privacy compliance reviews every 6 months to make sure that indeed we are just focusing on the event, on the situation, to know what is going on, and not worried about the individual; in addition to that, the National Operations Center has very robust auditing capability, that they go and review both the sites that are being done, how long they are on it, and what information is being implemented into the report.

We take these issues very seriously, sir. We absolutely understand and agree that these are——

Mr. MEEHAN. Who is directing what is being monitored?

Ms. CALLAHAN. Mr. Chávez.

Mr. CHÁVEZ. The key words, I guess, or the mechanism that we use to identify information that is coming across the media, whether it be social or the traditional media that is out there, again, these are key words associated with events that have happened in the past and also with the equities of the Department of Homeland Security, again, looking at the safety, security, and resilience missions that are out there.

So, as you said in your opening statement, I believe, that there are any number of blogs going on at any one time and a plethora of information that is flowing through there, there is no way we could look at all of it. So we use the tools, again, with these keyword searches that are commercially available for looking at search items, particularly, again, keywords, that we can pull out of there and look at, again, what the situation is that is evolving.

Mr. MEEHAN. But you are looking at keywords, but my question is, are there circumstances under which—who is the one that is waking up in this vast array of information out there? Because the limited number of people that you have working for you, unquestionably, without some sense of direction, they could be spending limitless time, in effect, floating on a sea without any kind of product that is produced.

So there has to be some sense of direction. Where does the line get drawn with regard to overlooking, sort of, general words out there versus looking at specific incidents, specific issues, and identifying people, as happened in Michigan?

Mr. CHÁVEZ. There are guidelines for sites that the individuals within the Media Monitoring Center can monitor. Again, those sites are submitted for approval through the Privacy Office, and they are strictly adhered to by the individuals who are actually looking at the information that is coming across there and gathering them for us.

So there is a series of checks and balances.

Ms. CALLAHAN. If I can, sir, in order to be transparent about this, in the Privacy Impact Assessment we have a list of the representative keywords. The Privacy Office reviews that list every 6 months and makes sure that we stay within it. The list is "disaster," it is, you know, "flood," "tornado," and things like that.

With regard to individuals, as I indicated in my oral testimony, we don't collect information on individuals. We do not monitor them with regard to any First Amendment activity. But individuals may be the first person at the scene, and so they may go and report there has been a train derailment in Michigan. We do not then go and say that, "Mary Ellen Callahan reported a train derailment." We then corroborate it with another source that is identified——

Mr. MEEHAN. My time has expired, so I am hoping some others will pick this up.

We know about the disasters. I don't think we are worried about the disasters. What we are worried about are the individual circumstances where there may be issues out there. I point back again to the Michigan circumstance where there was a controversial decision by the Government, and DHS played a role in assessing community response to that incident. That wasn't a natural disaster; that was an incident that was created by the Government, and the Government then was monitoring the community response.

That is where I want to—who is going to make the decisions? Who is making the protections against circumstances under which the Government is playing a role in not just analyzing but filtering back, recording, and reporting about things that people in the community have said about Governmental activity?

Ms. CALLAHAN. I would be happy to answer the Standish question whenever the Members have given me the time to do so.

Mr. MEEHAN. Thank you so much.

I will turn it over to the Ranking Member, Ms. Speier.

Ms. SPEIER. Thank you, Mr. Chairman.

I am deeply troubled by the document that has just been put into the record by EPIC.org. While you have probably not had the opportunity yet to review it, Mr. Chairman, I would like to request that after they do review it, that they report back to this committee and provide us with answers to the questions raised. But I am going to start with a couple of them.

They made a FOIA request back in April. DHS ignored it. Then EPIC filed a lawsuit on December 23, 2011, when the agency failed to comply with the FOIA deadlines. As a result of filing the lawsuit, DHS disclosed to EPIC 285 pages of documents.

So I am just making note of that. You shouldn't stonewall. When a FOIA request is made, you should comply with it within the deadlines. No entity should be required then to file a lawsuit. So I am just putting you on notice about that.

But what is interesting about what they have pointed out is that, while you say there is no personally identifiable information in this contract that General Dynamics has, in fact they point out that there are some exceptions to the no-PII rule. One of them allows for the collection of personally identifiable information of anchors, newscasters, or on-scene reporters who use traditional and/or social media. This would allow the agency to build files on bloggers and internet activists, in violation of the Privacy Act.

I find that outrageous. I would like to ask you to amend the contract with General Dynamics to exempt that kind of information from being collected.

Ms. CALLAHAN. First, ma'am, with regard to the FOIA response, I completely agree. It did not meet my standards in terms of the timeliness of the response, and I have taken action to look into why it was delayed. That was unacceptable, and I completely concur with your statement.

With regard to the reporters, to clarify, the reporter's information is collected—and, as noted in my written testimony, the only information we collect on the reporters, if at all, is the name, their affiliation, their title, if any, and their publicly available identification. We are only collecting the information if it adds to the credibility of the report or allows coordination.

So it is very rare that we actually collect any information about the reporters. But it could be a circumstance where you link to a reporter's blog who is at a news site. For example, in Michigan and the train derailment, if the person posted it on his personal blog, we may be authorized to link to it. We would not be authorized to collect it or use it for a personal—an individual, but only if the reporter is relevant and adds credibility to the report itself.

Furthermore——

Ms. SPEIER. I am——

Ms. CALLAHAN [continuing]. To clarify, ma'am, just to clarify, the reporter information is only stored in that report. We are not cutting across the different reports. We are not saying how many different reporters do it. It is information that is publicly available, and it is not associated with their opinions but instead with the situation or the event that is occurring.

Ms. SPEIER. I am suggesting to you that it is irrelevant, you do not need it, and you should suspend that part of the contract.

Now, this document also suggests that you are capturing public reaction to major Government proposals. Now, again, if this is, in fact, true, if this is part of the contract, I believe that should be suspended as well. This is not a political operation; it should not be a political operation. Capturing public reaction to major Government proposals is not something you should be doing.

Ms. CALLAHAN. I completely agree with you, ma'am. I 100 percent agree with you, which is why the report that they point to on page 118 in the FOIA report actually was never a live report. It was never disseminated by the National Operations Center. It would not have met the privacy standards that are in the five publicly available Privacy Impact Assessments we have done. Furthermore, it is an example of an early August 2009 example of what could be possible. We, together with the National Operations Center, agreed that that is well outside the scope.

In fact, if you look at the document, it is within a very early, February 2010, training manual as an identification of a weekly report, because it is a compilation of other elements. If you look at the previous pages, you can see that they identify, like, "This is not acceptable," "This is not appropriate," "Redact the personally identifiable information."

That Standish, Michigan, report is one that only appears—actually, the only place it exists in the Department is in my files be-

cause of the privacy compliance review we did before launching the initiative. It is——

Ms. SPEIER. All right. My time is about to expire, so let me suggest the following. EPIC makes three recommendations at the end of their report. They recommend you cease collecting information on journalists' activities, that you suspend the social network and media organization monitoring program until safeguards are put in place, and that you comply with providing Congress with an annual report that sets out in detail the legal standards for this activity. I, for one, wholeheartedly agree with their recommendations.

Mr. Chairman, I actually think we should have EPIC and others in the privacy community come and testify. I am deeply troubled by what we have heard so far this morning.

The fact that you agree with me but yet much of this conduct continues is deeply troubling.

I yield back.

Mr. MEEHAN. Thank you, Ranking Member Speier.

At this point in time, I would like to turn it over to the gentleman from Mississippi, the Ranking Member of the committee, Mr. Thompson, for questions he may have.

