
NEW YORK UNIVERSITY
JOURNAL OF LAW & LIBERTY

AGREEMENT AT THE SUPREME COURT: THE THREE IMPORTANT PRINCIPLES UNDERLYING *RILEY V. CALIFORNIA*

Brianne J. Gorod*

INTRODUCTION

When the Supreme Court term ended in June, many people proclaimed that unanimity at the Court was on the rise.[1] Although this was true by some measures, when it came to the term's most closely-watched cases, agreement as to the proper result generally belied sharp disagreement as to the reasoning behind that result.[2] One notable exception was the Court's decision in *Riley v. California* and *United States v. Wurie*, companion cases in which all nine justices agreed that that the police generally may not search an arrestee's cell phone without a warrant.[3]

---

* Appellate Counsel, Constitutional Accountability Center. I would like to thank Jeff Hauser, Doug Kendall, and Kelly Landis for their helpful comments and suggestions. The views expressed herein are solely my own.

[1] *See, e.g.*, Neal K. Katyal, Op-Ed., *The Supreme Court's Powerful New Consensus*, N.Y. TIMES, June 27, 2014, at A29.

[2] Brianne J. Gorod, *A Year of Contradictions*, 17 GREEN BAG 2D 405, 405-09 (2014).

[3] Riley v. California, 134 S. Ct. 2473 (2014).

In his opinion for the Court, Chief Justice Roberts put it plainly: "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."[4] As the Court explained, "modern cell phones . . . 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,"[5] and the type and quantity of information stored on modern cell phones means that a search of one's phone can present a significant intrusion on one's privacy.[6] For these reasons, the Court concluded that its prior precedent allowing searches of *physical* objects incident to an arrest did not make sense as applied to the digital content on cell phones.[7] The Court's decision in these cases was incredibly important, but just as important—and in some ways more surprising[8]—was the justices' broad agreement about the principles underlying that decision.

The Court has long had to grapple with how to apply the Fourth Amendment's privacy protections to new technologies,[9] and as the justices themselves have recognized, this will not be the last

---

[4] *Id.* at 2495.

[5] *Id.* at 2484.

[6] *Id.* at 2489-91.

[7] *Id.* at 2488.

[8] *See, e.g.*, Orin Kerr, *Initial Impressions from the Oral Argument in the Supreme Court Cell Phone Search Cases*, THE VOLOKH CONSPIRACY (Apr. 29, 2014), http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/04/29/initial-impressions-from-the-oral-argument-in-the-supreme-court-cell-phone-search-cases/ (discussing the different possible rules the Court might adopt and how different justices seemed to be leaning). Indeed, when the Court grappled with how to apply the Fourth Amendment to GPS technology in *United States v. Jones*, all nine justices agreed that the Fourth Amendment prohibits warrantless GPS tracking, but the Court split sharply as to the reasons. *See* United States v. Jones, 132 S. Ct. 945 (2012).

[9] *See, e.g.*, United States v. Knotts, 460 U.S. 276 (1983) (holding that using the signal of a beeper to monitor the transportation of a container of chemicals did not violate the Fourth Amendment); Olmstead v. United States, 277 U.S. 438, 466 (1928) (holding that wiretapping did not violate the Fourth Amendment), *overruled by* Katz v. United States, 389 U.S. 347 (1967).

time.[10] The Court's decision in *Riley* reflected that the justices all agree, at least to some degree, on three important principles. First, digital is different: digital information presents possibilities for intrusions on personal privacy that are categorically different from the intrusions made possible by physical objects. That difference affects the Court's analysis. Second, the Fourth Amendment's Framers may not have been able to conceive of email or Twitter, but the Framing is nonetheless relevant to understanding how the Fourth Amendment should apply to new technologies. Third, in the law enforcement context in which the Supreme Court's decision will be providing guidance to thousands of police officers on the streets, bright line rules are especially valuable. All three of these principles will no doubt affect the Court's analysis in other Fourth Amendment cases still to come.

