



Written by [Joe Wolverton, II, J.D.](#) on March 2, 2012

Homeland Security Officials Caught Hiding Online Spying Program from Congress

While it has been reported that these two bureaucrats were “[deliberately stonewalling](#),” the level of unwarranted searches of the online activity of those not accused or even suspected of any crime to which these witnesses testified is disturbing.

How disturbing? Here’s how [one commentator](#) described how the social media spying program works: “If you’re the first person to tweet about a news story, or if you’re a community activist who makes public Facebook posts — DHS will have your personal information.”



The snooping that caught the attention of Congress is part of the [Publicly Available Social Media Monitoring and Situational Awareness Initiative](#) begun last year by DHS’s National Operations Center (NOC). In the report on the initiative published by DHS, the intelligence-gathering arm of the DHS, the Office of Operations Coordination and Planning (OPS), gives itself permission to “gather, store, analyze, and disseminate” data on millions of users of social media (Twitter, Facebook, YouTube) and business networking sites (Linkedin).

Specifically, the initiative sets out the plan and purpose behind the DHS’s collection of personal information from news anchors, journalists, reporters, or anyone else who posts articles, comments, or other information to many popular web outlets. The report defines the target audience as anyone who may use “traditional and/or social media in real time to keep their audience situationally aware and informed.”

Journalists and bloggers need not worry, however. DHS promises that it will not routinely gather and use Personally Identifiable Information (PII). From the abstract of the Initiative:

While this Initiative is not designed to actively collect Personally Identifiable Information (PII), OPS is conducting this update to the Privacy Impact Assessment (PIA) because this initiative may now collect and disseminate PII for certain narrowly tailored categories. For example, in the event of an in extremis situation involving potential life and death, OPS will share certain PII with the responding authority in order for them to take the necessary actions to save a life, such as name and location of a person calling for help buried under rubble, or hiding in a hotel room when the hotel is under attack by terrorists.

In other words, the government promises that all the personal electronic data that it monitors and records will only be used in “narrowly tailored” circumstances — saving a life, for example. There is no requirement that the data be used only in those instances, but there is a promise that it will be.

This unconstitutional, unwarranted search of private information is designed by DHS “to provide situational awareness and establish a common operating picture” of target audiences.



Written by [Joe Wolverton, II, J.D.](#) on March 2, 2012

Prior to this new initiative, operative guidelines instructed NOC to collect data only “under authorization set forth by the written code,” whereas these new provisions permit agents of the NOC to track the online movements and postings of every level of writer or commentator from Brian Williams to nearly anonymous bloggers.

Writers aren’t the only group to be watched by the never-blinking eye of Homeland Security. According to the report, “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” may also be spied on and have their “usernames and passwords” recorded for future reference.

How many people might be shoe-horned into one of those categories if the federal government decided it wanted to put them under online surveillance?

At the hearing presided over by Representative Patrick Meehan (R-Penn.), the atmosphere was often charged, as Congressmen from both major political parties berated the Homeland Security apparatchiks for their casual disregard for the Fourth Amendment, as well as for their inability to clearly articulate the scope of the social media spying operation they run.

The agency’s apparent violations of the Fourth Amendment’s proscription on unwarranted searches and seizures were not the only constitutional contraventions called out by the members of the committee.

Representatives Billy Long (R-Mo.), Jackie Speier (D-Calif.), and Bennie Thompson (D-Miss.), for example, pummeled Chavez and Callahan with demands that they explain how monitoring the online activity of journalists and bloggers will not have a chilling effect on free speech.

The reply to these critical questions of constitutionally suspect activities was phrased in the language of double-talk common to bureaucrats:

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.

It may surprise DHS, but there is no constitutional authority for the monitoring, recording, and tracking of the online activity of citizens, so they needn’t concern themselves with balancing such activities against the First and Fourth Amendments.

Perhaps more damaging than the double-talk in the testimony given in that committee meeting on February 16 is the degree of deception perpetrated by these public servants. Information revealed in [a cache of classified documents](#) obtained by the Electronic Privacy Information Center (EPIC) makes it clear that not only did DHS officials lie about not having actually implemented the social media monitoring program, but their insistence that they had not hired an independent contractor to administer the plan was also false.

As explained by [Raw Story](#):

The documents released by EPIC in January and in February reveal that the Department [of Homeland Security] is paying defense contractor General Dynamics to monitor the Internet for “reports that reflect adversely on DHS and response activities,” including “reports that pertain to DHS and sub agencies — especially those that have a negative spin on DHS/Component preparation, planning, and response activities,” among other things.



Written by [Joe Wolverton, II, J.D.](#) on March 2, 2012

According to the information contained in those records, DHS is paying [General Dynamics](#) \$11.4 million of taxpayer money to follow the virtual trail of journalists, bloggers, and broadcasters, compile all “suspicious” searches and posts, and then report this data to their bosses in the executive branch.

The bottom line was succinctly stated by EPIC’s director of the Open Government Project, Ginger McCall. [In a letter](#) sent by McCall to members on the Counterintelligence and Intelligence Subcommittee, the reality of the depth of the department’s directive is set forth:

The DHS testimony, as well as the documents obtained by EPIC, indicate that the agency is monitoring constantly, under very broad search terms, and is not limiting that monitoring to events or activities related to natural disasters, acts of terrorism, or manmade disasters. The monitoring is designed to be over-broad, and sweeps in large amounts of First Amendment activity. The DHS has no legal authority to engage in this monitoring.

The takeaway from the testimony of Chavez and Callahan and the recently revealed truth that belies it is provided by McCall, as well:

This has a profound effect on free speech online if you feel like a government law enforcement agency — particularly the Department of Homeland Security, which is supposed to look for terrorists — is monitoring your criticism, your dissent, of the government.



Subscribe to the New American

Get exclusive digital access to the most informative,
non-partisan truthful news source for patriotic Americans!

Discover a refreshing blend of time-honored values, principles and insightful perspectives within the pages of "The New American" magazine. Delve into a world where tradition is the foundation, and exploration knows no bounds.

From politics and finance to foreign affairs, environment, culture, and technology, we bring you an unparalleled array of topics that matter most.



Subscribe

What's Included?

- 24 Issues Per Year
- Optional Print Edition
- Digital Edition Access
- Exclusive Subscriber Content
- Audio provided for all articles
- Unlimited access to past issues
- Coming Soon! Ad FREE
- 60-Day money back guarantee!
- Cancel anytime.