The Missed Opportunities of *Riley v. California*

Ric Simmons*

INTRODUCTION

Riley v. California was hailed by privacy advocates as a strong affirmation of our Fourth Amendment rights and an important acknowledgement that the rules need to be different in this age of new technology.[1] To be sure, the Court did increase protections for criminal defendants at the time of arrest by narrowing the government's ability to search through a specific type of item at arrest. And the majority opinion is full of wonderful sound bites for privacy advocates: "the Founders did not fight a revolution to gain the right to government agency protocols"[2] or "[o]ur 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."[3] The opinion even concludes with a dramatic flourish by quoting John Adams and denouncing the oppressive British general warrants of the 18th century.[4]

In truth, however, the *Riley* Court missed two significant opportunities—one to repair the critically flawed search incident to arrest doctrine and the other to provide useful guidance for law enforcement officers faced with emerging technologies. Like the Court's other search incident to arrest opinions, *Riley*'s rationale was confused and inconsistent. And like the Court's other Fourth Amendment technology cases, *Riley's* arguments focused too much on the technical details of a specific new technology and not enough on basic Fourth Amendment principles. As a result, the true legacy of *Riley* is likely to be further confusion both in rules and in underlying doctrine. Instead of being a true landmark case, *Riley* is—at best—merely one more tentative step towards a necessary re-evaluation of Fourth Amendment jurisprudence.

---

* Chief Justice Thomas J. Moyer Professor for the Administration of Justice and Rule of Law, The Ohio State University Moritz College of Law.

1 *See, e.g.*, Editorial, *The Court Saves Cellphone Privacy*, N.Y. TIMES (June 25, 2014), http://www.nytimes.com/2014/06/26/opinion/the-supreme-court-saves-cellphone-privacy.html ("[I]n a gratifyingly sweeping ruling on Wednesday, the court embraced a central reality of the digital age and protected such phones from being searched without a warrant during an arrest, except in rare circumstances.").

2 Riley v. California, 134 S. Ct. 2473, 2491 (2014).

3 *Id.* at 2495.

4 *Id.* at 2494.

I. THE PRE-*RILEY* STATE OF AFFAIRS

Riley had the potential to be a landmark because it addressed two separate areas of law that were in dire need of clarification or outright restructuring: the search incident to arrest doctrine and Fourth Amendment jurisprudence relating to emerging technologies.

A. *One Hundred Years of Confusion: The Search Incident to Arrest Doctrine Before* Riley

As Justice Alito noted in his concurrence in *Riley*, the right of law enforcement to search incident to an arrest has "ancient" roots, predating the Fourth Amendment itself "by at least a century."[5] But the Supreme Court did not formally recognize the search incident to arrest doctrine until the case of *Weeks v. United States*,[6] decided exactly one hundred years before the *Riley* case was handed down. *Weeks* confirmed that the broad purpose for these searches was "to discover and seize the fruits or evidences of crime,"[7] or, as Justice Alito put it: "the need to obtain probative evidence."[8] The scope of the search was consistent with the breadth of this purpose—in a case in 1927, the Court stated that the police could search "all parts of the premises used for the unlawful purpose."[9] This interpretation of the search incident to arrest doctrine became more and more controversial over the next few decades,[10] but in 1950 the Court affirmed these broad powers in *United States v. Rabinowitz*.[11] *Rabinowitz* confirmed that the police could search "the place where the arrest [was] made" in order to find "proofs of guilt within the control of the accused found upon arrest."[12]

However, this broad granting of powers to law enforcement did not survive the Warren Court. Throughout the 1960s, the Court began narrowing the purpose that justified these searches, stating for the first time that the purpose of the search was merely to prevent the defendant from destroying evidence or to seize any weapons which might be used against the arresting officers.[13] This shift

---

[5] *Id.* at 2495 (Alito, J., concurring).

[6] 232 U.S. 383, 392 (1914).

[7] *Id.* at 392.

[8] *Riley*, 134 S. Ct. at 2495 (Alito, J., concurring).

[9] Marron v. United States, 275 U.S. 192, 199 (1927).

