Riley v. California
134 S. Ct. 2473
Supreme Court 2014

David Leon RILEY, Petitioner,
v.
CALIFORNIA.

United States, Petitioner,
v.
Brima Wurie.

Nos. 13-132, 13-212.

Supreme Court of United States.

Argued April 29, 2014.
Decided June 25, 2014.

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.

I

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. See Cal.Penal Code Ann. §§ 12025(a)(1), 12031(a)(1) (West 2009).

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 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.

Riley was ultimately charged, in connection with that earlier shooting, with firing at an occupied vehicle, assault with a semiautomatic firearm, and attempted murder. The State alleged that Riley had committed those crimes for the benefit of a criminal street gang, an aggravating factor that carries an enhanced sentence. Compare Cal.Penal Code Ann. § 246 (2008) with § 186.22(b)(4)(B) (2014). 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. The trial court rejected that argument. At Riley's trial, police officers testified about the photographs and videos found on the phone, and some of the photographs were admitted into evidence. Riley was convicted on all three counts and received an enhanced sentence of 15 years to life in prison.

The California Court of Appeal affirmed. No. D059840 (Cal. App., Feb. 8, 2013), App. to Pet. for Cert. in No. 13-132, pp. 1a-23a. The court relied on the California Supreme Court's decision in *People v. Diaz*, 51 Cal.4th 84, 119 Cal.Rptr.3d 105, 244 P.3d 501 (2011), which held that the Fourth Amendment permits a warrantless search of cell phone data incident to an arrest, so long as the cell phone was immediately associated with the arrestee's person.

The California Supreme Court denied Riley's petition for review, and we granted certiorari.

[Second case description elided.]

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."

The two cases before us concern the reasonableness of a warrantless search incident to a lawful arrest. In 1914, this Court first acknowledged in dictum "the right on the part of the Government, always recognized under English and American law, to search the person of the accused when legally arrested to discover and seize the fruits or evidences of crime." *Weeks v. United States*, 232 U.S. 383, 392, 34 S.Ct. 341, 58 L.Ed. 652. Since that time, it has been well accepted that such a search constitutes an exception to the warrant requirement. Indeed, the label "exception" is something of a misnomer in this context, as warrantless searches incident to arrest occur with far greater frequency than searches conducted pursuant to a warrant. See 3 W. LaFave, Search and Seizure § 5.2(b), p. 132, and n. 15 (5th ed. 2012).

Although the existence of the exception for such searches has been recognized for a century, its scope has been debated for nearly as long. Three related precedents set forth the rules governing such searches:

[In] *Chimel v. California*, 395 U.S. 752, 89 S.Ct. 2034, 23 L.Ed.2d 685 (1969), police officers 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. The Court [found that] 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.

Four years later, in *United States v. Robinson*, 414 U.S. 218, 94 S.Ct. 467, 38 L.Ed.2d 427 (1973), the Court applied the *Chimel* analysis in the context of a search of the arrestee's person. A police officer had arrested Robinson for driving with a revoked license. The officer conducted a patdown search and felt an object that he could not identify in Robinson's coat pocket. He removed the object, which turned out to be a crumpled cigarette package, and opened it. Inside were 14 capsules of heroin. *Id.*, at 220, 223, 89 S.Ct. 2034.

The Court thus concluded that the search of Robinson was reasonable even though there was no concern about the loss of evidence, and the arresting officer had no specific concern that Robinson might be armed. *Id.*, at 236, 89 S.Ct. 2034. …A few years later, the Court clarified that this exception was limited to "personal property ... immediately associated with the person of the arrestee." United States v. Chadwick, 433 U.S. 1, 15, 97 S.Ct. 2476, 53 L.Ed.2d 538 (1977).

The search incident to arrest trilogy concludes with *Gant*, which analyzed searches of an arrestee's vehicle. The Court concluded that *Chimel* could authorize police to search a vehicle "only when the arrestee is unsecured and within reaching distance of the passenger compartment at the time of the search." 556 U.S., at 343, 129 S.Ct. 1710. *Gant* added, however, an independent exception for a warrantless search of a vehicle's passenger compartment "when it is `reasonable to believe evidence relevant to the crime of arrest might be found in the vehicle.'" That exception stems not from *Chimel*, the Court explained, but from "circumstances unique to the vehicle context."

