Four Takeaways From 'State v. Andrews'

"Four Takeaways From *State v. Andrews*" by Rachel Levinson-Waldman, originally published on Just Security, on April 1, 2016.

On Wednesday, an appellate court in Maryland handed down a major loss to the government, one that will send police and prosecutors back to the drawing board (or at least back to the magistrate for a warrant) when they want to track people in real-time using surreptitious, invasive technology. The tl;dr in *State v. Andrews* is that if you carry a cell phone, you have a right to expect that the government will not use it to track you without getting a warrant first.

Hidden behind that seemingly straightforward holding are a number of propositions that will hearten privacy and transparency advocates. I want to outline four key takeaways from this decision.

Background

First, a little background. The Baltimore police needed to find Kerron Andrews, who was wanted for attempted murder. They had a nifty device called a Hailstorm, which can force any cell phone in the vicinity to reveal its location. There was only one problem: The police department had promised the FBI it wouldn't tell anyone about the technology — including the courts. So the police asked a court for a different kind of order, one permitting the use of a "pen register / trap and trace" (PR/TT) device. PR/TT orders allow the police to detect which numbers are calling into, or being called from, a particular phone. If you want to find out if your target is communicating with the Mafia, it's just the ticket.

The police certified — misleadingly — that this was what they were doing. The application did reference a "cellular tracking device," but without giving any additional information about what it was or how it would be used. And because PR/TT orders require only a showing of relevance, the application didn't even have to demonstrate probable cause.

Armed with this order, a Baltimore police technical team asked Sprint, Andrews's service provider, for a variety of information about his phone, including "precision GPS data." Within hours, the police detectives started receiving Andrews's GPS coordinates, which narrowed down his location to a set of apartments at a particular address. After congregating there, a detective used the Hailstorm to locate the cell phone inside an individual apartment. The police arrested Andrews, got a search warrant for the apartment, and found a gun. He was ultimately indicted for an April 2014 attempted triple homicide.

When his defense attorney was finally notified that a "stingray" (a now-generic name for the type of device the police used) had been deployed to locate Andrews, he promptly asked the court to suppress the location evidence on the ground that its warrantless acquisition violated the Fourth Amendment, and the lower court granted his request. The government appealed, and the appeals court upheld the suppression decision in Wednesday's thoughtful and wide-ranging opinion. There are (at least) four aspects of the decision worth emphasizing.

1. You don't have to turn off your phone to be safe from warrantless government surveillance (at least in Maryland)

First, this appears to be the first case holding that a cell site simulator requires a warrant. Courts have addressed other methods of real-time cell phone tracking, and generally held that they require a warrant, but this decision is the first to take on this increasingly pervasive technology — probably in large part because of the insidious silence that surrounds them, as described below.

At the same time, the holding is quite broad: "[P]eople have a reasonable expectation that their cell phones will not be used as real-time tracking devices by law enforcement" and "an objectively reasonable expectation of privacy in real-time cell phone location information." This could equally apply to GPS or Wi-Fi monitoring as to cell-site surveillance. Count this as a significant win on the side of location privacy.

The court also roundly rejected the state Attorney General's argument that if you want to keep your location private, you can just turn off your phone. To the contrary, the panel held that individuals do not "volunteer to convey their location information simply by choosing to activate and use their cell phones and to carry the devices on their person." This approach owes much to Justice Sotomayor's concurrence in *United States v. Jones*, where she explained that location tracking could invade privacy at an unprecedented scale and chill First Amendment rights, and do so at such cheap cost and so surreptitiously as to "evade the ordinary checks that constrain abusive law enforcement practices: limited police resources and community hostility." So too, the *Andrews* court held, could "cell site simulators … allow the government to discover the private and personal habits of any user." In Maryland, at least, that won't fly anymore without a warrant.

2. Promising to withhold evidence from the court won't go well for the police

Remember how the police had promised the FBI that they wouldn't tell the court anything about the Hailstorm? Here's how it works: a private company, Harris Corporation, manufacturers Hailstorms and similar devices. When a police department wants to buy one, the company requires that the department sign a non-disclosure agreement with the FBI, promising to keep mum about its use. Those agreements have often been kept secret, but here, the court helpfully detailed the NDA between the FBI and the Baltimore City State's Attorney. The NDA is not a model of clarity, but it essentially prohibits the police from sharing any information about the equipment with

anyone, including the court. In the unlikely event that the court or public does get wind of its existence and asks for information, the State's Attorney is asked — nay, **directed** — to drop the case. (In fact,this has already happened.)