[10] *See* James J. Tomkovicz, *Divining and Designing the Future of the Search Incident to Arrest Doctrine: Avoiding Instability, Irrationality, and Infidelity*, 2007 U. ILL. L. REV. 1417, 1425 & n.52 (2007) (noting that by 1950, there had been three search incident to arrest cases in a row at the Supreme Court which were decided 5-4).

[11] 339 U.S. 56, 66 (1950).

[12] *Id.* at 61.

[13] Preston v. United States, 376 U.S. 364, 367 (1964).

culminated in *Chimel v. California*,[14] in which the Court narrowed the scope of the search to conform it to its more constricted purposes. Overruling *Rabinowitz*, the *Chimel* Court held that arresting officers could only search the defendant himself and his "wingspan," defined as "the area into which an arrestee might reach in order to grab a weapon or evidentiary items."[15]

Although the *Chimel* case remains (mostly) good law today, its wingspan rule suffers from a critical practical flaw which renders the search incident to arrest doctrine fundamentally unstable. When making an arrest, the first thing most arresting officers do is secure a suspect by handcuffing him and removing him from the scene of the crime. It is unlikely that an officer would simply announce that a suspect is under arrest and then leave the suspect standing unrestrained while the officer searched through the suspect's area of immediate control.

The Supreme Court recognized this exact flaw in *Arizona v. Gant*,[16] holding that if the defendant has in fact been secured, the police have no right to search his wingspan.[17] Since this effectively abolished the old search incident to arrest doctrine, the *Gant* Court created a new search incident to arrest doctrine: if the police have reason to believe that there is evidence related to the crime within the wingspan of where the defendant had been where he was arrested, the police can search that area.[18] However, the *Gant* Court held that this new rule should only apply to arrests made in automobiles, even though the rationale applies with equal weight to any arrest.

Since *Gant* there have been two versions of the search incident to arrest doctrine: one for arrests in cars, and one for arrests everywhere else. The *Riley* Court has continued this unfortunate trend of creating special rules for special situations. As a result, we now have three versions of the search incident to arrest doctrine: one for arrests in cars, one for searches of cell phones (and probably some other forms of digital evidence), and one for every other situation.

Before we turn to *Riley*, however, we need to review one other unhappy development in the evolution of the search incident to arrest doctrine. Between *Chimel* and *Gant*, the Court decided *United States v. Robinson*,[19] in which the police officer arrested the defendant for driving with a revoked license, searched him pursuant to the arrest, and recovered a cigarette box from the defendant's pocket. The cigarette box obviously did not contain any evidence of the crime, and once it was in the hands of the police officer, it posed no danger to him. Nevertheless, the Supreme Court held that the officer was allowed to look inside the cigarette box, because the right to search is automatic after an arrest, stating

---

[14] 395 U.S. 752 (1969).

[15] *Id.* at 763; United States v. Ingram 164 F. Supp. 2d 310, 314 (N.D.N.Y. 2001).

[16] 556 U.S. 332 (2009).

[17] *Id.* at 343.

[18] *Id.* at 335.

[19] 414 U.S. 218, 220–23 (1973).

that "[a] custodial arrest of a suspect based on probable cause is a reasonable intrusion under the Fourth Amendment; that intrusion being lawful, a search incident to the arrest requires no additional justification."[20] Thus, although the *Robinson* Court claimed to be basing its decision on *Chimel*, it in fact unmoored the search incident to arrest doctrine from the *Chimel* rationale.

In a sense, *Robinson* and *Gant* can be seen as the Court's two possible responses to the fundamental illogic of *Chimel*'s wingspan rule. One response is to reject the twin justifications of *Chimel* and return to the *Weeks* and *Rabinowitz* rationale, which gave the government an automatic right to search in order to find any evidence of any crime. This is essentially what *Robinson* did, although it maintained *Chimel*'s limitation on the scope of the search. The other response would be to take *Chimel*'s justifications to their logical conclusion and only permit a search incident to arrest when there is an actual danger of destruction of evidence or access to a weapon. This is essentially what *Gant* did, although it added on a right to search for evidence of the crime if it was reasonable to believe such evidence existed.

