No. 13-132

In the Supreme Court of the United States

DAVID LEON RILEY, PETITIONER

v.

STATE OF CALIFORNIA

ON WRIT OF CERTIORARI
TO THE COURT OF APPEAL OF CALIFORNIA,
FOURTH APPELLATE DISTRICT, DIVISION ONE

BRIEF FOR THE UNITED STATES
AS AMICUS CURIAE SUPPORTING RESPONDENT

DONALD B. VERRILLI, JR.
Solicitor General
Counsel of Record
DAVID A. O'NEIL
Acting Assistant Attorney General
MICHAEL R. DREEBEN
Deputy Solicitor General
JOHN F. BASH
Assistant to the Solicitor General
ROBERT A. PARKER
Attorney
Department of Justice
Washington, D.C. 20530-0001
SupremeCtBriefs@usdoj.gov
(202) 514-2217

QUESTION PRESENTED

Whether evidence admitted at petitioner's trial was obtained in a search of petitioner's cell phone that violated petitioner's Fourth Amendment rights.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases:

Cases—Continued: Page

Cases—Continued: Page

Constitution and statutes:

Statutes—Continued: Page

Miscellaneous:

Miscellaneous—Continued: Page

Miscellaneous—Continued: Page

In the Supreme Court of the United States

No. 13-132

DAVID LEON RILEY, PETITIONER

v.

STATE OF CALIFORNIA

ON WRIT OF CERTIORARI
TO THE COURT OF APPEAL OF CALIFORNIA,
FOURTH APPELLATE DISTRICT, DIVISION ONE

BRIEF FOR THE UNITED STATES
AS AMICUS CURIAE SUPPORTING RESPONDENT

INTEREST OF THE UNITED STATES

This case involves the Fourth Amendment implications of a police search of the contents of a cell phone found on a person after his lawful custodial arrest. Federal prosecutors rely on such evidence in federal criminal cases, and federal law-enforcement officers conduct similar cell-phone searches. This Court has granted certiorari in *United States* v. *Wurie*, No. 13-212, to consider related issues.

STATEMENT

1. A San Diego police officer stopped a vehicle driven by petitioner after noticing that it had expired tags. Pet. App. 3a, 5a. During the stop, the officer learned that petitioner had a suspended license. *Id.* at 5a. Consistent with departmental policy, the officer decided to impound the vehicle. *Ibid.* An inventory

search of the car at the scene revealed two handguns under its hood. *Id.* at 3a, 5a-6a. The officer then arrested petitioner for possession of concealed firearms. *Id.* at 6a; J.A. 23; see Cal. Penal Code §§ 12025(a)(1), 12031(a)(1) (West 2008).

The officer searched petitioner's person incident to the arrest, finding paraphernalia associated with the Lincoln Park Bloods, a violent street gang, and a cell phone. J.A. 8. The officer examined petitioner's cell phone and noticed that in certain textual entries, every word that began with the letter "K" was preceded by a "C." *Ibid.* He recognized that misspelling to be an abbreviation for "Crip Killer," indicating that petitioner was a member of the rival Bloods. *Ibid.*

The arresting officer contacted a detective specializing in gangs. About two hours later, at the stationhouse, the detective interviewed petitioner, whom he recognized as a member of the Lincoln Park gang and whom he suspected of involvement in a shooting three weeks earlier. J.A. 15-17; see Br. in Opp. 2. Because the detective knew that "gang members will often video themselves with guns or take pictures of themselves with the guns," he examined the contents of petitioner's phone to obtain "further evidence to prove that he was in possession of th[e] firearms that the officers found inside the car." J.A. 20; see Pet. App. 6a-7a. Some of the video clips on the phone depicted street boxing, a common gang-initiation activity. J.A. 11-12. Petitioner was heard on one clip shouting words of encouragement and referring to one of the boxers as "Blood." J.A. 12-13. The detective also observed photos of petitioner making gang signs. J.A. 30-32, 42-44.

2. a. In connection with the earlier shooting, petitioner was charged in the Superior Court of California with one count of attempted murder, Cal. Penal Code §§ 187(a), 664 (West 2008), one count of shooting at an occupied vehicle, *id.* § 246, and one count of assault with a semiautomatic firearm, *id.* § 245(b). Pet. App. 1a. He moved to suppress the videos and photographs showing his gang affiliation obtained from the search of his cell phone. *Id.* at 4a.

The superior court denied petitioner's suppression motion. J.A. 21-24. The court explained that under the search-incident-to-arrest doctrine articulated in *United States* v. *Robinson*, 414 U.S. 218 (1973), and *United States* v. *Edwards*, 415 U.S. 800 (1974), "in the case of a lawful arrest, a full search of the person is an exception to the warrant requirement of the [F]ourth [A]mendment and is reasonable under that amendment." J.A. 23. Applying that principle, the court further explained, courts "have allowed items on the person to be searched, including wallets, address books, papers and the like." *Ibid.* "Cell phones do contain personal information," the court noted, "but really no more so than wallets and purses and address books." *Ibid.* Because petitioner's cell phone "was on his person at the time of arrest," the court held, it "was taken out of the realm [of] protection [from] police interest for a reasonable time following the arrest." *Ibid.* The court also found that the search was part of "an investigation relating to the crime for which [petitioner] was arrested, which was the finding of the guns in the car." *Ibid.*

b. After a hung jury in petitioner's first trial, he was retried, and the superior court again ruled the phone evidence admissible. J.A. 26. At the second

trial, officers testified about the photos and videos on petitioner's phone, and three of the photos were admitted. J.A. 30-44. Petitioner was convicted on all counts and sentenced to a term of imprisonment of 15 years to life. Pet. App. 1a. Petitioner separately pleaded guilty to offenses arising out of the traffic stop, including carrying a concealed firearm in a vehicle. Pet. Br. 7 n.5.

3. The California Court of Appeal affirmed. Pet. App. 1a-23a. Relying on the California Supreme Court's decision in *People* v. *Diaz*, 244 P.3d 501, cert. denied, 132 S. Ct. 94 (2011), the court held that because petitioner's "cell phone was immediately associated with his person when he was arrested," the search of the phone "was lawful whether or not an exigency * * * existed." Pet. App. 15a (internal quotation marks omitted).

SUMMARY OF ARGUMENT

I. The Fourth Amendment permitted officers to search petitioner's cell phone incident to his lawful arrest. This Court has long confirmed that officers possess "unqualified authority" to search the person of an arrestee and any objects or containers found on his person for evidence of crime. *United States* v. *Robinson*, 414 U.S. 218, 225 (1973). Petitioner has not identified a single decision of this Court or any historical or practical basis supporting an item-specific exception to that rule.

