RILEY v. CALIFORNIA
SUPREME COURT OF THE UNITED STATES
June 25, 2014
[9 – 0]
[ELL Rating = J/R = ☺/8]

Heads Up. Justice Roberts: **"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."**

OPINION: CHIEF JUSTICE ROBERTS...**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.**

IA

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 often video themselves with guns or take

pictures of themselves with the guns." 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." 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. **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*, 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.

B

In the second case, a police officer performing routine surveillance observed respondent Brima Wurie make an apparent drug sale from a car. Officers subsequently arrested Wurie and took him to the police station. At the station, the officers seized two cell phones from Wurie's person. The one at issue here was a "flip phone," a kind of phone that is flipped open for use and that generally has a smaller range of features than a smart phone. Five to ten minutes after arriving at the station, the officers noticed that the phone was repeatedly receiving calls from a source identified as "my house" on the phone's external screen. A few minutes later, they opened the phone and saw a photograph of a woman and a baby set as the phone's wallpaper. They pressed one button on the phone to access its call log, then another button to determine the phone number associated with the "my house" label. They next used an online phone directory to trace that phone number to an apartment building.

When the officers went to the building, they saw Wurie's name on a mailbox and observed through a window a woman who resembled the woman in the photograph on Wurie's phone. They secured the apartment while obtaining a search warrant and, upon later executing the warrant, found and seized 215 grams of crack cocaine, marijuana, drug paraphernalia, a firearm and ammunition, and cash.

Wurie was charged with distributing crack cocaine, possessing crack cocaine with intent to distribute, and being a felon in possession of a firearm and ammunition. **He moved to suppress the evidence obtained from the search of the apartment, arguing that it was the fruit of an unconstitutional search of his cell phone. The District Court denied the motion. Wurie was convicted on all three counts and sentenced to 262 months in prison.**

A divided panel of the First Circuit reversed the denial of Wurie's motion to suppress and vacated Wurie's convictions for possession with intent to distribute and possession of a firearm as a felon. The court held that cell phones are distinct from other physical possessions that may be searched incident to arrest without a warrant, because of the amount of personal data cell phones contain and the negligible threat they pose to law enforcement interests.

We granted certiorari.

So, the Court is taking up two cases with similar issues. Riley enters the High Court as a loser and comes out a winner. Wurie enters as a winner and stays a winner.

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*. Our cases have determined that "where 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*. 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*. 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. **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*. 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.**

Although the existence of the exception for such searches has been recognized for a century, its scope has been debated for nearly as long. See *Arizona* v. *Gant* (noting the exception's "checkered history"). 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***, 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.

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."**

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.

Four years later, in ***United States* v. *Robinson***, 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.

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." As the Court explained, "the 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." 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."

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. 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, "having in the course of a lawful search come upon the crumpled package of cigarettes, the officer was entitled to inspect it." 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* (200-pound, locked

footlocker could not be searched incident to arrest), abrogated on other grounds by *California* v. *Acevedo*.

The search incident to arrest trilogy concludes with *Gant*, which analyzed searches of an arrestee's vehicle. *Gant*, like *Robinson*, recognized that the *Chimel* concerns for officer safety and evidence preservation underlie the search incident to arrest exception. As a result, 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." *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. Even less sophisticated phones like Wurie's, which have already faded in popularity since Wurie was arrested in 2007, have been around for less than 15 years. 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*. 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." Rather than requiring the "case-by-case adjudication" that *Robinson* rejected, 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." See also *Knowles* v. *Iowa* (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.

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. 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."

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 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." And any such threats from outside the arrest scene do not "lurk in all custodial arrests." *Chadwick*. 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.** See *Warden, Md. Penitentiary* v. *Hayden* ("The Fourth Amendment does not require police officers to delay in the course of an investigation if to do so would gravely endanger their lives or the lives of others.").

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.

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. 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. 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. 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, 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.** *Missouri* v. *McNeely*. 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*, which approved officers' reasonable steps to secure a scene to preserve evidence while they awaited a warrant.

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." *People* v. *Chiagles* (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. See *Chadwick* (searches of a person are justified in part by "reduced expectations of privacy caused by the arrest").

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." *Maryland* v. *King*. 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." **One such example, of course, is *Chimel. Chimel* refused to "characterize 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.