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…Both phones are based on technology nearly inconceivable just a few decades ago, when *Chimel* and *Robinson* were decided.

Absent more precise guidance from the founding era, we generally determine whether to exempt a given type of search from the warrant requirement "by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests." *Wyoming v. Houghton*, 526 U.S. 295, 300, 119 S.Ct. 1297, 143 L.Ed.2d 408 (1999). Such a balancing of interests supported the search incident to arrest exception in *Robinson*, and a mechanical application of *Robinson* might well support the warrantless searches at issue here.

But while *Robinson*'s categorical rule strikes the appropriate balance in the context of physical objects, neither of its rationales has much force with respect to digital content on cell phones. On the government interest side, *Robinson* concluded that the two risks identified in *Chimel* — harm to officers and destruction of evidence — are present in all custodial arrests. There are no comparable risks when the search is of digital data. In addition, *Robinson* regarded any privacy interests retained by an individual after arrest as significantly diminished by the fact of the arrest itself. Cell phones, however, place vast quantities of personal information literally in the hands of individuals. A search of the information on a cell phone bears little resemblance to the type of brief physical search considered in *Robinson*.

We therefore decline to extend *Robinson* to searches of data on cell phones, and hold instead that officers must generally secure a warrant before conducting such a search.

A

We first consider each *Chimel* concern in turn. In doing so, we do not overlook *Robinson*'s admonition that searches of a person incident to arrest, "while based upon the need to disarm and to discover evidence," are reasonable regardless of "the probability in a particular arrest situation that weapons or evidence would in fact be found." 414 U.S., at 235, 94 S.Ct. 467. Rather than requiring the "case-by-case adjudication" that *Robinson* rejected, *ibid.*, we ask instead whether application of the search incident to arrest doctrine to this particular category of effects would "untether the rule from the justifications underlying the *Chimel* exception," *Gant, supra,* at 343, 129 S.Ct. 1710. See also *Knowles v. Iowa,* 525 U.S. 113, 119, 119 S.Ct. 484, 142 L.Ed.2d 492 (1998) (declining to extend *Robinson* to the issuance of citations, "a situation where the concern for officer safety is not present to the same extent and the concern for destruction or loss of evidence is not present at all").

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. …

2

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

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.

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. The briefing reveals only a couple of anecdotal examples of remote wiping triggered by an arrest. See Brief for Association of State Criminal Investigative Agencies et al. as *Amici Curiae* in No. 13-132, pp. 9-10; see also Tr. of Oral Arg. in No. 13-132, p. 48. 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.

Moreover, in situations in which an arrest might trigger a remote-wipe attempt or an officer discovers an unlocked phone, it is not clear that the ability to conduct a warrantless search would make much of a difference. The need to effect the arrest, secure the scene, and tend to other pressing matters means that law enforcement officers may well not be able to turn their attention to a

cell phone right away. Cell phone data would be vulnerable to remote wiping from the time an individual anticipates arrest to the time any eventual search of the phone is completed, which might be at the station house hours later. Likewise, an officer who seizes a phone in an unlocked state might not be able to begin his search in the short time remaining before the phone locks and data becomes encrypted.

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. See Ayers 30-31. 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. They may not be a complete answer to the problem, see Ayers 32, but at least for now they provide a reasonable response. 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," — for example, circumstances suggesting that a defendant's phone will be the target of an imminent remote-wipe attempt — 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. Such a preventive measure could be analyzed under the principles set forth in our decision in *McArthur*, 531 U.S. 326, 121 S.Ct. 946, which approved officers' reasonable steps to secure a scene to preserve evidence while they awaited a warrant.

B

Not every search "is acceptable solely because a person is in custody." *Maryland v. King*, 569 U.S. ___, ___, 133 S.Ct. 1958, 1979, 186 L.Ed.2d 1 (2013). 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.'" 395 U.S., at 766-767, n. 12, 89 S.Ct. 2034. 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.

