

Michigan State Police using cell snooping devices

Joel Kurth, The Detroit News Published 11:32 p.m. ET Oct. 22, 2015 | Updated 10:18 a.m. ET Oct. 23, 2015



(Photo: Dale G. Young, The Detroit News)

For nearly a decade, the [Michigan State Police](http://www.michigan.gov/msp) has had secretive cellphone tracking devices that were bought to fight terrorism but instead are used to solve everyday crimes, internal documents show.

More than 250 pages of emails, invoices and other documents show the state police in 2006 acquired cellphone simulator technology, which lets police collect large amounts of data including the location of users. The equipment was upgraded in 2013 and an internal memo indicates it was used last year on 128 cases ranging from homicide to burglary and fraud, but not terrorism.

The documents are the first indication the state police have [Stingray and Hailstorm-type](http://arstechnica.com/tech-policy/2013/09/meet-the-machines-that-steal-your-phones-data/2/) tools from Florida-based defense contractor [Harris Corp.](http://harris.com/) The equipment has raised privacy concerns and reform efforts nationwide because it collects information from not only criminal suspects, but also anyone with cellphones within range of the devices.

The suitcase-sized contraption is installed in cars and pulls cell data for police. Its exact capabilities, though, aren't fully known because Harris Corp. requires that police agencies sign confidentiality agreements.

"This is technology initially designed for military and intelligence agencies and now it's being used in residential streets across the United States and Michigan, and it's being done in secrecy," said [Nathan Freed Wessler](https://www.aclu.org/bio/nathan-freed-wessler), a New York-based attorney for the American Civil Liberties Union.

"It's tricking every phone in broad areas and sweeping information about every innocent bystander nearby and reaching through walls."

The [ACLU](https://www.aclu.org/about-aclus-project-speech-privacy-and-technology) acquired the documents through the Freedom of Information Act and shared them with The Detroit News, which last year published a [two-day series](http://www.detroitnews.com/article/20140404/SPECIAL/304040043) about police tracking devices and data collection. At the time, the Oakland County Sheriff's Office was believed to be the only police agency in Michigan with Stingray-type equipment.

State Police First Lt. Christopher Hawkins said the agency secures warrants or court orders before using the devices except in "exigent circumstances" such as kidnappings. Its officials have met with the ACLU to discuss policies and are reviewing recent ones from the U.S. Department of Justice that require warrants before cell simulators are used, Hawkins said.

"As with every tool used to assist law enforcement investigations, we use the Constitution of the United States and Michigan as governance," said Hawkins, commander of the state police's legislative and legal resources section.

"It is a very effective tool that we've had great success in using. It's a tool to keep the citizens of Michigan safe."

He said he can't discuss specifics about "how and when" the technology is used, but the state police "understands the concerns about privacy and need for transparency."

"Our device does not retain any data from third-party cellphones," Hawkins said. "The device cannot be used to listen to calls (or) read text messages."

Nationwide, the ACLU has identified 57 police agencies in 22 states and the District of Columbia that own the devices known as cell site simulators. They masquerade as cell towers and send signals to trick phones in the area into transmitting their locations and identifying information.

Gear bought in 2006

The documents acquired by the ACLU indicate the state police paid Harris Corp. \$206,500 in 2006 for equipment that was "vital to the war on terrorism" and allows "the state to track the physical location of a suspected terrorist."

The equipment was fully funded by a U.S. Homeland Security grant and the cost matches Harris Corp. [prices lists](#) (https://www.gsaadvantage.gov/ref_text/GS35F0163N/GS35F0163N_online.htm) for its Stingray device, Wessler said.

In 2013, the state used asset forfeiture funds to pay Harris \$593,450 for "surveillance and countersurveillance equipment and supplies," records show. The product name is redacted in purchase orders but emails say it was for a "Stingray upgrade" to "allow the MSP to keep pace with current technology trends."

That is likely a Hailstorm, a cell tower simulator that is similar to Stingray but able to collect information over 4G networks, Wessler said.

A Jan. 21 internal state police memo indicates the technology led to 82 arrests, including 40 for [homicide](https://en.wikipedia.org/wiki/Homicide) and attempted murder, and the discovery of six missing persons. The memo also indicates it was used in 18 burglary cases, three frauds ones and two for smuggling.

"Not only did we experience a great deal of success in locating and arresting violent offenders, but our assistance also resulted in significant savings in labor costs through reduced surveillance and other investigative efforts," the unsigned memo stated.

Problem with trust

The frequency of the device's use — about once every three days — troubles former state Rep. Tom McMillin, R-Rochester Hills.

Last year, he hosted hearings about the technology and introduced bills to oversee cellphone simulators. The legislation would have required warrants for their use, created a board to oversee police surveillance technology and imposed criminal penalties for misuse.

The bills died and McMillin left his post because of term limits. No similar legislation has been introduced since.

" 'Just trust us' is something we've heard before. It doesn't work," said McMillin, an unsuccessful candidate for the U.S. House last year.

"We shouldn't believe (police) are just blindly following the rules. ... The general public doesn't have a problem using the latest technology to get bad guys, but there needs to be broad oversight and accountability."

Issue not 'ripe' for action

This year, [California and Washington](http://arstechnica.com/tech-policy/2015/10/california-governor-signs-new-law-mandating-warrant-for-stingray-use/) passed laws requiring police to get warrants to use Stingray-type devices, joining Virginia, Minnesota and Utah in regulating the devices. Before the laws, police typically secured "pen register and trap and trace orders" from judges, which require a lower standard of proof than warrants and don't require police to disclose they are using a Stingray.

State Rep. Kurt Heise, R-Plymouth Township, chairman of the House Criminal Justice Committee, said McMillin's bills would have "tied the hands of police."

"Right now, I don't think this is an issue ripe for state action," Heise said. "The burden is on law enforcement to demonstrate they are operating under the constitution ... If the ACLU wants to challenge this in court, then we may have to let the courts sort it out."

Heise said he wasn't aware the state police have the technology and isn't concerned about it.

Law enforcement in [Oakland County](https://www.oakgov.com/sheriff) and other agencies have offered assurances the devices don't eavesdrop on conversations, collect contents of text messages or phone numbers or store information of bystanders.

Undersheriff Mike McCabe said his department has secured warrants from "day one" to use cellular technology.

Wessler said even information like the location of cellphones is capable of revealing "an extraordinary amount of information about people's lives."

"Secrecy serves only to insulate (police) from scrutiny and enforcement of our constitutional rules in this country," he said. "As a society, we may decide it's appropriate to use the technology but we can't have that conversation if police are doing it in complete secrecy."

jkurth@detroitnews.com

Twitter: @cityhallinsider

Read or Share this story: <http://detne.ws/1LQuHAF>

