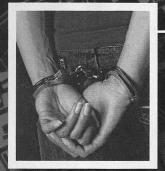
Police get cellphone data from phone companies to challenge a suspect's alibi.



FINDING A MISSING PERSON:

Using the GPS locator in a victim's cellphone, police can track the person in real time.

CASTING A NET: By getting lists of all cellphones using a particular tower at a particular time, police can find out who was in the vicinity of a crime scene.



ARE YOU BEING TRACKED?

That cellphone in your pocket is actually a sophisticated tracking device, and police departments are using this technology to solve crimes. What does that mean for your right to privacy?

BY PATRICIA SMITH

n the morning of Nov. 16, 2011, a student was kidnapped in a parking lot at Southern State Community College in Sardinia, Ohio, as she made her way to class. Her attacker threw her in the back of a pickup truck, locked her under a fiberglass cover, and sped away undetected.

But the young woman was saved by her cellphone. Using software that tracks someone's whereabouts by the GPS signal on their phone, police were able to intercept the truck on a remote country road—just 21 minutes after she called 911.

"Without it, she would have never been found," says Lt. Jim Heitkemper of the Adams County Sheriff's Office in West Union, Ohio. "She had no way of even knowing where she was because she couldn't see where she was going." Until recently, cellphone tracking technology was used mainly by federal agents in counter-terrorism operations and drug investigations. Now, police departments across the country are increasingly using cellphone surveillance—often with little or no court oversight.

Public Safety vs. Privacy Rights

The practice is raising concerns about civil liberties in a debate that pits public safety against privacy rights. The Fourth Amendment of the Constitution protects against "unreasonable searches and seizures." That's traditionally meant that police must have either a court-issued warrant or "probable cause" to search someone's property.

But the Framers couldn't have imagined technology like cellphones and global-positioning satellites. Both store vast amounts of personal information that can be accessed remotely and without the owner's knowledge. This raises the question of what constitutes an "unreasonable search and seizure" in the 21st century.

Existing laws do not provide clear guidance: Federal wiretap laws have been outpaced by technological advances; they don't explicitly cover the use of cellphone data to pinpoint a person's location, and local court rulings vary widely across the country (see box, facing page).

Police say phone tracking is a valuable weapon in emergencies like child abductions and suicide calls and in investigating things like drug cases and murders. In Wichita, Kansas, for example, police were recently able to track and rescue a young girl who was being taken out of state to be forced into prostitution. And cellphone records were key to the 2009 murder

conviction of a New York City nightclub bouncer who made several calls as he drove to a remote spot to dump a body.

But civil liberties advocates say cellphone tracking raises legal and constitutional questions, particularly when the police act without warrants.

How They Find You

Investigators can determine where someone's phone was by using phone records that show the phone's location at the beginning and end of a call. To track suspects or victims in real time, law enforcement officials must ask a phone company to "ping," or send a signal to, a phone. (The phone must be turned on, but it doesn't have to be in use.) The police can then use signal-tracking equipment to narrow down the location of the phone—and its owner.

The American Civil Liberties Union (ACLU), which has obtained phone-tracking records from more than 200 police departments, says both practices are in much wider use-with far looser safeguards—than previously acknowledged.

"It's become run-of-the-mill," says Catherine Crump, an ACLU lawyer. "And the advances in technology are rapidly outpacing the state of the law."

Congress and about a dozen states

Do electronic "searches"

violate the constitution?



are considering bills to tighten restrictions on the use of cellphone tracking.

The Supreme Court ruled last January that a GPS tracking device placed on a drug suspect's car without a warrant violated his Fourth Amendment rights against unreasonable searches. The ruling did not directly involve cellphones (many of which include GPS locators), but lawyers say it raised questions about the standards for cellphone tracking.

The practice has become big business

for wireless companies like Verizon, AT&T, and T-Mobile, which charge police departments surveillance fees to determine a suspect's location or trace calls and texts. Some departments log dozens of traces a month for both emergencies and routine investigations. Fees range from a few hundred dollars to more than \$2,000.

Lawyers and law enforcement officials agree there's uncertainty over what information the police are entitled to get without warrants from cell companies and when the courts must get involved. "It's terribly confusing, and it's understandable, when even the federal courts can't agree," says Michael Sussman, a Washington lawyer who represents cell carriers.

Some law enforcement officials say the legal uncertainties are outweighed by real-life benefits. The police in Grand Rapids, Michigan, for instance, used a cell locator last 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," says Roxann Ryan, a criminal analyst with Iowa's state intelligence branch. "We find people," she says, "and it saves lives."

What the courts have said about technology and the Fourth Amendment, which protects against "unreasonable searches and seizures"

GPS Tracking

The Supreme Court ruled earlier this year in United States v. Jones that placing a GPS tracking device on a drug suspect's car violated his Fourth Amendment right to privacy.

Cellphone Tracking

A judge can require police to get a warrant before obtaining cellphone records or location information from a cellphone company. The 2010 ruling came from the Third Circuit Court of Appeals in Philadelphia.

Warrantless Wiretapping

After the 9/11 attacks in 2001, President George W. Bush authorized the government to eavesdrop on phone calls and monitor the e-mails of terrorism suspects without obtaining warrants. In 2010, a federal judge ruled that the "warrantless wiretapping"program violated a 1978 federal law requiring court approval for domestic surveillance. The Obama administration says the program has been ended.

With reporting by Eric Lichtblau of The New York Times.