UNANIMOUS: COPS NEED A WARRANT TO ACCESS YOUR PHONE DATA

SCOTUS just unanimously held that cops generally need a warrant to access your cell phone data. Chief Justice Roberts wrote the opinion. The opinion is here.

I'm reading now to figure out what it means. Will update accordingly.

This passage is getting widely cited:

> These cases require us to decide how the search incident to arrest doctrine applies to modern cell phones, which are now 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. A smart phone of the sort taken from Riley was unheard of ten years ago; a significant majority of American adults now own such phones.

I'm amused by the way Roberts deals with the government's belated encryption argument.

> Encryption isa security feature that some modern cell phones use in addition to password protection. When such phones lock, data becomes protected by sophisticated encryption that the password. Brief for United States as *Amicus Curiae* in No. 13–132, p. 11.
>
> [snip]
>
> And data encryption is even further afield. There, the Government focuses on the ordinary operation of a phone's security features,apart from *any* active attempt by a defendant or his associates

> to conceal or destroy evidence upon arrest.
>
> We have also been given little reason to believe that either problem is prevalent.
>
> [snip]
>
> Similarly, the opportunities for officers to search a password-protected phone before data becomes encrypted are quite limited. Law enforcement officers are very unlikely to come upon such a phone in an unlocked state because most phones lock at the touch of a button or, as a default, after some very short period of inactivity. See, *e.g.,* iPhone User Guide for iOS 7.1 Software 10 (2014) (default lock after about one minute). This may explain why the encryption argument was not made until the merits stage in this Court, and has never been considered by the Courts of Appeals

This language should have application outside of this context (as I'll return to).

> 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 physicalrealities and tended as a general matter to constitute onlya narrow intrusion on privacy. See Kerr, Foreword: Accounting for Technological Change, 36 Harv. J. L. & Pub.Pol'y 403, 404–405 (2013). Most people cannot lug aroundevery piece of mail they have received for the past severalmonths, every picture they have taken, or every book or article they have read—nor would they have any reason toattempt to do so. And if they did, they would have to dragbehind 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*.
>
> But the possible intrusion on privacy is not physically limited in the same way when it comes to cell phones. The current top-selling smart phone has a standard capacity of 16 gigabytes (and is available with up to 64 gigabytes). Sixteen gigabytes translates to millions of pages of text, thousands of pictures, or hundreds of videos. See Kerr, *supra*, at 404; Brief for Center for Democracy & Technol- ogy et al. as *Amici Curiae* 7–8. Cell phones couple that capacity with the ability to store many different types of information: Even the most basic phones that sell for lessthan $20 might hold photographs, picture messages, text messages, Internet browsing history, a calendar, a thousandentry phone book, and so on. See *id.,* at 30; *United States* v. *Flores-Lopez*, 670 F. 3d 803, 806 (CA7 2012). We expectthat the gulf between physical practicability and digital capacity will only continue to widen in the future.
>
> The storage capacity of cell phones has several interrelated consequences for privacy. First, a cell phone collects in one place many distinct types of information—an address, a note, a

> prescription, a bank statement, a video—that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows even justone type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot besaid 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.[1]
>
> 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 abouttheir day. Now it is the person who is not carrying a cellphone, with all that it contains, who is the exception.According to one poll, nearly three-quarters of smartphone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower. See Harris Interactive, 2013 Mobile Consumer Habits Study (June 2013). A decade agopolice officers searching an arrestee might have occasionally stumbled across a highly personal item such as adiary. See, *e.g., United States* v. *Frankenberry*, 387 F. 2d 337 (CA2 1967) (*per curiam*). But those discoveries were likely to be few and far between. Today, by contrast, it isno exaggeration to say