Mr. THOMPSON. Thank you very much, Mr. Chairman.

Ms. Callahan, will you provide the committee with a copy of the FOIA information that you provided to EPIC?

Ms. CALLAHAN. Of course. Absolutely, sir.

Mr. THOMPSON. Thank you.

Also, will you provide us with your analysis of why the FOIA request went unresponded to and what did you do in that situation but also what will you do going forward so that other requests won't be treated so cavalierly?

Ms. CALLAHAN. Absolutely, sir.

Mr. THOMPSON. Mr. Chávez, do we create log-ons to monitor individuals in this process?

Mr. CHÁVEZ. Actually, we do not monitor individuals at all. What we are looking for, again, as I talked about, the keywords. Within the keywords you won't find anyone's name. Like, say, they are all verbs, those types of things that we are looking for. So, no, we don't create log-ins for individuals to do that, and we are not looking or monitoring individuals.

Mr. THOMPSON. Are there any times that you take down names of individuals?

Mr. CHÁVEZ. Again, given the seven criteria that we have for life-saving, those type of circumstances, are the only time that we would collect the names, use the PII.

Mr. THOMPSON. Who makes that determination?

Mr. CHÁVEZ. That is part of our training course that we do for the individuals who are doing the media monitoring. We look at those processes. Again, they are audited twice a year. The most recent one was just done in November.

Mr. THOMPSON. Who is "we" doing the training?

Mr. CHÁVEZ. Actually, the National Operations Center, in coordination with the Privacy Office.

Mr. THOMPSON. All right. How does this interface with the General Dynamics contract?

Mr. CHÁVEZ. Those are the individuals who are doing the media monitoring for us.

Mr. THOMPSON. So let me get this straight. DHS is training a private contractor to do the media monitoring?

Mr. CHÁVEZ. Part of it, yes, on their privacy rules and those types of things, indeed, we are.

Mr. THOMPSON. Why are we training private contractors?

Mr. CHÁVEZ. Well, to collect—their skill set, to collect the information we are. But what they don't come with is, again, the DHS guidance that we have to give them.

Mr. THOMPSON. I thought private contractors generally had an expertise that we didn't have internally as an agency, and we would go outside to pick that capacity up. But now what you just said is for some reason we are training the outside people to do the internal work.

Mr. CHÁVEZ. It is not overall training. Again, they do have those skill sets that they use. What we add from the Department, again, are those checks that we use to ensure, again, that the privacy guidelines are complied with. That is the part of the training that we do, and that is it.

Mr. THOMPSON. Well, explain to me what skill sets General Dynamics, with an $11 million contract, would have outside of DHS's capabilities.

Mr. CHÁVEZ. Well, what they offer, again, is the 24/7 monitoring of those sites. They are skilled technicians in surfing the web and also doing an analysis of the information that they get when they do get hits on websites and producing synopsized reports that, again, comply with the privacy guidelines that are out there, and pushing those out to us so we can send those out to our partners.

Mr. THOMPSON. So your testimony is we don't have the skill sets at DHS to monitor websites?

Mr. CHÁVEZ. We do. Right now, again, we have that as part of one of our contracts that is out there.

Mr. THOMPSON. Is it a sole source contract?

Mr. CHÁVEZ. No, it is not.

Mr. THOMPSON. Well, will you provide the committee with the procurement document? How long has it been out there?

Mr. CHÁVEZ. I will get back with you on that. I will give you the full details on it.

Mr. THOMPSON. Was the original contract for the $11 million a sole source contract?

Mr. CHÁVEZ. I do not know. I will have to check on that for you, sir.

Mr. THOMPSON. How long have you been working with the agency?

Mr. CHÁVEZ. Two years.

Mr. THOMPSON. How long has this General Dynamics contract?

Mr. CHÁVEZ. In the 2 years I have been there.

Mr. THOMPSON. So you inherited the General Dynamics contract?

Mr. CHÁVEZ. Yes, sir.

Mr. THOMPSON. All right. Well, please get it to me.

The questions raised by the EPIC insertion, as well as what everyone has commented, raise significant issues around safeguards. Mr. Chairman, I think you would help a lot of people if at some

point we could, as Ranking Member Speier suggested, maybe bring those individuals and others who might have an interest before the committee to talk about it.

I yield back.

Mr. MEEHAN. Thank you, Mr. Ranking Member. We appreciate your presence here today on the subcommittee.

The Chairman now recognizes the gentleman from Minnesota, Mr. Cravaack.

Mr. CRAVAACK. Thank you, Mr. Chairman.

Thank you for coming here today and briefing us.

I think what everybody is really concerned about here is our Constitutional rights. Because we in the United States, we have this great document called the Constitution, and we have to walk this fine line of data attainment to protect the United States but to, at the same time, make sure that we have safeguards in place that we have freedom of speech, which we value highly.

So, with that said, what safeguards are in place that when the DHS does collect and distribute personally identifiable information, PIIs, outside a specific narrow event such as a life-or-death situation, can you kind of expand upon that a little bit?

Then with that said, what would be the penalty associated with distributing that information illegally? Have there been any cases where that has occurred?

Is there a report currently going from General Dynamics to you, to Congress that would also, when these people are identified, that Congress is aware of that?

So, with that, Ms. Callahan, could you start off?

Ms. CALLAHAN. Absolutely, sir. Thank you very much for that question.

As I have described and Mr. Chávez has described, the only personally identifiable information that can be collected are these seven very narrow categories: Public officials or in a public event or making a public statement or life-or-death, as you pointed out.

As part of the review by the National Operations Center, every week they go and check to make sure no personally identifiable information is provided. I review each of the media monitoring that I receive as part of the ordinary course of business, just to see if they continue to comply with the privacy protections that we describe in our five publicly available Privacy Impact Assessments and privacy compliance reviews. We then do these semi-annual reviews of the entire system to look at all the processes therein.

Prior to me authorizing any personally identifiable information, there were, to my recollection, two circumstances where public officials were named in the circumstance—for example, President Obama. There was no circumstance with regard to individuals who are not in a public capacity who have been named.

Actually, that example of having a public official like the President is why we agreed to have those seven very narrow categories that could be disclosed. Again, identifying Gabrielle Giffords as the target of the attack in Arizona actually helped coordinate the response more quickly, because we had that authorization.

With regard to the penalty, if, indeed, that had taken place, there would be significant penalties. There would be training and

possibly taking them off the job if, indeed, there was a recidivist behavior. We have not yet seen that.

With regard to a report from General Dynamics, I don't know of that, but I do know that we have been doing these semi-annual privacy compliance reviews, which are available on our website, for exactly the reason that everyone has identified: To make sure that we are following the privacy protections that we have identified and that we are not monitoring, reviewing, or collecting First Amendment-protected speech.

Mr. CRAVAACK. Mr. Chávez, do you have any comment on that, as well?

Mr. CHÁVEZ. No, that is exactly it. Again, we follow the guidelines that the Privacy Office sets forth. We do audit on a regular basis the individuals who are doing those types of things. We have a series of individuals that are reviewing the data, again, to make sure that the PII is not inappropriately passed on, displayed, or stored.

Mr. CRAVAACK. Okay.

I would like to dovetail on what the Ranking Member said. Why did you pick General Dynamics, for example, to be the contractor for monitoring social sites and not keep it in-house, so to speak?

Mr. CHÁVEZ. Sir, again, that was before my time. That is the contract I inherited. But I can get you the information on that.

Mr. CRAVAACK. Okay. Who in DHS issued the directive for this establishment of this committee? You know, I agree, you have to get resource information and intelligence anywhere you can possibly get them, for various reasons. But who initiated the directive to initiate this social networking?