A. Contrary to petitioner's view, the narrowly focused law-enforcement interests set forth in *Chimel* v. *California*, 395 U.S. 752 (1969), do not support excluding cell phones from officers' search authority. Those interests have never delimited officers' authority to search objects on the person—an authority that rests

primarily on the reduced expectation of privacy caused by a lawful arrest, as well as the police's overriding interest in gathering evidence of crime during the critical period immediately following an arrest in a place where it is particularly likely to be found.

In any event, cell phones implicate the *Chimel* justifications more powerfully than virtually any other object. Unlike the physical contents of a container, digital contents can be concealed or destroyed before a warrant can be obtained even once the container is in police custody—sometimes within minutes. When an officer finds an unlocked cell phone at the scene of an arrest, searching it immediately may be her only chance to retrieve and preserve essential evidence. Petitioner's proposed solutions to that serious problem—such as equipping every officer with unwieldy forensic devices that cost several thousand dollars each—are entirely unrealistic.

B. Cell phones do not raise qualitatively different privacy concerns than items that the police have always had authority to search incident to arrest, such as letters, diaries, briefcases, and purses. Evidence of crime should not be insulated from traditional review because the arrestee maintains it in a technologically sophisticated form. Cell phones may contain a significantly greater quantity of information than traditional items, but where, as here, the search is conducted before "the administrative mechanics of arrest have been completed and the prisoner is incarcerated," *United States* v. *Edwards*, 415 U.S. 800, 804 (1974), officers would not be able to peruse the entire contents of the arrestee's cell phone.

Petitioner contends that cell phones' capacity to contain expressive material, such as text messages

and photos, calls for a special restriction on the police's search authority. But "the law has never distinguished between documents and other property found upon the person of one arrested." *United States* v. *Kirschenblatt*, 16 F.2d 202, 203 (2d Cir. 1926) (Hand, J.). The precedents petitioner cites concern either pre-*Chimel* searches of the *premises* of arrest, or seizures of expressive materials where "the basis for their seizure [was] the ideas which they contain[ed]," *Stanford* v. *Texas*, 379 U.S. 476, 485 (1965). They have no application here, and *Robinson* states the controlling test.

C. If the Court were inclined to resolve this case on narrower grounds, the government suggested two alternative approaches in its opening brief in *United States* v. *Wurie*, No. 13-212. One approach would permit officers to search a phone incident to arrest only when it is reasonable to believe that it contains evidence relevant to the offense of arrest; a second would limit the *scope* of any cell-phone search incident to arrest to actions reasonably related to legitimate law-enforcement objectives. U.S. *Wurie* Br. 45-55. Petitioner addresses only the first approach, contending that it would impose no meaningful limitation (while paradoxically maintaining that it would invalidate the search in this case). But an offense-of-arrest approach would prevent officers from searching cell phones incident to arrest for traffic offenses and other minor crimes where evidence could not be reasonably expected to be found on the phone.

D. Whether the Court applies *Robinson* or either of the narrower approaches the United States articulated, the search in this case was lawful: the cell phone was found on petitioner's person; the officers

had reason to believe it contained evidence of crime; and the search sought such evidence.

II. Petitioner's objection to the stationhouse search of his phone about two hours after his arrest lacks merit. This Court approved a delay of ten hours in *Edwards*. Here, the delay was much less and, as in *Edwards*, the search occurred before the administrative mechanics of arrest were completed. Deferring the search was particularly reasonable given that the on-the-scene search indicated that petitioner was likely involved in gang activity, and the arresting officer appropriately contacted a detective with special expertise in gangs, who examined the phone once it was brought to the stationhouse.

ARGUMENT

I. THE FOURTH AMENDMENT PERMITTED OFFICERS TO SEARCH PETITIONER'S CELL PHONE INCIDENT TO HIS ARREST

As the United States explained in its opening brief in *United States* v. *Wurie*, No. 13-212, this Court has long confirmed that the police may "search the person of the accused when legally arrested to discover and seize the fruits or evidences of crime," without obtaining a warrant, and that this procedure includes examining any object found on the person. *United States* v. *Robinson*, 414 U.S. 218, 224-225 (1973) (quoting *Weeks* v. *United States*, 232 U.S. 383, 392 (1914)).

In arguing that the police lacked authority to search his cell phone after he was arrested for concealing firearms under the hood of his car, petitioner contends, as did the First Circuit in *Wurie*, first, that the search of a cell phone does not advance the interests that this Court has invoked in defining the permissible spatial extent of a search of the *premises* of

arrest under *Chimel* v. *California*, 395 U.S. 752 (1969); and, second, that cell phones raise different privacy concerns than other objects, in part because they contain written material and other media.

Those arguments should be rejected. Far from preserving "that degree of privacy against government that existed when the Fourth Amendment was adopted," *Kyllo* v. *United States*, 533 U.S. 27, 34 (2001), petitioner's view would give arrestees a right that they have never had: protection against a full search of their persons and the effects found on their persons incident to a probable-cause arrest.

A. *Chimel* Does Not Support Precluding The Police From Searching A Cell Phone Incident To Arrest

Petitioner contends (Br. 15-24) that permitting the police to search a cell phone found on the person of an arrestee would "sever the search-incident-to-arrest doctrine forevermore from its conceptual underpinnings" (Br. 18) by allowing searches that do not serve the particularized interests identified in *Chimel*. That argument is wrong both legally and factually.

1. As the United States explained in *Wurie* (Br. 13-28), this Court's decisions have never held that the full authority to search the person of an arrestee, including any item found on his person, is limited by the particularized justifications—officer safety and the preservation of evidence that might be concealed or destroyed—set forth in *Chimel*. To the contrary, it has explained that the authority to search the person of an arrestee is primarily "justified by [the] reduced expectations of privacy caused by the arrest." *United States* v. *Chadwick*, 433 U.S. 1, 16 n.10 (1977), abrogated on other grounds by *California* v. *Acevedo*, 500 U.S. 565 (1991). Last Term, the Court twice reiterat-

ed that an arrest categorically authorizes the full search of the person of the arrestee. See *Maryland* v. *King*, 133 S. Ct. 1958, 1970-1971 (2013); *Missouri* v. *McNeely*, 133 S. Ct. 1552, 1559 n.3 (2013).

Petitioner nevertheless contends that the *Chimel* justifications narrow not only the spatial breadth of the search area around an arrestee, but also the types of items found on the person of an arrestee that the police may search. *Robinson*, *supra*, rejected precisely that argument. See 414 U.S. at 235. Petitioner would recast *Robinson* as resting exclusively on the need for officers to make "quick ad hoc judgment[s]" in arrest situations, *ibid.*, an interest he believes is not advanced by searches of digital contents. Pet. Br. 18. That is wrong. Although *Robinson* described that important interest as a benefit of the traditional rule, its holding is that if an arrest is lawful, a search of the person of the arrestee "requires no additional justification." 414 U.S. at 235.

