The New York Times
nytimes.com

July 16, 2007

When the Trill of a Cellphone Brings the Clang of Prison Doors

By ANEMONA HARTOCOLLIS

It was a Perry Mason moment in the trial of Paul Cortez, an actor and yoga teacher who was ultimately convicted of killing his former girlfriend Catherine Woods, a dancer who was working as a stripper.

After weeks of testimony and a parade of witnesses, the case against Mr. Cortez boiled down to this: a bloody fingerprint and data collected from a cellphone.

A record from a T-Mobile cellphone transmission tower on the day Ms. Woods was murdered showed that Mr. Cortez called her 13 times in the hour and a half before her death, and then never again. He had told the police in a written statement that he made the calls from his home.

But as he called, the record showed his cell signal hitting a tower on East 105th Street, near his apartment, and gradually shifting to towers on East 86th and East 84th Streets, near Ms. Woods's apartment. At trial, when the prosecutor questioned him about the discrepancy, Mr. Cortez changed course, saying he had made some of the calls from a Starbucks.

Examining cellphone data is a technique that has moved from being a masterful surprise in trials to being a standard tool in the investigative arsenal of the police and prosecutors, with records routinely provided by cellphone companies in response to subpoenas. Its use in prosecutions is often challenged, for privacy reasons and for technical reasons, especially when the data comes during the morning or evening rush, when circuits are crowded and calls can be redirected to other towers. But it is often allowed and is used by both prosecutors and defense attorneys to buttress their cases.

"It's one of the most important developments in technology in the courtroom in the last five years," said Mark J. Geragos, a Los Angeles defense lawyer known for his celebrity clients, who challenged cell tower data while defending Scott Peterson, a Modesto, Calif., fertilizer salesman sentenced to death in 2005 for killing his pregnant wife, Laci.

Many people know that cellphones can be used as global positioning devices in real time. Yet few are aware that phone companies keep records from transmitters for months or longer that can be used to trace approximately where a caller was at the time a crime was committed.

“It’s another arrow in the quiver,” said Joyce B. David, a lawyer whose client Darryl Littlejohn, a nightclub bouncer, is facing trial in the death of Imette St. Guillen, a graduate student found strangled in February 2006. When he was arraigned, the police and prosecutors said cell tower records from the day of the killing indicated movement from his home to near the spot in Brooklyn where Ms. St. Guillen’s body was found.

Ms. David said she would challenge the trustworthiness of cell records.

Daniel Castleman, chief of investigations for the Manhattan district attorney, Robert M. Morgenthau, described tower data as “circumstantial but convincing.”

Defense lawyers have also begun using cellphone, or cell site, records to establish alibis.

In January, George A. Farkas, a defense lawyer, presented such records to a judge in Brooklyn to show that his client Eric Wright, accused of killing a drug dealer, was in Newark about 13 minutes after the killing, which took place in East New York, Brooklyn.

The assistant district attorney who was prosecuting the case, Kenneth Mark Taub, ridiculed the alibi, contending that while the phone might have been in Newark, the defendant was not. Mr. Taub suggested that cell tower technology could lead to a new tactic by criminals of planting their phones “in a place other than where they’re committing the crime.”

Mr. Farkas said in an interview that he got the idea of going to Sprint for transmitter data after a jailhouse interview with his client. As Mr. Farkas was leaving, he said, Mr. Wright told him, almost as an afterthought: “The only reason I knew this happened was I was on the phone, talking to my friend Chris. He was in East New York, around the corner from where the shooting was.”

Mr. Farkas added: “I’ve been doing this for 30 years, and cellphones are relatively new to me. But I know the issue is, was he using his cellphone? If he was using his cellphone, then he’s where the cellphone was.” Mr. Wright’s trial is scheduled to begin on Aug. 13.

In the Peterson case, prosecutors introduced cell tower records to show Mr. Peterson’s movements on the day his wife disappeared.

“One of the theories was that when he said he had left the house at 9:30, in fact around 9:50 or

9:46 his phone call pinged on a tower near the house," Mr. Geragos said in an interview.

Mr. Geragos conducted what legal observers have come to consider a groundbreaking cross-examination of the prosecution's expert witness, focusing on the flaws in cellphone transmitter technology. He managed to disqualify two witnesses, he recalled, and forced a third witness, a telephone company employee, to admit that when cellphone traffic is very heavy, a signal can be redirected to a nearby tower.

Ms. David, the lawyer for Mr. Littlejohn, said her search for an expert witness led her to Jeff M. Fischbach, an electronic evidence analyst and chief executive of Second Wave, a consulting firm. Mr. Fischbach said that his first exposure to cellphone data evidence was about four years ago, and that demand for his services to debunk transmitter data had risen rapidly since.

"The important thing about cell tower data is not what it proves, but what it can't prove," he said. "Cell tower data cannot place a person at an exact location. And even if it could, if the phone is not surgically implanted, you still can't prove it."

Gerald L. Shargel, a Manhattan defense lawyer, vividly remembers the first time a client was confronted with cell tower records, in the late 1990s. "It was one of the earliest cases where cell site information was introduced," he recalled.

His client was Gurmeet Singh Dhinsa, who rose from car wash attendant to millionaire gas station mogul. In 1999, Mr. Dhinsa was convicted in federal court in Brooklyn of racketeering and orchestrating two contract killings.

Mr. Dhinsa was not just a confident businessman, but also a confident cellphone user. Through tower records, prosecutors traced him to within a short distance of a killing at the time it took place.

That his approximate whereabouts could be traced through cellphone calls came as a total surprise to Mr. Dhinsa. "He didn't know," Mr. Shargel said. "I didn't know. We got late discovery. I was like, 'Cell sites? What the?' I didn't know anything about it. I quickly called some telephone expert. No one had ever heard of it, including the judge."

Cellphone users who commit crimes are often caught because they are creatures of habit, Mr. Castleman, of the Manhattan district attorney's office, said. "For the most part, people don't think about those things," he said. "Organized crime figures have known for a long time that we can tap cellphones, and yet they continue to talk on them. It's just human nature."

But occasionally, those with something to hide are more calculating, as prosecutors have described the hedge fund traders accused of hatching an insider-trading scheme during a meeting at the Oyster Bar in Grand Central Terminal. The traders used disposable cellphones, federal investigators said when they announced their investigation in March.

But Mr. Castleman warns that even throwaway phones leave users vulnerable. “I’m not sure I want to advertise it,” he said, “but yes, every time the criminals come up with a new way of using technology, there’s a countermeasure.”

-