Mr. CHÁVEZ. DHS did, again, before my time, right after Hurricane Katrina. Again, with the advantages of looking at the media to get a more timely response, see what is going on, provide greater situational awareness, the decision was made to monitor the social—or the media monitoring, traditional media. Then later on it evolved into the social media.

Mr. CRAVAACK. Okay. One of the things that did kind of raise a red flag for me is reports on DHS components and other Federal agencies, positive or negative reactions to certain Federal organizations. Who gave that directive?

Ms. CALLAHAN. As I understand, sir, that is part of the General Dynamics contract. As was said, it predates Mr. Chávez.

The purpose of that is not to keep track of what they are negatively saying, but for operational purposes to understand whether or not the Department is candidly meeting its standards. If, indeed, there is a long line as TSA, we don't care who is in the long line, but if someone tweets and says there is a long line, we then convey that information to TSA. It is part of the operational awareness that the National Operations Center does.

Mr. CRAVAACK. Okay. My time has expired. I do have an issue with that, but I will yield back at this time. So thank you.

Mr. MEEHAN. Thank you. Thank you, Mr. Cravaack.

So, at this moment, the Chair will recognize the gentleman from—it is "Missoura" where you are from, right, not "Missouri"?

Mr. LONG. Right. You bet.

Mr. MEEHAN. Mr. Long.

Mr. LONG. Thank you, Mr. Chairman.

Mr. Chávez, what can the agency point to as your legal basis for your social network and media monitoring program, which a lot of us I think today have expressed concerns threaten important free speech and expression rights? What legal basis can you point us to that either this activity could even be concerned with——

Mr. CHÁVEZ. It was, again, Section 515 of the Homeland Security Act, as amended, to provide situational awareness and, again, that common operating picture.

Mr. LONG. That is the legal basis for it?

Mr. CHÁVEZ. Yes, sir, that is the legal basis.

Mr. LONG. Okay.

Ms. Callahan, I, as a lot of us today, are very concerned about the chilling effect on our core First Amendment rights to political speech and free speech in general. Are there—what can you point us to? Are there protections to ensure that only necessary personal data is used and retained no longer than necessary to protect against accidental or deliberate misuse?

Ms. CALLAHAN. I, too, sir, am very concerned about the First Amendment and want to make sure that that is wholly protected with regard to this activity. We spent 9 months designing this program and have detailed it in the public Privacy Impact Assessments and compliance reviews.

The standard by which we operate is, again, not the "who" but the "what is taking place." What is the event that is going on? If an individual alerts us to that event, then that is the first report, but not the exclusive report.

The way, sir, that we have the privacy protections embedded into the program is to make sure that no personally identifiable information is collected or disseminated unless it meets those seven categories.

Mr. LONG. No what information?

Ms. CALLAHAN. Personally identifiable information.

Mr. LONG. Okay.

Ms. CALLAHAN. No personally identifiable information is collected except for those public figures or in a life-or-death circumstance. The National Operations Center goes and very robustly audits that, and then we go in every 6 months to make sure that, indeed, the representations are correct.

The personally identifiable information, the very narrow topics—which, again, are public figures making public statements or part of an event, or a life-or-death circumstance—are stored only in the report. We are not doing a table or an analysis of each of the different reports. They are only stored in that.

In fact, I published a System of Records Notice, which is required under the Privacy Act. It was not necessary for me to do this; the general System of Records Notice for operations would have covered this activity. But for transparency purposes, when I finally authorized the use of personally identifiable information, we published that System of Records Notice to go and say, these are the seven categories that we are doing—public figures at public events, or life-or-death circumstances—in order to be very clear about what we are doing with information and, candidly, sir, what we are not doing with information.

Mr. LONG. So, in your mind, you are convinced that what you are doing is consistent with existing DHS policy?

Ms. CALLAHAN. Consistent with DHS policy, consistent with the Privacy Act, and consistent with the First Amendment, yes, sir.

Mr. LONG. Okay.

I have another question for you, Ms. Callahan. As the public becomes aware of Government activity monitoring social media to gain rapid understanding of events, what are the risks of people or groups trying to affect those events, I guess—say, people with bad intentions using the different platforms of social media to manipulate the Government understanding to their advantage? What can be done to guard against this problem?

Ms. CALLAHAN. My colleague Mr. Chávez may also have some thoughts about that. But I think that, because we don't rely on just one individual source but we actually confirm the sources and look for making sure that we have multiple sources identifying, for example, the train wreck in Michigan, would be one element.

Also, to confirm, the National Operations Center, the situational awareness, is not attempting to investigate or confirm the validity of the event, just that an event has been reported.

Mr. Chávez.

Mr. CHÁVEZ. Ms. Callahan is absolutely right. No single source of information ever provides us with a complete picture. Oftentimes we use multiple sources—or, all the time we use multiple sources of information to corroborate information that we are getting in.

So it is all part of the big picture. In order to get the big picture, again, in this environment, we look to multiple sources that are out there, not a single source, to corroborate that information that is being produced.

Mr. LONG. How does that affect people trying to I guess put a different spin or take advantage of——

Mr. CHÁVEZ. There is always that—yes, there is always that deception.

Mr. LONG. That was kind of my question.

Mr. CHÁVEZ. If it doesn't match up with the preponderance of information coming in that is counter to the information we are receiving, then we can pretty much write off that. Plus we are not investigating that information, we are turning that over to the appropriate law enforcement or Government agency to look at what is happening again and is it really happening.

Mr. LONG. Okay. I have no time to yield back, but if I did, I would.

Mr. MEEHAN. Well, thank you, Mr. Long. Thank you for your questions. I am going to exercise the prerogative to ask a couple of follow-up questions and certainly would make that opportunity available to anybody who would like to as well or not.

Ms. Callahan, you spent some time talking about the circumstances in Michigan and about some protections. I know you haven't stated it today I spent time going through your written testimony and other sorts of things. I know you suggested that this is an anomalous circumstance. This is being identified as an event that happened, but maybe the statement would be but it wouldn't happen today. You have a moment, tell me how you have cured that kind of a circumstance and how we would not have a repeat

where there is an incident that occurs in which the Government begins to be looking for the information that was disseminated, collected, and disseminated in Michigan.

Ms. CALLAHAN. Yes, thank you, sir. To clarify slightly, that information was never disseminated, it was never a live report, it does not meet the standards of the privacy impact assessments and would not have actually been done. It was an early example of what could possibly be done. Together with the National Operations Center, we both agreed that we don't care about First Amendment speech, we don't care about the events.

Mr. MEEHAN. Well, you do care. What you are trying to say is that is not what you are inquiring about?

Ms. CALLAHAN. We care about the events, not the First Amendment elements. Right, we care about the events. Candidly even in that example, Guantanamo Bay and the transition of any prisoners from Guantanamo Bay is actually not within the Homeland Security mission. So it wouldn't even have met that threshold question. That is the current threshold standard that we implemented since January 2010, making sure it is a Homeland Security mission and an event and a situation. So for those two that is kind of a threshold point. We then would not—as I said, no element of First Amendment protected speech is collected, disseminated, or analyzed.

We also make sure that—as I said, I review the media monitor reports when I receive them to make sure that they continue to be compliant, that we are only reporting on the what and not the who. So I think all of these multiple levels are an example of why that Standish, Michigan, to give an example, is an anomaly. It is obsolete, and it only is in the handbook that was done, that is 2 years old, and was quickly replaced once we started to work on the pilots and to fine-tune to make sure that we can provide situational awareness and protect privacy.