Under petitioner's reasoning, *Robinson*—as well as this Court's post-*Robinson* cases applying the same principle—were all wrongly decided. Petitioner's central premise is that "[o]nce the police have exclusive control over a smart phone and have secured it beyond an arrestee's grab area, there is no legitimate concern that the arrestee could alter or destroy the phone's digital contents." Pet. Br. 21. But precisely the same thing could have been said of the cigarette package at issue in *Robinson*—or any other object or container. Petitioner's only attempt to reconcile *Robinson*'s holding with his reasoning is to observe in a footnote that the police in the 1970s often gave cigarette packages back to arrestees. *Id.* at 19 n.7. The Court's opinion made no mention of that purported practice. In any

event, petitioner surely would not concede that a cell-phone search becomes lawful if the officer returns the phone after examining its contents.

Petitioner also contends that this Court's post-*Robinson* decisions in *Chadwick*, *supra*, and *Arizona* v. *Gant*, 556 U.S. 332 (2009), support his view. But as the United States explained in *Wurie* (Br. 21-23), both of those cases concerned the area around the arrestee, for which he has no reduced expectation of privacy, and neither decision cast doubt on officers' longstanding categorical authority to search items found on the *person* of an arrestee.

Furthermore, as Justice Scalia explained in *Thornton* v. *United States*, 541 U.S. 615 (2004), the search-incident-to-arrest doctrine was traditionally grounded in the "interest in gathering evidence relevant to the crime for which the suspect had been arrested." *Id.* at 629 (concurring in the judgment); see U.S. *Wurie* Br. 15. Searches of the arrestee's person were also justified based on officers' time-sensitive need to ascertain or confirm a suspect's identity. See *ibid.*; see also *King*, 133 S. Ct. at 1971. Petitioner does not argue that cell-phone searches fail to advance those historical justifications.

2. Not only is petitioner incorrect that cell-phone searches incident to arrest are justifiable only if officers "need to search [their] data to protect against the destruction of evidence" or ensure officer safety, Pet. Br. 16, he also misunderstands the tremendous challenges that mobile-communication technology poses in arrest situations. In light of those challenges it will often be critical that officers search a suspect's cell phone as soon as practicable after an arrest is made.

a. When an arresting officer finds an unlocked cell phone that may contain evidence of crime, she has sound reason to examine its contents immediately. See U.S. *Wurie* Br. 34-37. Most modern cell phones can be programmed to lock automatically after some period of inactivity—for example, between one minute and four hours on Apple's iPhone. See *iPhone User Guide for iOS 7.1*, at 10 (Mar. 2014) (iPhone Manual).[1] Once locked, data on the phone will be protected by sophisticated encryption walls that make it very difficult, and often impossible, to recover any information from the device unless the officers acquire the arrestee's passcode.

The iPhone, for example, uses an "AES [Advanced Encryption Standard] 256-bit key[] fused into the application processor during manufacturing." Apple, Inc., *iOS Security* 7 (Oct. 2012) (*iOS Security*).[2] In practice, that means that once locked, the iPhone is essentially "unbreakable": "no computer imaginable for the foreseeable future * * * would be able to crack a truly random 256-bit AES key." Simson Garfinkel, *The iPhone Has Passed a Key Security Threshold*, MIT Technology Review (Aug. 13, 2012).[3] Other device manufacturers and operating systems use similar methods to protect user data. Even for phones that use less sophisticated encryption technology than the iPhone, "the decryption of even a short

---

[1] http://manuals.info.apple.com/MANUALS/1000/MA1565/en_US/iphone_user_guide.pdf.

[2] https://www.apple.com/ipad/business/docs/iOS_Security_Oct12.pdf.

[3] www.technologyreview.com/news/428477/the-iphone-has-passed-a-key-security-threshold.

key would consume extraordinary amounts of government resources." Orin S. Kerr, *The Fourth Amendment in Cyberspace: Can Encryption Create a "Reasonable Expectation of Privacy"?*, 33 Conn. L. Rev. 503, 530 (Winter 2001).[4]

Turning off a phone or removing its battery—steps that petitioner and his amici confidently recommend—only exacerbates that encryption problem. While a cell phone is still powered on, a copy of the encryption key may remain saved in the device's accessible memory, making it possible in some instances for forensic labs, through a painstaking process, to recover the key. But once a phone is turned off, "the copy of the encryption key in the computer's accessible memory is erased," making it far more daunting to decrypt the device. Garfinkel, *supra*; see also Rick Ayers et al., National Institute of Standards and Technology, U.S. Department of Commerce, *Guidelines on Mobile Device Forensics (Draft)* 30-31 (Sept. 2013) (NIST Draft Guidelines).[5]

In addition to attempting to circumvent the encryption wall, law-enforcement agencies can try to ascertain the user's passcode. But it may take years of work in a forensic laboratory to break even a simple passcode. See *iOS Security* 9 (five-and-a-half years for a six-character alphanumeric passcode); Garfinkel, *supra* (25 years for a 10-digit numeric passcode). Re-

---

[4] See, *e.g.*, http://source.android.com/devices/tech/security (Google Android); http://docs.blackberry.com/en/admin/deliverables/16648/Encrypting_user_data_on_a_locked_BB_device_834471_11.jsp (Blackberry).

[5] www.nist.gov/forensics/research/upload/draft-guidelines-on-mobile-device-forensics.pdf.

alistically, law-enforcement agencies will not have the resources to attempt to break a passcode for any but the most serious cases. And even if great resources were applied, many phones have security features that thwart attempts to overcome the passcode. Apple, for example, allows a user "to have the device automatically wiped after 10 failed passcode attempts." *iOS Security* 9.

