**6 Government Surveillance Programs Designed to Watch What You Do Online**

***If you are a user of Facebook, Twitter, LinkedIn, YouTube, Craigslist or another popular site, the U.S. security state is watching you.***

*By* [***David Rosen***](https://www.alternet.org/authors/david-rosen-0) / [**AlterNet**](https://alternet.org/)

*June 6, 2012, 5:00 AM GMT*

President Eisenhower was right on point about the military-industrial complex, but he could not have predicted the emergence of the massive surveillance state -- combining the government and private sector -- that bolsters it.

Sadly, neither President Obama nor his Republican challenger, Mitt Romney, has the desire or moral courage to fight the growing power and influence of the Corporate Security State. We are witnessing the integration of spying on two levels, the government level (federal, state and local) and the corporate level (via telecom providers, web services and credit card companies).

If you are a user of Facebook, Twitter, LinkedIn, YouTube, Craigslist or another popular site, the U.S. security state is watching you. An increasing number of federal agencies are employing sophisticated means to monitor Americans' use of social networking sites. Federal entities from the National Security Agency (NSA) and the Defense Department to the Department of Homeland Security (DHS) to even the Internal Revenue Service (IRS) are involved in developing programs to track the American public online.

Bottom of Form

Here is a brief summary of some of the other programs.

**1. Justice Department.** The Electronic Frontier Foundation (EFF) [released a report](https://www.eff.org/files/filenode/social_network/20100303__crim_socialnetworking.pdf) from the DOJ’s Computer Crime and Intellectual Property section, "Obtaining and Using Evidence from Social Networking Sites," that describes how evidence from social networking sites can reveal personal communications that might help "establish motives and personal relationships."

It reports that monitored data from such sites can provide location information and "prove and disprove alibis." Perhaps most illuminating, it advises agents that “going undercover” on social media sites can enable law enforcement to communicate with suspects and targets, gain access to nonpublic information and map social relationships. The DOJ document notes that Twitter retains the last login IP address, but does not preserve data unless legally required to do so.

**2. The IRS** uses a variety of social media sites like Facebook, Google, Twitter, MySpace, YouTube and Second Life to investigate taxpayers. It seems to have started this practice in 2009, providing agents with special training on social networking. The EFF posted the IRS’ 38-page training that offers detailed tips to agents on how to conduct searches, locate relevant taxpayer information, [narrow down and refine results.](https://www.eff.org/foia/social-network-monitoring)

**3. The Office of the Director of National Intelligence** is seeking a tool that integrates all online information, including web searches, Wikipedia edits and traffic webcams.

**4. The Defense Department** has [solicited proposals](https://www.fbo.gov/index?s=opportunity&mode=form&id=6ef12558b44258382452fcf02942396a&tab=core&_cview=0) through DARPA for a $42 million “Social Media Strategic Communications” (SMISC) program, a tool that tracks social media and weeds out information. It has set four goals for the project: (i) to detect, classify and measure the development of ideas, concepts in hidden social media messages; (ii) specify the structure of the campaign and influence in social media sites and the community they create; (iii) identify the participants and intention in conducting a social media campaign of persuasion and measure its effect; and (iv) develop an effective counter-message to an identified campaign carried out against the enemy.

**5. The FBI** is soliciting a bid for a program that seems very similar to the DHS social-network monitoring program. Dubbed the "FBI Social Media Application,” the program would have "[the ability] to rapidly assemble critical open source information and intelligence ... to quickly vet, identify and geo-locate breaking events, incidents and emerging threats."

In the FBI’s 12-page solicitation, it requests a program that can quickly identify, display and locate alerts on geo-spatial maps and enable users to summarize the "who, what, when, where and why" of specific threats and incidents. Going further, it seeks to not simply detect “credible threats,” but to identify those organizing and taking part in gatherings and to predict upcoming events. According to the FBI, "Social media will be a valued source of information to the SIOC [i.e., Strategic Information and Operations Center] intelligence analyst in a crisis because it will be both eyewitness and first response to the crisis."

An FBI spokesperson insisted, "[We] will not focus on specific persons or protected groups, but on words that relate to 'events' and 'crisis' and activities constituting violations of federal criminal law or threats to national security. Examples of these words will include lockdown, bomb, suspicious package, white powder, active shoot, school lockdown, etc.” Rest assured, much like the assurances voiced by the DHS, the FBI insists that its monitoring won't be used to focus on [specific individuals or groups](https://www.cbc.ca/news/technology/story/2012/02/13/technology-fbi-social-media-app.html?cmp=rss&partner=skygrid).