Mr. MEEHAN. Let me go back then to prospectively where we may be looking at other kinds of events, as you say the who, not the what. Now I know there were attempts to look at things like the Olympics, there was an effort to track information that may be related to that. I can foresee a number of other events, conventions, are you going to be monitoring activity around conventions?

Ms. CALLAHAN. Again, I turn it over to Mr. Chávez, but we do monitor National security special events to make sure. For example, we monitored the Super Bowl. But again it is not about the who, but the what. How are the roads moving, how are the processes, are there any suspicious activities?

Mr. MEEHAN. You are not calling in the plays for Bill Belichick, are you?

Ms. CALLAHAN. I abstain on which—who I was supporting in the Super Bowl, but it is the what, it is the event.

Mr. CHÁVEZ. Holistically we are monitoring the whole Homeland Security enterprise, not just the events. We are looking for the same, again, keywords criteria that would indicate any type of action——

Mr. MEEHAN. You keep saying keywords. What I am trying to get to is who begins the process of identifying what should be analyzed.

I guess the what, not the who, but who is it that is saying to go after the what. I don't know where this has begun.

Mr. CHÁVEZ. Right. It is not the National Operations Center. Again the National Operations Center is the messenger.

Mr. MEEHAN. Who is giving the direction? I want your analysts to look into X. Where does that come from?

Mr. CHÁVEZ. That again does not come from the National Operations Center.

Mr. MEEHAN. I know it doesn't.

Ms. CALLAHAN. So if I can just step back for a second, sir. The National Operations Center is to provide situational awareness for the entire Homeland Security enterprise. The way that we implemented the Social Media Initiative was to provide these keywords that you can use on publicly commercially available software that you can basically refine, no see individual Tweets, but see what is trending and what is happening and if there are elements. The keywords, as I said, are disclosed in my privacy impact assessment.

Mr. MEEHAN. But when your analysts start work in the morning, do they just pick up a keyword book and start going out looking for——

Ms. CALLAHAN. No, it is programmed in all the time, is what I was going to say. It is programmed in all the time. We don't modify the keywords, disaster, flood, tornado, train wreck, derailment, those sorts of things.

Mr. MEEHAN. You keep talking to me about incidents that are disasters, and I get that. We are going to put that aside. Part of the mission here was to monitor activities that may be—we are Homeland Security, we are worried about the potential that there could be someone acting in some capacity that would threaten our homeland and cause harm to the American citizens. I get that, too. We are also worried about the fine line in which people may be talking about things they don't like about their Government, it is legitimate protest. So where are there activities that are taking place that it could be a collaboration of individuals from outside the country that are meeting at a convention all over the world. Does somebody say, hey, let's watch what is happening there. I need to know where this process begins, who's telling people to track the what?

Mr. CHÁVEZ. The individual Government agencies we provide, we will call them our customers, are the ones who determine whether or not the data is actionable or not, whether or not to pursue a follow-up, each of those executing their own authorities to do the investigations to collect intelligence in those type things. Often again the reports we provide through the social media monitoring are a supplement to getting the information to these organizations.

Mr. MEEHAN. So it might be a legitimate investigative agency that has the capacity to in their own right but using legitimate investigative tools and protections, they are asking you to get secondary publicly available information that fills a gap or something of some sort?

Mr. CHÁVEZ. Most definitely. Again once the reports come in we very seldom get the direction from an outside organization to look for specific things because under their own authorities they can

drill down farther than the National Operations Center can on information that was provided.

Mr. MEEHAN. Where does the top of the line come from; is this a career professional that makes these decisions or public appointee in the DHS who may be overseeing what is being looked at?

Mr. CHÁVEZ. Let me take an example of the intelligence field with their skill sets they have in the enterprise. There are individuals, both political appointees and senior officials, that again take a look at the information they have and decide whether or not to take action on to pursue investigations to open up whatever, again under their authorities, they can do to defend the homeland and produce that information in these reports.

Ms. CALLAHAN. If I could summarize, sir. The Situational Awareness Initiative we have been talking about is essentially breaking news, here is what is happening. To your point, if indeed someone receiving a report of breaking news and they have the underlying authority to investigate it, then they go off on their own track and the operations nor does the Privacy Office know they are doing it separate and apart from we are going to do audits and reviews of social media when the management directive is final. So they are breaking news and then other there are other authorities in the Department and also throughout the Federal Government.

Mr. MEEHAN. Final question. Breaking news, the Attorney General just decides he is going to try Guantanamo detainee in New York City. There is a lot of news about that now. Is it possible that you would be contacted by somebody who said follow what is happening, report to us what the reaction is to that?

Mr. CHÁVEZ. In the history of the time I have been at the National Operations Center, no, sir, that has not happened.

Mr. MEEHAN. What would be your protection against that kind of request? How to you tell a political appointee who is high up in the administration that is not appropriate for us to monitor?

Mr. CHÁVEZ. It is not only appropriate, it is not under our authority. It is illegal to do that.

Mr. MEEHAN. Well, that is a good answer to any kind of a political appointee. At this point I have gone well over my time.

Mr. Thompson.

Mr. THOMPSON. Yes, I do. Ms. Callahan, you talked about taking 9 months to put this program together.

Ms. CALLAHAN. Yes, sir.

Mr. THOMPSON. Did you vet the program with any outside stakeholders or was it strictly an internal process?

Ms. CALLAHAN. Actually, sir, with regard to the situational awareness I discussed it in my quarterly meeting with advocates that takes place, I believe after the initiative launched but before it became a program, so during the three pilot phrases.

In addition, one of my staff testified in front of my FACA committee, the Data Privacy and Integrity Advisory Committee early in the process. In fact in December I had hoped to have one of Mr. Chávez's colleagues testify in front of the Data Privacy and Integrity Advisory Committee, but unfortunately—he was there, he was prepared to testify about this very issue because of the importance

of the issue but we ran out of time. But yes, we have discussed this publicly and gotten advice on it.

Mr. THOMPSON. Well, I am concerned that given what I am picking up that there are a lot of people who have interest in privacy and this whole area that has not been included in the discussion. What I would like for to you do is provide us with those organizations or individuals who you have collaborated with over that 9 months to develop this program.

Ms. CALLAHAN. To be clear, sir, I did not discuss this outside the Department until it was launched as a pilot under the Haiti earthquake, but then I did discuss it, as I said, in several advocate meetings, that I have quarterly advocate meetings with advocates and we did discuss it publicly in the FACA committee. But we are happy to provide you that information. Yes, sir.

Mr. THOMPSON. Whoever the advocate, whoever attended, how broad that attendance is, all that, just please get it to us.

Ms. CALLAHAN. Absolutely.

Mr. THOMPSON. The other concern I have is taken off of from what the Chairman was talking about, is the notion of identifying political and journalistic activities that reflect adversely on the agency or the Federal Government. Ms. Chávez, it is your testimony that you don't do this?

Mr. CHÁVEZ. Indeed, we don't do that. What we do do again is if there are long lines at the airport, at the screening centers, those types of things, those would come up to us, and we would pass it on to the appropriate DHS component for action again through corroboration, is this really happening, what is happening and what we need to do to fix that. But identifying individuals again or an individual that is making that would be irrelevant to us. There is something happening, go check it out.

Mr. THOMPSON. Well, okay. I will go back to the General Dynamics contract again. Obviously some of us are troubled by it. Why would you ask them to look at the *Drudge Report* or *New York Times* or *L.A. Times?*

Mr. CHÁVEZ. We don't focus again on any one media source. There are many that are out there. It all goes back to the information that they are providing, not the provider of that information.

