Launch Week:
Reading Assignment #2
for
Prof. Goodno's Class on Case Briefing, Part II
(Thursday, Aug 18)

Instructions: *Please read and brief the following case. We will be discussing this brief during our second class session. On page 10, there is a case brief chart with some questions that we will be discussing during class. These questions may help guide you as you prepare your case brief.*

David Leon RILEY, Petitioner
v.

CALIFORNIA

573 U.S. __, 134 S. Ct. 2473. (2014)

ROBERTS, C.J., delivered the opinion of the Court, in which SCALIA, KENNEDY, THOMAS, GINSBURG, BREYER, SOTOMAYOR, and KAGAN, JJ., joined. ALITO, J., filed an opinion concurring in part and concurring in the judgment.

I

A

[P]etitioner 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. 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 . . . We granted certiorari.

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."

As the text makes clear, "the ultimate touchstone of the Fourth Amendment is 'reasonableness.' " *Brigham City v. Stuart*, 547 U.S. 398, 403, 126 S.Ct. 1943, 164 L.Ed.2d 650 (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, 115 S.Ct. 2386, 132 L.Ed.2d 564 (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, 68 S.Ct. 367, 92 L.Ed. 436 (1948). In the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement.

[The issue in the case] before us concerns 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) . . . . [The following] 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.

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.

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 of Appeals concluded that the search was unreasonable because Robinson was unlikely to have evidence of the crime of arrest on his person, and because it believed that extracting the cigarette package and opening it could not be justified as part of a protective search for weapons. This Court reversed, rejecting the notion that "case-by-case adjudication" was required to

determine "whether or not there was present one of the reasons supporting the authority for a search of the person incident to a lawful arrest." *Id.*, at 235, 89 S.Ct. 2034. As the Court explained, "[t]he authority to search the person incident to a lawful custodial arrest, while based upon the need to disarm and to discover evidence, does not depend on what a court may later decide was the probability in a particular arrest situation that weapons or evidence would in fact be found upon the person of the suspect." *Ibid.* Instead, a "custodial arrest of a suspect based on probable cause is a reasonable intrusion under the Fourth Amendment; that intrusion being lawful, a search incident to the arrest requires no additional justification." *Ibid.*

The Court thus concluded that the search of Robinson was reasonable . . . In doing so, the Court did not draw a line between a search of Robinson's person and a further examination of the cigarette pack found during that search. It merely noted that, "[h]aving in the course of a lawful search come upon the crumpled package of cigarettes, [the officer] was entitled to inspect it." *Ibid.*

***

III

[This case] require[s] 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 . . . [such 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 . . . 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 . . . .

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.

Perhaps the same might have been said of the cigarette pack seized from Robinson's pocket. Once an officer gained control of the pack, it was unlikely that Robinson could have accessed the pack's contents. But unknown physical objects may always pose risks, no matter how slight, during the tense atmosphere of a custodial arrest. The officer in *Robinson* testified that he could not identify the objects in the cigarette pack but knew they were not cigarettes. See 414 U.S., at 223, 236, n. 7, 94 S.Ct. 467. Given that, a further search was a reasonable protective measure. No such unknowns exist with respect to digital data. As the First Circuit explained, the officers who searched Wurie's cell phone "knew exactly what they would find therein: data. They also knew that the data could not harm them." 728 F.3d, at 10. . . .

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.

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. The briefing reveals only a couple of anecdotal examples of remote wiping triggered by an arrest. . . . 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. . . .

***

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 . . . .

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. *Robinson* focused primarily on the first of those rationales. But it also quoted with approval then-Judge Cardozo's account of the historical basis for the search incident to arrest exception: "Search of the person becomes lawful when grounds for arrest and accusation have been discovered, and the law is in the act of subjecting the body of the accused to its physical dominion." 414 U.S., at 232, 94 S.Ct. 467 (quoting *People v. Chiagles,* 237 N.Y. 193, 197, 142 N.E. 583, 584 (1923)); see also 414 U.S., at 237, 94 S.Ct. 467 (Powell, J., concurring) ("an individual lawfully subjected to a custodial arrest retains no significant Fourth Amendment interest in the privacy of his person"). Put simply, a patdown of Robinson's clothing and an inspection of the cigarette pack found in his pocket constituted only minor additional intrusions compared to the substantial government authority exercised in taking Robinson into custody . . . .

