Police use secret technology to trick, track cellphones - It's used locally; details on capacity and extent are not readily shared

Tampa Tribune, The (FL) - July 13, 2014

- Author/Byline: By ELAINE SILVESTRINI; Tribune staff; Stingray is the name of one model manufactured by a South Florida company.; By ELAINE SILVESTRINI; Tribune staff; Stingray is the name of one model manufactured by a South Florida company.

- Section: Metro
- Page: 1
- Readability: >12 grade level (Lexile: 1330)

- Abstract: p Law enforcement has a secret new tool to track cell phone locations. The Stingray collects info on all phones in its range, including innocent bystanders'. This has raised a ton of legal issues and the ACLU is fighting in court to get some info. FDLE has purchased $3 million worth of the devices and used them in more than 1,800 investigations, according to info the ACLU has collected. Some local law enforcement agencies, including HCSO, have signed agreements that let them borrow the equipment from FDLE. But they won't discuss its use.

TAMPA — When searching for dangerous criminals or missing crime victims, police have a covert weapon that can zero in on cellphones by pretending to be a signal tower.

The secret technology, often called Stingray, tricks mobile phones into communicating with investigators' equipment.

Not all agencies use the expensive technology, which is at the center of a divisive debate.

It can gather information about cellphone use by anyone, innocent people as well as investigative targets, within its range.

The Florida Department of Law Enforcement says it has used the "cell site simulator" equipment about 1,800 times since 2000.

Tampa police do not possess the technology, but a spokeswoman says the department has asked its law enforcement part

ners to borrow theirs in dozens of investigations during the past few years.

One case was the manhunt in June 2010 for Dontae Morris, recently sentenced to death for shooting to death two Tampa police officers during a traffic stop.

The equipment did not locate Morris, said police spokeswoman Laura McElroy.

The department has turned to its partners to help "track down our most dangerous criminals" as well as missing children, McElroy said.

The Hillsborough County Sheriff's Office declined to comment on the covert technology, although the American Civil Liberties Union, a chief critic of the equipment's use, says the agency is among many to sign an agreement with the FDLE allowing the sheriff's office to borrow it.

Clearwater police have also signed an agreement for borrowing the technology, the ACLU said, but police spokesman Rob Shaw said the department has not used it.

An FDLE spokeswoman said the agency doesn't loan out the equipment but allows it to be "used jointly" by FDLE task force partners.

? ? ?

The ACLU has tracked use of the technology and uncovered what it calls potential abuses across the country, including law enforcement agencies that have lied to or misled judges about use of the equipment.

Florida is one of about 1415 states where state or local law enforcement are known to use the cell site simulators, the ACLU says, along with about a dozen federal agencies including the FBI, U.S. Marshals Service and National Security Agency.

According to the ACLU, the equipment comes in a number of sizes, some handheld and some as big as a small suitcase, suitable for mounting in a car. Their signal ranges can be up to about a mile.

ACLU attorney Nathan Wessler said it's possible investigators operating the equipment may not see bystanders' phone information even though the equipment is capable of capturing it.

Stingray sends signals mimicking those sent by cellphone towers, forcing mobile phones within range to respond with information, including electronic serial numbers and locations.

“It’s sending signals through the walls of private homes and offices, forcing phones to report back their location,” Wessler said. “When you know a phone’s location, you almost always know a person’s location.”

There has been no evidence the equipment can intercept the contents of cellphone communications, such as conversations or texts, Wessler said.

Federal agencies’ use of the technology has been known for years, Wessler said. Use by local and state law enforcement was revealed only recently.

A key question, Wessler said, is whether the devices keep information obtained from the cellphones of people who are not investigation targets.

“We still don’t know the answer to that,” he said. “This is one of the most important pieces of information they should be making public for the public to understand whether their privacy rights are being violated, but we just don’t know.”

? ? ?

The Florida Depart ment of Law Enforcement uses the technology only when authorized by a court, spokeswoman Gretl Plessinger said.

“FDLE does not use this technology to eavesdrop on conversations, read text messages, access emails or examine private data,” Plessinger said. “We do not collect or retain information from citizens who are not subjects of an investigation.”

But Plessinger could not produce any court document specifically authorizing use of the equipment. She said court orders are sealed and could not be released.