Mr. THOMPSON. So they are the only source of—so in other words, they have this expertise that they can look at the blogs and read the newspapers better than the Department if that is what you want to do?

Mr. CHÁVEZ. Well, you have to look at it also. We are not in here currently watching television or looking at the media reports that are coming in. We all have a vested interest in this Homeland Security. So what we are providing is a service where we are looking at individual action or actions that could be happening around the United States and elsewhere that again we see and push that information out to the Federal Government and our State and local partners, the entire homeland security enterprise, to let them know that something is happening. They may already see it and be acting on it, in which case we would receive information from those agencies on here is what is currently going on with this also.

Mr. THOMPSON. Ms. Callahan, to your knowledge are there any other branches of the Federal Government who are doing similar kind of programs?

Ms. CALLAHAN. I don't have a comprehensive knowledge of this, but I do know that National Operations Center has a unique statutory responsibility to provide situational awareness to the Federal Government. So I am not aware that anyone else is doing that given the NOC's authorities.

Mr. THOMPSON. FBI, DOD, nobody to your knowledge?

Ms. CALLAHAN. I believe they are operating within their own authorities consistent with what I discussed with the Chairman.

Mr. THOMPSON. I just asked you.

Ms. CALLAHAN. I don't know, sir, sorry.

Mr. THOMPSON. So you don't know—you designed the program without any review of whether or not another agency is doing it?

Ms. CALLAHAN. As I said, sir, I believe the NOC's statutory authority is unique.

Mr. THOMPSON. No, no, no, just answer the question.

Ms. CALLAHAN. I do not have any other knowledge.

Mr. THOMPSON. You said it took 9 months to put the program together, and I just want to know as part of your due diligence did you check and see whether or not another agency within the Federal Government was doing something just like this. I would assume that the FBI would be doing something like this, I would assume that DOD would be doing something like this, just given their mission. If you say you don't know, I don't think that is the right answer from a due diligence standpoint.

Ms. CALLAHAN. I can check with my staff, and maybe Mr. Chávez is aware of what other people are doing in this. We are trying to be very transparent about what we are doing and perhaps the other departments have not necessarily taken that tack.

Mr. CHÁVEZ. I am not aware of anyone else that is doing the social media monitoring at again the unclassified level. The intelligence community with their skill craft may, but no, I don't.

Mr. THOMPSON. I yield back, Mr. Chairman.

Mr. MEEHAN. Thank you, Mr. Thompson. It appears to me as we have been going through this issue I have got the very difficult recognition that as I chastise my children about spending significant time on Facebook, they are now going to be saying to me, well, dad, it can be a career.

At this point let me turn it over to the gentleman from Minnesota for a few follow-up questions.

Mr. CRAVAACK. Thank you, Mr. Chairman. Does DHS use any other contractors to monitor to the best of your knowledge?

Mr. CHÁVEZ. Right now, no, we don't, sir.

Mr. CRAVAACK. Is there any plans to?

Mr. CHÁVEZ. Right now we have got all we need with, again, the services being provided.

Mr. CRAVAACK. Just kind of dovetailing what the Ranking Member was saying, one of the things I read is that you want to capture public reaction to major Government proposals. You are monitoring positive or negative reports on FEMA, CIA, ICE.

Mr. THOMPSON. Would the gentleman yield?

Mr. CRAVAACK. Yes, sir, I will yield.

Mr. THOMPSON. I asked you a question about the General Dynamics contract. You told me there was an RFP out right now. That was your answer to me on social monitoring. You look back to the gentleman, you said it wasn't sole source, it was open. That was your answer to me then.

Mr. CHÁVEZ. It is a firm fixed contract, not sole source.

Mr. THOMPSON. But you said there is an RFP out right now.

Mr. CHÁVEZ. RFP. I am sorry, I am not familiar.

Mr. THOMPSON. Request for proposal. We talked about the General Dynamics contract. We asked about it. Your conversation talked about whether or not it was sole sourced or it was open, and you indicated that we are going out looking for another contract right now.

Mr. CHÁVEZ. No. If I did, sir, I apologize, sir. I stand corrected. It is a firm, again, fixed contract and again not sole sourced.

Mr. THOMPSON. How long is this fixed for?

Mr. CHÁVEZ. Actually, I don't have that information. I don't have the fixed.

Mr. THOMPSON. Thank you. Thank you for yielding.

Mr. CRAVAACK. Yes, sir. I will reclaim my time. Going back, it was mentioned some of the—you know, FEMA, CIA, CBP, ICE—these are organizations that are outside of DHS. Now if somebody—if there was an organization outside of DHS requesting this information, would you provide it to them?

Mr. CHÁVEZ. We don't normally get, again, requests for information. We just take it from the media and push it to the organizations that are out there because they have their own information authorities, gathering authorities and those types of things that they use. So they use our media monitoring reports to supplement what they have already got.

Mr. CRAVAACK. The thing I am really having problems with I guess is the Government proposals, reactions to Government proposals and then feeding that information to different organizations within the Government. You are using a public sector source that may be used for private individual attainment of information for other reasons then that would benefit the public. That is what I am concerned with and how would you go about preventing this from occurring?

Mr. CHÁVEZ. That specific purpose of the media monitoring I have never encountered. Again, the only kind of evaluation, if you will, of the departments or other Government agencies is just, as I said, there is a service that is being provided, that again there is a hold-up at the airports, as Ms. Callahan said also, but to go out and solicit that information or to collect it. I have not seen this in my tenure at DHS.

Mr. CRAVAACK. Well, now this hearing has occurred, I think you have a higher profile. But my question would be what are the checks and balances in there from ensuring that this is not used for private initiatives?

Mr. CHÁVEZ. Again, with the information that comes in it is reviewed by a number of individuals throughout the National Operations Center and Operations Coordination and Planning to ensure that the compliance with the PIIs out there and the distribution lists also are pre-approved so that it doesn't get out to sectors,

again so we don't compromise proprietary information and those types of things.

Mr. CRAVAACK. Can you give me an example of what kind of information you have been gleaning thus far in regard to Government proposals?

Mr. CHÁVEZ. I am not aware of any information we have gathered on Government proposals.

Mr. CRAVAACK. Okay. All right. Say I am ICE or say I am those who would be interested in the gun walking down in Mexico and I want to get information in regards to what is the public reaction to this. Say I am an organization, I am just trying to use broad general terms so we don't have to get into another area, a realm. How would you go about that request?

Mr. CHÁVEZ. Again, that would not be a request that was appropriate or a function of the National Operations Center. Given our, again, authority under the Homeland Security Act for a situational awareness or operating picture, we are not a pollster, we don't again solicit for opinion. We are putting down actual incidents that are happening at any one time.

Mr. CRAVAACK. Okay, I am the Attorney General, I am asking for this information.

Mr. CHÁVEZ. Okay.

Mr. CRAVAACK. What are you going to tell him?

Mr. CHÁVEZ. Again, that is not the appropriate mission or within our authorities for the National Operations Center to gather that information. There are other organizations within in the Federal Government who do have the authority to gather that information more thoroughly, again, than we do.

Mr. CRAVAACK. Mr. Chávez, you are telling the Attorney General that I cannot acquire this information, this is a vital need for American security.

Mr. CHÁVEZ. It would be outside the skill set of what we actually do. We are not the source for that. So I would not be afraid to tell the Attorney General that we are not the organization that does that.

Mr. CRAVAACK. You are an Air Force officer, aren't you?

Mr. CHÁVEZ. Yes, sir.

Mr. CRAVAACK. Hooray. With that, I yield back.

Mr. MEEHAN. Mr. Long, do you have follow-up questions?