Lower courts applying *Robinson* and *Chimel*, however, have approved searches of a variety of personal items carried by an arrestee. See, *e.g., United States v. Carrion,* 809 F.2d 1120, 1123, 1128 (C.A.5 1987) (billfold and address book); *United States v. Watson,* 669 F.2d 1374, 1383–1384 (C.A.11 1982) (wallet); *United States v. Lee,* 501 F.2d 890, 892 (C.A.D.C.1974) (purse).

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). 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. See Kerr, *supra*, at 404; Brief for Center for Democracy & Technology 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 less than $20 might hold photographs, picture messages, text messages, Internet browsing history, a calendar, a thousand-entry phone book, and so on. See *id.*, at 30; *United States v. Flores–Lopez*, 670 F.3d 803, 806 (C.A.7 2012). 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]

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. See, *e.g., United States v. Frankenberry*, 387 F.2d 337 (C.A.2 1967) (*per curiam*). 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. See *Ontario v. Quon*, 560 U.S. 746, 760, 130 S.Ct. 2619, 177 L.Ed.2d 216 (2010). 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.

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. ——, ——, 132 S.Ct. 945, 955, 181 L.Ed.2d 911 (2012) (SOTOMAYOR, J., concurring) ("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 (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. See *New York v. Belton*, 453 U.S. 454, 460, n. 4, 101 S.Ct. 2860, 69 L.Ed.2d 768 (1981) (describing a "container" as "any object capable of holding another object"). 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 . . . .

****

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.

***

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.

[Here, Riley's cell phone contained massive amounts of data including contact lists and numerous videos, photos and text messages that spanned over a long period of time. The discovery of some of that data led to additional criminal charges against Riley.] We reverse the judgment of the California Court of Appeal . . . and remand the case for further proceedings not inconsistent with this opinion . . . .

It is so ordered.

Here is the case brief chart we discussed during our first session. These questions may help guide you as you prepare your brief of Riley.

Caption	*Who is the Petitioner? The Respondent? What roles did they play at trial (e.g., who was D?)*
Author(s)	*Who wrote the opinion and did all 9 justices agree with it?*
Facts	***Section I*** • *Why was D initially arrested?* • *Was D's arrest lawful (and why does this matter)?* • *What was searched and what was discovered?* • *Did the police get a warrant?* • *What evidence did the police find in the search and what charges did that lead to?*
Procedural History	• *State Trial Court (trial): outcome?* • *Cal Ct of Appeals: outcome?* • *Cal Sup Ct – outcome?*
Issue	• *Can you find the trigger words in the case that present the issue? (hint: see page 3)* • *How might the issue statement be written to make it more fact specific than the issue in Robinson (the case you read for our last class)?*
Rule	***Sections II - III*** ***General Rule*** • *What part of the Constitution is cited?* • *What is the general rule as announced in Chimel?* • *What precedent does the Court consider?* o *hint #1: How did the Court apply the rule in Chimel? In Robinson?* o *hint #2: The court cites other cases on p6 and Frankenberry (p8) – how was the rule applied in these cases?* • *In Section III, does the Court apply the Chimel/Robinson to cell phones?* o *In Section (A)(1), why isn't weapon use a valid concern in Riley?* o *In Section (A)(2), why isn't destruction of evidence a valid concern in Riley?* ***Policy:*** • *In Section III(B)(1)-(2), the Court considers the policy underlying the Robinson rule – what is that policy and why can't it be applied to Riley?*
Analysis (Reasoning)	***Section IV*** • *What trigger word suggests the Court is analyzing the case?* • *Would the police ever be able to search the digital data on Riley's phone?*
Holding (Conclusion)	*In the last paragraph, what does the Court mean when it states: "We reverse the judgment of the California Court of Appeal . . . and remand the case for further proceedings not inconsistent with this opinion . . . ."?*
Notes/ Questions	*What happens to D now?*