Print Close

Break the law and your new 'friend' may be the FBI

Published on 03-16-2010

Source: AP

WASHINGTON — The Feds are on Facebook. And MySpace, LinkedIn and Twitter, too.

U.S. law enforcement agents are following the rest of the Internet world into popular social-networking services, going undercover with false online profiles to communicate with suspects and gather private information, according to an internal Justice Department document that offers a tantalizing glimpse of issues related to privacy and crime-fighting.

Think you know who's behind that "friend" request? Think again. Your new "friend" just might be the FBI.

The document, obtained in a Freedom of Information Act lawsuit, makes clear that U.S. agents are already logging on surreptitiously to exchange messages with suspects, identify a target's friends or relatives and browse private information such as postings, personal photographs and video clips.

Among other purposes: Investigators can check suspects' alibis by comparing stories told to police with tweets sent at the same time about their whereabouts. Online photos from a suspicious spending spree — people posing with jewelry, guns or fancy cars — can link suspects or their friends to robberies or burglaries.

The Electronic Frontier Foundation, a San Francisco-based civil liberties group, obtained the Justice Department document when it sued the agency and five others in federal court. The 33-page document underscores the importance of social networking sites to U.S. authorities. The foundation said it would publish the document on its Web site on Tuesday.

With agents going undercover, state and local police coordinate their online activities with the Secret Service, FBI and other federal agencies in a strategy known as "deconfliction" to keep out of each other's way.

"You could really mess up someone's investigation because you're investigating the same person and maybe doing things that are counterproductive to what another agency is doing," said Detective Frank Dannahey of the Rocky Hill, Conn., Police Department, a veteran of dozens of undercover cases.

A decade ago, agents kept watch over AOL and MSN chat rooms to nab sexual predators. But those text-only chat services are old-school compared with today's social media, which contain mountains of personal data, photographs, videos and audio clips — a potential treasure trove of evidence for cases of violent crime, financial fraud and much more.

The Justice Department document, part of a presentation given in August by top cybercrime officials, describes the value of Facebook, Twitter, MySpace, LinkedIn and other services to government investigators. It does not describe in detail the boundaries for using them.

"It doesn't really discuss any mechanisms for accountability or ensuring that government agents use those tools responsibly," said Marcia Hoffman, a senior attorney with the Electronic Frontier Foundation.

The group sued in Washington to force the government to disclose its policies for using social networking sites in investigations, data collection and surveillance.

The foundation also obtained an Internal Revenue Service document that instructs employees on how to use to use Internet tools — including social networking sites — to investigate taxpayers. The document states that IRS employees are barred from using deception or creating fake accounts to get information, a directive the group says is commendable.

Covert investigations on social-networking services are legal and governed by internal rules, according to Justice Department officials. But they would not say what those rules are.

The Justice Department document raises a legal question about a social-media bullying case in which U.S. prosecutors charged a Missouri woman with computer fraud for creating a fake MySpace account — effectively the same activity that undercover agents are doing, although for different purposes.

The woman, Lori Drew, helped create an account for a fictitious teen boy on MySpace and sent flirtatious messages to a 13-year-old neighborhood girl in his name. The girl hanged herself in October 2006, in a St. Louis suburb, after she received a message saying the world would be better without her.

A jury in California, where MySpace has its servers, convicted Drew of three misdemeanor counts of accessing computers without authorization because she was accused of violating MySpace's rules against creating fake accounts. But last year a judge overturned the verdicts, citing the vagueness of the law.

"If agents violate terms of service, is that 'otherwise illegal activity'?" the document asks. It doesn't provide an answer.

Facebook's rules, for example, specify that users "will not provide any false personal information on Facebook, or create an account for anyone other than yourself without permission." Twitter's rules prohibit its users from sending deceptive or false information. MySpace requires that information for accounts be "truthful and accurate."

A former U.S. cybersecurity prosecutor, Marc Zwillinger, said investigators should be able to go undercover in the online world the same way they do in the real world, even if such conduct is barred by a company's rules. But there have to be limits, he said.

In the face-to-face world, agents can't impersonate a suspect's spouse, child, parent or best friend. But online, behind the guise of a social-networking account, they can.

"This new situation presents a need for careful oversight so that law enforcement does not use social networking to intrude on some of our most personal relationships," said Zwillinger, whose firm does legal work for Yahoo and MySpace.

Undercover operations aren't necessary if the suspect is reckless. Federal authorities nabbed a man

wanted on bank fraud charges after he started posting Facebook updates about the fun he was having in Mexico.

Maxi Sopo, a native of Cameroon living in the Seattle area, apparently slipped across the border into Mexico in a rented car last year after learning that federal agents were investigating the alleged scheme. The agents initially could find no trace of him on social media sites, and they were unable to pin down his exact location in Mexico. But they kept checking and eventually found Sopo on Facebook.

While Sopo's online profile was private, his list of friends was not. Assistant U.S. Attorney Michael Scoville began going through the list and was able to learn where Sopo was living. Mexican authorities arrested Sopo in September. He is awaiting extradition to the U.S.

The Justice document describes how Facebook, MySpace and Twitter have interacted with federal investigators: Facebook is "often cooperative with emergency requests," the government said. MySpace preserves information about its users indefinitely and even stores data from deleted accounts for one year. But Twitter's lawyers tell prosecutors they need a warrant or subpoena before the company turns over customer information, the document says.

"Will not preserve data without legal process," the document says under the heading, "Getting Info From Twitter ... the bad news."

Twitter did not respond to a request for comment for this story.

The chief security officer for MySpace, Hemanshu Nigam, said MySpace doesn't want to be the company that stands in the way of an investigation. "That said, we also want to make sure that our users' privacy is protected and any data that's disclosed is done under proper legal process," Nigam said.

MySpace requires a search warrant for private messages less than six months old, according to the company.

Facebook spokesman Andrew Noyes said the company has put together a handbook to help law enforcement officials understand "the proper ways to request information from Facebook to aid investigations."

The Justice document includes sections about its own lawyers. For government attorneys taking cases to trial, social networks are a "valuable source of info on defense witnesses," they said. "Knowledge is power. ... Research all witnesses on social networking sites."

But the government warned prosecutors to advise their own witnesses not to discuss cases on social media sites and to "think carefully about what they post."

It also cautioned federal law enforcement officials to think prudently before adding judges or defense counsel as "friends" on these services.

"Social networking and the courtroom can be a dangerous combination," the government said.

On the Net:

- Link to Justice Department document: http://tinyurl.com/yjc6mql