Mr. LONG. Well, you know that, sure. Thank you, and to my friend from Minnesota Mr. Chávez may be better known after this hearing but I just checked Twitter and we are not yet a trending topic on there.

The longer I sit here I think the more confused I get. The title of what we are supposed to be talking about today is "Department of Homeland Security Monitoring Social Networking and Media: Enhancing Intelligence Gathering and Ensuring Privacy." We are all kind of in agreement on that?

Ms. CALLAHAN. Yes, sir.

Mr. CHÁVEZ. Yes, sir.

Mr. LONG. Of course we had a classified briefing yesterday and I came away from that thinking what we were trying to do is protect the homeland and watch for events that may affect the security of citizens here in this country. But yet today I keep hearing

about breaking news, which Twitter is pretty good for that. So either one of you can answer this if you want. I appreciate you being here today, but what is your charge? I have a disconnect with the breaking news, trying to follow that up. I mean that is history, breaking news has happened. Prevention and protecting the citizens while ensuring their Constitutional rights is a whole different can of worms. So both of you can answer this: What is your charge? What do you visualize your job and the agency job as far as—am I completely off-base that we are supposed to be trying to protect the homeland while ensuring privacy, as they say?

Ms. CALLAHAN. You are correct that that is our mission. That is the point of this hearing. I think the disconnect perhaps is that, as I pointed out in my oral testimony, there are three uses of social media. We have been focusing on the second, which is the situational awareness, which is the breaking news element, to know there is an event that could impact the homeland.

The third element, which is the operational use you spoke to the under secretary yesterday, about when we would do it consistent with our authorities for law enforcement or other investigatory purposes using social media if there was a predicate, some sort of reasonable suspicion or elements for that. That is kind of the third element on the prevention side. Mr. Chávez and I have been speaking a lot about the situational awareness, which is the second of the three uses that the Department uses social media for.

Mr. CHÁVEZ. The National Operations Center again is part of the bigger picture out there. We are one of the tools that again the agencies use to again monitor the homeland and those types of things, again that they do under their own authority. So to put the intelligence piece in there with the Nation Operations Center, we are providing through the National Operations Center another piece of information that again those individuals who can use intelligence under their authorities or enhance their operations as with ICE, as was brought up in the other departments or components of DHS, that is what they do with it. We provides one piece of the information, the total information that is out there that they can use and that source again is the media portion of that.

Also, because the intelligence and all those other communities that are out there looking at it, again may not see something happening because they are executing a mission that is out there. What we do again is provide that service that something is happening, turn it over to the appropriate Government agency, to include State——

Mr. LONG. That is all after the fact, correct?

Mr. CHÁVEZ. Indeed. There are other organizations that again that are looking at the prevention piece and looking, doing assessments to determine what threats may be coming at us. We are dealing with the here and now.

Mr. LONG. I am sure there is something I am missing because I can't believe that we would go to all this effort to look into breaking news.

Ms. Callahan, another question for you to wrap up. I am going to try this, can you describe the Department's on-going privacy and civil liberty protection oversight process that is in place now to en-

sure citizens' Constitutional rights are not violated during the execution of the Department's social media monitoring?

Ms. CALLAHAN. Yes, sir. Thank you very much for that question. The Congress has been very generous with my oversight authority, and as I have described earlier, we have been doing mandated, required privacy compliance reviews that we publish on the website. To be clear about what is going on with regard, we are doing these reviews every 6 months, in fact February we started again.

We are also authorized to do investigations into individual types of use of social media, as I said kind of that third category in an operational sense. We are finalizing a management directive to make sure that everyone complies with privacy protections across the board with regard to investigations and operational use. In there we are requiring audits every 3 months, as well as specific investigation by my office. So we take this issue very seriously and we try to be as diverse and robust in working with the Office of Civil Rights and Civil Liberties in all three categories in which the Department uses it—communication, situational awareness, and operational use.

Mr. LONG. During those 3-month and 6-month checkups are you finding things that are of concern to you about people's Constitutional rights?

Ms. CALLAHAN. We have not. No, with regard to the situational awareness, the second use that the Department uses, the National Operations Center has been very consistent with the public-private protections that we have identified.

Mr. LONG. Thank you all for being here today and I yield back.

Ms. CALLAHAN. Thank you, sir.

Mr. MEEHAN. Thank you, Mr. Long. I want to express my appreciation to the panel for being with us here today. I think we have begun an important discussion, and there is appreciation of the difficult charge that you share with some of the other agencies here who not only protect our homeland but American interests around the world. I am grateful for your service in that capacity.

I think all Americans appreciate the huge challenge of fulfilling the responsibility of having the imagination to appreciate what could happen and connecting the dots real-time, all of things we are asking you to do to prevent another issue of terrorism here on American soil, but we also appreciate that you are one of the real protectors of the individual's rights to privacy, what it means to be an American, and this is a delicate and difficult area that I think we have to continue to explore. I am asking you to continue to use your diligence and most assuredly to assure that there isn't inappropriate interference politically, especially inappropriate political interference in which somebody takes your mission and uses it for another purpose, and that every effort be made to safeguard the rights, the privacy rights of individuals.

We may have another opportunity to follow up on things we did not get into because, as I say, I appreciate what you are doing at the DHS level. I am cognizant in my own State of Pennsylvania of the historic context in which State-run but related fusion centers and otherwise have conducted these same kind of inquiries, and that information found its way not just to Governmental entities but to private contractors, private businesses who were using it for

their own purpose. So this whole question of, you know, who is collecting what information, what are we doing to safeguard it and what are we doing to assure that at some appropriate time it disappears.

There is a lot here. I know it is part of your job. I thank you for the work that you are doing, but we are going to continue to ask these tough questions because it is vital to the protection of the most fundamental thing we have, which is our Constitutional rights as American citizens to privacy and to be free from inappropriate Governmental intrusion.

Thank for your work and thank you for your testimony. The Members of the committee may have additional questions for witnesses. If they do, we will ask you to respond in writing. I know there are some things that were asked that you go back and do your best to be responsive to the questions that the committee did ask. The hearing record will remain open for 10 days.

So without objection the committee stands adjourned.

[Whereupon, at 11:35 a.m., the subcommittee was adjourned.]

APPENDIX

LETTER SUBMITTED TO CHAIRMAN PATRICK MEEHAN FROM MARY ELLEN CALLAHAN AND RICHARD CHÁVEZ

MARCH 1, 2012.

The Honorable PATRICK MEEHAN,
Chairman, U.S. House of Representatives, Committee on Homeland Security, Subcommittee on Counterterrorism and Intelligence, Washington, DC 20515.

DEAR REPRESENTATIVE MEEHAN: Thank you for the opportunity to testify before you and your subcommittee on February 16, 2012 about Department of Homeland Security (DHS) review of publicly available social media websites. DHS remains fully committed to providing the subcommittee with all of the information it requires on this topic. We ask that our letter, along with the enclosed attachment, be incorporated into the official record for the February 16, 2012 hearing before your subcommittee.

At the hearing, questions were raised regarding contract language that appeared to permit the use of social media websites to track First Amendment-protected speech by collecting information on public dissent or disagreement on Government activities. As detailed in our written testimony DHS does not now, and has never collected or used, social media reporting for such purposes. We will modify the existing contract and all DHS documentation to clarify and align guidance language with the Privacy Impact Assessments (PIAs).

