

## In Rhode Island, State Police and Federal Marshals Detail Use of Cell-Phone Tracking Tech

December 8, 2017



(TNS) — Two different cases involving two different fugitives. Both considered dangerous, and potentially vulnerable to a controversial cellphone-tracking device known as a cell-site simulator.

Federal marshals operated the surveillance equipment twice in Rhode Island in September 2016, state police Lt. Col. Joseph F. Philbin told The Providence Journal. In one case, he said, marshals and state police zeroed in on a 23-year-old who had fatally shot a police officer in North Carolina. In the second, they pursued a fugitive from Puerto Rico who was thought to be wanted in a triple murder.

Cell-site simulators, known to some in law enforcement by brand names such as Triggerfish or StingRay, mimic a cell tower, leading cellphones in a targeted area to connect with the simulator device rather than with the tower. Information gained through that connection can help marshals pinpoint the location of a wanted individual if the person is carrying an identifiable cellphone.

"We use it all the time," said Philbin, referring to Rhode Island's violent fugitive task force, a multi-agency team that includes marshals with access to the equipment. "It's a very effective tool."

Providence police have also made use of the surveillance tactic, with help from federal authorities, on about six occasions, said Providence Public Safety Commissioner Steven Paré. Providence investigators, he said, are familiar with the device known as StingRay.

The StingRay can tap data not just from a target's cellphone but also from other phones nearby, which raises privacy concerns. Meanwhile, federal marshals will not acknowledge their own use of the technology.

For these reasons, the tactic is drawing objections and criticism from civil-liberties and privacy groups throughout the country.

"This technology represents an extraordinary invasion of the privacy of innocent residents," said the executive director of the American Civil Liberties Union of Rhode Island, Steven Brown.

Tricking cellphones into connecting with a police-operated device — rather than an actual cell site or cell tower — is a decades-old tactic.

Authorities employed the same basic strategy to track and kill Pablo Escobar, one of the world's most wanted fugitives, in 1993. This was long before cellphones were packed with personal data.

In 2009, at a time when that was starting to change, an FBI agent described using "a cell-site emulator" more than 300 times over a decade and indicated that the equipment was used on a daily basis by the U.S. Marshals Service, the Secret Service and other federal agencies, according to Wired magazine.

The Associated Press recently reported that at least 72 state and local law-enforcement departments in 24 states, plus 13 agencies, have used the devices.

Drew Wade, a spokesman who is chief of public affairs for the U.S. Marshals Service, said in an email that he cannot confirm use of any such equipment in Rhode Island.

"To do so would allow criminal defendants to determine our capabilities and limitations in this area," said Wade, who also asserted that the techniques of marshals are in line with federal policies and the law and subject to court approval.

"Any investigative techniques" employed by marshals are not performed "to conduct domestic surveillance, intelligence-gathering, or any type of bulk data collection," he said.

Philbin and Paré said they were not able to elaborate specifically on how investigators made use of the devices in Rhode Island more recently.

Philbin emphasized that the vast majority of cases involve joint operations in which troopers work closely with members of the fugitive task force. Federal marshals, he said, operate the equipment under their own procedures and rules.

Cranston's police chief, Col. Michael J. Winqvist, said he had knowledge of the marshals' use of cell-site simulators during his time commanding state police detectives, a stint that included several years of work prior to his departure from the state police in 2014. The tool, he said, was always employed to directly determine the physical location of a wanted fugitive using a phone number known to authorities. He said he had no knowledge of the equipment being used to gather other types of intelligence in other situations.

In a New York murder case in October, a judge in Brooklyn ruled that the New York Police Department must acquire a special eavesdropping warrant signed by a judge to use the device. Such a warrant requires a higher bar than the "reasonable suspicion" standard.

"These devices suck up tons of information about people's locations," said the ACLU's Brown, who argues that authorities should need permission from a judge to work with the technology, which should only be employed in a limited manner with rules governing the disposal of information gathered by the device.

"Without that," said Brown, "there are no limits on how police are using the technology."

*©2017 The Providence Journal (Providence, R.I.) Distributed by Tribune Content Agency, LLC.*

<http://www.govtech.com/data/In-Rhode-Island-State-Police-and-Federal-Marshals-Detail-Use-of-Cell-Phone-Tracking-Tech.html>