If ever a circumstance implicated the *Chimel* evidence-preservation interest, therefore, this is it. The combination of automatic locking and encryption means that officers who seize an unlocked cell phone—which may forever conceal its contents within a matter of minutes or hours—will have no idea, until it is too late, whether they can "reasonably obtain a warrant * * * without significantly undermining the efficacy of the search." *McNeely*, 133 S. Ct. at 1561. That is why forensic guides recommended that "[w]here possible, devices supporting encryption, such as Android and [Apple] iOS devices, should be triage processed at the scene if they are found in an unlocked state, as the data may no longer be available to an investigator once the device's screen is locked, or if the battery exhausts." NIST Draft Guidelines 35; accord FBI, *Mobile Forensics Field Guide: What Every Peace Officer Must Know* 3, V. 2.0 (2010) (Mobile Guide) ("Mobile devices can be set to self-lock and/or encrypt after a specified period of time elapses. If the device in question is currently in an unlocked state, but you think it is set to self-lock, immediately examining the device may be the only opportunity to collect evidence."); see Eoghan Casey & Benjamin Turnbull,

Digital Evidence on Mobile Devices 17, reprinted in *Digital Evidence and Computer Crime* (3d ed. 2011);[6] Richard P. Mislan et al., *The Growing Need for On-Scene Triage of Mobile Devices*, 6 Digital Investigation 112, 115 (2010) (Mislan).

b. The threat of "remote wiping" also poses a risk of evidence destruction. See U.S. *Wurie* Br. 37-40. On all major cell-phone platforms, data on a smartphone can quickly be erased by confederates or others who lack physical access to the device. See NIST Draft Guidelines 29; Mislan at 113, 118; *United States* v. *Flores-Lopez*, 670 F.3d 803, 808-809 (7th Cir. 2012). That could be done for at least some information on petitioner's phone. See Samsung Instinct User Guide 76 (2008) (cited Pet. Br. 22) ("If your device is lost or stolen, you can use Sprint Mobile Sync to remotely remove all the contacts information.").[7] And newer "geofencing" technology promises to enable users to preset their phones to automatically erase their contents when brought into a particular location, such as a police station. See U.S. *Wurie* Br. 38-39.

i. Petitioner and his amici suggest a host of solutions to the remote-wiping threat—all of which are far less certain to protect evidence than setting aside a cigarette package or an article of clothing. Petitioner states, for example, that officers could remove the memory card or the battery from the phone. But only some models allow the easy removal of a memory card or the battery, and it may not be obvious from the

---

[6] http://booksite.elsevier.com/9780123742681/Chapter_20_Final.pdf.

[7] http://support.sprint.com/global/pdf/user_guides/samsung/instinct/samsung_instinct_ug.pdf.

phone's exterior that removal is possible or how to do it. See Casey & Turnbull 17-18. Those steps also risk permanently losing evidence: removing a phone's battery may trigger a password lock that could make any evidence on the phone effectively irretrievable, and removable memory cards are easily damaged and may become encrypted when ejected. *Ibid.;* Mislan at 121.

Petitioner also points (Br. 22-23) to Faraday bags. As the government explained in *Wurie* (U.S. Br. 39-40), those can be effective at blocking a wireless signal, but they have the effect of quickly draining the phone's battery as the phone searches for a wireless signal. NIST Draft Guidelines 30.[8] To function properly, moreover, Faraday bags must be completely sealed—with no holes, gaps, or frays in the material—and even then they may fail to prevent wireless communication if the phone passes near a cell tower, an associated WiFi router, or another place where a signal is particularly strong. *Id.* at 30, 32; Mobile Guide 9 ("Faraday bags are reliable, but can't fully guarantee that signals will not reach the phone. Successfully blocking a signal depends on the quality of the bag, the distance to the closest cell tower, and the power of the transmitter in the mobile device."); David W. Bennett, *The Challenges Facing Computer Forensics Investigators in Obtaining Information from Mobile Devices for Use in Criminal Investigations*, Forensic

---

[8] Although battery drain could be averted by connecting the phone to a portable power source placed inside the Faraday bag, that would require every officer to carry a fully charged portable power source at all times, along with power cord adapters compatible with every type of phone. See Greg Gogolin, *Digital Forensics Explained* 59-60 (2013).

Focus (Aug. 20, 2011).[9] A Purdue University study found that, in a majority of cases, Faraday bags and similar enclosures "did not prevent network communication in all cases, and SMS [text] messages most often penetrated the device while shielded, followed by voice calls and MMS [multimedia] messages"—messages that could trigger remote wiping. NIST Draft Guidelines 32; see Eric Katz, *A Field Test of Mobile Phone Shielding Devices* (Dec. 10, 2010) (published M.S. thesis, Purdue University).[10]

Furthermore, because a remote-wiping command will be received and executed as soon as the phone reconnects to a network, the phone must continue to be shielded once it is removed from the bag. NIST Draft Guidelines 33. That means that local police departments will need not only cheap Faraday bags, but also Faraday *rooms* or other specialized equipment enveloped in protective material. *Ibid.*; Casey & Turnbull, 17.

Another option for preventing remote wiping is to put the phone in "airplane mode," which turns off the device's wireless communications. But to accomplish that successfully, an officer must be familiar with the configuration of each device she encounters, which can be challenging given the wide variation among different models of devices and versions of operating systems, as well as the ability of service providers and users to customize the appearance, layout, and default

---

[9] http://articles.forensicfocus.com/2011/08/22/the-challenges-facing-computer-forensics-investigators-in-obtaining-information-from-mobile-devices-for-use-in-criminal-investigations.

[10] http://docs.lib.purdue.edu/cgi/viewcontent.cgi?article=1033&context=techmasters.

language of each device. See Greg Gogolin, *Digital Forensics Explained* 57 (2013). And as with Faraday bags, putting a phone in airplane mode does nothing to prevent the phone from locking.

ii. Citing machines often referred to as Universal Forensic Extraction Devices (UFEDs), petitioner contends that officers can preserve cell-phone data by blindly copying the entire contents of a cell phone at the scene of an arrest. That suggestion is entirely unrealistic. A modern UFED sold by the leading manufacturer (Cellebrite) costs about $10,000, and the cost of associated hardware and software "could go * * * far above" that amount. *Product Information: Cellebrite UFED Touch Ultimate*, SC Mag. (May 1, 2013) (*Cellebrite Review*).[11] Annual maintenance and upgrade costs may add another "few thousand dollars per license." Gogolin 44. And a police department must pay for special training for each officer who uses a UFED. See, *e.g.*, Digital Shield, Inc., *Cellebrite UFED Certified Training*.[12] It would thus be incredibly expensive to supply each of the 461,000 local police officers across the country with a UFED—to say nothing of the 120,000 full-time federal officers authorized to make arrests. See Bureau of Justice Statistics, *Local Police* (2008 statistics);[13] Bureau of Justice Statistics, *Federal Law Enforcement Officers* (2008 statistics).[14]

---

[11] www.scmagazine.com/cellebrite-ufed-touch-ultimate/review/3870.

[12] www.digitalshield.net/cellebriteinfo.php.

[13] www.bjs.gov/index.cfm?ty=tp&tid=71.

[14] www.bjs.gov/index.cfm?ty=pbdetail&iid=4372.

UFEDs, moreover, are not iPhone-sized tools that officers could keep in their pockets. Although handheld, they are fairly sizeable devices, and because different phones use different types of data ports, UFED kits include dozens of different cords. See App., *infra* (reproducing picture of a UFED kit). The notion that each officer in the field who might make an arrest should carry one of those kits wherever she patrols is wholly unworkable.