Wessler said the FDLE and other agencies have failed to make available any policy governing the use and storage of information from people who aren’t targets, which suggests no such policy exists, he said.

Plessinger said the state’s laws governing this kind of information are “narrow in scope.” She said there’s no policy relating to innocent bystanders’ information because none is collected.

The equipment has been used to locate people wanted in homicide, home invasion and sexual battery investigations as well as missing children, she said.

The FBI declined to discuss the technology but did provide an affidavit filed in Tucson, Arizona, by a supervisory special agent who says details about the use of the equipment and how it works are not disclosed because they are considered sensitive.

Disclosure would enable criminals and foreign powers to create countermeasures, the affidavit states, and would “completely disarm law enforcement’s ability to obtain technology-based surveillance data in criminal investigations.”

? ? ?

The FBI says the technology is so sensitive that information the agency maintains about it is exempt from court rules requiring prosecutors to share information with defense lawyers.

Wessler said the ACLU has filed at least 37 records requests with law enforcement agencies in Florida and has determined that three local departments, in addition to FDLE, have the equipment. Those departments are in Miami, Miami-Dade and Sunrise.

Wessler said 15 departments have either provided no records or have told the ACLU they don’t use the equipment.

Police departments in Tampa, St. Petersburg and Clearwater, as well as the Pasco County Sheriff’s Office, said they didn’t have any relevant records. The Pinellas County Sheriff’s Office was still searching for records.

The ACLU is challenging the Sarasota Police Department over the equipment in a case recently moved to federal court in Tampa. The ACLU filed a public records request for applications and state court orders related to the use of the devices.

Sarasota police initially agreed to provide the records, but before they could, U.S. marshals seized the documents, saying they had been created by officers serving on a federal task force. A state judge later said the court had no jurisdiction over what were deemed to be federal records.

The ACLU insists they are not federal records because they were prepared by state employees for use in state court.

“Nowhere else do we have this crazy situation where a federal agency swoops in and seizes the records,” Wessler said.

The ACLU did obtain what Wessler called a “smoking gun” in the form of Sarasota police emails showing police deliberately conceal use

of the equipment from judges.

In the emails, Sarasota Sgt. Kenneth Castro says North Port police had specifically described the technology in a court document. The sergeant asks North Port to either change the document or at least change procedure so that wouldn't happen again.

The email says use of the equipment has not been revealed "so that we may continue to utilize this technology without the knowledge of the criminal element. In reports or depositions, we simply refer to the assistance as 'received information from a confidential source regarding the location of the suspect.' North Port responded that it can't change the court affidavit but will submit an addendum. The department pledges not to refer to the specific technology in future documents.

? ? ?

Wessler said his organi zation also has uncovered emails from federal prosecutors in California showing magistrates discovered investigators used the cell simulators after obtaining warrants to use pen registers and trap and trace devices, which record only the phone numbers that make and receive calls to and from a particular phone.

Warrants for that technology require a relatively low threshold of evidence because the information it gathers is much more limited than what is collected by cellphone simulators, Wessler said.

The magistrates, Wessler said, had "no idea" they were authorizing the cell site simulators when they signed the orders.

The ACLU recently won a court victory in Tallahassee when a judge unsealed a transcript of a 2008 hearing in which a Tallahassee police investigator discussed using the equipment to track a rape suspect after the victim informed detectives the attacker had taken her cellphone.

During that hearing, the prosecutor told the judge the courtroom needed to be closed because the investigator had signed a nondisclosure agreement with the equipment manufacturer.

The maker, Harris Corp., based in Melbourne, declined to comment for this story.

According to records obtained by the ACLU, the FDLE has purchased more than $3 million worth of cell site simulators from Harris since 2008. Wessler said each device can cost tens of thousands to hundreds of thousands of dollars.

The Tallahassee court transcript provides a rare glimpse into how the equipment was used in a particular case. Investigator Christopher Corbitt testified he underwent six days of training from the manufacturer.

Corbitt said police contacted the victim's cellphone provider, Verizon, which gave police information about the location of the cell tower the phone was communicating with. By emulating a cellphone tower with the equipment, Corbitt said, "we force that (cellphone) to register with us."