Either the *Robinson* path or the *Gant* path would make sense, and given the tortured history of the search incident to arrest doctrine, either path can be supported by precedent. But there is no way to logically maintain *Chimel, Robinson* and *Gant* simultaneously, since none of them are truly consistent with the other. *Riley* was the Court's most recent chance to choose one of these paths and restore consistency and reason to the search incident to arrest doctrine.

The Supreme Court had three possible options in *Riley*. First, it could have issued a strong affirmation of the *Robinson* rationale, holding that a search incident to arrest is an automatic right for law enforcement officers, even if there is no real danger that the suspect will gain access to a weapon or be able to destroy evidence. Second, it could have made the search incident to arrest doctrine consistent with the *Chimel* rationale by expanding the *Gant* precedent to cover all searches, not just those in cars. Third, the Court could have created a narrow exception for the specific type of search that occurred in *Riley*, thereby maintaining the internal inconsistency of the search incident to arrest doctrine and creating yet another layer of complication for police officers, lawyers, and judges seeking to apply this doctrine. Unfortunately, the Court chose the third option.

B. *Applying the Fourth Amendment to New Technologies*

The Fourth Amendment was written over two hundred and twenty-five years ago, and its drafters could not have conceived of the technological changes that have taken place in the intervening time period. This creates challenges for the Supreme Court, leading to infamous analogies, such as when the Court compared GPS tracking to a "very tiny" constable who could hide in a carriage,[21] and

---

[20] *Id.* at 235.

[21] United States v. Jones, 132 S. Ct. 945, 958 n.3 (2012) (Alito, J., concurring).

arbitrary distinctions, such as the pre-*Katz* precedents which allowed law enforcement to eavesdrop on a private office with a "slap mike" but not with a "spike mike."[22]

Roughly speaking, there are two categories of cases in which new technologies impact the application of the Fourth Amendment. The first category involves cases in which the suspect is using a new technology to send or store information, such as the telephone in *Olmstead v. United States*[23] or the cell phone in *Riley*, and law enforcement officers are trying to search that new technology. The second category involves cases in which the law enforcement officers are the ones with the new technology, such as the thermal imager at issue in *Kyllo v. United States*[24] or the GPS tracker discussed in *United States v. Jones*,[25] and they are using that new technology to conduct surveillance. Generally speaking, the Court has struggled when it applies the Fourth Amendment to surveillance *of* a new technology, but it has had more success when it applies the Fourth Amendment to surveillance *with* a new technology.

One of the most infamous examples of the Court applying the Fourth Amendment to surveillance *of* a new technology was the 1928 case of *Olmstead v. United States,* in which the Court held that the Fourth Amendment did not apply to government monitoring of telephone calls.[26] The Court reasoned that the defendant lost all protections once his conversations were transmitted outside of his home:

> The language of the amendment cannot be extended and expanded to include telephone wires, reaching to the whole world from the defendant's house or office. The intervening wires are not part of his house or office, any more than are the highways along which they are stretched. [27]

In the more recent case of *Smith v. Maryland*,[28] the Court held that the phone numbers dialed by the defendant were not protected by the Fourth Amendment because he had already shared them with the phone company—a third party—and so no longer had a reasonable expectation of privacy in the information.[29]

---

[22] *Compare* Goldman v. United States, 316 U.S. 129 (1942) ("slap mike" permitted because neither the Fourth Amendment nor the Wiretap Act protects the privacy of oral communication), *with* Silverman v. United States, 365 U.S. 505 (1961) ("spike mike" not permitted because a part of the listening device infringed on the defendant's property rights).

[23] 277 U.S. 438 (1928).

[24] 533 U.S. 27 (2001).

[25] 132 S. Ct. 945 (2012).

[26] 277 U.S. 438, 466 (1928).

[27] *Id.* at 465.

[28] 442 U.S. 735 (1979).

[29] *Id.* at 745–46.

Whatever its merits in the 1970s, this doctrine makes little sense in the modern world, in which almost all digital communications are sent through third parties and enormous amounts of personal data are stored by third parties. Lower courts have criticized the third-party doctrine as outdated in the digital age,[30] but the Court has refused to address the problem, so *Smith* remains good law.

