Americans' cellphones targeted in secret U.S. spy program

14. November 2014

By Devlin Barrett. The Wall Street Journal

WASHINGTON - The Justice Department is scooping up data from thousands of cellphones through fake communications towers deployed on airplanes, a high-tech hunt for criminal suspects that is snagging a large number of innocent Americans, according to people familiar with the operations.

The U.S. Marshals Service program, which became fully functional around 2007, operates Cessna aircraft from at least five metropolitan-area airports, with a flying range covering most of the U.S. population, according to people familiar with the program.

Planes are equipped with devices - some known as "dirtboxes" to law-enforcement officials because of the initials of the Boeing Co. unit that produces them - which mimic cell towers of large telecommunications firms and trick cellphones into reporting their unique registration information.

The technology in the two-foot-square device enables investigators to scoop data from tens of thousands of cellphones in a single flight, collecting their identifying information and general location, these people said.

People with knowledge of the program wouldn't discuss the frequency or duration of such flights, but said they take place on a regular basis.

A Justice Department official would neither confirm nor deny the existence of such a program. The official said discussion of such matters would allow criminal suspects or foreign powers to determine U.S. surveillance capabilities. Justice Department agencies comply with federal law, including by seeking court approval, the official said.

The program is the latest example of the extent to which the U.S. is training its surveillance lens inside the U.S. It is similar in approach to the National Security Agency's program to collect millions of Americans phone records, in that it scoops up large volumes of data in order to find a single person or a handful of people. The U.S. government justified the phone-records collection by arguing it is a minimally invasive way of searching for terrorists.

Christopher Soghoian, chief technologist at the American Civil Liberties Union, called it "a dragnet surveillance program. It's inexcusable and it's likely - to the extent judges are authorizing it - [that] they have no idea of the scale of it."

Cellphones are programmed to connect automatically to the strongest cell tower signal. The device being used by the U.S. Marshals Service identifies itself as having the closest, strongest signal, even though it doesn't, and forces all the phones that can detect its signal to send in their unique registration information. Even having encryption on one's phone, such as Apple Co.'s iPhone 6 now includes, doesn't prevent this process.

The technology is aimed at locating cellphones linked to individuals under investigation by the government, including fugitives and drug dealers, but it collects information on cellphones belonging to people who aren't criminal suspects, these people said. They said the device determines which phones belong to suspects and "lets go" of the non-suspect phones.

The device can briefly interrupt calls on certain phones. Authorities have tried to minimize the potential for harm, including modifying the software to ensure the fake tower doesn't interrupt anyone calling 911 for emergency help, one person familiar with the matter said.

The program cuts out phone companies as an intermediary in searching for suspects. Rather than asking a company for cell-tower information to help locate a suspect, which law enforcement has criticized as slow and inaccurate, the government can now get that information itself. People familiar with the program say they do get court orders to search for phones, but it isn't clear if those orders describe the methods used because the orders are sealed.

Also unknown are the steps taken to ensure data collected on innocent people isn't kept for future examination by investigators. A federal appeals court ruled earlier this year that over-collection of data by investigators, and stockpiling of such data, was a violation of the Constitution.

The program is more sophisticated than anything previously understood about government use of such technology. Until now, the hunting of digital trails created by cellphones had been thought limited to devices carried in cars that scan the immediate area for signals. Civil-liberties groups are suing for information about use of such lower-grade devices, some of them called Stingrays, by the Federal Bureau of Investigation.

By taking the program airborne, the government can sift through a greater volume of information and with greater precision, these people said. If a suspect's cellphone is identified, the technology can pinpoint its location within about three meters, down to a specific room in a building. Newer versions of the technology can be programmed to do more than suck in data: They can also jam signals and retrieve data from a target phone such as texts or photos. It isn't clear if this domestic program has ever used those features.

Similar devices are used by U.S. military and intelligence officials operating in other countries, including in war zones, where they are sometimes used to locate terrorist suspects, according to people familiar with the work. In the U.S., these people said, the technology has been effective in catching suspected drug dealers and killers. They wouldn't say which suspects were caught through this method.

The scanning is done by the Technical Operations Group of the U.S. Marshals Service, which tracks fugitives, among other things. Sometimes it deploys the technology on targets requested by other parts of the Justice Department.

Within the Marshals Service, some have questioned the legality of such operations and the internal safeguards, these people said. They say scooping up of large volumes of information, even for a short period, may not be properly understood by judges who approve requests for the government to locate a suspect's phone.

Some within the agency also question whether people scanning cellphone signals are doing enough to minimize intrusions into the phone system of other citizens, and if there are effective procedures in place to safeguard the handling of that data.

It is unclear how closely the Justice Department oversees the program. "What is done on U.S. soil is completely legal," said one person familiar with the program. "Whether it should be done is a separate question."

Referring to the more limited range of Stingray devices, Mr. Soghoian of the ACLU said: "Maybe it's worth violating privacy of hundreds of people to catch a suspect, but is it worth thousands or tens of thousands or hundreds of thousands of peoples' privacy?"

The existence of the cellphone program could escalate tensions between Washington and technology companies, including the telecom firms whose devices are being redirected by the program.

If a suspect is believed to have a cellphone from Verizon Inc., for example, the device would emit a signal fooling Verizon phones and those roaming on Verizon's network into thinking the plane is the nearest available Verizon cell tower. Phones that are turned on, even if not in use, would "ping" the flying device and send their registration information. In a densely populated area, the dirtbox could pick up data of tens of thousands of cellphones.

The approach is similar to what computer hackers refer to as a "man in the middle" attack, in which a person's electronic device is tricked into thinking it is relaying data to a legitimate or intended part of the communications system.

A Verizon spokesman said the company was unaware of the program. "The security of Verizon's network and our customers' privacy are top priorities," the spokesman said. "However, to be clear, the equipment referenced in the article is not Verizon's and is not part of our network."

An AT&T Inc. spokeswoman declined to comment, as did a spokeswoman for Sprint Corp.

For cost reasons, the flights usually target a number of suspects at a time, rather than just a single fugitive. But they can be used for a single suspect if the need is great enough to merit the resources, these people said.

The dirtbox and Stingray are both types of what tech experts call "ISMI catchers," named for the identification system used by networks to identify individual cellphones.

The name "dirtbox" came from the acronym of the company making the device, DRT, for Digital Recovery Technology Inc., people said. DRT is now a subsidiary of Boeing. A Boeing spokeswoman declined to comment.

"DRT has developed a device that emulates a cellular base station to attract cellphones for a registration process even when they are not in use," according to a 2010 regulatory filing Boeing made with the U.S. Commerce Department, which touted the device's success in finding contraband cellphones smuggled in to prison inmates.