EXHIBIT 12

Cellphone data spying: It's not just the NSA

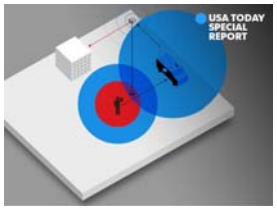
LAW ENFORCEMENT USING METHODS FROM NSA PLAYBOOK

Local police are increasingly able to scoop up large amounts of cellphone data using new technologies, including cell tower dumps and secret mobile devices known as Stingrays. Here's a closer look at how police do it.

Source: USA TODAY research
John Kelly, Kevin A. Kepple, Jerry Mosemak, Janet Loehrke and Jeff Dionise, USA TODAY

John Kelly, USATODAY (/staff/911/john-kelly) 5:10 p.m. EST December 8, 2013

Police maintain that cellphone data can help solve crimes, track fugitives or abducted children — or even foil a terror attack.



(Photo: Jerry Mosemak)

SHARE
17270
CONNECT
(https://twitter.com/intent/tweet?url=http://usat.ly/1dcpgrI&text=Cellphone

The National Security Agency isn't the only government entity secretly collecting data from people's cellphones. Local police are increasingly scooping it up, too.

Armed with new technologies, including mobile devices that tap into cellphone data in real time, dozens of local and state police agencies are capturing information about thousands of cellphone users at a time, whether they are targets of an investigation or not, according to public records obtained by USA TODAY and Gannett newspapers and TV stations.

The records, from more than 125 police agencies in 33 states, reveal:

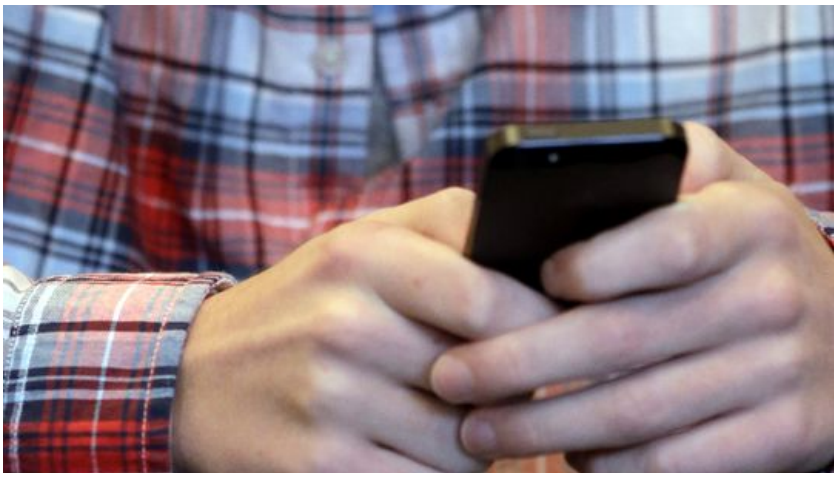
• About one in four law-enforcement agencies have used a tactic known as a "tower dump," which gives police data about the identity, activity and location of any phone that connects to the targeted cellphone towers over a set span of time, usually an hour or two. A typical dump covers multiple towers, and wireless providers, and can net information from thousands of phones.

MORE: Examples of data-gathering abuses (http://www.usatoday.com/story/news/nation/2013/12/08/cellphone-data-abuses/3902845/)

MORE: Cell data dumps: A legally fuzzy area (http://www.usatoday.com/story/news/nation/2013/12/08/cellphone-data-legal-issues-court/3902859/)

INVESTIGATION: How we did it (http://www.usatoday.com/story/news/nation/2013/12/08/cellphone-data-investigation-how/3902857/)

• At least 25 police departments own a Stingray, a suitcase-size device that costs as much as $400,000 and acts as a fake cell tower. The system, typically installed in a vehicle so it can be moved into any neighborhood, tricks all nearby phones into connecting to it and feeding data to police. In some states, the devices are available to any local police department via state surveillance units. The federal government funds most of the purchases, via anti-terror grants.



RECOMMENDED FOR YOU

Gov. Christie to take questions about bridge scandal
(/story/news/politics/2014/01/09/christie-

• Thirty-six more police agencies refused to say whether they've used either tactic. Most denied public records requests, arguing that criminals or

terrorists could use the information to thwart important crime-fighting and surveillance techniques.

Police maintain that cellphone data can help solve crimes, track fugitives or abducted children or even foil a terror attack.

Organizations such as the American Civil Liberties Union and Electronic Privacy Information Center (EPIC) say the swelling ability by even small-town police departments to easily and quickly obtain large amounts of cellphone data raises questions about the erosion of people's privacy as well as their Fourth Amendment protections against unreasonable search and seizure.

