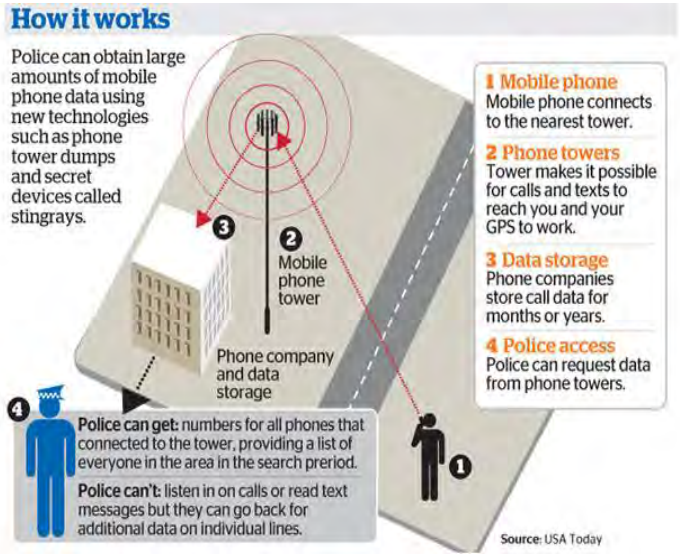
# AUSTRALIAN POLICE TRAWL PHONE DATA OF THOUSANDS

Ben Grubb and Emma Partridge July 7, 2014

Data concerns: Law enforcement agencies are conducting 'tower dumps' to find criminals. Photo: Robert Rough.

Australian federal and state police are ordering phone providers to hand over personal information about thousands of mobile phone users, whether they are targets of an investigation or not. Fairfax Media has confirmed Australian law-enforcement agencies are using a technique known as a "tower dump", which gives police data about the identity, activity and location of any phone that connects to targeted cell towers over a set span of time, generally an hour or two.




A typical dump covers multiple towers, and mobile providers, and can net information about thousands of mobile phones. The dumps are usually used in circumstances when police have few leads and can be a useful, powerful tool in tracking down criminals.

But privacy advocates say that while they may be helpful to police, they also target thousands of innocent people and don't have any judicial oversight. In addition to no warrant being required to request a tower dump containing the mobile phone data of thousands of people to track down one or more criminals involved in a crime, privacy advocates also question what is being done to the data collected once an investigation is complete. USA Today initially reported how US law-enforcement agencies were using the tower dump tactic earlier this year. (Read below)

NSW Police, Victoria Police and the Australian Federal Police all declined to comment. But Fairfax Media has been able to confirm that "tower dumps" were an investigation tool often used by NSW Police. A NSW Police spokesman said it would “not comment” on its “operational capabilities”. Victoria Police wouldn't discuss tower dumps either, saying it did not comment on "police methodology”. And the Australian Federal Police also said it would not comment on its "technical capabilities”. Some phone companies receiving the requests, however, admitted that tower dumps occurred.

“On occasion mobile network operators receive requests from Australian law-enforcement agencies to provide communications information from a specific tower,” a Vodafone spokeswoman told Fairfax. “These requests usually cover short periods and the information provided is only metadata.” Metadata is information about the time, duration and destination of calls but not their content. Metadata can also include location data about a mobile phone, even when it’s not on a call. Telstra wouldn’t say whether it received tower dump requests but believed they were lawful. “A request for non-content information on the use of a particular tower during a specified period of time may be lawful under certain circumstances,” a Telstra spokeswoman said.

Meanwhile, Optus would not comment on the tower dump practice at all, saying instead that it assisted “law-enforcement and national security agencies as required in the legislation...” Greens Party spokesman for communications, Scott Ludlam, said this was the first time the practice of tower dumps had been confirmed to occur in Australia. “It’s another example where [agencies] are collecting the entire haystack in order to find the needle,” Senator Ludlam said in an interview with Fairfax. “What we've seen with other techniques like this is there is no requirement to destroy the material that is collected incidentally after an investigation is complete,” Senator Ludlam said. He added that he would like to see more transparency around what type of crime needed to be committed in order for tower dumps to occur.

“What we need is transparency as to what's being done and who is doing it,” he said. “Ultimately I think we need a lawful warranting process to start to apply to [requests for data] like this.” Although the Attorney-General’s Department releases a once-a-year report detailing how many requests are made to telecommunications companies for metadata in Australia, it’s unclear whether a tower dump is counted as one metadata request or otherwise. Considering thousands of users are affected by tower dumps, Ludlam argues that they should count for the number of those who are affected. Around 330,000 requests for metadata were made by law-enforcement agencies in 2012-13, according to the latest report published by the Attorney-General’s Department.

http://www.illawarramercury.com.au/story/2399937/police-trawl-phone-data-of-thousands/?cs=300

# POLICE HOOVER UP MOBILE PHONE DATA OF EVERYDAY USERS

HANNAH FRANCIS JULY 07, 2014 11:45AM

Privacy advocates are up in arms after revelations that Australian law enforcement authorities are trawling through the metadata of thousands of mobile phone users -- revealing their location and identity -- regardless of whether they are under investigation or not. A Fairfax Media report found that government authorities had requested metadata from telco providers in what's known as a 'tower dump' -- acquiring data from mobile phone towers about the location and activity of mobile phone devices that connect to them over a specified time period. Mobile phones transmit data to towers whether or not a person is making a phone call.

