

The Snitch in Your Pocket

Law enforcement is tracking Americans' cell phones in real time—without the benefit of a warrant.

Amid all the furor over the Bush administration's warrantless wiretapping program a few years ago, a mini-revolt was brewing over another type of federal snooping that was getting no public attention at all. Federal prosecutors were seeking what seemed to be unusually sensitive records: internal data from telecommunications companies that showed the locations of their customers' cell phones—sometimes in real time, sometimes after the fact. The prosecutors said they needed the records to trace the movements of suspected drug traffickers, human smugglers, even corrupt public officials. But many federal magistrates—whose job is to sign off on search warrants and handle other routine court duties—were spooked by the requests. Some in New York, Pennsylvania, and Texas balked. Prosecutors "were using the cell phone as a surreptitious tracking device," said Stephen W. Smith, a federal magistrate in Houston. "And I started asking the U.S. Attorney's Office, 'What is the legal authority for this? What is the legal standard for getting this information?'"

Those questions are now at the core of a constitutional clash between President Obama's Justice Department and civil libertarians alarmed by what they see as the government's relentless intrusion into the private lives of citizens. There are numerous other fronts in the privacy wars—about the content of e-mails, for instance, and access to bank records and credit-card transactions. The Feds now can quietly get all that information. But cell-phone tracking is among the more unsettling forms of government surveillance, conjuring up Orwellian images of Big Brother secretly following your movements through the small device in your pocket.

How many of the owners of the country's 277 million cell phones even know that companies like AT&T, Verizon, and Sprint can track their devices in real time? Most "don't have a clue," says privacy advocate James X. Dempsey. The tracking is possible because either the phones have tiny GPS units inside or each phone call is routed through towers that can be used to pinpoint a phone's location to areas as small as a city block. This capability to trace ever more precise cell-phone locations has been spurred by a Federal Communications Commission rule designed to help police and other emergency officers during 911 calls. But the FBI and other law-enforcement outfits have been obtaining more and more records of cell-phone locations—without notifying the targets or getting judicial warrants establishing "probable cause," according to law-enforcement officials, court records, and telecommunication executives. (The Justice Department draws a distinction between cell-tower data and GPS information, according to a spokeswoman, and will often get warrants for the latter.)

The Justice Department doesn't keep statistics on requests for cell-phone data, according to the spokeswoman. So it's hard to gauge just how often these records are retrieved. But Al Gidari, a telecommunications lawyer who represents several wireless providers, tells NEWSWEEK that the companies are now getting "thousands of these requests per month," and the amount has grown "exponentially" over the past few years. Sprint Nextel has even set up a dedicated Web site so that law-enforcement agents can access the records from their desks—a fact divulged by the company's "manager of electronic surveillance" at a private Washington security conference last October. "The tool has just really caught on fire with law enforcement," said the Sprint executive, according to a tape made by a privacy activist who sneaked into the event. (A Sprint spokesman acknowledged the company has created the Web "portal" but says that law-enforcement agents must be "authenticated" before they are given passwords to log on, and even then still must provide valid court orders for all nonemergency requests.)

There is little doubt that such records can be a powerful weapon for law enforcement. Jack Killorin, who directs a federal task force in Atlanta combating the drug trade, says cell-phone records have helped his agents crack many cases, such as the brutal slaying of a DeKalb County sheriff: agents got the cell-phone records of key suspects—and then showed that they were all within a one-mile area of the murder at the time it occurred, he said. In the fall of 2008, Killorin says, his agents were able to follow a Mexican drug-cartel truck carrying 2,200 kilograms of cocaine by watching in real time as the driver's cell phone "shook



by **Michael Isikoff**

February 19, 2010

Nation

al gidari • cellular telephone • cell phones • person communication and meetings • department of justice • sprint nextel corporation

f t PRINT EMAIL COMMENT

Trending on Newsweek



How to Understand American Decline



What the JetBlue Guy Says About the Economy

cited in U.S. v. Pineda-Moreno, No. 08-30385 archived on August 26, 2010

hands" with each cell-phone tower it passed on the highway. "It's a tremendous investigative tool," says Killorin. And not that unusual: "This is pretty workaday stuff for us."