"I don't think that these devices should never be used, but at the same time, you should clearly be getting a warrant," said Alan Butler of EPIC.

In most states, police can get many kinds of cellphone data without obtaining a warrant, which they'd need to search someone's house or car. Privacy advocates, legislators and courts are debating the legal standards with increasing intensity as technology — and the amount of sensitive information people entrust to their devices — evolves.

VAST DATA NET

Many people aren't aware that a smartphone is an adept location-tracking device. It's constantly sending signals to nearby cell towers, even when it's not being used. And wireless carriers store data about your device, from where it's been to whom you've called and texted, some of it for years.

The power for police is alluring: a vast data net that can be a cutting-edge crime-fighting tool.

In October 2012, in Colorado, a 10-year-old girl vanished while she walked to school. Volunteers scoured Westminster looking for Jessica Ridgeway.

Local police took a clandestine tack. They got a court order for data about every cellphone that connected to five providers' towers on the girl's route. Later, they asked for 15 more cellphone site data dumps.

Colorado authorities won't divulge how many people's data they obtained, but testimony in other cases indicates it was at least several thousand people's phones.

The court orders in the Colorado case show police got "cellular telephone numbers, including the date, time and duration of any calls," as well as numbers and location data for all phones that connected to the towers searched, whether calls were being made or not. Police and court records obtained by USA TODAY about cases across the country show that's standard for a tower dump.

The tower dump data helped police choose about 500 people who were asked to submit DNA samples. The broad cell-data sweep and DNA samples didn't solve the crime, though the information aided in the prosecution. A 17-year-old man's mother tipped off the cops, and the man confessed to kidnapping and dismembering the girl, hiding some of her remains in a crawl space in his mother's house. He pleaded guilty and last month was sentenced to more than 100 years in prison.

Not every use of the tower dumps involved stakes so high.

Richland County (S.C) Sheriff Leon Lott ordered four cell-data dumps from two towers in a 2011 investigation into a rash of car break-ins near Columbia, including the theft of collection of guns and rifles from his police-issued SUV, parked at his home.

"We were looking at someone who was breaking into a lot of vehicles and was not going to stop," Lott said. "So, we had to find out as much information as we could." The sheriff's office says it has used a tower dump in at least one prior case, to help solve a murder.

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 calls, texts and locations.

Cellphone data sweeps fit into a broadening effort by police to collect and mine information about people's activities and movements.

Police can harvest data about motorists by mining toll-road payments, red-light cameras and license-plate readers. Cities are installing cameras in public areas, some with facial-recognition capabilities, as well as Wi-Fi networks that can record the location and other details about any connecting device.

SECRET STINGRAYS

Local and state police, from Florida to Alaska, are buying Stingrays with federal grants aimed at protecting cities from terror attacks, but using them for far broader police work.


RECOMMENDED FOR YOU
Gov. Christie to take questions about bridge scandal
(/story/news/politics/2014/01/09/christie-

With the mobile Stingray, police can get a court order to grab some of the same data available via a tower dump with two added benefits. The Stingray can grab some data from cellphones in real time and without going through the wireless service providers involved. Neither tactic — tower dumps or the Stingray devices — captures the content of calls or other communication, according to police.

Typically used to hunt a single phone's location, the system intercepts data from all phones within a mile, or farther, depending on terrain and antennas.

The cell-tracking systems cost as much as $400,000, depending on when they were bought and what add-ons they have. The latest upgrade, code-named "Hailstorm," is spurring a wave of upgrade requests.

Initially developed for military and spy agencies, the Stingrays remain a guarded secret by law enforcement and the manufacturer, Harris Corp. of Melbourne, Fla. The company would not answer questions about the systems, referring reporters to police agencies. Most police aren't talking, either, partly because Harris requires buyers to sign a non-disclosure agreement.

"Any idea of having adequate oversight of the use of these devices is hampered by secrecy," says Butler, who sued the FBI for records about its Stingray systems. Under court order, the FBI released thousands of pages, though most of the text is blacked out.

"When this technology disseminates down to local government and local police, there are not the same accountability mechanisms in place. You can see incredible potential for abuses," American Civil Liberties Union lawyer Catherine Crump says.

PRIVACY CONCERNS

Crump and other privacy advocates pose questions such as "Is data about people who are not police targets saved or shared with other government agencies?" and "What if a tower dump or Stingray swept up cell numbers and identities of people at a political protest?"

When Miami-Dade 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.

Most of the police agencies that would talk about the tactics said they're not being used for intelligence gathering, only in search of specific targets.

