COULD YOUR PHONE TESTIFY AGAINST YOU?

PROSECUTORS ARE INCREASINGLY USING CELLPHONE DATA IN COURT, WHICH RAISES CONSTITUTIONAL ISSUES THAT PIT PUBLIC SAFETY AGAINST PRIVACY RIGHTS

By Anne Barnard

Mikhail Mallayev pleaded not guilty when he was charged in the contract killing of a New York orthodontist whose wife wanted him dead. While he stayed off his cellphone the morning of the shooting, he chatted away later, unaware that his phone was acting like a tracking device and would destroy his alibi—that he was not in New York the day of the killing—and lead to his conviction.

In another case, Darryl Littlejohn, a New York nightclub bouncer, made call after call on his cellphone as he drove from his home to a desolate part of Brooklyn to dump the body of the graduate student he was convicted last summer of murdering.

The pivotal role that cellphone records played in these two murder trials highlights the growing use in law enforcement of increasingly sophisticated cellular tracking techniques to keep tabs on suspects before they are arrested, and build criminal cases against them by mapping their past movements.

But cellphone tracking is raising concerns about civil liberties in a debate that pits public safety against privacy rights. Existing laws do not provide clear guidelines: Federal wiretap laws, outpaced by technological advances, do not explicitly cover the use of cellphone data to pinpoint a person's location, and local court rulings vary widely across the country.

In one case that unsettled cellphone companies, a sheriff in Alabama told a carrier he needed to track a cellphone in an emergency involving a child—she turned out to be his teenage daughter, who was late coming home from a date.

Cellphone tracking isn't the only way digital technology is challenging the legal system. More mistrials are being declared because jurors use their cellphones to do their own Internet research, upending centuries of legal procedure in which the judge decides what information the jury can hear.

Courts are also struggling with how to handle search warrants when they apply to digital information. The Fourth Amendment, which protects against "unreasonable searches and seizures," requires investigators to show probable cause and specify where they want to search and what they're looking for in order to get a warrant. While searching, if they find evidence of a different crime, they're allowed to act on that unexpected evidence if it's in "plain view."

The question now is, how does the concept of "plain view" apply to unexpected finds in computer files and cellphones?

THE IMPACT OF G.P.S.

The ability to track suspects' movements through their cellphones has been a boon to law enforcement, as more phones are equipped with global-positioning technology that makes it possible to pinpoint a user's location within a few dozen yards.

To determine where a suspect's phone was in the past—as in the Mallayev and Littlejohn cases—investigators use phone-company records that show a phone's approximate location at the beginning and end of a call. To track suspects 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 for

the "ping" to work, though it doesn't have to be in use.) The police can then use a vehicle with signal-tracking equipment to narrow down the phone's—and the suspect's—location.

The frequency and ease with which law enforcement agencies can access cellphone data to track people is hard to assess. Civil liberties groups recently obtained data from the Justice Department showing that in some jurisdictions, including Florida and New Jersey, courts often allow prosecutors to track the location of cellphone users in real time without warrants.

Google recently announced that it would require search warrants before releasing G.P.S. data that pinpoints the movements of customers who use its mapping applications—like Latitude, which lets people see where their friends are—on their phones.

But phone and Internet companies want Congress to clarify the laws. Civil liberties groups don't oppose using cellphone surveillance to solve crimes or save people in emergencies, but they worry that the current gray area in the law is allowing it to happen without much scrutiny or discussion.

'UNKNOWINGLY TWITTERING'

"The cost of carrying a cellphone should not include the loss of one's personal privacy," says Catherine Crump, a lawyer for the American Civil Liberties Union (A.C.L.U.). Civil libertarians claim that users whose phones have G.P.S.-based services are unwittingly creating records that could give the government easy access to their movements.

But law enforcement officials argue that people who obey the law have nothing to fear from cellphone tracking.

"Law enforcement has a responsibility to keep pace with the latest advances in technology in order to improve its efficiency in combating crime," says Richard A. Brown, a New York City prosecutor, adding that criminals are "unknowingly Twittering with law enforcement" whenever they use their cellphones.

Investigators have used cellphone tracking in a variety of ways: to trace a fugitive suspected of killing his wife to a wilderness park in Michigan; to seek a suspected serial killer eventually killed in a police shootout in Florida; and to trace a ransom call in a kidnapping and rescue the victim in New York.

The Federal District Court in Pittsburgh ruled last year that a search warrant was required even for historical phone-location records, which the government had requested to track a suspect in a drug case. The decision upheld a lower court ruling that people have a reasonable expectation of privacy regarding their physical location. Most Americans, the ruling said, do not know that their cellphones create a record of their movements and "would be appalled" to learn that the government can access it without showing probable cause. The Justice Department has appealed the case.

The A.C.L.U. and the Electronic Frontier Foundation, which defends digital rights, support the lower court's decision, and say laws are needed, as the foundation puts it, to "keep Big Brother out of your pocket." ●

Anne Barnard is a metro reporter for The New York Times.