Corbitt said he used a car-mounted device to follow the signals to a particular apartment complex and then used a handheld device, walking from door to door in the complex, pointing it at every apartment until the victim's phone was found.

Wessler said it was particularly alarming that Corbitt said the equipment was "evaluating all the handsets in the area" to find the phone police were seeking.

This, he said, shows that innocent bystanders' information is captured.

esilvestrini@tampatrib.com

813-259-7837

Twitter: @ElaineTBO

STINGRAY, Page 16

TAMPA — When searching for dangerous criminals or missing crime victims, police have a covert weapon that can zero in on cellphones by pretending to be a signal tower.

The secret technology, often called Stingray, tricks mobile phones into communicating with investigators' equipment.

Not all agencies use the expensive technology, which is at the center of a divisive debate.

It can gather information about cellphone use by anyone, innocent people as well as investigative targets, within its range.

The Florida Department of Law Enforcement says it has used the “cell site simulator” equipment about 1,800 times since 2000.

Tampa police do not possess the technology, but a spokeswoman says the department has asked its law enforcement part

ners to borrow theirs in dozens of investigations during the past few years.

One case was the manhunt in June 2010 for Dontae Morris, recently sentenced to death for shooting to death two Tampa police officers during a traffic stop.

The equipment did not locate Morris, said police spokeswoman Laura McElroy.

The department has turned to its partners to help “track down our most dangerous criminals” as well as missing children, McElroy said.

The Hillsborough County Sheriff’s Office declined to comment on the covert technology, although the American Civil Liberties Union, a chief critic of the equipment’s use, says the agency is among many to sign an agreement with the FDLE allowing the sheriff’s office to borrow it.

Clearwater police have also signed an agreement for borrowing the technology, the ACLU said, but police spokesman Rob Shaw said the department has not used it.

An FDLE spokeswoman said the agency doesn’t loan out the equipment but allows it to be “used jointly” by FDLE task force partners.

? ? ?

The ACLU has tracked use of the technology and uncovered what it calls potential abuses across the country, including law enforcement agencies that have lied to or misled judges about use of the equipment.

Florida is one of about 1415 states where state or local law enforcement are known to use the cell site simulators, the ACLU says, along with about a dozen federal agencies including the FBI, U.S. Marshals Service and National Security Agency.

According to the ACLU, the equipment comes in a number of sizes, some handheld and some as big as a small suitcase, suitable for mounting in a car. Their signal ranges can be up to about a mile.

ACLU attorney Nathan Wessler said it’s possible investigators operating the equipment may not see bystanders’ phone information even though the equipment is capable of capturing it.

Stingray sends signals mimicking those sent by cellphone towers, forcing mobile phones within range to respond with information, including electronic serial numbers and locations.

“It’s sending signals through the walls of private homes and offices, forcing phones to report back their location,” Wessler said. “When you know a phone’s location, you almost always know a person’s location.”

There has been no evidence the equipment can intercept the contents of cellphone communications, such as conversations or texts, Wessler said.

Federal agencies’ use of the technology has been known for years, Wessler said. Use by local and state law enforcement was revealed only recently.

A key question, Wessler said, is whether the devices keep information obtained from the cellphones of people who are not investigation targets.

“We still don’t know the answer to that,” he said. “This is one of the most important pieces of information they should be making public for the public to understand whether their privacy rights are being violated, but we just don’t know.”

? ? ?

The Florida Depart ment of Law Enforcement uses the technology only when authorized by a court, spokeswoman Gretl Plessinger said.

“FDLE does not use this technology to eavesdrop on conversations, read text messages, access emails or examine private data,” Plessinger said. “We do not collect or retain information from citizens who are not subjects of an investigation.”

But Plessinger could not produce any court document specifically authorizing use of the equipment. She said court orders are sealed and could not be released.

Wessler said the FDLE and other agencies have failed to make available any policy governing the use and storage of information from

people who aren't targets, which suggests no such policy exists, he said.

Plessinger said the state's laws governing this kind of information are "narrow in scope." She said there's no policy relating to innocent bystanders' information because none is collected.

The equipment has been used to locate people wanted in homicide, home invasion and sexual battery investigations as well as missing children, she said.