But there is also plenty of reason to worry. Some abuse has already occurred at the local level, according to telecom lawyer Gidari. One of his clients, he says, was aghast a few years ago when an agitated Alabama sheriff called the company's employees. After shouting that his daughter had been kidnapped, the sheriff demanded they ping her cell phone every few minutes to identify her location. In fact, there was no kidnapping: the daughter had been out on the town all night. A potentially more sinister request came from some Michigan cops who, purportedly concerned about a possible "riot," pressed another telecom for information on all the cell phones that were congregating in an area where a labor-union protest was expected. "We haven't even begun to scratch the surface of abuse on this," says Gidari.

That was precisely what Smith and his fellow magistrates were worried about when they started refusing requests for cell-phone tracking data. (Smith balked only at requests for real-time information, while other magistrates have also objected to requests for historical data on cell-phone locations.) The grounds for such requests, says Smith, were often flimsy: almost all were being submitted as "2703(d)" orders—a reference to an obscure provision of a 1986 law called the Stored Communications Act, in which prosecutors only need to assert that records are "relevant" to an ongoing criminal investigation. That's the lowest possible standard in federal criminal law, and one that, as a practical matter, magistrates can't really verify. But when Smith started turning down government requests, prosecutors went around him (or "judge shopping," in the jargon of lawyers), finding other magistrates in Texas who signed off with no questions asked, he told NEWSWEEK. Still, his stand—and that of another magistrate on Long Island—started getting noticed in the legal community. Facing a request for historical cell-phone tracking records in a drug-smuggling case, U.S. magistrate Lisa Pupo Lenihan in Pittsburgh wrote a 56-page opinion two years ago that turned prosecutors down, noting that the data they were seeking could easily be misused to collect information about sexual liaisons and other matters of an "extremely personal" nature. In an unusual show of solidarity—and to prevent judge shopping—Lenihan's opinion was signed by every other magistrate in western Pennsylvania.

The issue came to a head this month in a federal courtroom in Philadelphia. A Justice Department lawyer, Mark Eckenwiler, asked a panel of appeals-court judges to overturn Lenihan's ruling, arguing that the feds were only asking for what amounted to "routine business records." But he faced stiff questioning from one of the judges, Dolores Sloviter, who noted that there are some governments, like Iran's, that would like to use such records to identify political protesters. "Now, can the government assure us," she pressed Eckenwiler, that Justice would never use the provisions in the communications law to collect cell-phone data for such a purpose in the United States? Eckenwiler tried to deflect the question, saying he couldn't speak to "future hypotheticals," but finally acknowledged, "Yes, your honor. It can be used constitutionally for that purpose." For those concerned about what the government might do with the data in your pocket, that was not a comforting answer.

   PRINT EMAIL COMMENT

Next: Virginia to Challenge Obama's 'Individual Mandate' »

More on Newsweek





Search **SEARCH**

Topics »

- Nation**
- Politics**
- World**
- Business**
- Culture**
- Health**

- The Gaggle** Press, Politics and Absurdity
- Declassified** Investigative Reporting in Real Time
- Tectonic Shifts** Dialed In. Wired Up.
- The Human Condition** Mind. Body. Culture.
- Jobbed** How America Works Now

Stories »

- The Case Against Celebrity Gossip
- Religious Pluralism at Ground Zero?
- Alvin Greene's Howls of Desperation
- 'The Big C' Is No Cancer Comedy
- We Read It: 'Packing for Mars'

Authors »

- | | | |
|----------------|----------------|---------------------|
| Jon Meacham | Sharon Begley | Daniel Lyons |
| Fareed Zakaria | Howard Fineman | Lisa Miller |
| Jonathan Alter | Daniel Gross | Robert J. Samuelson |
| Julia Baird | Raina Kelley | George F. Will |

msnbc.com

- Court halts California gay marriages pending ...
- Photos of accused 9/11 plotter surface
- Thai slaying: Brit, American drawn to kickboxing

Slate

- Slate V: Those Pesky Activist Judges
- What Paul Krugman, Rachel Maddow, and the press ...
- Mad Men, Season 4: Drunk typing.

TheStreet

- Feds Failed on For-Profit Schools - Today's ...
- Mid-Year Tax Check: Organize Now, Save Later
- Education Stocks in Freefall

The Washington Post

- Plan for the midterms? Democrats aren't sure.
- Petraeus: War strategy on track
- Avastin faces federal review

Aol News.

- 'Don't Ask, Don't Tell' Discharges Hit Lesbians ...
- Teen Charged With Vehicular Homicide Sues ...
- Bloomberg: A 'Sad Day' If Mbsque Opponents Win

cited in U.S. v. Pineda-Moreno, No. 08-30385 archived on August 26, 2010