When tweets can make you a jailbird

March 16 2010, By RICHARD LARDNER , Associated Press Writer

In this Oct. 13, 2009, file photo, Assistant U.S. Attorney Michael Scoville displays part of the Facebook page, and an enlarged profile photo, of fugitive Maxi Sopo in Seattle. 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. (AP Photo/Elaine Thompson)

(AP) -- Maxi Sopo was having so much fun "living in paradise" in Mexico that he posted about it on Facebook so all his friends could follow his adventures. Others were watching, too: A federal prosecutor in Seattle, where Sopo was wanted on bank fraud charges.

Tracking Sopo through his public "friends" list, the prosecutor found his address and had Mexican authorities arrest him. Instead of sipping pina

coladas, Sopo is awaiting extradition to the U.S.

Sopo learned the hard way: The Feds are on Facebook. And MySpace, LinkedIn and Twitter, too.

Law enforcement agents are following the rest of the Internet world into popular social-networking services, even going undercover with false online profiles to communicate with suspects and gather private information, according to an internal Justice Department document that surfaced in a lawsuit.

The document shows that U.S. agents are 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 the 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 crime.

The Justice document also reminds government attorneys taking cases to trial that the public sections of social networks are a "valuable source" of information on defense witnesses. "Knowledge is power," says the paper. "Research all witnesses on social networking sites."

The Electronic Frontier Foundation, a San Francisco-based civil liberties group, obtained the 33-page document when it sued the Justice Department and five other agencies in federal court.

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 a potential treasure trove of evidence.

The document, part of a presentation given in August by cybercrime officials, describes the value of Facebook, Twitter, MySpace, LinkedIn and other services to 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, which sued to force the government to disclose its policies for using social networking.

The foundation also obtained an Internal Revenue Service document that states IRS employees cannot use deception or create fake accounts to get information.

Sopo's case didn't require undercover work; his carelessness provided the clues. But covert investigations on social-networking services are legal and governed by internal rules, according to Justice officials. They would not, however, say what those rules are.

The document addresses 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, posed as a teen boy and flirted with a 13-year-old neighborhood girl. 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. Drew was convicted of three misdemeanors for 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 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.

"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.

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."

The chief security officer for MySpace, Hemanshu Nigam, said

MySpace doesn't want to stand 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."

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