However, the Court has come up with more sensible rules when it applies the Fourth Amendment to new technologies that are used to conduct surveillance. In *Katz v. United States*, the Court was examining the constitutionality of an electronic listening device.[31] The *Katz* Court jettisoned the outdated "physical trespass" test[32] and created a new test which was flexible enough to regulate nearly any kind of search in the modern era.[33] In *Kyllo v. United States*, the Court resisted the temptation to mechanically apply a formalist "off-the-wall" vs. "through the wall" distinction[34] and instead established a "general public use" test,[35] which realistically accounts for the suspect's privacy rights.

Before *Riley*, the Court's most recent attempt to apply the Fourth Amendment to new technologies used to conduct surveillance came in *United States v. Jones*, a case which evaluated the constitutionality of round-the-clock GPS surveillance.[36] The *Jones* Court had a precedent—*United States v. Knotts*—which gave the police the right to follow a car over public highways without implicating the Fourth Amendment.[37] But in voting to hold the search unconstitutional, the justices argued in favor of adopting an exception to *Knotts* because the vast quantities of data being collected by the new surveillance technology made the search qualitatively different. Speaking for a four-justice concurrence, Justice Alito noted:

> Under this approach, relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable. But the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy. For such offenses, society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single

---

[30] *See, e.g.*, United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) (finding a reasonable expectation of privacy in the content of e-mails stored on third party servers).

[31] 389 U.S. 347 (1967).

[32] Or so it seemed at the time. The *Jones* Court has informed us that *Katz* did not really jettison the physical trespass case, but merely supplemented it with another test. United States v. Jones, 132 S. Ct. 945, 950–52 (2012).

[33] *Katz*, 389 U.S. at 353–59.

[34] Kyllo v. United States, 533 U.S. 27, 35–36 (2012).

[35] *Id.* at 40.

[36] *See Jones*, 132 S. Ct. at 948.

[37] United States v. Knotts, 460 U.S. 276, 285 (1983).

> movement of an individual's car for a very long period. In this case, for four weeks, law enforcement agents tracked every movement that respondent made in the vehicle he was driving.[38]

Justice Sotomayor echoed the same concerns in her concurring opinion:

> In cases involving even short-term monitoring, some unique attributes of GPS surveillance relevant to the *Katz* analysis will require particular attention. GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.[39]

The four-justice *Jones* concurrence thus provided a narrowly tailored approach which resolved the specific question before the Court but failed to set out a general rule for future cases. As the *Jones* concurrence put it:

> We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark. Other cases may present more difficult questions. But where uncertainty exists with respect to whether a certain period of GPS surveillance is long enough to constitute a Fourth Amendment search, the police may always seek a warrant. We also need not consider whether prolonged GPS monitoring in the context of investigations involving extraordinary offenses would similarly intrude on a constitutionally protected sphere of privacy. In such cases, long-term tracking might have been mounted using previously available techniques.[40]

As we shall see, the *Riley* Court took a similarly cautious position.

II. THE COURT'S CHOICES IN *RILEY*.

A. *Riley as a Search Incident to Arrest Case.*

Upon first blush, *Riley* appears to ground its decision in the Court's trilogy of search incident to arrest cases of *Chimel*, *Robinson*, and *Gant*.[41] But then the *Riley* Court applies a balancing test, "'assessing, on the one hand, the degree to which

---

[38] *Jones*, 132 S. Ct. at 964 (Alito, J., concurring) (internal citations omitted).

[39] *Id.* at 955 (Sotomayor, J., concurring).

[40] *Id.* at 964 (Alito, J., concurring).

[41] Riley v. California, 134 S. Ct. 2473, 2477 (2014).

[the search] intrudes on an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.'"[42] Yet none of none of the cases in the trilogy—or, indeed, any search incident to arrest case—use a balancing test. Instead, the Court relies on language from *Wyoming v. Houghton*, a case involving the automobile exception to the warrant requirement.[43]