The United States asserts that a search of all data stored on a cell phone is "materially indistinguishable" from searches of these sorts of 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. Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse. A conclusion that inspecting the contents of an arrestee's pockets works no substantial additional intrusion on privacy beyond the arrest itself may make sense as applied to physical items, but any extension of that reasoning to digital data has to rest on its own bottom.

1

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)…We expect that 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 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. 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]…Allowing the police to scrutinize such records on a routine basis is quite different from allowing them to search a personal item or two in the occasional case….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.

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 which may incriminate him." *United States v. Kirschenblatt,* 16 F.2d 202, 203 (C.A.2). 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.

2

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." …The possibility that a search might extend well beyond papers and effects in the physical proximity of an arrestee is yet another reason that the privacy interests here dwarf those in *Robinson*.

* * *

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 the driving 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 Adams was there, and he would later write that "[e]very man of a crowded 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, 6 S.Ct. 524, 29 L.Ed. 746 (1886)).

Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold 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.

We reverse the judgment of the California Court of Appeal in No. 13-132 and remand the case for further proceedings not inconsistent with this opinion. We affirm the judgment of the First Circuit in No. 13-212.

It is so ordered.

[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.

[2] In Wurie's case, for example, the dissenting First Circuit judge argued that exigent circumstances could have justified a search of Wurie's phone. See 728 F.3d 1, 17 (2013) (opinion of Howard, J.) (discussing the repeated unanswered calls from "my house," the suspected location of a drug stash). But the majority concluded that the Government had not made an exigent circumstances argument. See *id.,* at 1. The Government acknowledges the same in this Court. See Brief for United States in No. 13-212, p. 28, n. 8.

[*] Cf. *Hill v. California,* 401 U.S. 797, 799-802, and n. 1, 91 S.Ct. 1106, 28 L.Ed.2d 484 (1971) (diary); *Marron v. United States,* 275 U.S. 192, 193, 198-199, 48 S.Ct. 74, 72 L.Ed. 231 (1927) (ledger and bills); *Gouled v. United States,* 255 U.S. 298, 309, 41 S.Ct. 261, 65 L.Ed. 647 (1921), overruled on other grounds, *Warden, Md. Penitentiary v. Hayden,* 387 U.S. 294, 300-301, 87 S.Ct. 1642, 18 L.Ed.2d 782 (1967) (papers); see *United*

States v. Rodriguez, 995 F.2d 776, 778 (C.A.7 1993) (address book); *United States v. Armendariz-Mata*, 949 F.2d 151, 153 (C.A.5 1991) (notebook); *United States v. Molinaro*, 877 F.2d 1341 (C.A.7 1989) (wallet); *United States v. Richardson*, 764 F.2d 1514, 1527 (C.A.11 1985) (wallet and papers); *United States v. Watson*, 669 F.2d 1374, 1383-1384 (C.A.11 1982) (documents found in a wallet); *United States v. Castro*, 596 F.2d 674, 677 (C.A.5 1979), cert. denied, 444 U.S. 963, 100 S.Ct. 448, 62 L.Ed.2d 375 (1979) (paper found in a pocket); *United States v. Jeffers*, 520 F.2d 1256, 1267-1268 (C.A.7 1975) (three notebooks and meeting minutes); *Bozel v. Hudspeth*, 126 F.2d 585, 587 (C.A.10 1942) (papers, circulars, advertising matter, "memoranda containing various names and addresses"); *United States v. Park Avenue Pharmacy*, 56 F.2d 753, 755 (C.A.2 1932) ("numerous prescriptions blanks" and a check book). See also 3 W. LaFave, Search and Seizure § 5.2(c), p. 144 (5th ed. 2012) ("Lower courts, in applying Robinson, have deemed evidentiary searches of an arrested person to be virtually unlimited"); W. Cuddihy, Fourth Amendment: Origins and Original Meaning 847-848 (1990) (in the pre-Constitution colonial era, "[a]nyone arrested could expect that not only his surface clothing but his body, luggage, and saddlebags would be searched").