NSW Police told the media outlet it had used the practice as investigative tool, while a number of telcos confirmed they had received requests for metadata from government agencies. "Looking at cell tower data gives anyone who's interested a rough approximation of your location," Swinburne University's Philip Branch told *Business Spectator.* "If someone is evading police is will give a rough approximation; they can also perhaps put together some sort of evidence around if someone receives a phone call and then makes a dash immediately after," Dr Branch said.

However, privacy advocates are concerned about the use of the practice in 'fishing expeditions' that net the data of thousands of innocent people. WA Senator Scott Ludlam, an outspoken advocate for online privacy, told *Fairfax Media* that a lawful warrants process should be introduced around the practice. "It's another example where [agencies] are collecting the entire haystack in order to find the needle," Senator Ludlam told the media outlet. According to Electronic Frontiers Australia, any government authority with some role in law enforcement or that collects public money -- such as city councils and the RSPCA -- is able to lawfully undertake tower dumps under the Telecommunications (Interception and Access) Act 1979.

Last year Wyndham City Council came under fire for using the practice to monitor residents for small infringements such as littering, unauthorised advertising and unregistered pets. The Act is currently under review by the Senate Legal and Constitutional Affairs References Committee. EFA executive officer Jon Lawrence said the legislation currently does not provide sufficient regulation around interception of mobile phone metadata. "We're not opposed to surveillance per se, what we're concerned about is the ubiquitous vacuuming up of data that has serious risks," Mr Lawrence said.

"It allows them to go on a fishing expedition and that's really worrying and very difficult to justify in anything but the most extreme circumstances." Mr Lawrence said the practice should only be allowed in the most serious of criminal investigations and should be restricted to certain organisations. "It's clearly open to far too wide a range of organisations," he said. "The RSPCA, Wyndham City Council and Australia Post have used this power. That needs to be tightened up quite dramatically and I believe law enforcements have actually called for that.

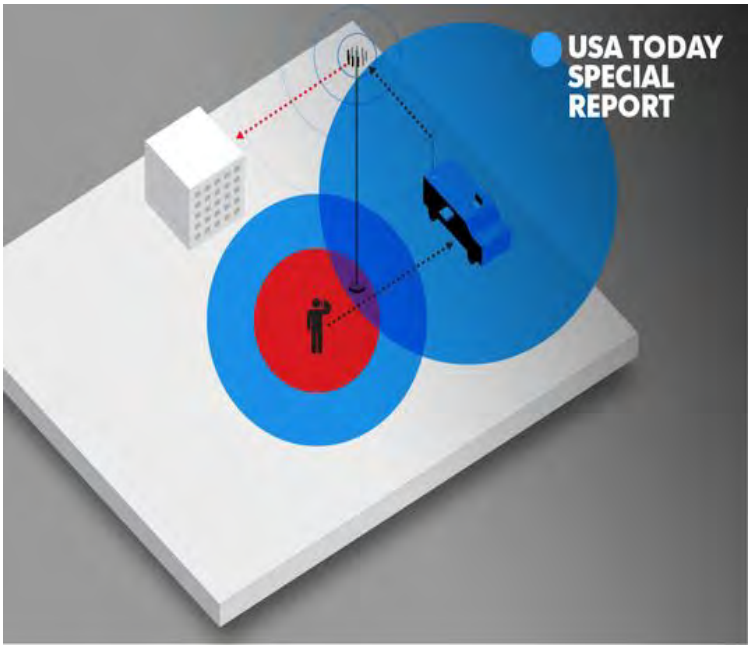
"There are no requirements on these organisations to delete the data and there's a real danger of people's privacy getting trampled over. Also presumption of innocence is being turned on its head." The revelations come as Federal Attorney-General George Brandis is set to introduce legislation into parliament next week that would increase the powers of national spy agencies. A separate bill to establish a mandatory data collection regime requiring telcos to store customer metadata for up to two years is also due to be introduced. The legislation is being formed in response to a report from the joint committee on intelligence and security, which was released in May last year.

http://www.theaustralian.com.au/business/latest/police-hoover-up-mobile-phone-data-of-everyday-users/story-e6frg90f-1226980267457

# CELLPHONE DATA SPYING: IT'S NOT JUST THE NSA

John Kelly, USA TODAY *June 13, 2014*

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. USA TODAY research John Kelly, Kevin A. Kepple, Jerry Mosemak, Janet Loehrke and Jeff Dionise, USA TODAY. *Police maintain that cellphone data can help solve crimes, track fugitives or abducted children — or even foil a terror attack.*




*(Photo: Jerry Mosemak)*

About 1 in 4 law-enforcement agencies have used a tactic known as a "tower dump". At least 25 police departments own a Stingray, a device that acts as a fake cell tower. 36 more police agencies refused to say whether they've used either tactic. 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.