In a slightly disingenuous move, the *Riley* opinion implied that prior search incident to arrest cases had in fact applied a balancing test. For example, it re-stated the *Robinson* holding in this way: "Put simply, a patdown of Robinson's clothing and an inspection of the cigarette pack found in his pocket constituted only minor additional intrusions compared to the substantial government authority exercised in taking Robinson into custody."[44] The *Riley* Court performed the same revisionism with *Chimel*, implying that *Chimel* performed some kind of calculation comparing the level of privacy invasion involved in the search of the defendant's house with the level of privacy invasion of an arrest: "Because a search of the arrestee's entire house was a substantial invasion beyond the arrest itself, the Court concluded that a warrant was required."[45] In fact, neither *Chimel* nor *Robinson* quantifies or balances the amount of privacy that was lost. Both of them instead hold that the search incident to arrest is justified by necessity—to protect officer safety and prevent the destruction of evidence. Both *Chimel* and *Robinson* define the proper scope of a search incident to arrest—*Chimel* holds that police cannot search an entire house, while *Robinson* holds that police can search containers found on the suspect's person. But their rationale in defining the scope is based on an assumption of what area a suspect could reach, not the amount of intrusion involved in the search.[46] Thus, when the *Riley* Court imported this balancing test into the search incident to arrest context, it changed the search incident to arrest analysis by adding a factor that had not previously been considered: the level of intrusion into the suspect's privacy.

After the *Riley* Court created this balancing test, the remainder of its analysis was easy. Modern cell phones contain larger amounts of data and more intimate

---

[42] *Id.* at 2478 (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999)).

[43] *Id.* at 2478. *See also Houghton*, 526 U.S. at 298.

[44] *Riley*, 134 S. Ct. at 2488.

[45] *Id.*

[46] As another example, the *Riley* Court noted that at one point *Robinson* quoted then-Judge Cardozo from a 1923 case. *Id.* In the case, Judge Cardozo approved a search incident to arrest because "the law is in the act of subjecting the body of the accused to its physical dominion." *Id.* (quoting *United States v. Robinson*, 414 U.S. 218, 232 (1973)) *See also People v. Chiagles*, 142 N.E. 583, 584 (1923). *Riley* claims that *Robinson* used this quotation to discuss the reduced privacy rationale as part of a balancing test. However, *Riley* takes this quotation out of context, since both the *Robinson* Court and Judge Cardozo were merely noting that a search incident to arrest was one of the "necessities of government," since the police officer must be "empowered to disarm" when he or she is taking custody of the suspect. *Robinson*, 414 U.S. at 232. In fact, *Robinson* focused entirely on the government's interest in officer safety and in preventing destruction of evidence—it never conducted nor even mentioned a balancing test.

types of data than any other item the Court has considered, and they hold that data for substantial amount of time.[47] Thus, if *Chimel* did not allow the police to search a house incident to arrest, then the *Riley* Court could not possibly allow the police to search a cell phone: "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."[48] In short, the *Riley* Court subtly reframed the search incident to arrest analysis from an evaluation of the possibility of danger to the officers or destruction of evidence into a balancing test which also considers the amount of intrusion of privacy. This shift allowed the Court to focus on the massive intrusion of privacy involved in searching a cell phone and ignore the inconsistencies inherent in the *Chimel/Robinson/Gant* trilogy.

Of course, as part of the new balancing test, the Court did consider the risk of danger to the officers and destruction of evidence, and its analysis of those factors was as illogical as it had been in the past precedents. Although it is true that the digital data inside a cell phone produces no danger of being used as a weapon against the arresting officer, that is equally true of any items inside a cigarette package that the police have already seized—or, for that matter, items inside of *any* container once the suspect has been handcuffed and secured. And the danger of destruction of evidence is far greater for data inside a cell phone than it is for any non-digital item. Once a suspect is secured in custody, the chances of him being able to destroy any physical evidence that is within his wingspan or inside a container that was found on his body is insignificant. But cell phone data can easily be erased, either remotely by a confederate or automatically when a phone leaves a certain geographic area. If the Court were sincerely concerned about destruction of evidence in the fact pattern of *Robinson*, it is difficult to see how they could not have an even greater concern in *Riley*.

