

THE HEARTLAND INSTITUTE

19 South LaSalle Street #903
Chicago, IL 60603
phone 312/377-4000 · fax 312/377-5000
<http://www.heartland.org>

Law Enforcement Use of Cell Info Raises New Privacy Concerns

Author: Celeste Ward Altus
Published by: The Heartland Institute
Published in: *Info Tech & Telecom News*
Publication date: July 2008

With cell phones currently more common than traditional landlines, law enforcement now often relies on data provided by wireless companies to help solve crimes.

But in missing-persons cases there is an unusual circumstance: Until a crime is suspected, no warrant can be issued. That changes the dynamics surrounding whether and how wireless providers disclose customer records to police.

Wireless companies don't hand out customer data for every request by a law enforcement authority. Without a warrant, authorities must present a compelling case why the customer information is vital to someone's safety, says Jonathan Kramer, an attorney with Kramer Telecom Law Firm in Los Angeles. Kramer says the information is neither easy to obtain nor free, as some companies charge a fee.

Erratic Availability

Robert O'Leary, a state police retiree and consultant and instructor for Warrington, Pennsylvania-based BK Forensics, a computer and cell phone forensics firm, said law enforcement agencies rarely have trouble accessing information from cellular service providers if the request to produce or preserve the records is received within the service provider's retention period. Because there is no mandated record retention period, law enforcement agencies experience varying degrees of success depending on the service provider's retention policy.

"Most of the carriers are generally willing to assist law enforcement, provided they can justify the authority under which the records are requested," O'Leary said. "Often, those records are pulled and provided in response to court orders. In cases of clearly articulated emergent need, service providers can produce the records based on verbal justification or authority pending delivery of the court order."

Potential for Misuse

There is a potential for misuse in some missing-persons cases, O'Leary notes. Law enforcement has to be able to discern whether a missing adult has vanished on purpose, for example, as an escape from an abusive spouse or partner. In that case the danger is in aiding the abuser by providing the location of the missing person.

However, O'Leary said, "Any abuses, such as acquisition of records without proper justification or authority, or any other misuse would render those records unusable. They can be submitted as evidence only if they were properly obtained within or under the prevailing rules of evidence."

Across the country, O'Leary said, "every day and multiple times per day" carriers are requested to provide records to law enforcement in the course of investigations, and do so.

Privacy Issues

Kramer says consumers often misunderstand their privacy rights. Though the content of phone calls is private, a cell phone number is property of the wireless provider, and thus can be tracked and used as the provider sees fit. As with banking records, people give up a certain level of privacy when they choose to use a cell phone, because their location and activity can be traced.

"We live in a very networked world," Kramer noted. "People have a higher expectation of privacy than actually exists."

Bonnie Russell, founder of FamilyCourtLaw.com and an expert in family cases, says she is not happy with the level of government use of cell phone records.

"People should know there are no 'boundaries,'" Russell said. "I think most Americans realize there is no privacy, period. So it seems silly to pretend otherwise."

Policy Concerns

O'Leary, by contrast, is concerned company policies may cause important information to be lost. Policymakers should establish mandated retention periods for telecommunication records to ensure such records are available to law enforcement as investigations proceed, O'Leary said. In many cases the records are available for only a short time, such as a billing period.

In the course of an investigation, law enforcement may not become aware of the existence of telecommunications records immediately, and when they do become aware of the records, the service provider's retention period may have lapsed, O'Leary notes.

Celeste Ward Altus (celeste.altus@gmail.com) writes from San Francisco, California.