I. BACKGROUND

A. *RILEY V. CALIFORNIA*

In *Riley v. California*, the police stopped David Riley because he was driving with expired registration tags, but then realized that his license had been suspended. At that point, they impounded his car, and during an inventory search discovered two handguns under the car's hood. Riley was arrested for possession of concealed and loaded firearms.[11] Following his arrest, the police searched Riley's smart phone, both at the scene and two hours later at the police station. They found evidence that they believed suggested he was a member of a gang and had been involved in a shooting.[12] Riley was

---

[10] *See, e.g.*, Elena Kagan: Supreme Court Hasn't "Gotten To" Email, CBS (Aug. 21, 2013, 12:07 PM), http://www.cbsnews.com/news/elena-kagan-supreme-court-hasnt-gotten-to-email/; Supreme Court Will Likely Rule on NSA Programs, Antonin Scalia and Ruth Bader Ginsburg Suggest, Reuters (Apr. 17, 2014, 6:17 PM), http://www.huffingtonpost.com/2014/04/17/supreme-court-nsa_n_5170559.html.

[11] 134 S. Ct. at 2480.

[12] *Id.* at 2481.

charged with, among other things, attempted murder. He was convicted and sentenced to 15 years to life in prison.

A California Court of Appeal affirmed his conviction, relying on an earlier California Supreme Court decision that held that the Fourth Amendment permits searches of cell phones seized incident to an arrest.[13] According to the California Supreme Court, its result was dictated by "binding" Supreme Court precedent that made clear that the police could not only "'seize' anything of importance they find on the arrestee's body, but also . . . *open and examine* what they find."[14]

B *UNITED STATES V. WURIE*

In *United States v. Wurie*, police arrested Brima Wurie after observing him making an apparent drug sale from a car. They took him to the police station, at which point they seized two cell phones from him. One of these phones was a flip phone – when it started ringing, the police opened the phone and accessed its call log. They used the information they found to identify his home and obtained a warrant to search it, ultimately finding drugs and firearms in the apartment. Wurie was charged with, among other things, distributing crack cocaine. He was convicted and sentenced to 262 months in prison.

The First Circuit vacated Wurie's conviction, concluding that "warrantless cell phone data searches strike us as a convenient way for the police to obtain information related to a defendant's crime of arrest—or other, as yet undiscovered crimes—without having to secure a warrant," and "nothing in the Supreme Court's search-

---

[13] People v. Diaz, 244 P.3d 501 (Cal. 2011).
[14] *Id.* at 509 (internal citation omitted).

incident-to-arrest jurisprudence . . . sanctions such a 'general evidence-gathering search.'"[15]

C. THE SUPREME COURT DECISION

Although the cases were argued separately and involved different types of phones, the Court concluded that its message to the police in both cases was the same: "get a warrant."[16] According to the Court, its prior precedent allowing searches incident to arrest struck "the appropriate balance in the context of physical objects," but "neither of its rationales [preventing harm to offers and destruction of evidence] has much force with respect to digital content on cell phones."[17] Thus, although "other case-specific exceptions [such as exigent circumstances] may still justify a warrantless search of a particular phone,"[18] the police may not justify a warrantless search of the digital contents of an arrestee's cell phone simply by pointing to the fact that it was found on the arrestee at the time of his arrest. All nine justices agreed, at least in large part, with the Chief Justice's opinion for the Court.

Justice Alito wrote separately to make two points. First, he was unconvinced 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."[19] Thus, he would not "allow that reasoning to affect cases like these that concern the search of the person of arrestees."[20] But he agreed with the Court that it would not be right to "mechanically apply the rule used in the predigital era to the search of a cell

---

[15] United States v. Wurie, 728 F.3d 1, 13 (1st Cir. 2013).

[16] 134 S. Ct. at 2495.

[17] *Id.* at 2484.

[18] *Id.* at 2494.

[19] *Id.* at 2495 (Alito, J., concurring in part and concurring in the judgment). According to Justice Alito, "the basis for the rule . . . was the need to obtain probative evidence." *Id.*

[20] *Id.* at 2496.

phone."[21] Second, Justice Alito said he "would reconsider the question presented here if either Congress or state legislatures . . . enact legislation that draws reasonable distinctions based on categories of information or perhaps other variables."[22]

II. THREE PRINCIPLES

A. DIGITAL IS DIFFERENT

One of the most interesting aspects of *Riley* and *Wurie* was the fact that they were decided against the background of significant case law that was in some senses exactly on point, but in other senses not on point at all. Although many Supreme Court cases addressed the proper scope of searches incident to arrest, none of those cases involved searches of devices that contain digital information.