The Court offers three reasons why the risk of destruction of evidence is not a concern for cell phones. First, the Court notes that *Chimel* discussed the danger of the *suspect himself* destroying the evidence, whereas the risk in *Riley* is that a *third party* (or the device itself) would destroy the evidence.[49] Although this observation is correct, the Court does not explain why it matters. There is nothing in *Chimel*'s language or reasoning would lead one to believe that it makes any difference *how* the evidence is destroyed—after all, the evidence is equally unavailable regardless of the method that was used to destroy it. Second, the Court relies on the fact that there the government could not produce any data to show that remote wiping of phones after a suspect is in custody is "prevalent."[50] This foray into empiricism is, to say the least, unusual. The Court did not seem at all curious

---

[47] *Riley*, 134 S. Ct. at 2478–79.

[48] *Id.* at 2491.

[49] *Id.* at 2486–87.

[50] *Id.* at 2486.

in *Chimel* or *Robinson* about *how often* arrestees might destroy an item or use it as a weapon against the police.

Finally, the *Riley* Court notes that the police have certain countermeasures they can take against remote wiping, such as removing phone's battery[51] or "disabl[ing] a phone's automatic-lock feature in order to prevent the phone from locking and encrypting data."[52] Yet many smart phones do not have removable batteries, and given the variety and increasing sophistication of smart phones, it is unrealistic to assume that every arresting officer will know how to disable the auto-lock feature on every defendant's phone.[53]

B. *Riley as a Fourth Amendment Technology Case.*

In applying the Fourth Amendment to a new type of technology, the *Riley* case follows the same pattern as the *Jones* case did two years earlier. In the same way that the four-Justice *Jones* concurrence stated that recording massive amounts of location data violated the defendant's reasonable expectation of privacy, the *Riley* Court based its decision in part on the sheer quantity of data found inside of cell phones:

> [I]t is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate. Allowing the police to scrutinize such records on a routine basis is quite different from allowing them to search a personal item or two in the occasional case.[54]

In both *Jones* and *Riley,* the Court is getting close to adopting the "mosaic theory," which states that the government can learn so much from gathering and processing massive amounts of public data that, at some point, the gathering and processing of that data infringes on an individual's reasonable expectation of privacy and thus becomes a Fourth Amendment search. Although neither *Jones* nor *Riley* used the term "mosaic," the D.C. Circuit discussed the theory in *United*

---

[51] *Id.* at 2487.

[52] *Id.*

[53] The *Riley* Court's reliance on such counter-measures only confirms the Court's reputation for not understanding modern technological devices. The Court was roundly criticized for its inability to grasp basic technological concepts after the oral arguments in the recent case of City of Ontario v. Quon, 130 S. Ct. 2619 (2010). *See* Transcript of Oral Arguments, *Quon*, 130 S. Ct. 2619 (No. 08-1332), *available at* http://www.supremecourt.gov/oral_arguments/argument_transcripts/08-1332.pdf. During the oral arguments, Chief Justice Roberts asked if a person who was texting would get a "busy signal" if the recipient were simultaneously texting someone else. *Id.* at 44. Justice Scalia was concerned that texts could be shared with third parties because the recipient could "print them out" and circulate the printed materials. *Id.* at 49.

[54] *Riley*, 134 S. Ct. at 2490 (internal citations omitted).

States v. Maynard, which is what the *Jones* case was called in the lower courts.[55] As the D.C. Circuit held: "Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble."[56] The *Riley* Court echoed this argument: "The average smart phone user has installed 33 apps, which together can form a revealing montage of the user's life."[57]

And just as the *Jones* concurrence failed to propose a general rule regarding when the mosaic theory should apply, the *Riley* Court also sets out a very narrow holding that applies only to searches of data on cell phones.[58] The Court made no comment about digital evidence generally, or any other type of device that might contain digital evidence. Lower courts must now try to apply this narrow holding to a broad array of searches involving digital evidence, such as photos on a digital camera, files on a laptop computer, or even playlists on an iPod. Does the answer depend on the type of information which is being searched, or the storage capacity of the device, or some other factor? And how will the *Riley* holding affect other areas of Fourth Amendment jurisprudence, such as the plain view doctrine, the special needs doctrine, or the proper scope of a consent search? The Court provided no guidance on these issues.

