Bloomberg BNA

Digital Discovery & e-Evidence®

SUPREME COURT DECISION

Crowell & Moring's Justin P. Murphy and Louisa K. Marion address the Supreme Court's guidance on six major aspects of the *Riley* decision and explore its implications for the future of privacy jurisprudence.

Riley v. California: The Dawn of a New Digital Age of Privacy

BY JUSTIN P. MURPHY AND LOUISA K. MARION

In a far-reaching decision, the Supreme Court unanimously answered ''the question of what police must do before searching a cell phone seized incident to an arrest.'' Resolving federal and state court conflicts on the issue, Chief Justice John G. Roberts's forceful opinion in *Riley v. California*, 573 U.S. __ (2014), instructed law enforcement that the answer to their concerns is ''simple'': ''*get a warrant.*''

In so doing, the Court swept away years of inconsistent lower court jurisprudence that struggled to define Fourth Amendment protections applicable to modern technologies.

Significantly, the Court rejected a common analogy—that cell phones (which the Court calls ''minicomputers'') are ''closed containers'' (e.g., notebooks, wallets/purses, or cigarette packs), whose contents are fair game once the container is lawfully opened.

Instead, the Court concluded that today's cell phones are fundamentally different than physical containers: their storage capacity is virtually unlimited; they contain a broad variety of information (photographs, texts, personal contacts, financial information, geolocation information, and search history, among others); they have long memories (often containing information predating the devices themselves); and they are gateway devices (that is, a portal to limitless other information, often through mobile application software (apps) connected to the Cloud).

As discussed in greater detail below, the Court's opinion continues a sea-change started with Justice Sotomayor's concurrence in *United States v. Jones*, 132 S.Ct. 945 (2012).

In *Riley*, citing to our Founding Generation's abhorrence to general warrants, the Court voiced profound concern about providing law enforcement warrantless windows into our lives, as well as deep skepticism about the government's officer-safety and preventing-evidence-destruction rationales.

Recognizing the revolutionary nature of modern technologies—and it is clear that the Court's analysis extends well beyond cell phones—the Court affirmed that mobile media is just *different*. With *Riley*, the Court ushers in a new age of digital privacy.

Justin P. Murphy is a counsel in Crowell & Moring's Washington, D.C. office where he practices in the firm's White Collar & Regulatory Enforcement Group and E-Discovery and Information Management Group.

Louisa K. Marion is an associate in Crowell & Moring's Washington, D.C. office, where she practices in the firm's White Collar and Privacy & Cybersecurity Groups.''

Background

The Court's decision arises from a state-circuit split on the permissibility of warrantless cell phone searches

in *Riley v. California*, 2013 BL 34220, Cal. App. 4 Dist., D059840, 02/08/13, and *United States v. Wurie*, 728 F.3d 1 (1st Cir. 2013).

Wurie. In *Wurie*, law enforcement officers searched the defendant's cell phone incident to his arrest on suspicion that he was dealing drugs.

While at the police station, Wurie's phone received repeated incoming calls from a number identified as ''my house.''

After reviewing the phone's call log and retrieving the phone number, officers obtained a search warrant for the property associated with that number.

A search of the property turned up drugs, drug paraphernalia, and firearms, and Wurie was charged with drug possession and distribution and firearms charges.

Wurie moved to suppress what he alleged were the fruits of an unlawful cell phone search. The Court denied the motion and Wurie was convicted.

On review, the First Circuit panel reversed, eschewing a fact-specific approach in favor of a bright-line rule: ''The search-incident-to-arrest exception does not authorize the warrantless search of data on a cell phone seized from an arrestee's person.'' The panel held that the evidence should have been suppressed and vacated Wurie's conviction.

Riley. The search in *Riley* was much broader. Police stopped Riley for driving with expired registration tags. After an inventory search of Riley's vehicle revealed two handguns, police arrested Riley and searched him incident to the arrest. The officers found gang-related materials on his person and seized and searched Riley's smartphone, which also revealed information connecting Riley to the same gang.

A few hours later, a detective specializing in gangs further examined the contents of Riley's phone. The officer found text (''presumably in text messages or a contacts list'') that appeared to relate to ''Crip Killers,'' videos seemingly connecting Riley to a gang, and a picture of Riley in front of a car that officers suspected had been involved in a recent shooting.

Riley was charged in connection with the shooting and moved to suppress all evidence obtained from his cell phone. The lower court denied the motion and Riley was convicted on all charges. The California Court of Appeal affirmed, and the California Supreme Court denied review.

The Court set forth a bright line rule: law enforcement must get a warrant.