UFEDs have still other problems. They are unable to retrieve data from every phone. See Gogolin 48; Casey & Turnbull 19; Bennett, *supra*. Even for some common phones that are usually compatible with a UFED, the device may not work with all models and versions of the operating system. See Ronen Engler & Christa M. Miller, *6 Persistent Challenges with Smartphone Forensics*, Digital Forensic Investigator News (Feb. 8, 2013);[15] see also Gogolin 43. And even if the UFED works with a particular phone, that does not mean that it can extract every type of data on the phone. See Gogolin 58. Moreover, to function effectively, a UFED generally requires an officer to know the make, model, and service provider of the phone. NIST Draft Guidelines 38. That information may not be readily apparent from the exterior of the phone, particularly in a tense, nighttime arrest situation. *Id.* at 38-40. And the inexpensive disposable cell phones favored by drug dealers and terrorists (commonly known as "burner" phones) often lack the data ports necessary to use a UFED at all. Engler & Miller, *su-*

---

[15] www.dfinews.com/articles/2013/02/6-persistent-challenges-smartphone-forensics.

pra; Mobile Guide 6 ("With cheaper versions [of prepaid phones], there isn't always a means of copying data off the phone for an examination.").

Additionally, preserving the contents of a phone with a UFED is not instantaneous. An independent review of the most advanced Cellebrite device found that extracting certain types of information that would otherwise be readily viewable on the phone by an officer at the scene, such as text messages and call logs, takes between 2 and 15 minutes, depending on the phone. *Cellebrite Review*, *supra*. A forensic copy of the phone's contents takes at least 20 to 45 minutes. *Ibid.* Particularly when an arrest has not been planned and coordinated in advance, or where officers seize multiple phones from multiple arrestees, it will often be impracticable for an arresting officer to spend such time extracting data from a phone.

iii. Some of petitioner's amici suggest that remote wiping is not a real problem. See, *e.g.*, DKT Liberty Project Amicus Br. 34-35. But petitioner and his amici themselves point to federal and state law-enforcement guidelines instructing officers to take steps to prevent remote wiping, which would be puzzling if it posed no threat. See, *e.g.*, Pet. Br. 23 nn.8-9; see also, *e.g.*, Gogolin 59; Mislan at 113; Casey & Turnbull 3, 13. Although appellate decisions reporting remote wiping are unlikely (destroyed evidence cannot be introduced), such events occur. See Press Release, U.S. Attorney's Office, S.D. Ga., Martinez Man Sentenced to More Than 24 Years for Attempted Online Enticement of a Minor and Destruction of Evidence (Jan. 22, 2014) ("Shortly []after [the suspect's arrest], he contacted his wife from jail and * * *

instructed her to delete his e-mail account and remotely wipe his phone.").[16]

c. Petitioner limits his discussion of *Chimel*'s officer-safety justification to the question whether cell-phone data can be used as a weapon. See Br. 16-19. But reviewing recent text messages or emails can alert officers that confederates or others are headed to the scene of an arrest, potentially creating a dangerous situation. See U.S. *Wurie* Br. 41-42.

d. Although petitioner suggests (Br. 20) that officers can quickly procure search warrants, "[e]ven with modern technological advances, the warrant procedure imposes burdens" and therefore "[w]hen a warrantless search is justified, requiring the police to obtain a warrant may 'unjustifiably interfer[e] with legitimate law enforcement strategies.'" *Fernandez* v. *California*, 134 S. Ct. 1126, 1137 (2014) (quoting *Kentucky* v. *King*, 131 S. Ct. 1849, 1860 (2011)) (third alteration in *Fernandez*). The search of items seized from an arrestee's person has historically been justified as a legitimate investigative procedure. And even with advances in obtaining warrants, delay in searching a cell phone poses a significant risk that evidence will be lost forever.

Finally, any claim to exempt cell phones from the traditional search-incident-to-arrest doctrine because of the supposed possibility of obtaining a warrant encounters a basic practical problem: cell phone technology is rapidly evolving, and unforeseen threats to such delayed searches may well emerge in the future.

---

[16] www.fbi.gov/atlanta/press-releases/2014/martinez-man-sentenced-to-more-than-24-years-for-attempted-online-enticement-of-a-minor-and-destruction-of-evidence.

Cf. *City of Ontario, Cal.* v. *Quon*, 130 S. Ct. 2619, 2629 (2010) ("The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."). It would be unwise to establish new and categorical constitutional limits on the police's traditional search authority based on a snapshot in time of a fast-changing technology.

B. Privacy Concerns Do Not Justify A Cell-Phone Exception To Officers' Search-Incident-To-Arrest Authority

Petitioner argues (Br. 24-38) that unique privacy concerns in cell phones justify a special exemption from officers' traditional search authority incident to lawful arrests. He fears (Br. 11) that every citizen will be subject to arrest at any time and that police will use such custodial arrests as pretexts to review individuals' private e-Book libraries and to probe their innermost "thoughts, wonders, and concerns."

That speculation has little connection to the arrests in this case and in *Wurie*: each involved probable-cause arrests for serious offenses, and the police conducted a search of the arrestees' cell phones to gather evidence relevant to the offense of arrest and to advance other vital law-enforcement objectives. The Court has no evidence that would justify treating these cases as atypical—or for fashioning a rule to address supposed abuses unrelated to these cases. Although cell phones can store more information than physical items such as diaries, address books, wallets, or purses, that characteristic is no reason to interpret the Fourth Amendment to deny officers a longstanding feature of their arrest authority, thereby ham-

stringing investigations as criminals have become more technologically sophisticated.

1. a. Petitioner contends (Br. 11) that because cell phones can contain a great deal of personal information, searching them is "the modern equivalent" of the sort of "general search" that the Fourth Amendment was adopted to prevent. But petitioner's central premise—that searching a cell phone incident to arrest "gives law enforcement the ability to obtain personal information formerly beyond its reach" (Br. 13)—is erroneous. Cell phones do not contain qualitatively different information than other sorts of items that courts have long permitted police to search incident to arrest. A cell phone can contain a list of contacts, but so can an address book. *E.g.*, *United States* v. *Smith*, 565 F.2d 292, 294 (4th Cir. 1977). Text messages and emails are modern-day letters. *E.g.*, *Dillon* v. *O'Brien & Davis*, 16 Cox C.C. 245, 248 (Exch. Div. Ir. 1887). And petitioner has cited no case holding that the police lack the power to examine photographs or other pictures found on an arrestee—often critical evidence of serious crimes, like the distribution of child pornography.[17]

---

[17] Petitioner suggests in passing (Br. 34 n.11) that this Court should overrule its longstanding precedent that a search may be conducted for "mere evidence" of crime, at least as to papers. But as this Court has held, "[n]othing in the language of the Fourth Amendment supports the distinction between 'mere evidence' and instrumentalities, fruits of crime, or contraband." *Warden* v. *Hayden*, 387 U.S. 284, 301 (1967). Petitioner cites no case or Founding-era source limiting the search of papers incident to a lawful arrest. And the law review article on which he relies acknowledges "a powerful argument that the original understanding did permit narrow, brief, and regulated seizures of papers.

