134 S.Ct. 2473
Supreme Court of the United States

David Leon RILEY, Petitioner
v.
CALIFORNIA.
United States, Petitioner
v.
Brima Wurie.

Nos. 13–132, 13–212. | Argued April 29, 2014. |
Decided June 25, 2014.

Opinion

Chief Justice ROBERTS delivered the opinion of the Court.

These two cases raise a common question: whether the police may, without a warrant, search digital information on a cell phone seized from an individual who has been arrested.

In the first case, petitioner David Riley was stopped by a police officer for driving with expired registration tags. In the course of the stop, the officer also learned that Riley's license had been suspended. The officer impounded Riley's car, pursuant to department policy, and another officer conducted an inventory search of the car. Riley was arrested for possession of concealed and loaded firearms when that search turned up two handguns under the car's hood.

An officer searched Riley incident to the arrest and found items associated with the "Bloods" street gang. He also seized a cell phone from Riley's pants pocket. According to Riley's uncontradicted assertion, the phone was a "smart phone," a cell phone with a broad range of other functions based on advanced computing capability, large storage capacity, and Internet connectivity. The officer accessed information on the phone and noticed that some words (presumably in text messages or a contacts list) were preceded by the letters "CK"—a label that, he believed, stood for "Crip Killers," a slang term for members of the Bloods gang.

At the police station about two hours after the arrest, a detective specializing in gangs further examined the contents of the phone. The detective testified that he "went through" Riley's phone "looking for evidence, because ... gang members will ***2481** often video themselves with guns or take pictures of themselves with the guns." App. in No. 13–132, p. 20. Although there was "a lot of stuff" on the phone, particular files that "caught [the detective's] eye" included videos of young men sparring while someone yelled encouragement using the moniker "Blood." *Id.*, at 11–13. The police also found photographs of Riley standing in front of a car they suspected had been involved in a shooting a few weeks earlier. . . .

Prior to trial . . . , Riley moved to suppress all evidence that the police had obtained from his cell phone. He contended that the searches of his phone violated the Fourth Amendment, because they had been performed without a warrant and were not otherwise justified by exigent circumstances….

II

The Fourth Amendment provides:

> "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

[1] [2] [3] As the text makes clear, "the ultimate touchstone of the Fourth Amendment is 'reasonableness.' " Our cases have determined that "[w]here a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing, ... reasonableness generally requires the obtaining of a judicial warrant." Such a warrant ensures that the inferences to support a search are "drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime." In the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement.

The two cases before us concern the reasonableness of a warrantless search incident to a lawful arrest. . . . Although the existence of the exception for such searches has been recognized for a century, its scope has been debated for nearly as long. . . . That debate has focused on the extent to which officers may search property found on or near the arrestee. Three related precedents set forth the rules governing such searches:

The first, *Chimel v. California*, 395 U.S. 752, 89 S.Ct. 2034, 23 L.Ed.2d 685 (1969), laid the groundwork for most of the existing search incident to arrest doctrine. Police officers in that case arrested Chimel inside his home and proceeded to search his entire three-bedroom house, including the attic and garage. In particular rooms, they also looked through the contents of drawers. *Id.*, at 753–754, 89 S.Ct. 2034.

[4] The Court crafted the following rule for assessing the reasonableness of a search incident to arrest:

> "When an arrest is made, it is reasonable for the arresting officer to search the person arrested in order to remove any weapons that the latter might seek to use in order to resist arrest or effect his escape. Otherwise, the officer's safety might well be endangered, and the arrest itself frustrated. In addition, it is entirely reasonable for the arresting officer to search for and seize any evidence on the arrestee's person in order to prevent its concealment or destruction.... There is ample justification, therefore, for a search of the arrestee's person and the area 'within his immediate control'—construing that phrase to mean the area from within which he might gain possession of a weapon or destructible evidence." *Id.*, at 762–763, 89 S.Ct. 2034.

The extensive warrantless search of Chimel's home did not fit within this exception, because it was not needed to protect officer safety or to preserve evidence. *Id.*, at 763, 768, 89 S.Ct. 2034.

III

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. See A. Smith, Pew Research Center, Smartphone Ownership—2013 Update (June 5, 2013)....

A

We first consider each *Chimel* concern [officer safety and/or destruction of evidence] in turn. . . .

1

[9] 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 United States and California both suggest that a search of cell phone data might help ensure officer safety in more indirect ways, for example by alerting officers that confederates of the arrestee are headed to the scene. There is undoubtedly a strong government interest in warning officers about such possibilities, but neither the United States nor California offers evidence to suggest that their concerns are based on actual experience. The ***2486** proposed consideration would also represent a broadening of *Chimel* 's concern that an *arrestee himself* might grab a weapon and use it against an officer "to resist arrest or effect his escape." 395 U.S., at 763, 89 S.Ct. 2034. And any such threats from outside the arrest scene do not "lurk[ ] in all custodial arrests." *Chadwick*, 433 U.S., at 14–15, 97 S.Ct. 2476. Accordingly, the interest in protecting officer safety does not justify dispensing with the warrant requirement across the board. To the extent dangers to arresting officers may be implicated in a particular way in a particular case, they are better addressed through consideration of case-specific exceptions to the warrant requirement, such as the one for exigent circumstances….

2

The United States and California focus primarily on the second *Chimel* rationale: preventing the destruction of evidence.

Both Riley and Wurie concede that officers could have seized and secured their cell phones to prevent destruction of evidence while seeking a warrant. That is a sensible concession. . . . And once law enforcement officers have secured a cell phone, there is no longer any risk that the arrestee himself will be able to delete incriminating data from the phone.

