Supreme Court Says Law Enforcement Can't Search Mobile Phones Without A Warrant

The Supreme Court released its ruling in the Riley/Wurie cases that examine whether or not the police can search through your mobile phone without a warrant. Both the Riley and Wurie cases basically deal with the same issue, though one (Riley) involves a smartphone, while the other (Wurie) is about a more old-fashioned flip phone. I had significant problems with the government's arguments in defending such warrantless searches and so did the Supreme Court, which has made it clear that police **cannot** search phones without a warrant.

In short, the Supreme Court actually believes in the 4th Amendment. This ruling is likely to become a very key one in a number of other upcoming questions about where the 4th Amendment applies to new technologies. The Court recognizes that existing precedent allows for searches of *physical* containers, but thankfully declines to accept the government's argument that searching digital devices is the same thing. First, it notes that a big part of the reasoning that allowed the search of physical containers was to make sure there weren't any dangerous weapons. Here (despite the claims of some rather confused police) the Court realizes this is ridiculous.

> *Digital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee's escape. Law enforcement officers remain free to examine the physical aspects of a phone to ensure that it will not be used as a weapon—say, to determine whether there*

> *is a razor blade hidden between the phone and its case. Once an officer has secured a phone and eliminated any potential physical threats, however, data on the phone can endanger no one.*

The ruling basically says that if the data on the phone is important, law enforcement can go get a warrant and then do the search later. It's not an emergency situation that needs to be viewed immediately. The court completely brushes off the argument from the government that remote wiping capability means content searches may be urgent by basically saying that it's not likely to happen very often or to be much of an issue. In short, this hypothetical situation of remotely wiping phones isn't likely to be a real problem – and notes that police have alternative ways to deal with that hypothetical "risk."

The court digs into just how different a digital device is than a physical container, and how the implications for allowing a search would be extreme.

> *Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person. The term "cell phone" is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.*
>
> *One of the most notable distinguishing features of modern cell phones is their immense storage capacity. Before cell phones, a search of a person was limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy…. Most people cannot lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or*

> *article they have read—nor would they have any reason to attempt to do so. And if they did, they would have to drag behind them a trunk of the sort held to require a search warrant in Chadwick, supra, rather than a container the size of the cigarette package in Robinson.*

More important than that is how this impacts your privacy:

> *The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier. A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a phone.*
>
> *Finally, there is an element of pervasiveness that characterizes cell phones but not physical records. Prior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day. Now it is the person who is not carrying a cell phone, with all that it contains, who is the exception.*

And, from that, the court notes, the world with smartphones is a very different world:

> *In 1926, Learned Hand observed … that it is "a totally different thing to search a man's pockets and use against him what they contain, from ransacking his house for everything which may incriminate him." … If his pockets contain a cell phone, however, that is no longer true. Indeed, a cell phone search would typically expose to the government far more than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private*

> *information never found in a home in any form— unless the phone is.*

Furthermore, the court notes that it's not just the storage on the phone that's at issue, but the fact that most phones reach out into the cloud:

> *To further complicate the scope of the privacy interests at stake, the data a user views on many modern cell phones may not in fact be stored on the device itself. Treating a cell phone as a container whose contents may be searched incident to an arrest is a bit strained as an initial matter…. But the analogy crumbles entirely when a cell phone is used to access data located elsewhere, at the tap of a screen. That is what cell phones, with increasing frequency, are designed to do by taking advantage of "cloud computing." Cloud computing is the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself. Cell phone users often may not know whether particular information is stored on the device or in the cloud, and it generally makes little difference.*

The ruling then walks through and rejects each of the attempts by the government to offer up ways in which it should be allowed to search phones. One important one involves the government's argument that the ruling in Smith v. Maryland (which we've discussed a lot – covering how there's no privacy expected in data handed to third parties) means retrieving the phone's call log is permitted. However, here the court notes this is **not** the same thing.

> *We also reject the United States' final suggestion that officers should always be able to search a phone's call log, as they did in Wurie's case. The Government relies on Smith v. Maryland,… which held that no warrant was required to use a pen register at telephone company premises to identify numbers dialed by a particular caller. The Court in that*

> *case, however, concluded that the use of a pen register was not a "search" at all under the Fourth Amendment. …. There is no dispute here that the officers engaged in a search of Wurie's cell phone. Moreover, call logs typically contain more than just phone numbers; they include any identifying information that an individual might add, such as the label "my house" in Wurie's case.*

The court also – importantly – highlights how attempts by the government to claim that looking through photographs on a phone is "analogous" to looking through photos in a wallet are not, in fact, analogous:

> *But the fact that a search in the pre-digital era could have turned up a photograph or two in a wallet does not justify a search of thousands of photos in a digital gallery. The fact that someone could have tucked a paper bank statement in a pocket does not justify a search of every bank statement from the last five years. And to make matters worse, such an analogue test would allow law enforcement to search a range of items contained on a phone, even though people would be unlikely to carry such a variety of information in physical form.*

That tidbit seems like it could be quite useful in future cases in which the government defends its collection of *bulk* data. That said, the court does note (in a footnote clearly directed at this issue) that this ruling is *not* about such bulk collections:

> *Because the United States and California agree that these cases involve searches incident to arrest, these cases do not implicate the question whether the collection or inspection of aggregated digital information amounts to a search under other circumstances.*

That said, the framework discussed in the ruling does, quite strongly, suggest that the Supreme Court will be fairly skeptical towards the government's defense of bulk collections. Now we just need to wait for a case challenging those programs to actually reach the Court.

Download (PDF, Unknown)