That is why one of the most significant principles coming out of the Court's decision in *Riley* is that digital is different, and the difference matters. In *United States v. Robinson*, the Court held that the police could lawfully inspect a crumpled cigarette package found on a person during his arrest.[23] In *Riley*, the Court acknowledged that "a mechanical application of *Robinson* might well support the warrantless searches at issue here," but as noted above, the balance it struck in the context of physical objects did not make sense in the context of digital content on cell phones.[24] As the Chief Justice put it: "The United States asserts that a search of all data stored on a cell phone is 'materially indistinguishable' from searches of [the] sorts of physical items [searched in previous cases]. That is like saying a ride on horseback is materially indistinguishable from a flight to the

---

[21] *Id.* Justice Alito believed that the Court's approach would "lead[] to anomalies," but saw no "workable alternative." *Id.*

[22] *Id.* at 2497.

[23] 414 U.S. 218, 236 (1973).

[24] 134 S. Ct. at 2484.

moon. Both are ways of getting from point A to point B, but little else justifies lumping them together."[25]

The Court made clear that digital is different for two important reasons. First, the concerns that previously led the Court to allow searches-incident-to-arrest simply make no sense in the context of digital content. As the Court explained it, "unknown physical objects may always pose risks [to police officers], no matter how slight . . . . No such unknowns exist with respect to digital data."[26] 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."[27] Second, and perhaps more importantly, "[m]odern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of" the physical objects at issue in the Court's previous cases.[28] The significant intrusion on privacy posed by searches of modern cell phones figured prominently in the Court's analysis.[29] Indeed, the Court acknowledged that its "decision . . . will have an impact on the ability of law enforcement to combat crime," but concluded that "[p]rivacy comes at a cost."[30]

B. THE SIGNIFICANCE OF FRAMING-ERA HISTORY

The Court was surely right to give significant weight to the privacy interests at stake in these cases because it was just such an intrusion into privacy that the Fourth Amendment was adopted to prevent. Indeed, while the Framers may not have been able to envi-

---

[25] *Id.* at 2488.
[26] *Id.* at 2485.
[27] *Id.* at 2486.
[28] *Id.* at 2488-89.
[29] *Id.* at 2489 (observing that "the possible intrusion on privacy is not physically limited in the same way when it comes to cell phones"); *id.* at 2491 (noting that "the privacy interests here dwarf those in *Robinson*").
[30] *Id.* at 2493.

sion the modern cell phone, they certainly could imagine significant intrusions on personal privacy. When the Framers drafted the Fourth Amendment, they were responding, in significant part, to the British use of "general warrants" and "writs of assistance," documents that authorized generalized searches in the absence of any individualized suspicion of wrongdoing.[31]

Although the Court in *Riley* noted the absence of "precise guidance from the founding era" and thus focused primarily on its own precedent and the challenges posed by new technologies, it nonetheless recognized the relevance of this Framing-era history. In doing so, the Court, of course, broke no new ground. It is a bedrock principle of constitutional interpretation that one must look to the Constitution's text and history to understand its meaning.[32] But at least some justices have struggled with how to use Framing-era history in cases in which exact analogues are not available.[33] Here, the Court plainly recognized that even in the absence of exact analogues, Framing-era history can highlight the underlying principles the constitutional provision was adopted to protect.

When it comes to the Fourth Amendment, those underlying principles are quite clear. As the Court explained, "the Fourth Amendment was the founding generation's response to the reviled

---

[31] *See, e.g.*, United States v. Chadwick, 433 U.S. 1, 7-8 (1977) (noting that "the Fourth Amendment's commands grew in large measure out of the colonists' experience with the writs of assistance and their memories of the general warrants formerly in use in England.").

[32] *See, e.g.*, N.L.R.B. v. Canning, 134 S. Ct. 2550, 2561 (2014) (looking to constitutional text and history).

[33] *See, e.g.*, United States v. Jones, 132 S. Ct. at 958 (Alito, J., concurring in the judgment) (agreeing with the Court that "'we must "assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted,'" but noting that "it is almost impossible to think of late-18th-century situations that are analogous to what took place in this case."). The Court took issue with Justice Alito's suggestion in *Jones*, but noted that "[i]n any case, it is quite irrelevant whether there was an 18th-century analog. . . . [O]ur task, *at a minimum*, is to decide whether the action in question would have constituted a 'search' within the original meaning of the Fourth Amendment." *Id.* at 950 n.3.