The United States and California argue that information on a cell phone may nevertheless be vulnerable to two types of evidence destruction unique to digital data—remote wiping and data encryption. Remote wiping occurs when a phone, connected to a wireless network, receives a signal that erases stored data. This can happen when a third party sends a remote signal or when a phone is preprogrammed to delete data upon entering or leaving certain geographic areas (so-called "geofencing"). . . . . Encryption is a security feature that some modern cell phones use in addition to password protection. When such phones lock, data becomes protected by sophisticated encryption that renders a phone all but "unbreakable" unless police know the password. Brief for United States as *Amicus Curiae* in No. 13–132, p. 11.

As an initial matter, these broader concerns about the loss of evidence are distinct from *Chimel* 's focus on a defendant who responds to arrest by trying to conceal or destroy evidence within his reach. See 395 U.S., at 763–764, 89 S.Ct. 2034. With respect to remote wiping, the Government's primary concern turns on the actions of third parties who are not present at the scene of arrest. 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…. In any event, as to remote wiping, law enforcement is not without specific means to address the threat. Remote wiping can be fully prevented by disconnecting a phone from the network. There are at least two simple ways to do this: First, law enforcement officers can turn the phone off or remove its battery. Second, if they are concerned about encryption or other potential problems, they can leave a phone powered on and place it in an enclosure that isolates the phone from radio waves. Such devices are commonly called "Faraday bags," after the English scientist Michael Faraday. They are essentially sandwich bags made of aluminum foil: cheap, lightweight, and easy to use…. In fact, a number of law enforcement agencies around the country already encourage the use of Faraday bags.

To the extent that law enforcement still has specific concerns about the potential loss of evidence in a particular case, there remain more targeted ways to address those concerns. If "the police are truly confronted with a 'now or never' situation," …. they may be able to rely on exigent circumstances to search the phone immediately…. Or, if officers happen to seize a phone in an unlocked state, they may be able to disable a phone's automatic-lock feature in order to prevent the phone from locking and encrypting data….

B

[11] The search incident to arrest exception rests not only on the heightened government interests at stake in a volatile arrest situation, but also on an arrestee's reduced privacy interests upon being taken into police custody….

[12] The fact that an arrestee has diminished privacy interests does not mean that the Fourth Amendment falls out of the picture entirely. Not every search "is acceptable solely because a person is in custody." To the contrary, when "privacy-related concerns are weighty enough" a "search may require a warrant, notwithstanding the diminished expectations of privacy of the arrestee." *Ibid.* One such example, of course, is *Chimel*. *Chimel* refused to "characteriz[e] the invasion of privacy that results from a top-to-bottom search of a man's house as 'minor.' " Because a search of the arrestee's entire house was a substantial invasion beyond the arrest itself, the Court concluded that a warrant was required.

[13] The United States asserts that a search of all data stored on a cell phone is "materially indistinguishable" from searches of [other] physical items. That is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together….

1

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.*

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….

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 just one 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 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….

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. According to one poll, nearly three-quarters of smart phone 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 ago police officers searching an arrestee might have occasionally stumbled across a highly personal item such as a diary. But those discoveries were likely to be few and far between. Today, by contrast, it is no 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.…

Although the data stored on a cell phone is distinguished from physical records by quantity alone, certain types of data are also qualitatively different. An Internet search and browsing history, for example, can be found on an 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….

Mobile application software on a cell phone, or "apps," offer a range of tools for managing detailed information about all aspects of a person's life. There are apps for Democratic Party news and Republican Party news; apps for 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 transactions may 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 of the popular lexicon. The average smart phone user has installed 33 apps, which together can form a revealing montage of the user's life.

In 1926, Learned Hand observed (in an opinion later quoted in *Chimel*) that it is "a totally different thing to search a man's ***2491** 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….

IV

We cannot deny that our decision today will have an impact on the ability of law enforcement to combat crime. Cell phones have become important tools in facilitating coordination and communication among members of criminal enterprises, and can provide valuable incriminating information about dangerous criminals. Privacy comes at a cost.

Our holding, of course, is not that the information on a cell phone is immune from search; it is instead that a warrant is generally required before such a search, even when a cell phone is seized incident to arrest. Our cases have historically recognized that the warrant requirement is "an important working part of our machinery of government," not merely "an inconvenience to be somehow 'weighed' against the claims of police efficiency." *Coolidge v. New Hampshire*, 403 U.S. 443, 481, 91 S.Ct. 2022, 29 L.Ed.2d 564 (1971). Recent technological advances similar to those discussed here have, in addition, made the process of obtaining a warrant itself more efficient. See *McNeely*, 569 U.S., at ——, 133 S.Ct., at 1561–1563; *id.*, at ——, 133 S.Ct., at 1573 (ROBERTS, C.J., concurring in part and dissenting in part) (describing jurisdiction where "police officers can e-mail warrant requests to judges' iPads [and] judges have signed such warrants and e-mailed them back to officers in less than 15 minutes")….

[19] In light of the availability of the exigent circumstances exception, there is no reason to believe that law enforcement officers will not be able to address some of the more extreme hypotheticals that have been suggested: a suspect texting an accomplice who, it is feared, is preparing to detonate a bomb, or a child abductor who may have information about the child's location on his cell phone. The defendants here recognize—indeed, they stress—that such fact-specific threats may justify a warrantless search of cell phone data. The critical point is that, unlike the search incident to arrest exception, the exigent circumstances exception requires a court to examine whether an emergency justified a warrantless search in each particular case. See *McNeely, supra*, at ——, 133 S.Ct., at 1559.

….Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold ***2495** for many Americans "the privacies of life," *Boyd, supra*, at 630, 6 S.Ct. 524. The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. 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.

* * * * *

It is so ordered.