The Supreme Court Tells Cops to Back Off Your Cell Phone

By: Julian Sanchez
June 26, 2014

For years, the police could arrest you for almost nothing as an excuse to search your device without a warrant.

Well my iPhone is locked, so is the tablet in my pack, and I know my rights, so you gon' need a warrant for that. That, with apologies to Jay-Z, is the upshot of the Supreme Court's unanimous ruling today in Riley v. California (PDF), which holds that police must get a judge's approval before rummaging through the cell phones of people they arrest—closing a potentially massive loophole in the Fourth Amendment's protection against unreasonable searches and seizures.

The Court's 9-0 decision limits the scope of a longstanding exception to the Fourth Amendment's requirement that law enforcement officers obtain a warrant based on "probable cause" to conduct intrusive searches. Under the so-called "search incident to arrest exception," when police place someone under arrest, they can conduct a warrantless search of the person and their immediate surroundings to look for weapons that might pose a threat to the arresting officer, as well as evidence the suspect might attempt to hastily destroy.

In the era of the smartphone, however, legal scholars have long worried that exception could metastasize, with lethal consequences for privacy. As Justice John Roberts wrote for the court, pocket-sized computers holding gigabytes of profoundly intimate data have become "such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." With increasingly powerful mobile devices routinely holding entire photo albums, personal videos, records of Web-browsing history, and vast archives of private correspondence, Roberts noted, giving police free reign to look through a modern phone "would typically expose to the government far more than the most exhaustive search of a house."

That's what David Riley learned after being pulled over for driving with expired registration tags and (police soon discovered) an expired license, along with two concealed handguns. Suspecting

that Riley might be a member of the Bloods street gang, the arresting officer seized his smartphone and handed it over to detectives at the station house, who "went through" it "looking for evidence." He found "a lot of stuff" as he probed the files on the phone—including videos suggestive of gang involvement and a photo of Riley with a car police had tied to a shooting weeks earlier.

What he didn't find, however, was a judge to issue a warrant authorizing the search. That, the Court held, was a mistake. The Fourth Amendment exception for searches incident to arrest was meant to ensure officer safety and protect evidence—not provide an excuse for police go on free-range fishing expeditions through gigabytes worth of a person's most private data. Even when it comes to "dumb" phones, the Court said, police must get a warrant to look through digital information on a mobile device, absent some special emergency.

The Court's unanimous rejection of such warrantless searches closes off two nightmare scenarios that had haunted the dreams of civil libertarians.

First, there was the specter of the Supreme Court's 5-4 ruling in a 2001 case called *Atwater v. Lago Vista*. There, the Court had held that the Fourth Amendment does not place any limits on the "seriousness" of an offense for which someone can be arrested. That means police have the discretion to arrest people for even trivial infractions such as failure to wear a seat belt—the "crime" for which Gail Atwater had been hauled to jail.

An unlimited "search incident to arrest" exception, combined with the *Atwater* ruling, threatened to give police a dangerous incentive: Why jump through all the hoops needed to convince a judge to issue a digital search warrant when you can pop a suspect for loitering or jaywalking and have a free pass to delve through their e-mails and photos?

Second, and compounding the risk of such pretextual searches, there was the growing popularity of powerful forensic devices, like those manufactured by the company Cellbrite, capable of quickly copying a smartphone's entire contents. That meant that even if a suspect were held only briefly, their files could be retained and scrutinized at leisure, with the owner potentially none the wiser.

For once, privacy advocates can sleep a bit easier. The Court's "answer to the question of what police must do before searching a cell phone seized incident to arrest is… simple—get a warrant."

-Julian Sanchez is a senior fellow at the Cato Institute where he studies issues at the busy intersection of technology, privacy, and civil liberties, with a particular focus on national security and intelligence surveillance.