



FBI Pursues Social Media Surveillance to Gather Intelligence

In a formal “request for information,” the Federal Bureau of Investigation (FBI) asked software companies for a digital tool that would systematically scan the entire social media realm to find potential terrorist-related threats and intelligence information. While hundreds of intelligence analysts are already probing overseas Facebook and Twitter posts, U.S. law enforcement officials claim digital software could sift through more data than humans ever could.

The FBI is the latest in a growing catalog of agencies, such as the Department of Defense and the office of the Director of National Intelligence, that have pursued methods to monitor conversations and other information on a myriad of social media platforms. In an [article](#) published last month, when the surveillance plan was originally proposed, *the Atlantic* explained how several government agencies have utilized this technology:



Other federal agencies have similar programs. DARPA, the Department of Defense’s advanced-projects incubator, put out an open call for “memetrackers” trained in social-network analysis in August. The CIA has maintained a social-media tracking center in Virginia for years, a continuation of the station’s original mission to sort through online sources like Daily Kos. But the primary difference between the DoD/CIA projects and FBI’s are likely a matter of jurisdiction: the FBI, as the federal government’s highest law-enforcement agency, will focus primarily on domestic threats while the CIA and DoD focus their efforts on intelligence gathering abroad. ...

“Social media has emerged to be the first instance of communication about a crisis, trumping traditional first responders that included police, firefighters, EMT, and journalists,” FBI officials [wrote](#) in their request. “Social media is rivaling 911 services in crisis response and reporting.”

The bureau’s aim is to establish an early-warning system that can deliver live open source intelligence that will [enhance](#) the “FBI’s overall situational awareness.” According to the agency’s request, the system must “have the ability to rapidly assemble critical open source information and intelligence that will allow SIOC [Strategic Information and Operations Center] to quickly vet, identify, and geo-locate breaking events, incidents, and emerging threats.”

Some critics question the effectiveness of the initiative, as the sheer volume of material that social media services produce has dramatically altered the type of information available on the web. In a



Written by [Brian Koenig](#) on February 14, 2012

recent news conference, Twitter CEO Dick Costolo attested that users of the micro-blogging website transmit an average of one billion tweets every three days.

For this reason, software developers would have to overcome an array of technological challenges, including teaching computers how to read data effectively. The programs must somehow compute the subtleties of meanings in tweets, messages, and blog posts to distinguish between a serious statement and a joke or meaningless quip.

For example, the information-gathering company Linguastat Inc. coordinated an effort with the Centers for Disease Control (CDC) during the 2009 swine flu outbreak to monitor public concerns on social media platforms to measure the reactions of the CDC's public health disclosures. However, Linguastat co-founder John Pierre acknowledged that tracing public sentiment goes far beyond extracting simple words or phrases. "Just because they mention it, do they like it, do they not, are they saying it in the right context? Is it a band called The Swine Flu?" Pierre asserted.

Moreover, the rising trend of "bots" — which have flooded platforms such as Twitter with junk posts similar to email spam — could throw off the data. This is significant because an onslaught of bot programs could dupe the tracking software into thinking that some social trend is occurring, when it's really not. "We have all the data. How do we know what's real and what's not?" said Tim Hwang, who has programmed his own bots to research just how effectively they can influence social networks.

Other critics question the government intrusions such methods will have on civil liberties. While the FBI was careful to note that its surveillance procedures adhere strictly to analyzing "publicly available" data, privacy advocates remain skeptical. For instance, argued Jennifer Lynch, an attorney for the Electronic Freedom Frontier, most social-media users anticipate that only their friends and approved followers are reading their posts, which grants them "the sense of freedom to say what they want without worrying too much about recourse... but these tools that mine open source data and presumably store it for a very long time, do away with that kind of privacy. I worry about the effect of that on free speech in the U.S."

Ginger McCall, head of the open government project at the Electronic Privacy Information Center, added that the U.S. government should not have the authority to monitor free speech without a narrow, targeted law enforcement purpose: "Any time that you have to worry about the federal government following you around peering over your shoulder listening to what you're saying, it's going to affect the way you speak and the way that you act."



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.