> that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate. See *Ontario* v. *Quon*, 560 U. S. 746, 760 (2010). Allowing the police to scrutinize such records on a routine basis is quite different fromallowing them to search a personal item or two in the occasional case.
>
> Although the data stored on a cell phone is distinguished from physical records by quantity alone, certaintypes of data are also qualitatively different. An Internet search and browsing history, for example, can be found onan Internet-enabled phone and could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD. Data on a cell phone can also reveal where a person has been. Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building.See *United States* v. *Jones*, 565 U. S. ___, ___ (2012) (SOTOMAYOR, J., concurring) (slip op., at 3) ("GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.").
>
> Mobile application software on a cell phone, or "apps," offer a range of tools for managing detailed informationabout all aspects of a person's life. There are apps for Democratic Party news and Republican Party news; appsfor alcohol, drug, and gambling addictions; apps for sharing prayer requests; apps for

> tracking pregnancy symptoms; apps for planning your budget; apps for every conceivable hobby or pastime; apps for improving your romantic life. There are popular apps for buying or selling just about anything, and the records of such transactionsmay be accessible on the phone indefinitely. There are over a million apps available in each of the two major app stores; the phrase "there's an app for that" is now part ofthe popular lexicon. The average smart phone user has installed 33 apps, which together can form a revealing montage of the user's life. See Brief for Electronic PrivacyInformation Center as *Amicus Curiae* in No. 13–132, p. 9.
>
> In 1926, Learned Hand observed (in an opinion later quoted in *Chimel*) 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 whichmay incriminate him." *United States* v. *Kirschenblatt*, 16 F. 2d 202, 203 (CA2). 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 ofprivate information never found in a home in any form—unless the phone is.

But note this footnote, which is critical:

> [1]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.

This language, noting that some people's phones access cloud stored data, may be significant in the case of the 11th Circuit cell location case.

> 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. See Brief for Electronic Privacy Information Center in No. 13–132, at 12–14, 20. Moreover, the same type of data may bestored locally on the device for one user and in the cloud for another.
>
> The United States concedes that the search incident to arrest exception may not be stretched to cover a search of files accessed remotely—that is, a search of files stored in the cloud. See Brief for United States in No. 13–212, at 43–44. Such a search would be like finding a key in asuspect's pocket and arguing that it allowed law enforcement to unlock and search a house. But officers searching a phone's data would not typically know whether the information they are viewing was stored locally at the time of the arrest or has been pulled from the cloud.

And I love this snark.

> Alternatively, theGovernment proposes that law enforcement agencies"develop protocols to address" concerns raised by cloud computing. Reply Brief in No. 13–212, pp. 14–15. Probably a good idea, but the Founders did not fight a revolution to gain the right to government agency protocols.

Though it may actually be important snark. Developing protocols is how the US deals with privacy problems at NSA.

OK, this paragraph may be critically important. Very excited about this paragraph.

> 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*, 442 U. S. 735 (1979), which held thatno 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 underthe Fourth Amendment. See *id.,* at 745–746. There is no dispute here that the officers engaged in a search of Wurie's cell phone. Moreover, call logs typically containmore than just phone numbers; they include any identifying information that an individual might add, such as thelabel "my house" in Wurie's case

Given how often Otis has been raised in the last year, Roberts' mention of it is significant, I think.

> Our cases have recognized that the Fourth Amendment was the founding generation's response to the reviled"general warrants" and "writs of assistance" of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity. Opposition to such searches was in fact one of thedriving forces behind the Revolution itself. In 1761, the patriot James Otis delivered a speech in Boston denouncing the use of writs of assistance. A young John Adamswas there, and he would later write that "[e]very man of acrowded audience appeared to me to go away, as I did,ready to take arms against writs of assistance." 10 Works

> of John Adams 247–248 (C. Adams ed. 1856). According to Adams, Otis's speech was "the first scene of the first act of opposition to the arbitrary claims of Great Britain. Then and there the child Independence was born." *Id.,* at 248 (quoted in *Boyd* v. *United States*, 116 U. S. 616, 625 (1886)).

If they're smart, the ACLU will integrate this into their advertising campaigns. [Update: literally seconds after I posted this I saw this, which had just been posted]

> Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple— get a warrant.