LAPTOP
THE PULSE OF MOBILE TECH

How Your Cellphone Lets the Government Track You

September 20th, 2011 by Jesse Emspak, SecurityNewsDaily

Big Brother may be watching you — but you won't necessarily be told about it.

Government agencies often ask for geolocation data about individual cellphones from cellular carriers, and they usually get it — even without a warrant.

In fact, such usage of cellular networks for surveillance purposes may be part of the "hidden interpretation" of the USA PATRIOT Act that two senators alluded to this past May — a suspicion that was only raised by the cryptic testimony of a National Security Agency lawyer to a congressional committee last month.

"There are certain circumstances where that authority may exist," said NSA general counsel Matthew Olsen, in response to a question by Sen. Ron Wyden, D-Ore., that asked whether the government thought it within its rights to "use cell site data to track the

Two weeks earlier, Sens. Ron Wyden, D-Ore., and Mark Udall, D-N.M., had sent a letter to Director of National Intelligence James Clapper asking point-blank if any law-abiding citizens had been tracked this way, and what authority the government had to do so.

Neither senator's office has said whether Clapper, or anyone else in the Obama administration, has responded.

Only the government knows

Wyden and Udall made headlines in May when they told the Senate that the Justice Department was interpreting an unspecified portion of the USA-Patriot Act to spy on Americans in a previously undisclosed manner.

As members of the Senate Select Committee on Intelligence, Wyden and Udall could not disclose exactly what they meant. But Wyden did say, during debate over the reauthorization of the Patriot Act, that "when the American people find out how their government has secretly interpreted the Patriot Act, they will be stunned and they will be angry."

“Americans would be alarmed if they knew how this law is being carried out,” said Udall.

Clear and not so clear

If the NSA or other government agencies are indeed using cellphone networks to track and locate Americans, it’s not exactly new.

Regulations requiring cellular service providers to locate handsets in case of emergencies date back to 1996. That’s one reason 911 operators ask you to stay on the line if you’re on a cellphone. Carriers have long been able to triangulate user locations by gauging distances from cellular towers, and it’s a small step to hand that data over to authorities if they ask for it.

Some judges will ask for warrants before approving such requests, but many won’t, said Chris Calabrese, legislative counsel at the American Civil Liberties Union in Washington D.C.

“Sometimes they try ‘magistrate shopping,’” Calabrese said.

When it comes to using GPS devices, which rely on satellites rather than cellular towers to locate individuals, it’s a murkier area.

The U.S. Supreme Court will decide this term the legal limits of using GPS devices to track suspects. The D.C. Circuit Court decided that law enforcement needs a warrant, but three others disagree, so the Department of Justice has asked the Supreme Court to decide.

Just a few weeks ago, a federal appeals panel in the District of Columbia upheld a ruling that the government needs to reveal how such information was used in cases where the suspect was convicted.

“The disclosure sought by the plaintiffs would inform this ongoing public policy discussion by shedding light on the scope and effectiveness of cell phone tracking as a law enforcement tool,” wrote Judge Merrick Garland in the 3-0 decision.

Because most smartphones have GPS units built in, a Supreme Court ruling mandating warrants could put more constraints on using geolocation data from those devices.

Technically speaking, tracking a cellphone’s location is easy. The most intrusive method would be to use a virus or malware that simply transmitted the location data from both Android and iPhone devices.

But for authorities, it’s easier to simply ask the phone carriers for the data.

Loose ends tied together?

So if geolocation of individual suspects is so well established, what are Udall and Wyden worried about?

Julian Sanchez, a research fellow at the Cato Institute, a Washington, D.C., libertarian think tank, wonders whether geolocation of American citizens is being done on a massive scale, with the results being fed through computers as part of a data-mining effort.

"It's one thing if [surveillance] involves suspects and their known associates," Sanchez told the International Business Times in a recent article. "It would be another thing altogether if it involved mining lots of people's records who had no first- or second-degree connection to the target of the investigation."

Such data mining for surveillance purposes has been going for decades in other areas. For example, the famous Echelon program has computers that listen to overseas calls, keeping electronic ears open for words like "bomb" and "terrorist."

Sanchez thinks the Justice Department might be tying together two previously unrelated sections of the Patriot Act: the "business-records" provision of the Patriot Act, Section 215, which allows for immediate seizure of all records belonging to a commercial enterprise, and the "pen register" provision, Section 214, which allows for wiretaps and phone tracing of anyone, whether a suspect or not.

"The business record provision [could] be tied to the pen registers to allow not just the acquisition of historical records but real-time tracking" of individuals, Sanchez told the IBT.

Usage of both provisions 214 and 215 requires approval by the secret Foreign Intelligence Surveillance Act (FISA) court. But the Bush administration routinely bypassed the FISA court, as was revealed in 2005 during the warrantless wiretapping controversy.

Do we care enough?

So what if the government's tracking our every move? Do the American people really care?

The truth is that geolocation data-abuse has become a big issue, not only with respect to governments, but regarding private entities as well.

Apple and Google were castigated by Sen. Al Franken, D-Minn., in May when it came out that individual iPhones and Android devices kept records of their own movements. Both companies have said the data is stripped of anything that could personally identify the user.

Sen. Wyden is co-sponsoring a bill that would restrict the use of location information and clarify the rules under which such eavesdropping can be done. Rep. Jason Chaffetz, R-Utah, is sponsoring another version in the House.

The bill, which has been referred to the Judiciary Committees of the Senate and House, requires warrants for getting geolocation data. (There are exceptions carved out for international terrorism investigations, emergencies, and cases in which parents want their children tracked.)

In the meantime, smartphone users can refuse to permit their devices to use location services if they aren't absolutely necessary, and remember to always encrypt backup data and to password-protect their devices.

The truly paranoid can do what Will Smith did in "Enemy of the State" and drop the phone into a Mylar potato-chip bag — or can just leave their phones turned off.

As Catherine Crump, a lawyer for the American Civil Liberties Union, which successfully fought to have the District of Columbia ruling upheld, put it, "I highly doubt that the 90 percent of Americans who carry cellphones thought that when they got cellphone service they were giving up their privacy in their movements."

Article provided by SecurityNewsDaily, a sister site to Laptopmag.com.