The police generally may not, without a warrant, search digital information on a cell phone seized from an individual who has been arrested.[Riley v. California](14-3-9)

On June 25, 2014, the United States Supreme Court answered the question of what police must do before searching a cell phone seized incident to an arrest— get a warrant.

¶ 14-3-9. **Riley v. California**, No. 13–132, 573 U.S.___ (6/25/2014). On Writ of Certiorari to the Court of Appeal of California, Fourth Appellate District, Division One.

Facts: 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. App. in No. 13–132, at 24, 26. 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, 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. See id., at 93, 244 P. 3d, at 505–506.

The California Supreme Court denied Riley's petition for review, App. to Pet. for Cert. in No. 13–132, at 24a, and we granted certiorari, 571 U. S. ___ (2014).

Held: reversed and remanded

Opinion: ROBERTS, C. J., delivered the opinion of the Court, in which SCALIA, KENNEDY, T HOMAS, G INSBURG, B REYER, S OTOMAYOR, and KAGAN, JJ., joined. ALITO, J., filed an opinion concurring in part and concurring in the judgment.

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."*

As the text makes clear, "the ultimate touchstone of the Fourth Amendment is 'reasonableness.'" Brigham City v. Stuart, 547 U. S. 398, 403 (2006). 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." Vernonia School Dist. 47J v. Acton, 515 U. S. 646, 653 (1995). 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." Johnson v. United States, 333 U. S. 10, 14 (1948). In the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement. See Kentucky v. King, 563 U. S. ___, ___ (2011) (slip op., at 5–6).

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. 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 de- bated for nearly as long. See Arizona v. Gant, 556 U. S. 332, 350 (2009) (noting the exception's "checkered his- tory"). 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 (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.

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.

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. 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. See also Knowles v. Iowa, 525 U. S. 113, 119 (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").

1

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.

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. See Brief for Petitioner in No. 13–132, p. 20; Brief for Respondent in No. 13–212, p. 41. That is a sensible concession. See Illinois v. McArthur, 531 U. S. 326, 331–333 (2001); Chadwick, supra, at 13, and n. 8. 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"). See Dept. of Commerce, National Institute of Standards and

Technology, R. Ayers, S. Brothers, & W. Jansen, Guidelines on Mobile Device Forensics (Draft) 29, 31 (SP 800– 101 Rev. 1, Sept. 2013) (hereinafter Ayers). 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. 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.

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. See Brief for Criminal Law Professors as Amici Curiae 9. 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. See, e.g., Dept. of Justice, National Institute of Justice, Electronic Crime Scene Investigation: A Guide for First Responders 14, 32 (2d ed. Apr. 2008); Brief for Criminal Law Professors as Amici Curiae 4–6.

B

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.

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. Brief for United States in No.

13–212, p. 26. 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

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. See Kerr, Foreword: Accounting for Technological Change, 36 Harv. J. L. & Pub. Pol'y 403, 404–405 (2013).

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. 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.

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. 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 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. See Brief for Electronic Privacy Information 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 which may 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 of private information never found in a home in any form— unless the phone is.

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.

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 (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 ___ (slip op., at 11–12); id., at ___ (ROBERTS, C. J., concurring in part and dissenting in part) (slip op., at 8) (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").

Moreover, even though the search incident to arrest exception does not apply to cell phones, other case-specific exceptions may still justify a warrantless search of a particular phone. "One well-recognized exception applies when '"the exigencies of the situation" make the needs of law enforcement so compelling that [a] warrantless search is objectively reasonable under the Fourth Amendment.'" Kentucky v. King, 563 U. S., at ___ (slip op., at 6) (quoting Mincey v. Arizona, 437 U. S. 385, 394 (1978)).

Conclusion: 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. 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.