The Supreme Court's Decision

The Supreme Court's grant of certiorari in both cases promised to help lower courts determine the permissibility of electronic searches incident to arrest, and (if so) the scope of such searches. And the Court set forth a bright line rule: Law enforcement must get a warrant.

Although the Court's opinion provides a wealth of guidance, we address here several particularly important observations:

(1) cell phones and digital devices *are different* from traditional physical containers;

(2) government interests have less force when balanced against the breadth and nature of digital content;

(3) cell phones are ''gateway devices'' that reach far beyond their physical borders;

(4) the government's traditional officer-safety and risk-of-evidence-destruction rationales for searches incident to arrest carry little weight in the digital context;

(5) there are necessarily limits and exceptions to the bright line rule; and

(6) the Court's decision, although ground breaking, rests on familiar turf: our Founders' abhorrence of general searches.

Cell Phones Are Different

The sheer pervasiveness of cell phone use in today's society is a key factor that underlies the Court's trailblazing decision. Chief Justice Roberts noted at the outset that ''modern cell phones . . . are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude that they were an important feature of human anatomy.'' *Id.* at 9.

When the court aligned this pervasiveness of cell phone use with their computer-like storage capacity, and the fact that they are gateway devices to virtually unlimited content in the Cloud, it was left with the inescapable conclusion that ''minicomputer'' (and presumably by extension, computer, iPad, other digital storage device, etc.) searches are *different* than physical searches.

The Digital Age Has Arrived. This acknowledgment is likely the most important and far-reaching aspect of the Court's opinion, because it concedes that we are indeed in a new digital age. Chief Justice Roberts categorically rejected the government's argument that cell phones are ''materially indistinguishable'' from physical containers, noting that ''[t]hat 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.'' *Id.* at 17.

Indeed, ''[m]odern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse.'' *Id.*

In support of its conclusion that digital devices are different than physical containers, Chief Justice Roberts identified significant quantitative differences between cell phones and traditional containers:

■ Modern cell phones have immense storage capacity, and are minimally limited by physical constraints. While individuals 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 [—] if they did, they would have to drag behind them a trunk of the sort held to require a search warrant,'' *id.*,— they could easily do so on their mobile device; and the ''gulf between physical practicability and digital capacity will only continue to widen in the future.'' *Id.* at 18.

■ Modern cell phones can provide unique insight deep into an individual's past. Where previously an in-

  DDEE ISSN 1941-3882

dividual might have carried a photo or two in his wallet, today the sum of his private life can be reconstructed through the thousands of digital photographs (labeled with dates, locations and descriptions) and other data that might predate the phone. *Id.*

Second, Chief Justice Roberts identified significant qualitative differences: That is, the *nature* of data contained on modern cell phones renders them ''different.'' These minicomputers contain, for example:

■ A vast array of information, and could as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps or newspapers. *Id.* at 17. As such, they are a digital record of nearly every aspect of their owner's life, from the intimate to the ordinary. ''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.'' *Id.* at 19.

■ Internet search histories, which reveal an individual's private interests and/or concerns. *Id.*

■ Data that can reveal where a person has been and when they were there. *Id.*

■ Mobile apps, which offer a range of tools for managing detailed information about all aspects of a person's life and ''together can form a revealing montage of the user's life.'' *Id.* at 20.

Gateway Devices. Perhaps most significantly, the Court recognized that cell phones are gateway devices, highlighting that the privacy issues at stake do not just reside on a cell phone in an arrestee's hand, but also in data stored elsewhere that can be accessed with the tap of a screen. The ''analogy [of a cell phone to a physical container] crumbles entirely when a cell phone is used to access data located elsewhere.'' *Id.* at 21.

Chief Justice Roberts added that cell phone users may not know if certain data is stored on the device or on a remote server, and law enforcement officers would typically not know either. ''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.'' *Id.*

Moreover, a cell phone search would typically expose to law enforcement ''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.'' *Id.* at 20-21.

Traditional Government Interests Have Little Force When Juxtaposed With The Nature and Scope of Digital Devices

The Court's opinion cemented that minicomputers are ''different'' through a discussion of the Court's ''search incident to arrest trilogy,'' and distinguished the treatment of digital data under each long-established exception.

Under its previous precedent in *Chimel v. California*, 395 U.S. 752 (1969), the Court had held it was reasonable to search an arrestee's person and/or the area within his/her immediate control from which the arrestee might gain access to a weapon or destroy evidence.

Four years later, in *United States v. Robinson*, 414 U.S. 218 (1973), the Court extended *Chimel*, categorically permitting the search of personal property (in *Robinson*, a cigarette pack) immediately associated with the person of the arrestee.

