Unregulated Cellphone Surveillance Tool Can Also Block Calls from the Innocent

December 27, 2016

(TNS) — It's no secret that state and local law enforcement agencies have grown more militarized in the past decade, with armored personnel carriers, drones and robots.

But one item in their arsenal has been kept largely out of public view, to the dismay of civil liberties advocates who say its use is virtually unregulated — and largely untracked.

The device is a suitcase-size surveillance tool commonly called a StingRay that mimics a cellphone tower, allowing authorities to track individual cellphones in real time. Users of the device, which include scores of law enforcement agencies across the country, sign a nondisclosure agreement when they purchase it, pledging not to divulge its use, even in court cases against defendants the device helped capture.

Those restrictions remain in place despite a decision last year by the police in Charlotte, N.C., to disclose to judges more details about the device's use in criminal cases and laws in several states that require warrants whenever the device is employed.

A report this week by the House Reform and Government Oversight Committee raised new concerns about the devices' popularity. " Cell-site simulator use inside the United States raises far-reaching issues concerning the use, extent and legality of government surveillance authority," it said.

The FBI is one of the major users of the device. The House of Representatives report said that agency alone had more than 194 cell-site simulators in use across the country.

Yet even as the federal government has encouraged the use of the simulators, the FBI has demanded that Harris Corp., the defense contractor that manufactures the most commonly used of the devices, provide notification every time it sells a device to law enforcement agencies. In turn, the FBI requires those agencies to sign a nondisclosure agreement that blocks them from telling the public of the purchase or acknowledging the device's use in court proceedings.

Until recently, the FBI avoided disclosing its own use of the surveillance apparatus and also "its role in assisting state and local law enforcement agencies in obtaining the devices," the oversight committee report said.

Cell-site simulators were developed for battlefield use, allowing roving infantry teams or airborne units to track the cellphone signatures of enemy combatants and kill them.

Their civilian use has soared, however. In addition to the FBI's 194 devices, the report found them sprinkled among federal agencies: the U.S. Marshals Service has 70, Immigration and Customs Enforcement has 59 and even the Internal Revenue Service maintains two of the electronic tools in its investigative arsenal.

The House report provided only limited details about the spread of the devices to state and local agencies. But the American Civil Liberties Union tallies 68 agencies in 23 states and the District of Columbia that have StingRay tracking devices. States with broad usage include North Carolina, Florida, Texas and California.

Even small city police departments can obtain StingRays. The police department in Sunrise, Fla., a municipality of 90,000 people northwest of Fort Lauderdale, has two, the House report said.

Much of the federal government won't talk about use of the StingRays.

"The FBI does not comment on specific tools or techniques," spokesman Raushaunah Muhammad said.

Harris Corp., headquartered in Melbourne, Fla., was equally reticent: "We are unable to comment for your story," spokesman Jim Burke said.

"Right now, it's the Wild West for the use of these devices," said Mike Katz-Lacabe, director of research at the Center for Human Rights and Privacy, a nonprofit group he founded in San Leandro, Calif. "We don't know how often they are used, what they are used for and whether we'd consider such a use acceptable."

Federal authorities have approved cell-site simulators from two companies. In addition to models of the StingRay by Harris Corp., a second branded device is commonly called a Dirtbox and is made by a Boeing Corp. subsidiary, Digital Receiver Technology Inc.

of Germantown, Md. The House report said the devices cost between $41,500 and $500,000, depending on their capabilities.

Federal authorities have approved cell-site simulators from two companies. In addition to models of the StingRay by Harris Corp., a second branded device is commonly called a Dirtbox and is made by a Boeing Corp. subsidiary, Digital Receiver Technology Inc. of Germantown, Md. The House report said the devices cost between $41,500 and $500,000, depending on their capabilities.

That is one of the concerns of civil liberties groups, that cellphones unconnected with a law enforcement investigation are also captured by the device. While some cell-site simulators allow 911 emergency calls to pass through to legitimate towers, other calls routinely fail. Should an emergency unfold, cell users in the vicinity probably would find their calls dropped or signals jammed.

“Even if there is a 911 pass-through feature, there are still plenty of other calls that people might want to make,” said Christopher Soghoian, principal technologist at the American Civil Liberties Union. “You might want to call your children’s school. You might want to call your wife or husband.”

Police with little training can use the cell-site simulators and affect all phones in a given area while looking for single individuals, he said. Poor minority communities, where many residents have ditched landlines, are disproportionately affected, he added.

It’s hard to know with certainty how many innocent cellphone users have experienced jamming due to police use of cell-site simulators. Federal restrictions on information about their use prevents collecting such details.

“There are real privacy interests at stake when the government sends probing electronic signals into the homes of innocent people. These devices cannot be used in a way that only enters the home of the target,” Soghoian said.

“This is not a scalpel. It is a shotgun,” he added.

In the past decade or so, technologies developed by the intelligence community and military have trickled down to law enforcement, from drones and license plate readers to the armored personnel carriers visible in Ferguson, Mo., in the 2014 protests over the fatal shooting of a young African-American male by a white police officer.

“I think (cell-site simulators) are definitely part of the police militarization trend,” said Alan Butler, senior counsel for the Electronic Privacy Information Center, a nonprofit public interest research group in Washington that focuses on democratic values in a digital era.

A number of nondisclosure agreements from law enforcement agencies have leaked out over the years, including from the Florida Department of Law Enforcement, the Sacramento County sheriff, the Kansas City Police Department, the Tacoma, Wash., Police Department and the California Department of Justice.

Federal demands that law enforcement not acknowledge the use of the devices in court proceedings has led some police to bend rules about how to use information that is gathered.

“Sometimes they would say in court filings that they had a ‘ confidential informant,’” Butler said.

A trio of civil rights groups filed a complaint in August with the Federal Communications Commission against the Baltimore Police Department, saying widespread use of the cell-site simulators there had disproportionately affected black communities and disrupted 911 calls.

The House report, which said grants from the Departments of Justice and Homeland Security were widely used to provide state and local agencies with money for the simulators, said police increasingly were using the devices “for everyday crime-fighting activities.”

It cited the lack of a uniform national policy governing the devices’ use, noting that in some jurisdictions the standard for employing cell-site simulators is lower than for obtaining a search warrant. The House report called on Congress to pass a uniform nationwide standard that would require all law enforcement agencies to use “clarity and candor” with courts so that the devices are employed transparently in criminal investigations.

“Lack of oversight is huge here. I don’t think it can be overstated,” said Butler, the lawyer for the Electronic Privacy Information Center.

http://www.govtech.com/public-safety/Unregulated-Cell-Phone-Surveillance-Tool-Can-Also-Block-Calls-From-the-Innocent.html