To further illustrate this point, this week Director Chávez issued the enclosed memorandum to the National Operations Center (Attachment 1) stating that the Office of Operations Coordination and Planning and the Privacy Office are currently reviewing the 2011 Media Monitoring Analyst's Desktop Binder to ensure alignment with the PIAs. Although the media monitoring efforts are in accordance with the privacy guidelines outlined in the PIAs it is important that all documentation relating to media monitoring be similarly aligned. The Privacy Office will complete its fourth Privacy Compliance Review in mid-March 2012 and this alignment will be part of the review.

Director Chávez's memorandum to the National Operations Center also reiterates the privacy guidelines that have been in place since the start of this program: Collection of personally identifiable information from social media websites is permitted only in specific circumstances and is limited to the categories described in our written testimony and in the January 6, 2011 PIA. The information that is collected may be retained only in the report that is generated, and is not cross-referenced or tracked in any other way.

We appreciate the subcommittee's interest in our efforts in this regard. We would be happy to meet with subcommittee staff or Members individually the week of March 5, 2012 to provide you with any further information or discussion of these issues you may require. NOC media monitoring reports are also available for your review.

Sincerely,

MARY ELLEN CALLAHAN,
Chief Privacy Officer, U.S. Department of Homeland Security,

RICHARD CHÁVEZ,
Director, Office of Operations Coordination and Planning, U.S. Department of Homeland Security.

MEMORANDUM FOR: National Operations Center
FROM: Richard Chávez, Director, Office of Operations Coordination and Planning
SUBJECT: Media Monitoring Guidance Reminder

As part of the fourth Privacy Compliance Review that is scheduled to occur in mid-March 2012, the National Operations Center (NOC), in coordination with the DHS Privacy Office, will review the 2011 Media Monitoring Analyst's Desktop Binder, any associated standard operating procedures, and the existing media monitoring support services contract to ensure conformity with all *Publicly Available Social Media Monitoring and Situational Awareness Initiative* Privacy Impact Assessments (PIAs) and to ensure the scope and purpose of the NOC Media Monitoring Capability (MMC) are accurately reflected and recommend clarifications and updates to the language if necessary. In the interim, the NOC will continue to use the PIAs as the authoritative source to guide the program.

The NOC MMC should continue to limit the review, use, collection, and dissemination of non-personally identifiable information and the seven narrow categories of personally identifiable information to information that affect the operations of the Department of Homeland Security (memorialized in the January 2011 PIA). No First Amendment-protected speech relating to dissent or disagreement with the Department and its activities should be reviewed, used, collected, or disseminated.

The MMC can review, use, collect, and disseminate information intended to provide guidance on DHS programs and initiatives that inform the general public. An example would be the Transportation Security Administration's PreCheck program. The MMC can also review, use, and collect information related to oversight reports about DHS components such as DHS Inspector General Reports or Government Accountability Office Reports.

The MMC cannot review, use, collect, or disseminate information related to individuals' positive or negative opinions or reports on the Department, but for the narrow circumstance where the MMC reviews and informs the relevant Component of an operational issue adversely impacting the Component. Examples of these issues include security violations at airports or ports of entry. In this narrow operational circumstance, no personally identifiable information can be collected, stored, or disseminated to the relevant Component.

QUESTIONS SUBMITTED BY RANKING MEMBER BENNIE G. THOMPSON FOR MARY ELLEN CALLAHAN AND RICHARD CHÁVEZ

Question 1. Please explain the circumstances under which DHS might collect information on journalists.

Answer. DHS does not collect information on journalists (other than recording the name of the author when saving a particular article so as to ensure proper attribution, or including a individual journalist's name that is part of that journalist's social media internet link). As described below, DHS collects information on events.

In support of its statutory mission to provide situational awareness and a common operating picture for the Federal Government and for other homeland security enterprise partners, the National Operations Center (NOC) within the DHS Office of Operations Coordination and Planning reviews publicly available traditional and social media postings to gain an enhanced awareness of rapidly emerging or evolving incidents and events concerning homeland security, emergency management, and National health. If a journalist posts a report on a publicly available social media site about a breaking news incident relevant to homeland security, the NOC's media monitoring analysts may use the information posted to build a report that is distributed to DHS leadership and other homeland security partners including Federal interagency, State, local, Tribal, and territorial government entities. The NOC may include reporters' names and affiliations in the reports as described below.

The NOC includes a particular journalist's name with recorded media in accordance with the guidelines set forth in the Publicly Available Social Media Monitoring and Situational Awareness Initiative Privacy Impact Assessment (PIA) (dated June 22, 2010) and its January 6, 2011 update. As stated in the PIA update and the February 1, 2011 System of Records Notice, personally identifiable information on seven narrow categories of individuals may be collected when it lends credibility to the report or facilitates coordination with Federal, State, local, Tribal, territorial, foreign, or international government partners. In such instances DHS will only collect the following limited pieces of information from journalists: Names, titles, and organizational affiliation of anchors, newscasters, or on-scene reporters who are known or identified as reporters in their post or article or who use traditional and/or social media in real time to keep their audience situationally aware and informed. Fre-

quently with breaking news on social media, the individual journalist's name or names of other key individuals will be part of the story's internet link. In order to disseminate these publically available links, the NOC must include the personally identifiable information contained in the link address. Removing the PII from the link address will render the link, and thus the story, unusable.

All National Operations Center (NOC) social media initiative PIAs are available to the public at *www.dhs.gov/privacy.*

Question 2. Please explain how DHS came to report on information related to citizens' opinions on moving Guantanamo Bay Detainees to Standish, MI, and whether this is an appropriate use of social media by DHS.

Answer. The DHS Office of Operations Coordination and Planning (OPS) never reported on potential plans to move detainees to Standish, MI. During the development of the Media Monitoring capability, OPS developed a Social Networking/Media Capability Analyst Handbook also known as a Desktop Binder. The purpose of the Desktop Binder was to serve as a desk reference for media monitoring analysts. In an early draft version of the Desktop Binder, an example was created based on actual information related to citizens' opinions regarding moving Guantanamo Bay Detainees to Standish, MI. This document was part of a "weekly report example," not an actual report in a very early, and obsolete version of the Desktop Binder. This version of the Desktop Binder was created while OPS was still in the midst of developing its media monitoring processes, and before the media monitoring reports were ever distributed. This example has been removed from the Desktop Binder, and this information was never released through the situational awareness reporting channels.

To maintain a capability focused on reviewing incident and event information, OPS trains analysts to review information in compliance with the parameters set forth in the Privacy Impact Assessments (PIAs). During the report production process, reports are reviewed multiple times to ensure PII is not inadvertently included. Reports are reviewed at least twice, once by the analyst generating the report and then again by the analyst's counterpart. Each report is then checked by the media monitoring lead prior to dissemination. All reports distributed during each 24-hour period are checked by a media monitoring capability senior reviewer, and the media monitoring capability's quality control leads conduct weekly reviews of all distributed reports to ensure any inadvertent PII inclusions are identified and corrective action is taken. As described previously, the Privacy Office conducts Privacy Compliance Reviews every 6 months to ensure OPS is complying with the PIAs.

Question 3. Please explain the terms of the contract and the rationale for contracting with General Dynamics to conduct social media situational awareness reporting.

Answer. To fulfill the National Operations Center's (NOC) statutory responsibility to provide situational awareness, the NOC examines publicly available traditional and social media, compares it with many other sources of information, and includes it where appropriate into NOC reports. At the time the contract was awarded, the Office of Operations Coordination & Planning (OPS) did not have available Federal employees to complete this task. OPS procured contracted services to fulfill this function. Additionally, OPS has not ascertained if this service will be required on a permanent basis, making it more economical to utilize contractor services in the interim.

OPS is continuing to assess current performance to determine the most efficient and effective mechanism for performing the media monitoring function in light of operational needs and budgetary direction.

