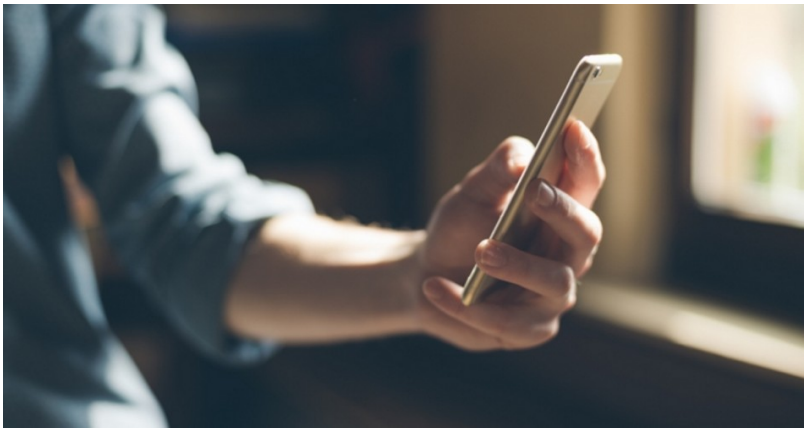
New American

Written by C. Mitchell Shaw on September 23, 2017

D.C. Court Rules Unwarranted Use of Cellphone Spying Tools is Unconstitutional



The D.C. Court of Appeals ruled Thursday that police using cell-site simulators to track mobile phones without a warrant is unconstitutional. In making its decision, the court overturned the conviction of a man found guilty in 2014 of robbery and sexual assault, since D.C. police had used location information from his phone without a warrant to gather evidence that led to the conviction.

In making the 2-1 decision, the court joined a growing number of courts that have similarly ruled the unwarranted use of cell-site simulators as unconstitutional. One other such court is Maryland's Court of Special Appeals, which ruled in April 2016 that "cellphone users have an objectively reasonable expectation that their cellphones will not be used as real-time tracking devices, through the direct and active interference of law enforcement." In that case, the Maryland court's decision resulted in overturning a conviction for attempted murder.

Cell-cite simulators — popularly known as "Stingrays" after one of the earliest and most used models — are highly sophisticated and expensive surveillance tools that capture information from cell tower traffic. They essentially conduct a "man-in-the-middle" attack by mimicking a cell tower and fooling all mobile phones in the area into connecting to them. The devices — which are about the size of a suitcase and can be transported in the back of a police car — then harvest data from the phones including the numbers of the phones, the numbers the phones are calling or texting, the location of the phones, and information about the phones themselves. Once the cell-site simulators have that information, they relay the connection to the nearest real tower in the area and then repeat the process in reverse to capture data going from the tower to the phone.

Echoing the sentiment of the Maryland court's previous decision about these devices, the D.C. Court of Appeals — which has appellate jurisdiction over cases arising from the D.C court system and should not be confused with the Federal Court of Appeals for the District of Columbia Circuit — ruled that the use of cell-site simulators without a warrant in the case it was deciding "invaded a reasonable expectation of privacy" and was therefore a violation of the protection against unreasonable searches and seizures enshrined in the Fourth Amendment. Judge Corinne Beckwith wrote in the majority opinion: "The simulator's operation involved exploitation of a security flaw in a device that most people now feel obligated to carry with them at all times. Allowing the government to deploy such a powerful tool without judicial oversight would surely 'shrink the realm of guaranteed privacy' far below that which 'existed when the Fourth Amendment was adopted.'" She added that the court's acquiescence of the unwarranted use of cell-site simulators would "place an individual in the difficult position either of accepting the risk that at any moment his or her cellphone could be converted into a tracking device or of foregoing 'necessary use of' the cell phone."

The court's decision stems from the case of Prince Jones, who had been sentenced to 66 years in prison.

Jones was accused of sexually assaulting and robbing two women within days of each other in 2013. The women both said they had agreed to meet a man they had met online and that when they met with him, he threatened them with a knife, sexually assaulted them, and robbed them.

Police — taking the shortest path instead of using tried and true investigative techniques — used a cell-site simulator to track the phone used to contact the women. The location led them to Jones, and when police searched the car he was in, they found items taken in the robberies.

This case — which is a victory for privacy and liberty — underscores the risks of police departments cutting constitutional corners. This is far from the first — and likely far from the last — case to be tossed out because the evidence was properly declared "fruit of the poisoned tree" because of the use of a cell-site simulator without a warrant. In fact, what makes this case different from previous ones is that D.C. police admitted they used the device. As this writer reported in a previous article from August 2015:

> While the use of Stingrays does bring about arrests, many of the cases are dropped or reduced to get a conviction on lesser charges in exchange for a confession. Why is that? Because police departments have to sign non-disclosure agreements with the FBI to even obtain or use Stingrays. As a result, police often do not — cannot — disclose (even to prosecutors) that they used the device. This means that police are caught between a rock and a hard place when it comes to testifying in court. If the officer discloses the fact that the reason he knew where to find the suspect was that he used a Stingray to sniff out his phone, the officer could be liable for violating the non-disclosure agreement. If he testifies falsely, he would be guilty of perjury. So the case is either dropped or the charges are reduced.

So, while that trend may be shifting and courts are lining up to declare the unwarranted use of these devices verboten, the fact remains that police departments all over the country continue to use them without a warrant since those departments are not bound by a DOJ policy from September 2015 requiring a warrant for their use.

While requiring police everywhere to obtain a warrant before using a cell-site simulator would go part of the way to answering the constitutional conundrum of where privacy and liberty must yield the right of way to intrusive investigative practices, there are concerns that a warrant cannot allay. The very nature of cell-site simulators means that *all traffic* within the range of the device is captured — not just the particular phone that is being "targeted." Because of this, the use of these devices always constitutes an invasion of privacy for the people whose phone traffic is vacuumed up in the process.

What should happen — though in this age of nearly ubiquitous surveillance, is not likely to — is for cell-site simulators to be added to the ash heap of items and practices that — because they never should have existed — are no longer used. Police departments have a plethora of tools in their toolboxes for investigating crimes, identifying criminals, making arrests, and bringing about convictions. Tools that require infringing on the rights of citizens don't belong in that toolbox.

Photo: Thinkstock