epic.org

ELECTRONIC PRIVACY INFORMATION CENTER

Statement for the Record of
The Electronic Privacy Information Center (EPIC)

Marc Rotenberg, EPIC President
Ginger McCall, Director, EPIC Open Government Project

Hearing on

"DHS Monitoring of Social Networking and Media: Enhancing Intelligence Gathering and Ensuring Privacy"

Before the

House Homeland Security Committee's Subcommittee on
Counterterrorism and Intelligence
U.S. House of Representatives

February 16, 2012
311 Cannon House Office Building
Washington, DC

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 online 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

---

[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-media-monitoring/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.

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 online 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 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 online 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

[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.
[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/2012-02-13-PNI0213wir-FBI-social-media_ST_U.htm

by the Constitution and the US 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 online comments, dissent, and criticism for the purpose of subsequent investigation send a chilling message to online 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

---

[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:

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 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 US 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

---

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.

[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.

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 US government, it has transformed its purpose from protecting the American public to protecting simply itself.

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

[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/

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.

Attachment 1

Department of Homeland Security: Statement of Work: "Media Monitoring and Social Media/Networking Support Services for the Office of Operations Coordination and Planning's National Operations Center"

(Source: EPIC, DHS Social Media Monitoring Documents, at p. 77)

situations, and provide valuable information/imagery that can be used to corroborate and/or reconcile first reports. The Contractor shall understand DHS critical information requirements and monitor open sources news coverage for new incidents (Items of Interest – IOI) and with a perspective of how a story may be related to other important ongoing events and DHS activities. The Critical Information Requirements (CIR) are: Potential threats and hazards to the homeland, to DHS, other Federal agencies, state and local response units, facilities, and resources; Private sector; Public safety; Potential impact on DHS capability to accomplish the HSPD-5 mission; Identifying events with operational value and/or corroborating critical information; Identifying media reports that reflect adversely on the U. S. Government, DHS or prevent, protect, respond or recovery activities; The National planning scenarios.

4.1.1 The contractor shall perform a broad open sources search for information on breaking news stories. The contractor shall:

4.1.1.1 Monitor major broadcast news networks
4.1.1.2 Monitor and review all Associated Press (AP) stories generated within the U.S. by each state's AP bureau
4.1.1.3 Monitor and receive alerts on other wire service stories via categorized/focused Really Simple Syndication (RSS) feeds.
4.1.1.4 Monitor and receive alerts on local and regional broadcast news via categorized/focused text/video feeds
4.1.1.5 Monitor appropriate Internet web sites on breaking situational events
4.1.1.6 Monitor and receive full motion video (FMV) or other streaming media

4.1.2 In the event an incident has occurred and an Items of Interest (IOI) follow-on analysis is underway or research is ongoing on a National Security Situation/ International Security Situation (NSS/ISS), the contractor shall:

4.1.2.1 Continue to monitor major broadcast news networks (cable service)
4.1.2.2 Query and search Associated Press (AP) stories for information specific to the incident
4.1.2.3 Query and search broadcast news via categorized/focused text/video feeds for information specific to the incident
4.1.2.4 Query and search RSS feeds for information specific to the incident
4.1.2.5 Query and search the Internet using other search engines such as Google and Yahoo
4.1.2.6 Monitor and receive full motion video (FMV) or other streaming media specific to the incident