The Media Monitoring contract was competed for and awarded to General Dynamics Advanced Information Systems (GDAIS) on May 27, 2010, under the GSA Mission Oriented Business Integrated Services (MOBIS) contract vehicle. The Period of Performance (POP) for this contract is July 1, 2010 through December 31, 2014, and the total contract value is $11.3 million. The contract includes tasks to monitor open sources for incidents relating to potential and emerging threats and hazards to the homeland.

In accordance with the Federal Acquisition Regulation, the award to GDAIS was based on the Evaluation Team's review and assessment of the qualifications of multiple vendors that submitted a quotation in response to the Request for Quotation (RFQ). The Evaluation Team made a recommendation to the Source Selection Authority (SSA) that GDAIS offered the best value quote for fulfilling the Department's social media situational awareness reporting requirement. After a thorough review of the Evaluator's assessment which included an evaluation of the strengths, weaknesses, and risks of the quotes received, the SSA determined that GDAIS would provide superior performance of the Government's objectives, and was the most technically competent contractor that had submitted a quotation.

Question 4. Please describe the way that DHS solicited feedback from the privacy community regarding DHS' use of social media.

Answer. In addition to the five Privacy Impact Assessments (dealing with the three pilots, the program, and the update to include seven narrow categories of personally identifiable information) and three Privacy Compliance Reviews, the DHS Privacy Office has engaged in dialogue with the privacy community regarding DHS' use of social media in a number of ways. These include several quarterly advocate outreach meetings (Privacy Information for Advocates), Chief Privacy Officer Testimony before the Data Privacy and Integrity Advisory Committee (DPIAC) in public meetings, DHS Privacy Office staff testimony before the DPIAC, and inter-agency and intra-agency discussions. The Privacy Impact Assessments and other documentation are available at *www.dhs.gov/privacy.*

The Chief Privacy Officer invites privacy organizations and privacy advocates (who have requested to participate) to quarterly informational meetings during which the Chief Privacy Officer provides updates on DHS privacy issues. To date, 24 distinct organizations have requested invitations. The quarterly Privacy Information for Advocates meetings allow the Chief Privacy Officer and privacy advocates to discuss privacy issues that impact DHS and individuals. In 2010 and 2011, Chief Privacy Officer Mary Ellen Callahan spoke in depth about DHS's use of social media and the situational awareness initiative at four of the quarterly meetings. Additionally, the March 2012 Privacy Information for Advocates meeting provided an opportunity to update advocates on the social media situational awareness initiative at length, including discussing examples, as well as clarifying misconceptions.

The DPIAC was established by the Secretary of Homeland Security as a discretionary committee under the Federal Advisory Committee Act to provide advice to the Secretary and to the DHS Chief Privacy Officer, upon request, on policy, programmatic, operational, administrative, and technological issues within DHS that relate to personally identifiable information, as well as data integrity and other privacy-related matters. Committee members are individuals from the private sector, academia, non-governmental organizations, and State government who have expertise in privacy, security, and emerging technologies.

The DPIAC holds several public meetings throughout the year to receive updates from the DHS Privacy Office, learn more about how DHS components have implemented privacy, and gain information on specific DHS programs that have privacy implications. In 2010 and 2011, Chief Privacy Officer Mary Ellen Callahan provided public testimony on the development, progression, and modification of the social media situational awareness initiative at four of these meetings. Additionally, DHS Privacy Office staff publicly testified at DPIAC meetings on the social media situational awareness initiative. In September 2010, one of the Associate Directors for Privacy Compliance testified on the development of Privacy Compliance Reviews generally, and how public Privacy Compliance Reviews focusing on the social media situational awareness initiative function. In March 2011, another Associate Director for Privacy Compliance publicly testified on the social media situational awareness initiative, focusing on the addition of the seven narrow categories of personally identifiable information that would be collected. Finally, in December 2011, staff from the National Operations Center (NOC), which runs the social media situational awareness initiative, was scheduled to publicly testify on the social media situational awareness initiative and the associated Privacy Compliance Reviews. However, the testimony was postponed due to extended deliberations by the DPIAC on pending recommendations from the committee to the Department. Information about DPIAC, and the publicly available meetings, can be found at *www.dhs.gov/privacy.*

Throughout 2010–2012, the DHS Privacy Office also provided information about DHS' use of social media, whether for public communications and outreach, situational awareness, or operational use, to interagency privacy groups, including the Innovation and Emerging Technologies Subcommittee of the CIO Council Privacy Committee. These briefings were provided as examples of ways to embed privacy protections in Government use of social media generally, including developing Privacy Impact Assessments and System of Records Notices as necessary.

In addition to providing information via interagency fora, in 2011, the DHS Privacy Office hosted an intra-agency privacy compliance meeting where staff from the National Operations Center updated DHS Component Privacy Officers on the social media situational awareness initiative and corresponding Privacy Compliance Reviews, as well as fielded questions from the Component Privacy Officers about the initiative.

Question 5. Please explain who/what determines what the NOC looks at and searches for on social media sites.

Answer. The Senior Watch Officer (SWO) within the National Operations Center (NOC), as guided by the Privacy Impact Assessments (PIAs), determines the NOC's search parameters. There are 13 broad Items of Interest (IOI) that focus analysts' efforts when searching publicly available social media sites. The IOI categories provide a general framework for the NOC's searches. The following are the categories:

(1) terrorism (includes media reports on the activities of terrorist organizations in the United States and abroad);
(2) weather/natural disasters, emergency management (includes all-hazard reports, such as reports on hurricanes, tornadoes, flooding, and earthquakes);
(3) fire (includes reports on the ignition, spread, response, and containment of wildfires, industrial fires, and explosions);
(4) trafficking/border control issues (includes reports on the trafficking of narcotics, people, weapons, and goods into and out of the United States);
(5) immigration (includes reports on apprehension of illegal immigrants and border control events or incidents);
(6) HAZMAT (includes reports on chemical, biological, and radiological hazardous materials discharges);
(7) nuclear (includes reports terrorist attempts to obtain nuclear materials, security incidents at nuclear facilities, and potential threats to nuclear facilities);
(8) transportation security (includes reports on security breaches and incidents or threats involving rail, air, road, and water transit);
(9) infrastructure (includes reports on attacks or failures in transportation networks, telecommunications networks, energy grids, utilities, domestic food and agriculture, Government facilities, and financial infrastructure);
(10) National and international security (includes reports relating to threats against American citizens, political figures, military installations, embassies, and consulates);
(11) National and international health concerns (includes reports on outbreaks of infectious diseases and recalls of food or other items dangerous to public health);
(12) public safety (includes reports on public safety incidents, building lockdowns, bomb threats, mass shootings, and building evacuations); and
(13) cybersecurity (includes reports on cybersecurity matters such as cyber attacks, computer viruses, and the use of technology for terrorism purposes).

There were originally 14 IOI categories. IOI 14 was "Reports on DHS, Components, and other Federal agencies: Includes both positive and negative reports on FEMA, CIS, CBP, ICE, etc. as well as organizations outside of DHS." This IOI has been subsequently eliminated in order to prevent misunderstandings about the intended use of this information.

Analysts conduct searches using publicly available streaming media and news-based search engines. These tools allow analysts to search by keyword or a collection of terms. The keywords and terms that inform searching are pre-loaded onto the publicly available search tools. The core social media websites utilized by the NOC are listed in Appendix A of the January 6, 2011 Privacy Impact Assessment that is available to the public via *www.dhs.gov/privacy.* The core search terms, or keywords, utilized by the NOC are listed in Appendix B of the same publicly available document.