The panel was not pleased. It objected that this information embargo "prevents the court from exercising its fundamental duties under the Constitution." The court recognized something subtle and sophisticated: Adequately assessing the constitutional issues implicated by a surveillance device requires understanding its technological capabilities. And when the department tried to abide by the restrictions of the non-disclosure agreement it had signed, it failed to explain to the lower court what it was actually doing. The state's attempt to justify that move was, the court determined, both "detrimental to its position and inimical to the constitutional principles we revere." Not words the State's Attorney likely wanted to hear from the court.

3. In fact, when the government lies to the court, the court might not let it keep its evidence

The court's displeasure over the government's candor didn't stop with a mere rebuke. Instead, and somewhat remarkably, it held that because the police's use of the stingray was unconstitutional, the government couldn't use the evidence it captured to prosecute Andrews. This may seem like a no-brainer, but courts have traditionally been very uneasy about letting suspected (or convicted) criminals out of jail, and they often give the government a pass, especially when it comes to new technologies.

In effect, courts frequently say to the police: You shouldn't have used that technology without a warrant, and you can't do it anymore, but you had no reason to know that at the time, so no harm, no foul. The court gets to establish Fourth Amendment guidelines without releasing anyone from prison. This approach — the "good faith" exception to the exclusionary rule — is generally justified on the grounds that suppressing evidence is meant to deter police misconduct, and if the police were acting in good faith at the time they got the evidence, there is no reason to punish them by keeping it out.

The court here took a very different tack, not only issuing a serious reprimand to the conduct of the police, but making them pay the price for their error. The panel leaves aside entirely the question of whether the police should have known at the time they requested the PR/TT order that conducting real-time location tracking requires a warrant. Instead, the court methodically lists the ways in which the police misled the lower court in its "overreaching" application: failing to name or even describe the Hailstorm, failing to impose any geographical limitations on its use, failing to "fully apprise" the judge of the information it might collect, failing to explain what would happen with that information, and concealing the fact that the technology could easily capture information about innocent users in Andrews' vicinity. As a result, the "ensuing order did not support the use of the Hailstorm device, nor did it, in any way, serve as a de facto warrant for the use of the Hailstorm device."

Based on the government's lack of candor, the panel suppressed both the evidence about Andrews's location and — as the "fruit of the poisonous tree" — the gun that was uncovered during the subsequent search. Lest the lesson be lost, the court chided the officers for their "misleading order application and unconstitutionally intrusive conduct." When crucial evidence in an attempted murder investigation is deemed out of bounds, police and prosecutors tend to take notice.

4. The third-party doctrine is ready for its close-up

Finally, the court took on the third-party doctrine, which says that if you reveal information in order to use a company's services — say, giving a check to a bank or dialing a phone number — it is as if the information has been revealed to the world, and the police can get the same data from the company without having to get a warrant. In short, the third-party doctrine conflates secrecy and privacy: If you didn't keep something secret, you didn't keep it private either.

This principle has been the subject of increasingly loud criticism in recent years, most notably by Justice Sotomayor in her concurrence in *Jones*. But it has not been overturned by the Supreme Court, and courts have pointed to it for the proposition that because location information is conveyed to the cell provider, the data is fair game for law enforcement as well. The court here was having none of that, and rejected the state's efforts to rely on the doctrine.

As the court pointed out, the seminal Supreme Court decisions establishing the doctrine rested on the fact that the defendants there had knowingly and voluntarily conveyed the information in question (bank records and dialed phone numbers). Here, Andrews did nothing to share his location information; the Hailstorm pulled it directly from the phone, not from his cell service provider. Moreover, not only was he not even using his phone when the Hailstorm pinpointed it, but the detective's testimony revealed that a cell site simulator *will not work* if the phone is in use; it must be hung up before the simulator can find it. Thus, it is only when the average person would have no reason to think his phone is revealing his location — because he is not using it — that it is vulnerable to this kind of surreptitious tracking.

*** * ***

Needless to say, this is just one decision, and from a state appellate court at that. It will not be binding on any of the federal courts, nor the other 50 state courts (including DC), that will be increasingly confronted with the constitutional questions raised here. But the panel's careful, in-depth treatment of the issues, and its warning about the consequences of failing to deal candidly with the court, will be a warning flag for the many police departments and prosecutors using these technologies.

(Photo: Flickr/GonzaloBaeza)