Robinson is the only decision from this Court applying *Chimel* to a search of the contents of an item found on an arrestee's person. In an earlier case, this Court had approved a search of a zipper bag carried by an arrestee, but the Court analyzed only the validity of the arrest itself. Lower courts applying *Robinson* and *Chimel*, however, have approved searches of a variety of

personal items carried by an arrestee. *United States* v. *Carrion* (**billfold and address book**); *United States* v. *Watson* (**wallet**); *United States* v. Lee (**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. 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. 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*, 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. 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. 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.

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. 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. 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. *United States* v. *Jones* (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.

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*. 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. See *New York* v. *Belton* (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. Cell phone users often may not know whether particular information is stored on the device or in the cloud, and it generally makes little difference. Moreover, the same type of data may be stored locally on the device for one user and in the cloud for another.

The United States concedes that the search incident to arrest exception may not be stretched to cover a search of files accessed remotely—that is, a search of files stored in the cloud. Such a search would be like finding a key in a suspect's pocket and arguing that it allowed law enforcement to unlock and search a house. But officers searching a phone's data would not typically know whether the information they are viewing was stored locally at the time of the arrest or has been pulled from the cloud.

Although the Government recognizes the problem, its proposed solutions are unclear. It suggests that officers could disconnect a phone from the network before searching the device—the very solution whose feasibility it contested with respect to the threat of remote wiping. Alternatively, the Government proposes that law enforcement agencies "develop protocols to address" concerns raised by cloud computing. Probably a good idea, but the Founders did not fight a revolution to gain the right to government agency protocols. 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.*

C

Apart from their arguments for a direct extension of *Robinson*, the United States and California offer various fallback options for permitting warrantless cell phone searches under certain circumstances. Each of the proposals is flawed and contravenes our general preference to provide clear guidance to law enforcement through categorical rules. "If police are to have workable rules, the balancing of the competing interests . . . 'must in large part be done on a categorical basis—not in an ad hoc, case-by-case fashion by individual police officers.'" *Michigan* v. *Summers*.

The United States first proposes that the *Gant* standard be imported from the vehicle context, allowing a warrantless search of an arrestee's cell phone whenever it is reasonable to believe that the phone contains evidence of the crime of arrest. But *Gant* relied on "circumstances unique to the vehicle context" to endorse a search solely for the purpose of gathering evidence. JUSTICE SCALIA's *Thornton* opinion, on which *Gant* was based, explained that those unique circumstances are "a reduced expectation of privacy" and "heightened law enforcement needs" when it comes to motor vehicles. For reasons that we have explained, cell phone searches bear neither of those characteristics.

At any rate, a *Gant* standard would prove no practical limit at all when it comes to cell phone searches. In the vehicle context, *Gant* generally protects against searches for evidence of past crimes. In the cell phone context, however, it is reasonable to expect that incriminating information will be found on a phone regardless of when the crime occurred. Similarly, in the vehicle context *Gant* restricts broad searches resulting from minor crimes such as traffic violations. That would not necessarily be true for cell phones. It would be a particularly inexperienced or unimaginative law enforcement officer who could not come up with several reasons to suppose evidence of just about any crime could be found on a cell phone. Even an individual pulled over for something as basic as speeding might well have locational data dispositive of guilt on his phone. An individual pulled over for reckless driving might have evidence on the phone that shows whether he was texting while driving. The sources of potential pertinent information are virtually unlimited, so applying the *Gant* standard to cell phones would in effect give "police officers unbridled discretion to rummage at will among a person's private effects."

The United States also proposes a rule that would restrict the scope of a cell phone search to those areas of the phone where an officer reasonably believes that information relevant to the crime, the arrestee's identity, or officer safety will be discovered. This approach would again impose few meaningful constraints on officers. The proposed categories would sweep in a great deal of information, and officers would not always be able to discern in advance what information would be found where.

We also reject the United States' final suggestion that officers should always be able to search a phone's call log, as they did in Wurie's case. The Government relies on *Smith* v. *Maryland*, which held that no warrant was required to use a pen register at telephone company premises to identify numbers dialed by a particular caller. The Court in that case, however, concluded that the use of a pen register was not a "search" at all under the Fourth Amendment. There is no dispute here that the officers engaged in a search of Wurie's cell phone. Moreover, call logs typically contain more than just phone numbers; they include any identifying information that an individual might add, such as the label "my house" in Wurie's case.