Lott, the sheriff in the South Carolina gun-theft case, said police weren't interested in seeing data about the other residents whose information was collected as a byproduct of his agency's tower dumps.

"We're not infringing on their rights," Lott said. "When they use that phone, they understand that information is going to go to a tower. We're not taking that information and using it for any means whatsoever, unless they're the bad guy or unless they're the victim."

Brian Owsley, a former magistrate who reviewed many police requests for bulk cellphone data, grew skeptical because authorities were not always forthcoming about the technology or what happened with "collateral data" of innocent bystanders.

"What is the government doing with the data?" asks Owsley, now a law professor at Texas Tech University.

Surveillance regulation is being tinkered with piecemeal by courts and legislators. This year, Montana and Maine passed laws requiring police to show probable cause and get a search warrant to access some cellphone data, as they would to search a car or home. State and federal courts have handed down seemingly contradictory rulings about which cellphone data is private or not. Seattle's City Council requires police to notify the council of new surveillance technology deployed in the city.

"We have to be careful because Americans deserve an expectation of privacy, and the courts are mixed right now as to what is an expectation of privacy when using a cellphone," says U.S. Rep. Dennis Ross, R-Fla., who says Congress needs to clarify the law. "More and more, we're seeing an invasion of what we would expect to be private parts of our lives."

Legislative and judicial guidance is needed to match police surveillance rules to today's technology, says Wayne Holmes, a prosecutor for two Central Florida counties. He has weighed frequent local police requests for tower dumps and Stingray surveillance. "The clearer the law, the better the law is."

Americans "are sensitized right now" to cellphone surveillance because of reports about potential abuses by the NSA, said Washoe County Sheriff Michael Haley of Reno. He is opting not to use the Stingray.

"I'm being cautious about how I access information, because at the end of the day I know that I will be in court if I access information using systems and techniques that are not constitutionally vetted," Haley said.

Contributing: Clark Fouraker, Nicole Vap, Martha Bellisle and Noah Pransky


RECOMMENDED FOR YOU
Gov. Christie to take questions about bridge scandal
(/story/news/politics/2014/01/09/christie-

SHARE 17270 CONNECT 2052 TWEET (https://twitter.com/intent/tweet?url=http://usat.ly/1dcpgrI&text=Cellphone%20data%20spying:%20It's

NSA PHONE TRACKING (/TOPIC/AA28C8B6-36D2-4912-
614E-1DA7ED1/NSA-PHONE-TRACKING/)
RECOMMENDED FOR YOU

Gov. Christie to take questions about bridge scandal
(/story/news/politics/2014/01/09/christie-
NSA controversies spur states into action

(/story/news/nation/2014/01/09/stateline-nsa-controversies-spur-states-into-action/4387927/)
(/story/news/nation/2014/01/09/stateline-nsa-controversies-spur-states-into-action/4387927/)

Maggie Clark

European Parliament invites Snowden to testify

(/story/news/world/2014/01/09/europe-parliament-snowden-nsa/4387153/)
(/story/news/world/2014/01/09/europe-parliament-snowden-nsa/4387153/)

Sen. Paul says he's suing over NSA policies

(/story/news/politics/2014/01/04/paul-senate-nsa-phones/4316833/)
(/story/news/politics/2014/01/04/paul-senate-nsa-phones/4316833/)

U.S. spy court: NSA to keep collecting phone records

(/story/news/politics/2014/01/03/governme surveillance-ruling-appeal/4308143/)
(/story/news/politics/2014/01/03/government-surveillance-ruling-appeal/4308143/)

Stephen Braun and Kimberly Dozier

The surprises of 2013

(http://www.wbir.com/story/news/nation/20 surprises-of-2013/4276505/)
(http://www.wbir.com/story/news/nation/2014/01/01/the-s-of-2013/4276505/)

RECOMMENDED FOR YOU ✖

Gov. Christie to take questions about bridge scandal

(/story/news/politics/2014/01/09/christie-

Ex-NSA chief calls for Obama to reject recommendations

(/story/news/politics/2013/12/30/gen-michael-hayden-urges-obama-reject-nsa-commission-recommendations/4249983/)

(/story/news/politics/2013/12/30/gen-michael-hayden-urges-obama-reject-nsa-commission-recommendations/4249983/)

Susan Page

USA NOW

(/media/cinematic/video/4389621/coachella-what-you-need-to-know-usa-now/)

Coachella: What you need to know | USA NOW

Jan 09, 2014

RECOMMENDED FOR YOU

Gov. Christie to take questions about bridge scandal

(/story/news/politics/2014/01/09/christie-