The third installment in the ''trilogy,'' *Arizona v. Gant*, 556 U.S. 332 (2009), extended *Chimel* and *Robinson* to vehicles. However, the Court determined that law enforcement officers were permitted to search a vehicle ''only when the arrestee is unsecured and within reaching distance of the passenger compartment at the time of the search,'' and when it is ''reasonable to believe evidence relevant to the crime of arrest might be found in the vehicle.'' *Id.* at 333.

Data Doesn't Cause Physical Injury. In *Riley*, Chief Justice Roberts found the balance between intrusions upon individual privacy and government interests weighed differently in the digital context. Under *Robinson*, the government interest in preventing potential harm to officers and destruction of evidence—present in all custodial arrests—outweighed a privacy interest diminished by the fact of arrest.

In the digital context, however, the Court found no comparable risk of harm to officers or data, but a significant privacy interest: since cell phones ''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*.'' *Riley*, 573 U.S. at 9-10. As such, the Court found that officers must generally secure a warrant before searching for data on cell phones.

The Court also analyzed, and dismissed, the government's concerns recognized in *Chimel*. As the Court explained, digital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or aid in an arrestee's escape. In fact, once a phone is secure and other *physical* threats are removed, the data will not endanger anyone. The reason for that is simple, as the Court noted: when you search a phone, you know exactly what you will find—*data*. *Id.* at 11.

''The interest in protecting officer safety does not justify dispensing with the warrant requirement across the board.''

CHIEF JUSTICE JOHN G. ROBERTS, JR.

Addressing the government's arguments that a search of a cell phone would alert officers that *accomplices* of the arrestee were headed to the scene of the arrest, Chief Justice Roberts reminded the government that *Chimel* focused on the *arrestee* and whether the *arrestee* might grab a weapon and use it against an officer. The Court concluded that the ''interest in protecting officer safety does not justify dispensing with the warrant requirement across the board.'' *Id.*

Finally, Chief Justice Roberts addressed *Chimel's* second rationale: preventing the destruction of evidence. He concluded that once law enforcement offi-

cers have secured a cell phone, the danger that the arrestee could destroy any data from the phone is eliminated.

With regard to potential dangers of remote wiping or remote encryption of data, the Court noted that officers could turn off the cell phone, remove its battery, or place the device in a Faraday Bag, which isolates the device from radio waves. *Id.* at 14.

These simple approaches allow law enforcement to specifically address remote-wiping threats while taking steps to obtain a warrant.

Flaws In The Government's Proposed Solutions

The Court rejected a number of additional rationales advanced by the government for some warrantless cell phone searches:

■ Citing *Gant*, the government argued for warrantless searches whenever it is reasonable to believe that the cell phone contains evidence of the crime of arrest. Chief Justice Roberts noted that cell phones do not bear the *Gant* exception characteristics: There is no reduced expectation of privacy in cell phones, as there is in cars, and there are no heightened law enforcement needs. Moreover, *Gant* prohibits broad searches for minor traffic violations and given the almost unlimited sources of data available on cell phones, the Court said, ''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.'' *Id.* at 23 (internal quotation omitted).

■ The government proposed restricting the scope of a warrantless cell phone search to those *areas* of the cell phone that law enforcement reasonably believes contain information relevant to the crime, the arrestee's identity, or officer safety. The Court countered that this proposal ''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.'' *Id.* at 24.

■ The Court also rejected the government's suggestion that law enforcement should always be able to search a phone's call log, noting that call logs contain more information than just phone numbers, including labels or other identifying information that the phone's owner might have added. *Id.*

■ Finally, the Court rejected the government's assertion at oral argument that officers should be able to search cell phone data if they could have obtained the same information from a pre-digital counterpart:

> ''[T]he 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.''

Id. at 24-25. Chief Justice Roberts added that such an analogue test would force courts to draw lines to determine what was comparable to physical records and it was unclear how officers could make such decisions in the field. *Id.* at 25.

Limits to the Court's Decision

The Court acknowledged the impact that its decision will have on law enforcement's ability to combat crime. Although adding that ''privacy comes at a cost,'' *id.*, the Court also noted that its holding was not absolute: the ''exigencies of the situation [might] make the needs of law enforcement so compelling that a warrantless search is objectively reasonable under the Fourth Amendment.'' *Id.* at 26.

The Court provided examples of such exigent circumstances, including the need to prevent imminent destruction of evidence in individual cases or to assist persons seriously injured or threatened with imminent injury, among others. But, Chief Justice Roberts reminded, the exigent circumstance exception requires a court to examine whether an emergency justified a warrantless search in each particular case. *Id.* at 27.

Riley Is Grounded in Our Founding Generation's Beliefs

The *Riley* opinion unanimously reaffirms constitutional protections for an individual's privacy against warrantless intrusions by the government. And while the opinion focuses on new technologies, the Court's voice echoes that of our founders: as Chief Justice Roberts explained, 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.'' *Id.* at 27.

