The New American

# *More Police Agencies Using Warrantless Cell Phone Tracking in Surveillance*

**Written by Dave Bohon**
**Thursday, 05 April 2012 09:25**

Law enforcement agencies around the nation are increasingly turning to tracking cell phones in surveillance operations, and, according to a recent report by the ACLU, they are doing so largely without the benefit of a warrant. According to the secular legal group, many of the more than 200 police departments that responded to the ACLU survey on their use of such tracking said that their officers do not bother with a warrant to access such investigative resources.

According to the *New York Times*, many police departments insist that with the ubiquitous presence of cell phones, tracking them has become "a valuable weapon in emergencies like child abductions and suicide calls and investigations in drug cases and murders." The *Times* cited one police training manual as describing cell phones as "the virtual biographer of our daily activities," tracking individuals' calls, travel, Internet activity, personal and business contacts, and more.

Predictably, cell phone companies have discovered that such law enforcement activity has the potential of providing them with a unique and lucrative revenue stream. The *Times* noted that some companies are now "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."

But groups such as the ACLU argue that the practice rides roughshod over the Constitution's Fourth Amendment prohibition against the unreasonable search of an individual's person or effects. "While many departments require warrants to use phone tracking in non-emergencies," reported the *Times*, "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."

“What we have learned is disturbing,” ACLU spokeswoman Catherine Crump said of her group’s research. “The government should have to get a warrant before tracking cell phones. That is what is necessary to protect Americans’ privacy, and it is also what is required under the Constitution.” She noted that the fact some law enforcement agencies do get warrants demonstrates that “a probable-cause requirement is a completely reasonable and workable policy, allowing police to protect both public safety and privacy.”

Interest in the issue has peaked since the Supreme Court ruled in January that law enforcement officials violated a suspected drug dealer’s Fourth Amendment guarantees after they placed a Global Positioning System (GPS) device on his car to track his whereabouts. Although the ruling did not directly target cell phones, legal experts said that since most smart phones include GPS technology they would likely fall under a similar ruling.

In its research the ACLU found a wide range of responses by police wishing to access cell phone data. A few agencies appear to genuinely try to follow what they perceive to be the proper legal requirements, while others seem to close their eyes even to the spirit of the law. One Utah sheriff’s department, for example, leaves it up to the cell phone company to decide how far police must go to cover the legal requirements. “Some companies ask that when we have time to do so, we obtain court approval for the tracking request,” that agency told the ACLU.

Whether small or large, however, all law enforcement agencies agree that using cell phone tracking has become a surveillance tactic of choice. In Arizona, reported the *Times*, “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.”

Even as debate increases about how far police can go, law enforcement experts say that many departments are willing to bend the perceived rules because of the benefit. “It’s pretty valuable, simply because there are so many people who have cellphones,” Roxann Ryan, a criminal analyst with Iowa’s state intelligence branch, insisted to the *Times*. “We find people,” she said, adding the caveat that exploiting such technology might even “saves lives.”

According to columnist James Temple, writing in the *San Francisco Chronicle*, the rule bending includes exerting whatever pressure is necessary on cell phone service carriers to compel them to release desired data to law enforcement. Temple cited, for example, materials from New Hampshire-based NTI Law Enforcement Systems, a company that trains police in accessing and analyzing phone data. In one segment on how to pressure phone companies to relinquish text message data, NTI training materials advise that phone company personnel “will tell you it can’t be done or they may tell you they just won’t do it. Don’t believe them; it can be done; you just have to exert the proper amount of legal and ‘other’ force.”

Temple noted that other NTI materials "suggest getting the phone company to help 'clone' a cell phone, so that investigators can intercept a text message while the intended recipient's phone is turned off." Another document obtained by the ACLU from the Irvine, California police department "included templates for demanding cell phone data from Apple, Google, and others," Temple wrote. "One example included a fill-in-the-blank line about the phone in question, followed by this instruction: 'It is hereby further ordered that Apple shall assist law enforcement in searching the cell phone, assistance that shall include, but is not limited to, bypassing the Cell Phone user's passcode.'"

Since existing court cases on the issue tend to provide contradictory guidance for law enforcement, "orders" such as the one above have little or no legal force behind them, relying instead on pure police bluff.

Julian Sanchez of the Cato Institute advised his readers not to be surprised if they're not aware of such surveillance taking place in their community, It probably is anyway. "Training materials obtained by the ACLU instruct police to never mention such tracking capabilities when speaking to media, and to omit them as far as possible from police reports," Sanchez noted. "The goal, no doubt, is to avoid reminding criminals that any powered-on phone is a potential tracker."

But there is a more sinister angle, as well, Sanchez added, warning it "also means that a signally intrusive form of government monitoring has become widespread with minimal public awareness, let alone discussion or debate. Let's hope media attention to these disclosures changes that."