The limited authority to search incident to arrest differs critically from general warrants, such as the hated writs of assistance. A "general warrant specified only an offense—typically seditious libel—and left to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched." *Steagald* v. *United States*, 451 U.S. 204, 220 (1981); see *Wilkes* v. *Wood*, 98 K.B. 489, 498 (1763) (describing a "general warrant" as one "where no offenders[']names are specified" and "therefore a discretionary power [is] given to messengers to search wherever their suspicions may chance to fall"). A search incident to arrest requires probable cause to arrest, and, as applied here, the search is limited to the person and objects found on his person at the time of arrest.

Cell phones do differ from objects that police have searched incident to arrest since the Founding era in their greater storage capacity: not different kinds of information, but potentially more of it. That concern does not justify dramatically curtailing officers' investigative tools. At least where, as here, the search occurs before "the administrative mechanics of arrest have been completed and the prisoner is incarcerated," *United States* v. *Edwards*, 415 U.S. 800, 804 (1974), officers could never review the entire contents of an arrestee's E-book library or peruse years' worth

---

Search upon arrest was a familiar feature of Founding-era practice" and "there is no known instance of a court holding the seizure of papers from an arrested person to be unconstitutional." Donald A. Dripps, *"Dearest Property": Digital Evidence and the History of Private "Papers" as Special Objects of Search and Seizure,* 103 J. Crim. L. & Criminology 49, 108 (2013).

of the arrestee's personal correspondence. Although in that period officers may be able to run searches on a collection of emails or other files for evidence of crime and review photos or contacts for potential criminal associations, the suggestion that officers will use that period to delve into the "thoughts, wonders, and concerns" of arrestees, rather than seek evidence and accomplish other legitimate law-enforcement objectives, is unfounded.

b. Petitioner also overstates what a warrant to search a cell phone would accomplish. He contends that a warrant would identify "which files to search, how far back in time to search, and which attachments or links to activate." Pet. Br. 31. But a warrant would not so specify. When the police show probable cause, the "place" to be searched is the cell phone, and the officers may search for evidence for which they have probable cause through "at least a cursory review of each file" on the phone that may contain the object of the search. *United States* v. *Williams*, 592 F.3d 511, 522 (4th Cir.) (computer search), cert. denied, 131 S. Ct. 595 (2010); see *Andresen* v. *Maryland*, 427 U.S. 463, 482 n.11 (1976) ("In searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized.").

A warrant requirement would foreclose searches where officers could not show probable cause to believe that a phone contains evidence of crime. But that is the type of search that the Fourth Amendment has long authorized for address books, wallets, purses, and papers on the arrestees' person because of his reduced expectation of privacy and the common-sense

intuition that evidence of an arrestee's crime is likely to be found on his person.

Finally, the risk that officers might abuse their authority and publicly disseminate sensitive information found on an individual's phone (Pet. Br. 37 n.12) also exists for a search under a warrant. The remedy for such isolated misconduct is internal discipline and possibly tort liability, not depriving all officers nationwide of their traditional search authority.

2. Petitioner also argues (Br. 31-38) that this Court should apply heightened Fourth Amendment scrutiny because "smart phones hold information that implicates First Amendment concerns." Pet. 31 (capitalization altered). As this Court has explained, however, "[t]here is no special sanctity in papers." *Gouled* v. *United States*, 255 U.S. 298, 309 (1921), overruled on other grounds by *Warden* v. *Hayden*, 387 U.S. 294 (1967). While "the requirements of the Fourth Amendment must be applied with 'scrupulous exactitude'" when seized materials may have First Amendment protection, *Zurcher* v. *Stanford Daily*, 436 U.S. 547, 564 (1978) (citation omitted), search-incident-to-arrest authority under the Fourth Amendment has *always* allowed the inspection of papers found on an arrestee's person. U.S. *Wurie* Br. 25-26.

Petitioner cites two sets of cases to support his novel limitation on search-incident-to-arrest authority. First, he cites (Br. 34-36) pre-*Chimel* search-incident-to-arrest cases analyzing whether a particular search of the *premises* of an arrest was reasonable. See Pet. Br. 34-35. That reasonableness standard, however, did not categorically insulate papers from officers' search authority. See *Hill* v. *California*, 401 U.S. 797, 799-802 & 800 n.1 (1971) (upholding search

of diary incident to arrest); *United States* v. *Bennett*, 409 F.2d 888, 897 (2d Cir.) (Friendly, J.) (cited at Pet. Br. 36) (upholding the warrantless review of letter "discovered in a lawful search of [arrestee's] pocketbook for narcotics * * * to see whether it was an 'instrumentality' for effecting the conspiracy"), cert. denied, 396 U.S. 852 (1969). In addition, the case on which petitioner places the greatest weight, *United States* v. *Lefkowitz*, 285 U.S. 452 (1932), rested primarily on the now-discredited view that, even under a warrant, officers lack authority to seize "mere evidence" of crime. See *id.* at 464-466; note 17, *supra*.

In any event, this Court has never suggested that officers' "unqualified authority" to search the person of the arrestee is diminished with respect to written material. *Robinson*, 414 U.S. at 225. Even in *Lefkowitz*, this Court did not cast doubt on the court of appeals' holding that the seizure of papers from the person of the arrestee was lawful. See 285 U.S. at 458, 461. As Judge Hand explained, "the law has never distinguished between documents and other property found upon the person of one arrested." *United States* v. *Kirschenblatt*, 16 F.2d 202, 203 (2d Cir. 1926).

Second, petitioner relies (Br. 33-34) on First Amendment cases involving the content-based seizure, under a warrant, of books or films. In *Marcus* v. *Search Warrant*, 367 U.S. 717 (1961), and *A Quantity of Copies of Books* v. *Kansas*, 378 U.S. 205 (1964), for example, "the material seized fell arguably within First Amendment protection, and the taking brought to an abrupt halt an orderly and presumptively legitimate distribution or exhibition." *Roaden* v. *Kentucky*, 413 U.S. 496, 504 (1973). The Court held that without

a valid warrant that described the allegedly unlawful media with sufficient specificity, the seizures constituted "a form of prior restraint." *Ibid.*; see *id.* at 506. The Court's central concern in the cases petitioner cites was the "use by government of the power of search and seizure as an adjunct to a system for the suppression of objectionable publications," *ibid.* (quoting *Marcus*, 367 U.S. at 724)—that is, the use of broad warrants to seize books and other material where "the basis for their seizure is the ideas which they contain," *Stanford* v. *Texas*, 379 U.S. 476, 485 (1965).