Chief Justice Roberts highlighted the words of little-known American Revolutionary James Otis, who inspired a young John Adams in denouncing the British's use of writs of assistance. Adams emphatically recounts that a speech by Otis in 1761 was ''the first scene of the first act of opposition to the arbitrary claims of Great Britain. Then and there the child Independence was born.'' *Id.* at 27-28.

Noting that modern cell phones hold for man the ''privacies of life,'' the Court resoundingly concluded its opinion: ''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.'' *Id.* at 28.

What Does This Decision Mean?

The Court's decision and reasoning in *Riley* is a breathtaking leap forward for digital privacy rights delivered in a loud, clear, and unanimous voice. The decision, grounded in our founding generation's 18th century abhorrence of general warrants, is a bold reaffirmation of individual privacy rights against government intrusion, and leaves very little wiggle-room for warrantless searches of modern cell phones. In cementing that ''minicomputers'' are subject to a different set of

  DDEE ISSN 1941-3882

rules than physical evidence, the Court brings the Fourth Amendment into the digital age.

A Glimpse Into the Future? The decision also signals how the Court may approach other looming privacy issues, including the need for warrants before obtaining Cloud-based data, geolocational data, and content data stored with third-party providers. Its deep concern that modern technologies contain the ''sum of an individual's life''—including the individual's associates, activities, locations, and interests—suggest that the Court might be edging toward a ''mosaic theory'' of privacy (even though the Court expressly caveats that the cases before it ''[did] not implicate the question whether the collection or inspection of aggregated digital information amounts to a search under other circumstances''). Proponents of a mosaic approach would recognize a personal privacy interest in data points that might be innocuous individually, but when accumulated and considered together can paint a detailed picture of one's life.

In addition, the Court's concern that mobile apps provide a gateway to data stored in the Cloud implies that the Court may be close to recognizing a Fourth Amendment privacy interest in Cloud-based data. This would be a significant shift from its longstanding jurisprudence, outlined in *Smith v. Maryland*, 442 U.S. 735 (1979), and its progeny, that there is no privacy interest in data voluntarily surrendered to third parties—which Cloud-based data almost always is.

The question of what, if any, Fourth Amendment privacy protection applies to the increasing quantities of personal (and arguably very private) data voluntarily disclosed to third parties seems likely to be the next question for the Court. The Court's concern in *Riley* about the *pervasiveness* of technologies seems particularly applicable in this context.

Today, numerous technologies rely on disclosure of private information to third parties—such as geolocation information transmitted by one's cell phone or vehicle, Cloud-based e-mail, or Dropbox data, to name a few. Following *Riley's* lead, the Court might be ready to rethink *Smith v. Maryland* in the digital context and conclude that use of technologies that necessarily disclose such private information to third parties should not result in a wholesale waiver of the privacy of that information.

Justice Sotomayor's concurrence in *Jones* suggests that at least one Justice is already ready to do so. In *Jones*, Justice Sotomayor concluded that even short-term warrantless GPS surveillance of a suspect moving on public streets could intrude on her constitutionally protected privacy. In determining whether such an invasion occurred, she ''would [have] ask[ed] whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on.'' *Id.* at 956. She continued:

> More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers. Perhaps, as Justice Alito notes [in a separate concurrence in *Jones*], some people may find the ''tradeoff'' of privacy for convenience ''worthwhile,'' or come to accept this ''diminution of privacy'' as ''inevitable,''. . . and perhaps not. I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection. *Id.* at 957.

Spurring Statutory Reform

The sea-change may be beginning, but it probably will not occur quickly. The more immediate effect of the Court's decision may be to light a fire under the near-dead proposals to reform the Electronic Communications Protection Act, or ''ECPA'' (18 U.S.C. § 2701).

ECPA—and in particular its provisions known as the Stored Communication Act—was enacted in 1986, well before widespread cloud computing made long-term storage of user content by third-party providers the norm. In what now seems an arbitrary distinction, its provisions permit government authorities to compel a third-party service provider to disclose user content that has been stored on its servers for less than 180 days only pursuant to a court-issued *warrant*, while unopened e-mails and content stored for more than 180 days may be compelled with a *subpoena or a court order* (neither of which requires a finding of probable cause by a neutral judicial officer).

Although reform proposals have been advanced in both the Senate and the House for the past several congressional terms, they have gained limited traction. (Nevertheless, the Department of Justice dropped its long-standing opposition to a warrant requirement before government officials can obtain content stored in the Cloud in April 2013.) The Court's recognition of privacy rights in Cloud-based content may again spur Congress to action.