

The Spy in Your Pocket

Your mobile knows where you are—and, for a price, so can others

By KRISTINA DELL

WESLEY CLARK BUILT A CAMPAIGN for President as an expert in national security. But he recently discovered a hole in his personal security—his cell phone. A resourceful blogger, hoping to call attention to the black market in phone records, turned the general into his privacy-rights guinea pig in January. For \$89.95, he purchased, no questions asked, the records of 100 cell-phone calls that Clark had made. (He revealed the ruse to Clark soon after.) “It’s like someone taking your wallet or knowing who paid you money,” Clark says. “It’s no great discovery, but it just doesn’t feel right.” Since then, Clark has become a vocal supporter of the movement to outlaw the sale of cell-phone records to third parties.

The U.S.’s embrace of mobile phones—about 65% of the population are subscribers—has far outpaced efforts to keep what we do with them private. That has cleared the way for a cottage industry devoted to exploiting phone numbers, calling records and even the locations of unsuspecting subscribers for profit. A second business segment is developing applications like anonymous traffic monitoring and employee tracking. It’s not just the con artists who are a worry. Every new mobile-phone technology, even a useful, perfectly legal one, comes with unintended privacy concerns.

Clark’s allies in Congress drafted a bill to ban the sale of wireless-phone records, but it stalled in the Senate last week. In the meantime, spy outfits pose as subscribers to obtain records, then sell them to private investigators, divorce lawyers or anyone else with a credit card. Verizon Wireless and other carriers shut down one notorious data broker, Locatecell.com. “There are thousands of companies doing this,” says Robert Douglas, a security consultant and former private investigator. He notes that

WHO'S KEEPING AN EYE ON YOU?

Fraudsters can grab your call records and sell them to third parties for profit

Cell phones can be triangulated to within about 300 yards. Police with a court order can then track the movements of suspects

Using collated GPS data, officials can alert drivers via cell phone about gridlock and reroute them

Employers can know when you're playing hooky, thanks to a program embedded in your company phone

there are about 60,000 licensed private investigators in the U.S. “Unfortunately, anyone worth his salt knows who to turn to for phone records,” he says. Wireless carriers are also revamping their practices to deter infiltration. Most will no longer release calling records by fax or e-mail. They have even tightened rules about giving records to people who claim to have lost a cell phone.

Before widespread cell-phone use, lawmakers tried to address privacy with the

Telecommunications Act of 1996. But it appears the law never envisioned the booming software industry that grew out of the demand for wireless-phone data. Most mobile phones are powerful tracking devices, with global-positioning systems (GPS) inside. Companies like Xora combine GPS data with information about users to create practical applications. One similar technology allows rental-car companies to track their cars with GPS. California imposed restrictions on the practice last year after a company fined a customer \$3,000 for crossing into Nevada, violating the rental contract.

Other applications have not yet been challenged. For about \$26 a month per employee, a boss can set up a “geofence” to track how workers use company-issued cell phones or even if they go home early. About 1,000 employers use the service, developed by Xora with Sprint-Nextel.

The companies selling those services insist that they care about privacy. AirSage, for example, gets data from wireless carriers to monitor drivers’ cell-phone signals and map them over road grids. That lets it see exactly where gridlock is forming and quickly alert drivers to delays and alternative routes. The data it gets from carriers are aggregated from many users and scrambled, so no one can track an individual phone. “No official can use [the data] to give someone a speeding ticket,” says Cy Smith, CEO of AirSage.

Privacy advocates say that even with those safeguards, consumers should have a choice about how their information is used. Even anonymous data could, for example, reveal where a large group of people is headed for a protest. “These programs start out with the best intentions, but they expand,” says Barry Steinhardt, director of the Technology and Liberty Program at the A.C.L.U. Some responsibility, of course, rests with the individual. Since his data were revealed, Clark took his mobile number off his business cards. Wireless carriers also recommend that customers avoid giving out their mobile numbers online. But Clark insists that the law should change to protect our privacy, no matter how much technology allows us to connect. “One thing we value in this country,” he says, “is the freedom to be left alone.” ■