Finally, at oral argument California suggested a different limiting principle, under which officers could search cell phone data if they could have obtained the same information from a pre-digital counterpart. See *Flores-Lopez* ("If police are entitled to open a pocket diary to copy the owner's address, they should be entitled to turn on a cell phone to learn its number."). But the fact that a search in the pre-digital era could have turned up a photograph or two in a wallet does not justify a search of thousands of photos in a digital gallery. The fact that someone could have tucked a paper bank statement in a pocket does not justify a search of every bank statement from the last five years. And to make matters worse, such an analogue test would allow law enforcement to search a range of items contained on a phone, even though people would be unlikely to carry such a variety of information in physical form. In Riley's case, for example, it is implausible that he would have strolled around with video tapes, photo albums, and an address book all crammed into his pockets. But because each of those items has a pre-digital analogue, police under California's proposal would be able to search a phone for all of those items—a significant diminution of privacy.

In addition, an analogue test would launch courts on a difficult line-drawing expedition to determine which digital files are comparable to physical records. Is an e-mail equivalent to a letter? Is a voicemail equivalent to a phone message slip? It is not clear how officers could make these kinds of decisions before conducting a search, or how courts would apply the proposed rule after the fact. An analogue test would "keep defendants and judges guessing for years to come." *Sykes* v. *United States* (SCALIA, J., dissenting) (discussing the Court's analogue test under the Armed Career Criminal Act).

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*. Recent technological advances similar to those discussed here have, in addition, made the process of obtaining a warrant itself more efficient. See *McNeely* (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").

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*. Such exigencies could include the need to prevent the imminent destruction of evidence in individual cases, to pursue a fleeing suspect, and to assist persons who are seriously injured or are threatened with imminent injury. In *Chadwick*, for example, the Court held that the exception for searches incident to arrest did not justify a search of the trunk at issue, but noted that "if officers have reason to believe that luggage contains some immediately dangerous instrumentality, such as explosives, it would be foolhardy to transport it to the station house without opening the luggage."

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.

Why the ELL “reasoning rating” of 8? Well, I am concerned that enforcement will chip away at the “exigent circumstances” that will still enable a search without a warrant. And, as in the warrantless search of a house for items “in plain view” and no further, would a warrantless search be limited to the “texts” of/to a suspected accomplice waiting to detonate a bomb?

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 "every man of a crowded audience appeared to me to go away, as I did, ready to take arms against writs of assistance." 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."

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." 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.

CONCURRENCE: ALITO, concurring in part and concurring in the judgment. I agree with the Court that law enforcement officers, in conducting a lawful search incident to arrest, must generally obtain a warrant before searching information stored or accessible on a cell phone. I write separately to address two points.

IA

First, **I am not convinced at this time that the ancient rule on searches incident to arrest is based exclusively (or even primarily) on the need to protect the safety of arresting officers and the need to prevent the destruction of evidence.** This rule antedates the adoption of the Fourth Amendment by at least a century. In *Weeks* v. *United States*, we held that the Fourth Amendment did not disturb this rule. See also Stuntz, The Substantive Origins of Criminal Procedure ("The power to search incident to arrest—a search of the arrested suspect's person . . .—was well established in the mid-eighteenth century, and nothing in . . . the Fourth Amendment changed that"). And neither in *Weeks* nor in any of the authorities discussing the old common-law rule have I found any suggestion that it was based exclusively or primarily on the need to protect arresting officers or to prevent the destruction of evidence.

On the contrary, when pre-*Weeks* authorities discussed the basis for the rule, what was mentioned was the need to obtain probative evidence. For example, an 1839 case stated that "it is clear, and beyond doubt, that . . . constables . . . are entitled, upon a lawful arrest by them of

one charged with treason or felony, to take and detain property found in his possession which will form material evidence in his prosecution for that crime." The court noted that the origins of that rule "derive from the interest which the State has in a person guilty (or reasonably believed to be guilty) of a crime being brought to justice, and in a prosecution, once commenced, being determined in due course of law."