It trivializes that important principle to contend that the search of an arrestee's cell phone to find evidence of crime or to confirm his gang affiliation presents a "serious hazard of suppression of innocent expression." *Marcus*, 367 U.S. at 729; cf. *Roaden*, 413 U.S. at 505 (distinguishing seizures from commercial theatres from seizures where there is probable cause to arrest because "contraband is changing hands or * * * a robbery or assault is being perpetrated"). Petitioner does not even contend that his phone was unlawfully *seized*, defeating any analogy to prior-restraint cases, and in any event he makes no claim that the seizure inhibited him from disseminating expressive material to the public or that his phone was seized because of the content of his expression. No case of this Court has ever held that private correspondence and similar communicative content—often the most important evidence of criminal conspiracies—enjoys a special protection from police inquiry.

Finally, petitioner asserts (Br. 33-34) that searching an arrestee's phone for evidence impinges on associational freedoms. But for serious criminal offenses, investigating a suspect's associations—confederates,

suppliers, witnesses, victims—is basic police work. That everyday law-enforcement activity has no relationship to the restrictions on associational freedoms, such as the compelled disclosure of membership lists of law-abiding political associations, that this Court has condemned. Cf., *e.g.*, *NAACP* v. *Alabama ex rel. Patterson*, 357 U.S. 449, 465 (1958) (distinguishing an organization engaged in "acts of unlawful intimidation and violence").

C. A Total Prohibition On Cell-Phone Searches Incident To Arrest Cannot Be Justified

1. In *Wurie*, the United States argues (Br. 45-49) that, if cell-phone searches incident to arrest were not thought categorically permissible under *Robinson*, the Court should at a minimum permit them when officers reasonably believe that a phone contains evidence of the offense of arrest. This Court adopted that standard in *Gant* for vehicle searches incident to arrest that do not sufficiently implicate the *Chimel* evidence-preservation and safety interests. See 556 U.S. at 335, 343.

Petitioner objects (Br. 38-43) to that proposal for two reasons, neither of which is sound. First, petitioner observes that *Gant* cited "circumstances unique to the vehicle context" in establishing its standard. 556 U.S. at 343. He speculates about the Court's concerns, but no need for speculation exists: the Court cited Justice Scalia's concurrence in *Thornton*, which explained that "motor vehicles" are "a category of 'effects' which give rise to a reduced expectation of privacy." 541 U.S. at 631. The same is true for objects found on the person of an arrestee. See *Chadwick*, 433 U.S. at 16 n.10; *Edwards*, 415 U.S. at 808-809; *Robinson*, 414 U.S. at 237 (Powell, J., concurring).

Justice Scalia derived that standard, moreover, primarily from the general interest in evidence-gathering that undergirded the search-incident-to-arrest doctrine as an original matter. See *Thornton*, 541 U.S. at 629-632.

Second, petitioner contends that under a *Gant*-based standard, "a curious police officer will virtually always be able to assure himself that he has reason to believe that an arrestee's smart phone contains evidence of the crime(s) of arrest" (Br. 42)—while arguing a page later that the standard is not met in this case. Petitioner's concern is unfounded. As with other Fourth Amendment doctrines that require officers to conduct on-the-scene reasonableness determinations (see, *e.g.*, *Terry* v. *Ohio*, 392 U.S. 1 (1968)), courts would develop guidelines about when officers can reasonably conclude that a phone is likely to contain evidence relevant to particular crimes, and suppression would be available where officers transgress those limits.

The United States has provided examples when a *Gant*-based standard would and would not be satisfied. See U.S. *Wurie* Br. 47-48. In particular, most traffic offenses would not justify a search of an arrestee's cell phone under that standard. (Petitioner cites no evidence supporting his speculation (Br. 41) that officers can determine the speed at which a motorist was driving from the locational information on a cell phone.) Likewise, officers could not search the phones of those arrested for "jaywalking, littering, or riding a bicycle the wrong direction." Pet. Br. 2. But petitioner's blanket prohibition on cell-phone searches would deprive officers of a longstanding tool even for serious offenses like drug trafficking and gang-related

violence. No Fourth Amendment justification compels that result.

2. The United States also suggested in *Wurie* (Br. 49-55) that if concern about the amount of private information contained on a cell phone persuades this Court to draw an item-specific exception from the *Robinson* categorical rule, it could address that concern by limiting the *scope* of any search in this context to the areas of the phone reasonably related to finding evidence relevant to the crime of arrest, identifying the arrestee, and protecting officers. Petitioner does not address such a scope-limited approach. But that approach would dispel the theoretical fears of vast "exploratory" searches raised by petitioner and his amici.

D. The Search Of Petitioner's Cell Phone Was Lawful

Under the settled search-incident-to-arrest doctrine articulated in *Weeks*, *Robinson*, and other decisions of this Court, officers had authority to search petitioner's cell phone after he was lawfully arrested. But the search was also valid under either of the narrower approaches suggested by the United States—a *Gant*-based standard or a scope-limited standard.

With respect to the first approach, the superior court found that the search "relat[ed] to the crime for which [petitioner] was arrested." J.A. 23. Officers had reason to believe that petitioner was a member of the Lincoln Park Bloods based on the paraphernalia he was carrying and that the phone might contain photographic evidence linking petitioner to the firearms for which he had been arrested. *Ibid.* Additionally, the offenses of arrest carried an enhancement if "the person is an active participant in a criminal street gang." Cal. Penal Code §§ 12025(b)(3), 12031(a)(2)(C)

(West 2008). It was reasonable to believe that his phone might contain evidence of his gang affiliation.

Similarly, under a scope-limited approach, the officers' review of texts, photos, and videos on petitioner's cell phone was reasonably related to discovering evidence of the crime of arrest and to the "identification and isolation of gang members before they are admitted" to a detention facility. *Florence* v. *Board of Chosen Freeholders*, 132 S. Ct. 1510, 1519 (2012). No evidence was introduced that fell outside of those categories. See 134 S. Ct. 999 (2014) (limiting question presented to whether "evidence admitted at petitioner's trial was obtained in a search * * * that violated petitioner's Fourth Amendment rights").

