The Washington Post

National Security

Secrecy around police surveillance equipment proves a case's undoing

By Ellen Nakashima February 22 at 3:10 PM

TALLAHASSEE — The case against Tadrae McKenzie looked like an easy win for prosecutors. He and two buddies robbed a small-time pot dealer of $130 worth of weed using BB guns. Under Florida law, that was robbery with a deadly weapon, with a sentence of at least four years in prison.

But before trial, his defense team detected investigators' use of a secret surveillance tool, one that raises significant privacy concerns. In an unprecedented move, a state judge ordered the police to show the device — a cell-tower simulator sometimes called a StingRay — to the attorneys.

Rather than show the equipment, the state offered McKenzie a plea bargain.

Today, 20-year-old McKenzie is serving six months' probation after pleading guilty to a second-degree misdemeanor. He got, as one civil liberties advocate said, the deal of the century. (The other two defendants also pleaded guilty and were sentenced to two years' probation.)

McKenzie's case is emblematic of the growing, but hidden, use by local law enforcement of a sophisticated surveillance technology borrowed from the national security world. It shows how a gag order imposed by the FBI — on grounds that discussing the device's operation would compromise its effectiveness — has left judges, the public and criminal defendants in the dark on how the tool works.

That secrecy, in turn, has hindered debate over whether the StingRay's use respects Americans' civil liberties.

"It's a terrible violation of our constitutional rights," asserted Elaine Harper, McKenzie's grandmother, who raised the young man. "People need to know — the public needs to know — what's going on."

The StingRay is a box about the size of a small suitcase — there's also a handheld version — that simulates a cellphone tower. It elicits signals from all mobile phones in its vicinity. That means it collects information not just about a criminal suspect's communications but also about the communications of potentially hundreds of law-abiding citizens.

The Tallahassee police used the StingRay or a similar device in more than 250 investigations over a six-year period, from mid-2007 through early 2014, according to a list of cases compiled by the Tallahassee Police Department and provided to the American Civil Liberties Union.

That's 40 or so instances a year in a city of 186,000, a surprisingly high rate given that the StingRay's manufacturer, Harris Corp., has told the Federal Communications Commission that the device is used only in emergencies. At least 48

state and local law enforcement agencies in 20 states and the District of Columbia have bought the devices, according to the ACLU.

The secrecy surrounding the device's use has begun to prompt a backlash in cities across the country. In Baltimore, a judge is pushing back against the refusal of police officers to answer questions while testifying. In Charlotte, following a newspaper investigation, the state's attorney is reviewing whether prosecutors illegally withheld information about the device's use from defendants.

In Tacoma, Wash., after a separate newspaper investigation found that judges in almost 200 cases had no idea they were issuing orders for the StingRay, the courts set new rules requiring police to disclose the tool's use. The state legislature is weighing a bill to regulate police use of the equipment.

The FBI and Tallahassee police say that the device is used only with an appropriate court order and that they do not collect the content of calls or text messages. The FBI also said it retains only location data that is relevant to an investigation and immediately discards all other data.

So far, there is virtually no case law on how the Fourth Amendment — which prohibits unreasonable searches and seizures — should apply to this technology.

Pot purchase gone wrong

The robbery, judging from police reports, legal documents and interviews, was small-time.

At about 6 p.m. on March 4, 2013, McKenzie, then 18, and two friends met a young man named Jamal Williams at a local Taco Bell. They had set up a deal to buy some marijuana from Williams, whom McKenzie had first met at a party, with the intent of robbing him of the dope.

During the robbery, one of McKenzie's buddies pulled what appeared to be a 9mm handgun out of his pocket, pointed it at Williams and demanded "everything you got."

The other friend removed what looked to be a shotgun from the trunk of a car and leveled it at Williams. "I'm not scared to put a hole in you," he said, Williams recalled.

Both weapons were BB guns. But they scared Williams enough that he gave the men the pot, left behind his iPhone and fled in a car driven by a friend who had escorted him to the Taco Bell.

That evening, Williams reported to police that he had been robbed of cash and his phone when he tried to buy marijuana from some dealers he did not know. Later he admitted that he, in fact, was the seller and assessed the stolen pot's value at $130.

The police had little to go on beyond vague descriptions of the three men, a license-plate number and a cellphone number that McKenzie had provided. A check of the tag number turned up nothing. McKenzie had not given his real name.

The day after the robbery, the police obtained a court order from a judge to authorize Verizon to hand over data collected from cell towers that would show the approximate locations where the phone in question had been used.

Two days after the robbery, shortly after 4 a.m., several police officers drove to a house at 3197 Springhill Rd., on the south side of town, and set up surveillance.

About 6 a.m., McKenzie left the house, got into his car and pulled away. The officers tailed him past Sam's Tires and Repairs, past the Family Dollar store, past Jerusalem Baptist Church, past Tony's Gas. Three and a half miles later, they pulled him over. The youth, a senior looking to graduate, had been on his way to school, which began at 6:45 a.m.

The police found some marijuana and zip-top bags in the car. They detained McKenzie and took him to the police station. He confessed, giving police the names of his two friends and showing investigators where they lived. All three were charged with robbery with a deadly weapon.

Tracing a phone's location

Months passed. The case dragged along.