The FBI declined to discuss the technology but did provide an affidavit filed in Tucson, Arizona, by a supervisory special agent who says details about the use of the equipment and how it works are not disclosed because they are considered sensitive.

Disclosure would enable criminals and foreign powers to create countermeasures, the affidavit states, and would "completely disarm law enforcement's ability to obtain technology-based surveillance data in criminal investigations."

? ? ?

The FBI says the technology is so sensitive that information the agency maintains about it is exempt from court rules requiring prosecutors to share information with defense lawyers.

Wessler said the ACLU has filed at least 37 records requests with law enforcement agencies in Florida and has determined that three local departments, in addition to FDLE, have the equipment. Those departments are in Miami, Miami-Dade and Sunrise.

Wessler said 15 departments have either provided no records or have told the ACLU they don't use the equipment.

Police departments in Tampa, St. Petersburg and Clearwater, as well as the Pasco County Sheriff's Office, said they didn't have any relevant records. The Pinellas County Sheriff's Office was still searching for records.

The ACLU is challenging the Sarasota Police Department over the equipment in a case recently moved to federal court in Tampa. The ACLU filed a public records request for applications and state court orders related to the use of the devices.

Sarasota police initially agreed to provide the records, but before they could, U.S. marshals seized the documents, saying they had been created by officers serving on a federal task force. A state judge later said the court had no jurisdiction over what were deemed to be federal records.

The ACLU insists they are not federal records because they were prepared by state employees for use in state court.

"Nowhere else do we have this crazy situation where a federal agency swoops in and seizes the records," Wessler said.

The ACLU did obtain what Wessler called a "smoking gun" in the form of Sarasota police emails showing police deliberately conceal use of the equipment from judges.

In the emails, Sarasota Sgt. Kenneth Castro says North Port police had specifically described the technology in a court document. The sergeant asks North Port to either change the document or at least change procedure so that wouldn't happen again.

The email says use of the equipment has not been revealed "so that we may continue to utilize this technology without the knowledge of the criminal element. In reports or depositions, we simply refer to the assistance as 'received information from a confidential source regarding the location of the suspect.' North Port responded that it can't change the court affidavit but will submit an addendum. The department pledges not to refer to the specific technology in future documents.

? ? ?

Wessler said his organi zation also has uncovered emails from federal prosecutors in California showing magistrates discovered investigators used the cell simulators after obtaining warrants to use pen registers and trap and trace devices, which record only the phone numbers that make and receive calls to and from a particular phone.

Warrants for that technology require a relatively low threshold of evidence because the information it gathers is much more limited than what is collected by cellphone simulators, Wessler said.

The magistrates, Wessler said, had "no idea" they were authorizing the cell site simulators when they signed the orders.

The ACLU recently won a court victory in Tallahassee when a judge unsealed a transcript of a 2008 hearing in which a Tallahassee police investigator discussed using the equipment to track a rape suspect after the victim informed detectives the attacker had taken her cellphone.

During that hearing, the prosecutor told the judge the courtroom needed to be closed because the investigator had signed a

nondisclosure agreement with the equipment manufacturer.

The maker, Harris Corp., based in Melbourne, declined to comment for this story.

According to records obtained by the ACLU, the FDLE has purchased more than $3 million worth of cell site simulators from Harris since 2008. Wessler said each device can cost tens of thousands to hundreds of thousands of dollars.

The Tallahassee court transcript provides a rare glimpse into how the equipment was used in a particular case. Investigator Christopher Corbitt testified he underwent six days of training from the manufacturer.

Corbitt said police contacted the victim's cellphone provider, Verizon, which gave police information about the location of the cell tower the phone was communicating with. By emulating a cellphone tower with the equipment, Corbitt said, "we force that (cellphone) to register with us."

Corbitt said he used a car-mounted device to follow the signals to a particular apartment complex and then used a handheld device, walking from door to door in the complex, pointing it at every apartment until the victim's phone was found.

Wessler said it was particularly alarming that Corbitt said the equipment was "evaluating all the handsets in the area" to find the phone police were seeking.

This, he said, shows that innocent bystanders' information is captured.

esilvestrini@tampatrib.com

813-259-7837

Twitter: @ElaineTBO

Stingray

From Page 1