Two 19th-century treatises that this Court has previously cited in connection with the origin of the search-incident-to-arrest rule suggest the same rationale. See F. Wharton, Criminal Pleading and Practice ("Those arresting a defendant are bound to take from his person any articles which may be of use as proof in the trial of the offense with which the defendant is charged"); J. Bishop, Criminal Procedure (if an arresting officer finds "about the prisoner's person, or otherwise in his possession, either goods or moneys which there is reason to believe are connected with the supposed crime as its fruits, or as the instruments with which it was committed, or as directly furnishing evidence relating to the transaction, he may take the same, and hold them to be disposed of as the court may direct").

What ultimately convinces me that the rule is not closely linked to the need for officer safety and evidence preservation is that these rationales fail to explain the rule's well-recognized scope. It has long been accepted that written items found on the person of an arrestee may be examined and used at trial. But once these items are taken away from an arrestee (something that obviously must be done before the items are read), there is no risk that the arrestee will destroy them. Nor is there any risk that leaving these items unread will endanger the arresting officers.

The idea that officer safety and the preservation of evidence are the sole reasons for allowing a warrantless search incident to arrest appears to derive from the Court's reasoning in *Chimel* v. *California,* a case that involved the lawfulness of a search of the scene of an arrest, not the person of an arrestee. As I have explained, *Chimels* reasoning is questionable and I think it is a mistake to allow that reasoning to affect cases like these that concern the search of the person of arrestees.

B

Despite my view on the point discussed above, I agree that we should not mechanically apply the rule used in the predigital era to the search of a cell phone. Many cell phones now in use are capable of storing and accessing a quantity of information, some highly personal, that no person would ever have had on his person in hard-copy form. This calls for a new balancing of law enforcement and privacy interests.

The Court strikes this balance in favor of privacy interests with respect to all cell phones and all information found in them, and this approach leads to anomalies. For example, the Court's broad holding favors information in digital form over information in hard-copy form. Suppose that two suspects are arrested. Suspect number one has in his pocket a monthly bill for his land-line phone, and the bill lists an incriminating call to a long-distance number. He also has in his a wallet a few snapshots, and one of these is incriminating. Suspect number two has in his pocket a cell phone, the call log of which shows a call to the same incriminating number. In addition, a number of photos are stored in the memory of the cell phone, and one of these is incriminating. Under established law, the police may seize and examine the phone bill and the snapshots in the

wallet without obtaining a warrant, but under the Court's holding today, the information stored in the cell phone is out.

While the Court's approach leads to anomalies, I do not see a workable alternative. Law enforcement officers need clear rules regarding searches incident to arrest, and it would take many cases and many years for the courts to develop more nuanced rules. And during that time, the nature of the electronic devices that ordinary Americans carry on their persons would continue to change.

II

This brings me to my second point. **While I agree with the holding of the Court, I would reconsider the question presented here if either Congress or state legislatures, after assessing the legitimate needs of law enforcement and the privacy interests of cell phone owners, enact legislation that draws reasonable distinctions based on categories of information or perhaps other variables.**

The regulation of electronic surveillance provides an instructive example. After this Court held that electronic surveillance constitutes a search even when no property interest is invaded, see *Katz* v. *United States*, Congress responded by enacting Title III of the Omnibus Crime Control and Safe Streets Act of 1968. Since that time, electronic surveillance has been governed primarily, not by decisions of this Court, but by the statute, which authorizes but imposes detailed restrictions on electronic surveillance.

Modern cell phones are of great value for both lawful and unlawful purposes. They can be used in committing many serious crimes, and they present new and difficult law enforcement problems. At the same time, because of the role that these devices have come to play in contemporary life, searching their contents implicates very sensitive privacy interests that this Court is poorly positioned to understand and evaluate. Many forms of modern technology are making it easier and easier for both government and private entities to amass a wealth of information about the lives of ordinary Americans, and at the same time, many ordinary Americans are choosing to make public much information that was seldom revealed to outsiders just a few decades ago.

In light of these developments, it would be very unfortunate if privacy protection in the 21st century were left primarily to the federal courts using the blunt instrument of the Fourth Amendment. Legislatures, elected by the people, are in a better position than we are to assess and respond to the changes that have already occurred and those that almost certainly will take place in the future.