New American

Written by **Joe Wolverton, II, J.D.** on January 13, 2012

Homeland Security Is Reading and Recording Every Keystroke

The Department of Homeland Security's National Operations Center (NOC) released its Publicly Available Social Media Monitoring and Situational Awareness Initiative last year and in that report 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.

A story in the *New York Times* reports on the specific sites that show up on the DHS radar:

Homeland Security seems to have a real affinity for Twitter. It advises its employees to follow not only Twitter itself but also Twitter search sites like Monitter, Tweetzi and Tweefind and more than 10 Twitter trend sites like TweetStats and Trendistic.

It monitors Facebook and, while it also recommends monitoring MySpace, it notes the once-popular social network has "limited search" capabilities. Homeland Security employees also monitor video sites like YouTube, Vimeo and Hulu — "situational awareness" apparently entails full episodes of "The Bachelor."

Among the blogs the department follows: Wired's Threat Level and Danger Room, Krebs on Security and, at *The New York Times*, The Lede blog. The list also includes more controversial sites like JihadWatch, Wikileaks and "Narcotráfico en México."

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, the following individuals may also be spied on and have their "usernames and passwords" recorded for future reference:

1) U.S. and foreign individuals in extremis 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 post or article or who use traditional and/or social media in real time to keep their audience situationally aware and informed; 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.

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?

An article published by RT.com asked a very relevant question: "Why [is] the government … going out of their way to spend time, money and resources on watching over those that helped bring news to the masses?"

The specific procedure followed by NOC agents is described in the initiative, as well:

To monitor social media, NOC Media Monitoring analysts only use publicly available search engines, content aggregators, and site-specific search tools to find items of potential interest to DHS. Once the analysts determine an item or event is of sufficient value to DHS to be reported, they extract only the pertinent, authorized information and put it into a specific web application (MMC application) to build and format their reports.

Once the raw data is collected and collated and a picture of the person's behavior is compiled, DHS will "disseminate relevant and appropriate information to federal, state, local, and foreign governments, and private sector partners."

The piece in RT.com reports some of the partners to have availed themselves of the critical online information secretly amassed by the DHS.

The development out of the DHS comes at the same time that U.S. District Judge Liam O'Grady denied

pleas from supporters of WikiLeaks who had tried to prevent account information pertaining to their Twitter accounts from being provided to federal prosecutors. Jacob Applebaum and others advocates of Julian Assange's whistleblower site were fighting to keep the government from subpoenaing information on their personal accounts that were collected from Twitter.

Last month the Boston Police Department and the Suffolk Massachusetts District Attorney subpoenaed Twitter over details pertaining to recent tweets involving the Occupy Boston protests.

Fast Company reports that in addition to federal, state, and local government agencies, DHS is sharing with "international partners" the information gathered under the new guidelines.

Nowhere in the 23-page document does the DHS make clear what it takes to make an "item or event" of "sufficient value," and that's how the government wants to keep it. What the report does make very clear, however, is that every keystroke, whether it be Google searches or Facebook status updates, will be recorded and cataloged by DHS snoops who will then rifle through it and see if there is anything that might someday be useful in compiling a profile of activity of a target individual. Then, that profile may reveal activities, interests, or posts that can be presented to another nameless bureaucrat who can authorize a more thorough investigation into that person's private life.

Another gap in the report on this initiative is precisely what means were employed by the federal government to bypass the Fourth Amendment's guarantee of "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."

The official responsible for implementing the directives contained in the "Publicly Available Social Media Monitoring and Situational Awareness Initiative Update" is the Acting Director of the National Operations Center Office of Operations Coordination and Planning, Donald Triner. His phone number is (202) 282-8611.