

[◀ Back to Article](#)[🖨 Click to Print](#)

Wednesday, Aug. 15, 2007

What Your Cell Knows About You

By Hilary Hylton/Austin

From crucial tracking evidence in the Scott Peterson murder trial to exculpatory call records in the Duke alleged rape case, cell phones have emerged as an important resource for both criminal investigators and defense lawyers. Now a small group of international forensic code breakers is working to go beyond the obvious and familiar — the call logs and address books — and tap deeper into our phones, into a hidden gold mine of personal information. Their work is prompting kudos from crime busters while raising concern among civil libertarians.

"Cell phones are ubiquitous in today's world and nearly all crimes have a digital component to them," says Rick Mislán, an assistant professor of computer and information technology at Purdue University. Mislán, a former U.S. Army electronic warfare officer, is one of a handful of experts working on forensic methods to access the inner secrets in cell phones. Twenty years ago it would have taken a police agency months of shoe leather and paper hunting to assemble the kind of information that is available on a cell phone's internal memory and which can be extracted by a deep probe. Says Chris Calabrese of the American Civil Liberties Union technology and liberty program: "They contain a great amount of information that essentially is a subjective picture of our habits, our friends, our interests and activities, and now some even have location tracking."

Most cell phone owners think simply removing a phone's SIM card removes personal information, but the phone's internal memory, even communication exchanged between the phone and its server, remain. Phone manuals detail how to perform multiple reset commands to erase personal information and some online recycling phone services offer command sets for specific phones, but most people never bother to go through the tedious process, Mislán says. For example, child predators who stalk "moblogs" — the cell phone equivalent of web blogs that are popular with young phone users — may believe they have deleted text messages and postings, but the evidence may still exist within the phone's memory. Mislán recently

examined the cell phone of an alleged child pornography ringleader and pulled off 250 "deleted" contacts from its memory.

However, few U.S. law enforcement agencies have the forensic tools at hand and criminals often exploit that advantage, stymieing investigators with simple if crude methods. Drug dealers, Mislan says, will buy throwaway phones, assign distinctive rings to customers or suppliers, and then destroy the screen, leading an arresting officer to believe the phone is broken or the phone's information is inaccessible. (Old-style forensics often means laboriously photographing cell phone screen after cell phone screen to record evidence.)

Typically, law enforcement agencies rely on simply "thumbing through" a cell phone to retrieve data, says Sgt. Michael Harrington, a detective with the Michigan State police. Another tool, as anyone who has watched the nightly cable crime news shows knows, is "pinging" a phone to search for its location, helpful in missing-persons cases and in tracking suspects. A more complex forensic approach now available utilizes a command system developed in the late 1970s to initialize modems to ask the phone specific questions about the information it may be storing. Those commands, known as AT, were one of the tools 17-year-old hacker George Hotz used to unlock his iPhone from the AT&T network. "Coming into this project I didn't know that cell phones used AT commands," Hotz wrote on his blog last week, as he thanked his fellow hackers for their help.

But not all cell phones respond to modem-style commands and some cell phone developers are often loath to share their proprietary technology. Nokia phones are particularly hard to crack, Harrington says. In the U.S. alone there are over 2,000 models of phones — and even within one model line there may be a dozen phones using different codes for each function. "We are in a constant state of catch-up — a company rolls out new models every three to six months," Mislan says. The Holy Grail for the cell phone code breakers is to develop a forensics tool — a "Swiss Army knife" as Harrington calls it — that can be used easily in the field.

Europe's single, standardized GSM network, as opposed to the multi networks — GSM, CDMA and iDEN found in the U.S. — gave European forensics investigators an edge as they began to develop ways of accessing a phone's internal memory. Two of the leading cell phone forensics experts are British — West Yorkshire Detective Constables Steve Hirst and Steve Miller. Like their American colleagues — "tinkerers" as Mislan calls them — the two spend their evenings buying up old cell phones on eBay, deconstructing and decoding them, and then sharing their research online with colleagues around the world.

In Europe, Constable Miller says, so-called "flasher boxes" are used to hold a cell phone's memory while

repairs are under way. The boxes are the size of a deck of cards and come with about 100 cables that can be connected to specific data points on different phones and offer direct access to memory. Flasher technology allows the investigator to do a "hex dump" of the cell phone's memory — a large amount of hexadecimal code — and then write software to decode the information. It is not the 30-second process seen on the popular *CSI* television shows, but can take hours of downloading, followed by days and weeks of software development, but the results can be revealing. "You get a fingerprint of who the person is," says Harrington. Recently, Dutch forensics experts were able to extract vital information via hex dump from the remains of a phone, shattered and soaked in blood and water. "Let's talk about hex!" is the slogan on phone-forensics.com, a popular online forum where the code breakers chat.

Meanwhile, the demands on the code breakers exceed their ranks, despite a growing number of computer and cell phone forensics programs at U.S. universities. Recently, an Indiana state prison official handed Mislán a bag of smuggled phones confiscated from inmates who are suspected of using them to conduct criminal activities from behind bars, but Mislán says that because of other investigative work, it will be six to 12 months before he has the time to take a look at them.

The legal system also is not keeping pace with forensic investigation methods. There have been several conflicting appellate opinions on warrantless cell phone searches and the law is not "settled" at this point, ACLU's Calabrese says. Just as emerging fingerprint and DNA technologies were challenged, cell phone evidence is under scrutiny. In the meantime, all of us — innocent citizen and criminals alike — continue to pump ever more data into cell phones and PDAs, those indispensable companions that have so much to say about us.

 [Click to Print](#)

Find this article at:

<http://www.time.com/time/health/article/0,8599,1653267,00.html>

Copyright © 2007 Time Inc. All rights reserved. Reproduction in whole or in part without permission is prohibited.

[Privacy Policy](#) | [Add TIME Headlines to your Site](#) | [Contact Us](#) | [Customer Service](#)