"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."[34] Indeed, the Court noted that "[o]pposition to such searches was in fact one of the driving forces behind the Revolution itself."[35] Chief Justice Roberts even made the point in somewhat more humorous fashion when he responded to the government's suggestion that "law enforcement agencies [could] '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."[36] The Chief's point was clear: one of the reasons the Framers fought a revolution was to ensure that the government cannot, as a general matter, intrude on a person's privacy without some individualized suspicion of wrongdoing, and it is the Court's responsibility to prevent such government intrusions on privacy.

C. BRIGHT LINE RULES

In addition to the suggestion that law enforcement agencies develop protocols, both the United States and California "offer[ed] various fallback options for permitting warrantless cell phone searches under certain circumstances."[37] Some of these options seemed to gain some traction at oral argument in the cases—for example, the suggestion that the police could search when it was "reasonable to believe that the phone contains evidence of the crime of arrest"[38]—and following argument, commentators speculated about the different nuanced rules the Court might adopt.[39]

---

[34] 134 S. Ct. at 2494.
[35] *Id.*
[36] *Id.* at 2491.
[37] *Id.*
[38] *Id.* at 2492; *see* Transcript of Oral Argument at 43, *Riley*, 134 S. Ct. 2473.
[39] *See* 134 S. Ct. at 2488.

But as noted, the Court went for clarity over nuance, adopting a broad, unequivocal holding requiring a warrant whenever a cell phone is searched, absent some other exception to the warrant requirement. The Court rejected these middle-of-the-road approaches in part because they would have done little to constrain police officers—as the Court explained, "[i]t 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"[40]—but it also surely reflects the Court's recognition that only a bright line rule can provide the guidance the police need when they are doing their jobs. As the Court noted, "Each of [the government] proposals . . . contravenes our general preference to provide clear guidance to law enforcement through categorical rules."[41] Justice Alito also made this point explicit, noting that "[l]aw enforcement officers need clear rules regarding searches incident to arrest."[42]

The Court gave them a "clear rule" in *Riley*: "get a warrant."

III. LOOKING AHEAD

In the years ahead, *Riley* will provide guidance not only to the police, but also to judges who are attempting to apply the Fourth Amendment's protections to other situations involving new technologies. As Richard Re pointed out immediately following the decision, "*Riley* will be remembered as the inauguration of a new era of Fourth Amendment doctrine not so much because of its specific holding, but rather because its reasoning clears the way for even more doctrinal change."[43] As he explains, *Riley* suggests that "when

---

[40] 134 S. Ct. at 2492.

[41] *Id.* at 2491.

[42] *Id.* at 2497 (Alito, J., concurring in part and concurring in the judgment).

[43] Richard Re, *Symposium: Inaugurating the digital Fourth Amendment*, SCOTUSBLOG (June 26, 2014. 12:37 PM), http://www.scotusblog.com/2014/06/symposium-inaugurating-the-digital-fourth-amendment/.

it comes to new technologies, lower courts are on notice that they shouldn't too quickly follow broad statements from pre-digital opinions, even if those opinions emanated from the Supreme Court itself."[44]

Many lower courts will benefit from that notice because other cases involving the application of the Fourth Amendment to new technologies are rapidly working their way through the lower courts. For example, the ACLU has challenged the National Security Agency's bulk telephony metadata collection program. A district court has held that the program does not violate the Fourth Amendment, but an appeal is pending.[45] And while other cases have already been decided at the appellate level, these issues will continue to percolate in the lower courts until the Supreme Court steps in. For example, earlier this year, the Second Circuit held that the Fourth Amendment prohibits the government from indefinitely retaining files on a computer that were seized pursuant to a warrant but are not responsive to it.[46] And there is already a division in the lower courts regarding whether the police must obtain a warrant to collect cellphone location data.[47] These are just a few examples: as new technologies develop, there can be little doubt that new legal issues will too.

A full exploration of these new issues is beyond the scope of this essay, but one thing seems sure: the Court's reasoning in *Riley* will play a significant role in how all of these cases are decided.

---

[44] *Id.*

[45] ACLU v. Clapper, 959 F. Supp. 2d 724 (2013).

[46] United States v. Ganias, 755 F.3d 125 (2d Cir. 2014).

[47] *Compare* United States v. Davis, 754 F.3d 1205, 1215 (11th Cir. 2014) (concluding that "the government's warrantless gathering of his cell site location information violated his reasonable expectation of privacy"), *with* In re Application of the United States for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013) (holding that "orders to obtain *historical* cell site information for specified cell phones at the points at which the user places and terminates a call are not categorically unconstitutional").