•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.

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

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. Alan Butler of EPIC. "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.

We had to find out as much information as we could. Richland County Sheriff Leon Lott. 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. 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. What is the government doing with the data?

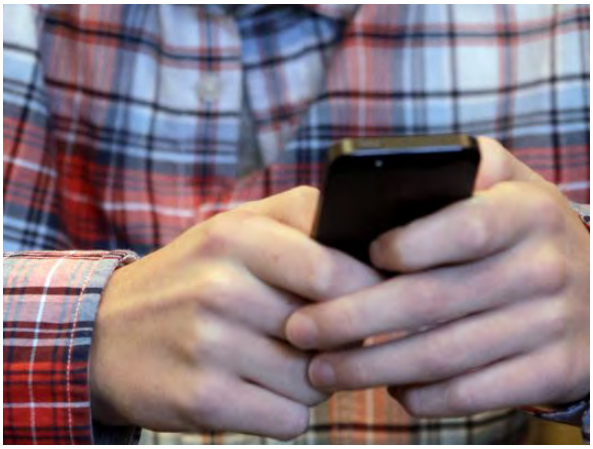
Brian Owsley, law professor at Texas Tech University. Surveillance regulation is being tinkered with piecemeal by courts and legislators. This year, Montana and Maine passed laws requiring police to show probable cause and get a search warrant to access some cellphone data, as they would to search a 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*

http://www.usatoday.com/story/news/nation/2013/12/08/cellphone-data-spying-nsa-police/3902809/



## EXAMPLES OF DATA-GATHERING ABUSES

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

John Kelly,*12:23 p.m. EDT June 10, 2014*

*(Photo: Nam Y. Huh, AP)*

Some examples of documented misuse of data-gathering technology:

In Minnesota: State auditors found that 88 police officers in departments across the state misused their access to personal data in the state driver's license database to look up information on family, friends, girlfriends or others without proper authorization or relevance to any official investigation in 2012. And those were just the clear-cut cases. Auditors said that more than half of the law enforcement officers in the state made questionable queries of the database, which includes photos and an array of sensitive personal data.

In Florida: The state's Supreme Court is hearing a case in which a lower court found Broward County law enforcement overreached by conducting real-time tracking of the GPS location of a man's cellphone, using still-undisclosed techniques in collaboration with the cellphone carrier. The problem in that case: The police did so under authority of a court order that defense lawyers said authorized them to get only historical location data about his cellphone.

In Illinois: A suburban Chicago police officer responsible for overseeing access to the department's criminal history database used the system to look up his girlfriend's record. Similar cases have shown up in other states, resulting in cases involving harassment, stalking and identity theft, among others.

http://www.usatoday.com/news/

## CELL DATA DUMPS: A LEGALLY FUZZY AREA

John Kelly and Susanne Cervenka, USA *December 8, 2013. (Photo: Robin Loznak for USA TODAY).*

The rules governing how police obtain and use data from cellphones is a target on the move, as state legislatures act to protect residents' privacy and real-life criminal cases wend their way through state and federal courts.

Consider New Jersey, where the state's Supreme Court ruled this summer that individuals' privacy rights do extend to cellphone data. The Jersey ruling arose from a string of 2006 burglaries in Middletown. Police, hunting down suspect Thomas Earls, went to his wireless service provider T-Mobile three times in one night asking the company to give them the location of the cellphone towers that the man's mobile phone was connecting to at the time.

They didn't get a warrant. In its ruling, the New Jersey high court said cellphones have become "an indispensable part of modern life" and users do not intend for their location information to be shared with authorities or others. Location data available from cellphone use today is far more precise than it was even at the time of that case, the court noted. "Viewed from the perspective of a reasonable expectation of privacy, what was problematic in 2006 is plainly invasive today," the New Jersey justices wrote.

The National Security Agency isn't the only government entity secretly collecting data from people's cellphones. Police are increasingly scooping it up, too. VPC Other court rules have made different rulings about the level of privacy afforded to cellphone data. Lawmakers in various states are starting to weigh in.

Montana and Maine this year passed state laws requiring police demonstrate probable cause and get a search warrant to access some cellphone data, as they would to search a person's house or car. Similar legislation stalled in Texas and California, though the topic is expected to come up again in both states. At least eight other states are considering similar laws. Scrutiny has also been applied at the city and county level.

http://www.usatoday.com/story/news/nation/2013/12/08/cellphone-data-legal-issues-court/3902859/