II. THE STATIONHOUSE SEARCH OF PETITIONER'S CELL PHONE OCCURRED WITHIN A REASONABLE TIME AFTER HIS ARREST

Petitioner argues that, even if officers had authority to search his phone, the second search at the stationhouse took place too long after his arrest to be justified as a search incident to that arrest. That contention lacks merit.

A. This Court held in *Edwards*, *supra*, that a search of the person incident to arrest may occur at the stationhouse rather than at the scene of arrest. In that case, the Court deemed a delay of ten hours in seizing the clothing of the arrestee and sending it to a laboratory for forensic analysis to be a "reasonable delay." 415 U.S. at 805. The Court explained that "both the person and the property in [an arrestee's] immediate possession may be searched at the station house after the arrest has occurred at another place and if evidence of crime is discovered, it may be seized and admitted in evidence." *Id.* at 803. That rule fol-

lows, the Court continued, from the basic principle that an arrest "for at least a reasonable time" takes the arrestee's "privacy out of the realm of protection from police interest in weapons, means of escape and evidence." *Id.* at 808-809 (citation omitted).

Petitioner would limit *Edwards* (Br. 49-51) to property still in a suspect's possession at the place of detention. *Edwards* did not rely on that fact. Nor can petitioner's view be reconciled with the Court's holding that objects seized at the place of detention could be "later subjected to laboratory analysis"—a search that, under petitioner's view, would be insufficiently contemporaneous with the arrest—or with the Court's statement that a search is permissible even if it occurs "at a later time" than the seizure. 415 U.S. at 804, 807. And contrary to petitioner's characterization (Br. 50), *Edwards* plainly applied the search-incident-to-arrest doctrine, not the inventory-search doctrine; the critical part of the Court's analysis was set forth before its brief discussion of *Cooper* v. *California*, 386 U.S. 58 (1967).

Importantly, *Edwards*'s holding applies to searches of the arrestee's *person* and items on his person—not items found near the location of arrest. The distinction flows from the different expectations of privacy. As discussed, *Chadwick* held that "[o]nce law enforcement officers have reduced * * * personal property *not immediately associated with the person of the arrestee* to their exclusive control," they no longer may search it without a warrant. 433 U.S. at 15 (emphasis added). But *Robinson* and *Edwards* rely on the arrestee's reduced expectations of privacy in his person for a different rule for searches of the person and his immediate possessions.

Like *Chadwick*, the two pre-*Edwards* decisions that petitioner cites—*Preston* v. *United States*, 376 U.S. 364 (1964), and *Dyke* v. *Taylor Implement Manufacturing Co.*, 391 U.S. 216 (1968)—concerned the search of an object found near the scene of arrest (the suspect's vehicle), not on the arrestee's person. And the leading circuit decision petitioner cites for his timing argument (Br. 47 n.16) explained, citing *Edwards* and *Chadwick*, that "[s]earches of the person and articles immediately associated with the person of the arrestee are treated differently" because "an arrest diminishe[s] one's expectation of privacy in one's person, thereby rendering reasonable any later search." *United States* v. *$639,558 in U.S. Currency*, 955 F.2d 712, 716 n.6 (D.C. Cir. 1992) (internal quotation marks and citation omitted) (search of 80-pound suitcase). Thus, at least where a search of items on the arrestee's person is conducted "a reasonable time" after the arrest, it is valid under *Edwards*. 415 U.S. at 809.

B. That approach makes practical sense. As discussed above, officers are entitled to conduct a full search of an individual upon arrest "to discover and seize the fruits or evidences of crime." *Robinson*, 414 U.S. at 224-225 (quoting *Weeks*, 232 U.S. at 392). That rule is justified in part because, in the aftermath of an arrest, the police must act quickly to apprehend confederates and quell threats to public safety. See U.S. *Wurie* Br. 30-31. But it may be unsafe or infeasible to conduct that search at the scene of arrest. It may be dark, or the weather may be bad; the officer may be dealing with multiple arrestees, witnesses, and victims; or the officer could perceive danger to herself or the arrestee. Thus, it is sensible to permit the officer, "for at least a reasonable time" after the arrest, to re-

tain the authority to conduct the evidentiary search that she could have conducted "on the spot at the time of arrest." *Edwards*, 415 U.S. at 803, 808-809.

Petitioner seeks (Br. 51-53) a phone-specific exception to *Edwards* on the ground that new data could be sent to the phone between the time of arrest and the time of the search. He offers no Fourth Amendment justification for that request. Information sent to the phone immediately after an arrest may be particularly likely to contain evidence of the crime of arrest—for example, a confederate's inquiry into the arrestee's whereabouts. Although an officer's affirmative use of a phone to view files stored elsewhere raises different privacy issues, that limitation is not implicated where other individuals transmit information to an arrestee's phone following an arrest. The arrestee's diminished expectation of privacy continues to justify a warrantless search of the phone.

Finally, petitioner errs in suggesting (Br. 52-53) that the search of a cell phone incident to arrest might violate Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. 2511-2522, or the Stored Communications Act, 18 U.S.C. 2701, 2703(a). Title III is not implicated when stored e-mails are accessed, because the interception is not "contemporaneous with transmission." *United States* v. *Steiger*, 318 F.3d 1039, 1047-1049 (11th Cir) (citing decision of two other circuits), cert. denied, 538 U.S. 1051 (2003). Likewise, it would not violate the Stored Communications Act to review any item stored on the phone itself. See *id.* at 1049. In any event, statutory restrictions do not define the Fourth Amendment's scope. *Quon*, 130 S. Ct. at 2632.

C. The stationhouse search in this case was valid. The search took place soon after petitioner arrived at the stationhouse and, as in *Edwards*, before "the administrative mechanics of arrest ha[d] been completed." 415 U.S. at 804; J.A. 15-16; Br. in Opp. 2. The delay, moreover, was reasonable. The initial search at the scene of arrest, including of petitioner's cell phone, revealed evidence of gang involvement, and the arresting officer brought in a detective specializing in gangs to interview petitioner and review his phone. As this Court has explained, the police have a substantial interest in identifying gang members as part of a custodial arrest. See *Florence*, 132 S. Ct. at 1519. A reasonably prompt search could also provide evidence to allow police to focus their investigation, locate witnesses or confederates, and anticipate any immediate repercussions in the community that the arrest might cause.

CONCLUSION

The judgment of the court of appeal should be affirmed.

Respectfully submitted.

DONALD B. VERRILLI, JR.
Solicitor General
DAVID A. O'NEIL
Acting Assistant Attorney General
MICHAEL S. DREEBEN
Deputy Solicitor General
JOHN F. BASH
Assistant to the Solicitor General
ROBERT A. PARKER
Attorney

APRIL 2014

http://norhursttactical.com/training/professional-individual-training/advanced-mobile-forensics/