**6. Department of Homeland Security**. A more aggressive [monitoring program](https://epic.org/foia/epic-v-dhs-media-monitoring/) was recently revealed by the Electronic Privacy Information Center (EPIC) when it secured from the DHS a list of approximately 380 keywords that the agency tracks. The allegedly threatening terms were found in the DHS’ Analyst Desktop Binder, part of its 2011 Media Monitoring Capability (MMC) program.

These terms are organized into nine categories:

Agencies – 26 terms, including “DHS,” “FBI”, “CIA,” “Air Marshal,” “United Nations” and “Red Cross”;

Domestic security – 52 terms, including "assassination," "dirty bomb," “crash,” “first responder,” “screening” and “death.”

Hazardous materials – 34 terms, including "hazmat," “nuclear," “leak,” “burn” and “cloud.”

Public health – 47 terms, including "ebola," "contamination," “wave,” “pork” and “agriculture.”

Infrastructure security – 35 terms, including “AMTRAK,” “airport," "subway," “port,” “electric” and “cancelled.”

Southwest border violence – 65 terms, including "drug cartel," "decapitated," “gunfight,” “marijuana,” “heroin,” “border” and “bust.”

Terrorism – 55 terms, including “Jihad,” “biological weapons,” “suicide attack,” “plot” and “pirates.”

Emergencies and weather – 41 terms, including “disaster,” "hurricane," "power outage," “ice,” “storm” and “help.”

Cyber security – 25 terms, including “cyber terror,” “malware,” “virus,” “hacker,” “worm,” “China” and “Trojan.”

The DHS has been engaged in monitoring social networking sites like Facebook, Twitter, Flickr, YouTube and LinkedIn as well as blogs since at least 2010. Its effort is run through the Office of Operations Coordination and Planning (OPS), National Operations Center (NOC), and is entitled “Publicly Available Social Media Monitoring and Situational Awareness (Initiative).” Its ostensible purpose is to provide situational awareness and strengthen its common operating picture.

The scope of DHS’ practice of social monitoring was unexpectedly revealed in a special congressional hearing, the House Subcommittee on Counterintelligence and Intelligence, headed by Rep. Patrick Meehan (R-PA), in February. Two DHS officials, Chief Privacy Officer Mary Ellen Callahan and Director of Operations Coordination and Planning Richard Chavez, raised the representatives' ire by appearing to be deliberately stonewalling on the scope and practice of the agency's social media surveillance.

Most disturbing, the DHS reps appeared unsure about the monitoring program’s goals, how the gathered information would be used and whether it would be shared with other agencies. In an unusual show of bipartisan unity, Reps. Billy Long (R-MO), Jackie Speier (D-CA) and Bennie Thompson (D-MS) joined Rep. Meehan in chastising the DHS officials.

Under intense congressional probing, DHS reps revealed that the keywords chosen for monitoring were drawn from commercially available, off-the-shelf database programs that were customized to meet its specifications. The agency was particularly interested in determining first witnesses to breaking events like the 2011 Tucson shooting of Gabrielle Giffords and others and the January 2012 bomb threat at an Austin school.

The DHS reps insisted that data gathered was only used to confirm other news reports and that information on private citizens was not being collected. In addition, they claimed that that all personally identifying information was regularly scrubbed from the agency’s servers.

Few should feel comforted by the DHS assurances. At the House hearing, it was also revealed that the agency was involved in what appears to be an ongoing campaign to monitor the actions and beliefs of individual Americans engaged in community-based political activism. It compiled a report, “Residents Voice Opposition Over Possible Plan to Bring Guantanamo Detainees to Local Prison-Standish MI,” that tracked community reactions to the proposed location of Guantánamo detainees in a local Michigan prison.

The DHS report is part of the EPIC documents acquired through a Freedom of Information request. It details that information was gathered from a variety of sources, including newspaper articles and responses, blogs by local activists, and Twitter and Facebook posts.

The House hearing also shed light on the DHS practice of outsourcing keyword tracking of social media through a sole-source contract to the giant defense contractor, General Dynamics. In 2011, General Dynamics had revenues of $5.5 billion of which 84 percent ($4.6 billion) came from government contracts. Earlier this year, it’s Advanced Information Systems division was awarded a $14 million DHS contract to (in the words of a press release) “provide constant and continual watch operations for critical communications to the agency's National Coordinating Center.” In addition, it will “identify the possible impacts of potentially disruptive events.

In keeping with the prevailing ethos of corporate unaccountability, it turns out if the General Dynamics employees are found to have misused the information garnered from a social network user, including a journalist or public figure, the employee must take a training course or, worst case, lose his/her job. No criminal penalties are specified.

**A word to the wise, Big Brother is watching you!**