Millions caught in cell phone tracking by US police agencies

Joseph Kishore
10 December 2013

With the support of the Obama administration, police agencies in the US receive detailed call and location records of Americans' cell phone activity without a warrant, according to reports released yesterday. The information could be used to track the movements of individuals and quickly determine who is involved in protests or other political activity.

Cell phone information, which includes location data, is gathered by police in at least two different ways:

1. By obtaining cell phone "tower dumps" of data from major telecommunication companies;

2. By utilizing special mobile devices, known as Stingrays, that masquerade as a cell phone tower to intercept data in the surrounding area.

A report by the *Washington Post* was based on information revealed in a US Senate inquiry, while the USA Today and Gannett newspapers published a separate analysis based on public records.

Telecommunication companies reported more than 9,000 tower dump requests last year, according to the *Post*, with each request covering hundreds or even thousands of individuals. This means that the information on potentially millions of people is involved, with those caught up in the data collection never informed.

In at least one instance, a Stingray device was used specifically for the purpose of political monitoring. According to *USA Today*, "When Miami-Dade [Florida] police bought their Stingray device, they told the City Council the agency needed to monitor protesters at an upcoming world trade conference, according to purchasing records."

Since the Stingray device can be mounted in a police van and used to gather cell phone data in a given area, it can be used to obtain the identity of anyone involved in a political protest or meeting, so long as they have a cell phone turned on. Cell phones regularly interact with phone towers, or police devices masquerading as a phone tower, even when a call is not being made.

The revelations of massive police access of cell phone records follow a report last week, based on documents from whistleblower Edward Snowden, that the National Security Agency collects *5 billion records every day* on cell phone users around the world, including many Americans. (See "US tracks billions of cell phone location records daily")

As with the NSA, federal, state and local police agencies generally request and receive the cell phone information without obtaining a warrant—a clear violation of the Fourth Amendment of the US Constitution, which states that "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."

The records are obtained under the Electronic Communications Privacy Act, which only requires a judge to find that the information is "relevant and material" to a criminal investigation—a very loose requirement. Arguing against this reasoning, however, a federal judge in Texas ruled earlier this year that "the collection of cell-site location records effectively enables 'mass' or 'wholesale' electronic surveillance, and raises greater Fourth Amendment concerns than a single electronically surveilled car trip."

According to the *USA Today* and Gannett study, based on records from more than 125 police agencies in 33 states, about one quarter of all agencies have accessed records from telecommunication companies. At least 25, or one-fifth of those surveyed, own a Stingray device. In addition, local police can often access Stingray devices from state agencies.

The amount of information obtained can go beyond

the cell phone records themselves. The *Post*, citing an investigation being led by Senator Edward Markey (Democrat of Massachusetts), notes that a survey of eight US phone companies "has also revealed that carriers, following requests from law enforcement agencies, are providing a range of other records as well. Those include GPS location data, web site addresses and, in some cases, the search terms Americans have entered into their cell phones." Markey is proposing minor reforms to the police powers, without any essential changes.

In addition, *USA Today* writes, "Law-enforcement records show police can use initial data from a tower dump to ask for another court order for more information, including addresses, billing records and logs of class, texts and locations."

The Stingray devices, by mimicking cell phone towers, can also collect the actual content of any cell phone conversations or text messages. Police claim that the devices are not set up to do this, but the use and operation of the technology is shrouded in secrecy.

The use of both methods for obtaining cell phone information has increased in recent years. The *Post* cites William Petersen, the general counsel for Verizon Wireless, as reporting: "The industry as a whole in recent years experienced a substantial increase in these demands," with requests approximately doubling over the past five years. Verizon, along with other major telecommunication companies, has also been implicated in the NSA's program to collect phone records, as revealed in documents released by Snowden earlier this year.

The Stingrays, which can cost hundreds of thousands of dollars, have generally been purchased with federal funds obtained through the Department of Homeland Security.

The constitutionality of the use of Stingray devices, which are made by the Harris Wireless Products Group based in Florida, has been the subject of multiple lawsuits. One involves an Arizona man, Daniel David Rigmaiden, whose 2008 arrest for tax fraud became the first case in which the use of the devices was revealed in court documents.

Earlier this year, a US district court in Arizona ruled in favor of the Obama administration's Justice Department by throwing out legal challenges to the evidence obtained with the Stingray device, which was used to locate Rigmaiden. The FBI is also opposing efforts to force the government to reveal the extent of the use of Stingrays.

Responding to the decision of the US district court, ACLU attorney Linda Lye noted, "They're using them, there are just very few cases where the government has admitted it."

Dismissing constitutional concerns over the collection of cell phone data, a Justice Department official, speaking to the *Post* anonymously, insisted that the information could be "useful" in locating drug traffickers or gang members.

In fact, what is at issue is not whether this information is "useful" to police, but whether the mass collection of location data without a warrant is legal and constitutional.

The collection of cell phone data is part of massive spying operations that have ballooned over the past decade, involving both intelligence agencies and police, and targeting individuals inside and outside the United States. Under the Obama administration, the breadth of these operations has expanded enormously.

In addition to illegally monitoring the communications and Internet activity of billions of people all over the world through secret NSA programs, the US government and police agencies are building up huge databases of license plates, photographs, and other information that constitute an assault on basic democratic rights.