

# **EXHIBIT 6**

## The New York Times

Reprints

This copy is for your personal, noncommercial use only. You can order presentation-ready copies for distribution to your colleagues, clients or customers [here](#) or use the "Reprints" tool that appears next to any article. Visit [www.nytreprints.com](http://www.nytreprints.com) for samples and additional information. [Order a reprint of this article now.](#)

March 31, 2012

# Police Are Using Phone Tracking as a Routine Tool

By **ERIC LICHTBLAU**

WASHINGTON — Law enforcement tracking of cellphones, once the province mainly of federal agents, has become a powerful and widely used surveillance tool for local police officials, with hundreds of departments, large and small, often using it aggressively with little or no court oversight, documents show.

The practice has become big business for cellphone companies, too, with a handful of carriers marketing a catalog of “surveillance fees” to police departments to determine a suspect’s location, trace phone calls and texts or provide other services. Some departments log dozens of traces a month for both emergencies and routine investigations.

With cellphones ubiquitous, the police call phone tracing a valuable weapon in emergencies like child abductions and suicide calls and investigations in drug cases and murders. One police training manual describes cellphones as “the virtual biographer of our daily activities,” providing a hunting ground for learning contacts and travels.

But civil liberties advocates say the wider use of cell tracking raises legal and constitutional questions, particularly when the police act without judicial orders. While many departments require warrants to use phone tracking in nonemergencies, others claim broad discretion to get the records on their own, according to 5,500 pages of internal records obtained by the [American Civil Liberties Union](#) from 205 police departments nationwide.

The [internal documents](#), which were provided to The New York Times, open a window into a cloak-and-dagger practice that police officials are wary about discussing publicly. While cell tracking by local police departments has received some limited public attention in the last few years, the A.C.L.U. documents show that the practice is in much wider use — with far looser safeguards — than officials have previously acknowledged.

The issue has taken on new legal urgency in light of a Supreme Court ruling in January finding that a Global Positioning System tracking device placed on a drug suspect’s car

violated his Fourth Amendment rights against unreasonable searches. While the ruling did not directly involve cellphones — many of which also include GPS locators — it raised questions about the standards for cellphone tracking, lawyers say.

The police records show many departments struggling to understand and abide by the legal complexities of cellphone tracking, even as they work to exploit the technology.

In cities in Nevada, North Carolina and other states, police departments have gotten wireless carriers to track cellphone signals back to cell towers as part of nonemergency investigations to identify all the callers using a particular tower, records show.

In California, state prosecutors advised local police departments on ways to get carriers to “clone” a phone and download text messages while it is turned off.

In Ogden, Utah, when the Sheriff’s Department wants information on a cellphone, it leaves it up to the carrier to determine what the sheriff must provide. “Some companies ask that when we have time to do so, we obtain court approval for the tracking request,” the Sheriff’s Department said in a written response to the A.C.L.U.

And in Arizona, even small police departments found cell surveillance so valuable that they acquired their own tracking equipment to avoid the time and expense of having the phone companies carry out the operations for them. The police in the town of Gilbert, for one, spent \$244,000 on such equipment.

Cell carriers, staffed with special law enforcement liaison teams, charge police departments from a few hundred dollars for locating a phone to more than \$2,200 for a full-scale wiretap of a suspect, records show.

Most of the police departments cited in the records did not return calls seeking comment. But other law enforcement officials said the legal questions were outweighed by real-life benefits.

The police in Grand Rapids, Mich., for instance, used a cell locator in February to find a stabbing victim who was in a basement hiding from his attacker.

“It’s pretty valuable, simply because there are so many people who have cellphones,” said Roxann Ryan, a criminal analyst with Iowa’s state intelligence branch. “We find people,” she said, “and it saves lives.”

Many departments try to keep cell tracking secret, the documents show, because of possible backlash from the public and legal problems. Although there is no evidence that the police

have listened to phone calls without warrants, some defense lawyers have challenged other kinds of evidence gained through warrantless cell tracking.

“Do not mention to the public or the media the use of cellphone technology or equipment used to locate the targeted subject,” the Iowa City Police Department warned officers in one training manual. It should also be kept out of police reports, it advised.

In Nevada, a training manual warned officers that using cell tracing to locate someone without a warrant “IS ONLY AUTHORIZED FOR LIFE-THREATENING EMERGENCIES!!” The practice, it said, had been “misused” in some standard investigations to collect information the police did not have the authority to collect.

“Some cell carriers have been complying with such requests, but they cannot be expected to continue to do so as it is outside the scope of the law,” the advisory said. “Continued misuse by law enforcement agencies will undoubtedly backfire.”

Another training manual prepared by California prosecutors in 2010 advises police officials on “how to get the good stuff” using cell technology.

The presentation said that since the Supreme Court first ruled on wiretapping law in 1928 in a Prohibition-era case involving a bootlegger, “subtler and more far-reaching means of invading privacy have become available to the government.”

Technological breakthroughs, it continued, have made it possible for the government “to obtain disclosure in court of what is whispered in the closet.”

In interviews, lawyers and law enforcement officials agreed that there was uncertainty over what information the police are entitled to get legally from cell companies, what standards of evidence they must meet and when courts must get involved.

A number of judges have come to conflicting decisions in balancing cellphone users’ constitutional privacy rights with law enforcement’s need for information.

In a 2010 ruling, the United States Court of Appeals for the Third Circuit, in Philadelphia, said a judge could require the authorities to obtain a warrant based on probable cause before demanding cellphone records or location information from a provider. (A similar case from Texas is pending in the Fifth Circuit.)

“It’s terribly confusing, and it’s understandable, when even the federal courts can’t agree,” said Michael Sussman, a Washington lawyer who represents cell carriers. The carriers “push back a lot” when the police urgently seek out cell locations or other information in what are

purported to be life-or-death situations, he said. “Not every emergency is really an emergency.”

Congress and about a dozen states are considering legislative proposals to tighten restrictions on the use of cell tracking.

While cell tracing allows the police to get records and locations of users, the A.C.L.U. documents give no indication that departments have conducted actual wiretapping operations — listening to phone calls — without court warrants required under federal law.

Much of the debate over phone surveillance in recent years has focused on the federal government and counterterrorism operations, particularly a once-secret program authorized by President George W. Bush after the Sept. 11 attacks. It allowed the National Security Agency to eavesdrop on phone calls of terrorism suspects and monitor huge amounts of phone and e-mail traffic without court-approved intelligence warrants.

Clashes over the program’s legality led Congress to broaden the government’s eavesdropping powers in 2008. As part of the law, the Bush administration insisted that phone companies helping in the program be given immunity against lawsuits.

Since then, the wide use of cell surveillance has seeped down to even small, rural police departments in investigations unrelated to national security.

“It’s become run of the mill,” said Catherine Crump, an A.C.L.U. lawyer who coordinated the group’s gathering of police records. “And the advances in technology are rapidly outpacing the state of the law.”