In November 2013, after McKenzie's original lawyer dropped out, his case was assigned to a public defender, Carrie McMullen. Around that time, the attorney for one of the co-defendants began to wonder: How did the police figure out that McKenzie was at 3197 Springhill Rd. that morning?

McMullen's office hired a lawyer with technology expertise. John Sawicki, the expert, produced a map on which he plotted all the locations provided by Verizon, and they clumped in three different areas of town.

Cell-tower data can show general geographical areas where a phone was used, but "they will not tell you he's in House X," Sawicki said. "That's how imprecise it is."

In March, the defense team deposed police investigator Robert Newberry. The lawyers tried to get Newberry to explain how the police zeroed in on 3197 Springhill Rd. He mentioned the cell-tower records and then, under probing, acknowledged that they had not been sufficient on their own to locate the suspect.

He said a "Sergeant Corbitt" in the department's technical operations unit had identified the phone's location. "He would have to tell you how he got to that," Newberry said, referring to Christopher Corbitt, who handles electronic surveillance operations.

There were other questions about whether the police had reasonable suspicion to pull McKenzie over. The descriptions Williams gave of the suspects were vague, and in fact, none closely matched McKenzie's appearance.

The descriptions fit "two-thirds of the young black males living on the south side of town," Sawicki said.

Newberry could not fully explain how Corbitt determined the phone's location. "I can't address it because I don't know the magic behind it," he said.

In April, the defense team deposed Corbitt. He told the attorneys that he turned up the address on Springhill Road by running phone numbers that the suspect's phone had dialed through a subscription database, called Accurint, that helps law enforcement agencies locate individuals through data such as phone numbers, property records and court records.

But how did he know that the phone was in the house at 6 in the morning? The phone was a "burner" — one not registered under McKenzie's name.

"We do have specific equipment that allows us to . . . direction-find on the handset, if necessary," Corbitt said.

"What is that, and how does that work?" McMullen asked.

"I can't go into that," he said. "Due to [a] nondisclosure agreement with the FBI, we're not able to get into the details of how the equipment operates."

He acknowledged that the device was a cell-tower simulator.

He also acknowledged that the device, whose model name he could not give, was used to "assist in locating or determining the person in possession" of the cellphone, and that it could elicit signals from a target's phone even when the phone was not in use.

"It is not nearly as invasive or as sinister as it is sometimes characterized to be," he said.

"I so wish that I could tell you how this equipment operates, because I think I could put so many people at ease," Corbitt said. "Unfortunately, I am not able to do that."

He said that if the defense wanted more specific information, then he had "a specific protocol" to follow requiring him to notify the FBI and the Justice Department.

The Tallahassee police declined to comment for this article.

'100 percent' reliable

In June, in response to a motion for public access by the ACLU, the state released a transcript from a closed court hearing in 2010 relating to a Tallahassee rape case in which Corbitt testified that he had used a cell-site simulator to identify a suspect in an apartment complex. "In essence, we emulate a cellphone tower," he said. "We force that handset to register with us. We identify that we have the correct handset and then we're able to — by just merely direction-finding on the signal emanating from that handset — we're able to determine a location."

He noted that the equipment "is evaluating all the handsets in the area."

"Using portable equipment," he said, "we were able to actually basically stand at every door and every window in that complex and determine, with relative certainty . . . the particular area of the apartment that that handset was emanating from."

He said the Tallahassee police began using the device in the spring of 2007. From that point until August 2010, he said, the police had used it "200 or more times" to locate a cellphone.

How reliable was it? "Truthfully," he said, "100 percent."

In September, McMullen drew up a motion to suppress the evidence obtained against McKenzie prior to his arrest, alleging that his Fourth Amendment rights were violated by the use of the StingRay. She argued that the police had not obtained a warrant based on probable cause to use the device.

"By scooping up all manner of information from a target cellphone, as well as nearly all cellphones in the general area, a StingRay device engages in exploratory rummaging," she wrote.

McMullen also argued that the order the police did obtain not only failed to meet the requirements of a warrant but was also obtained without telling the judge that it would be used to operate a StingRay.

Then, in October, McMullen sought a subpoena to compel Corbitt to show the device in court. In November, Florida Circuit Court Judge Frank Sheffield held a hearing on the issue.

The state's attorney, Courtney Frazier, argued that details of the equipment's operation were protected from disclosure under a law enforcement exception to the state open-records law.

Sheffield broke in. "What right does law enforcement have to hide behind the rules and to listen in and take people's information like the NSA?" he said.

Frazier protested that the information about the device was sensitive and that disclosure could inhibit the police's ability to catch criminals.

"Inhibiting law enforcement's rights are second to protecting mine!" Sheffield thundered, gesturing with both hands and fixing his gaze on the prosecutor.

On Dec. 2, Sheffield signed the subpoena forcing Tallahassee police to show the device they used.

Two days before Corbitt was due to show up with the device, McMullen received notice of the plea deal from the prosecutor. She had never gotten such a sweet deal on a case.

The defense attorneys were disappointed that they would not see the device, but they couldn't refuse the plea bargain.

"How do you not take it?" Sawicki said. "How do you take these kids' future away?"

Julie Tate in Washington contributed to this report.

Ellen Nakashima is a national security reporter for The Washington Post. She focuses on issues relating to intelligence, technology and civil liberties.