This lack of guidance is especially problematic given the basic nature of the mosaic theory that the *Riley* holding and the *Jones* concurrence rely upon. Essentially, the mosaic doctrine states that a search which would be legal under most conditions can become an illegal search because of the sheer amount and breadth of the data that is recovered. But the Court has failed to clarify the *point* at which a legal search becomes illegal.[59] The majority decision in *Jones* was skeptical of the mosaic doctrine for this very reason, stating that "it remains unexplained why a 4-week investigation is 'surely' too long."[60] Somewhere between tracking a car for one trip and tracking a car for every trip during a 28-day period, police conduct becomes unconstitutional. And somewhere between collecting a few outgoing telephone numbers and searching the entire phone log and contact list, the search incident to arrest becomes illegal.

Given the amount of metadata that is available to law enforcement officers today, the mosaic theory could conceivably apply to many different types of searches. What about a years' worth of credit-card charges? A month's worth of browsing history? A week's worth of terms entered into a search engine? *Riley* provides almost no help in answering these questions.

---

[55] 615 F.3d 544 (D.C. Cir. 2010).

[56] *Id.* at 562.

[57] *Riley*, 134 S. Ct. at 2490.

[58] *Id.* at 2485.

[59] *See, e.g.*, Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 346 (2012).

[60] United States v. Jones, 132 S. Ct. 945, 954 (2012).

But the most disappointing aspect of *Riley* was not that it failed to provide guidance for any existing type of digital "container" other than a cell phone, but that it failed to provide guidance for all the digital containers that have yet to be invented. *Katz* and *Kyllo* were both landmark cases because they looked beyond their narrow, specific fact pattern and fashioned a rule that could apply for decades. The *Riley* decision was cautious to a fault. If the *Katz* Court had been as cautious, it would have left the "physical trespass" standard in place and simply created a special rule against eavesdropping on telephone booths. A similarly cautious *Kyllo* Court would have merely issued a narrow holding prohibiting the use of thermal imagers on the outside of a home. These rules about phone booths and thermal imagers would have been of little help in guiding law enforcement or lower courts in deciding future cases, especially as phone booths gradually disappeared from the urban landscape and as other surveillance devices replaced thermal imagers. Similarly, a ruling on cell phones may seem very significant today, but it is likely to not be very significant in ten or twenty years, when we store and send our information using devices quite different from anything we can currently imagine. In short, *Riley* missed an opportunity to set out a broad rule. Just as it failed to fix the broken doctrine of the search incident to arrest doctrine, it also failed to bring clarity to the application of the Fourth Amendment to searches of new kinds of technology.

If the *Riley* Court had been bolder, it had a number of options. It could have embraced the mosaic theory, and in so doing explained when an otherwise legal search (such as the one in *Knotts* or *Robinson*) turns into an illegal search (such as the one in *Jones* or *Riley*). The Court could have established an "intimate information" test, or a "high-data-volume" test, or held that police are only allowed to conduct warrantless surveillance if they obtain results that are no more intrusive than what they would have found with a traditional, pre-digital search.[61]

Conversely, the Court could have endorsed a switch from a "rules" based approach to a "standards" based approach. Such an approach would allow the police to conduct a search when it is "reasonable" under the circumstances. Searches incident to arrest would no longer be subject to bright-line (and occasionally arbitrary) tests, such as whether the evidence being gathered was digital or whether it had been found within the wingspan of the suspect. Instead, a reviewing court would balance the invasiveness of the search with the severity of the crime and the level of suspicion of the searching officer. Some lower courts have already been moving in this direction. For example, in *United States v. Flores-Lopez*,[62] the Seventh Circuit applied a version of a standards based approach. *Florez-Lopez* holds that police should have the automatic right to search a cell phone if the information they retrieve is "no more invasive than, say, a frisk

---

[61] *See* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476 (2011).

[62] 670 F.3d 803 (7th Cir. 2012).

or the search of a conventional container,"[63] but if the search of a cell phone is so intrusive that is the equivalent of a "strip search," then "the risk of the officers' safety or to the preservation of evidence of crime must be greater to justify the search."[64] Thus, under the Seventh Circuit standard, the police might have an automatic right to check the cell phone's contact list, but would not an automatic right to look through photos and read old text messages.

CONCLUSION

The Court has been too cautious for too long in these critical areas of the law. The search incident to arrest doctrine has suffered from a fundamental conflict between its rationale and its scope ever since *Chimel* was decided in 1969, and the recent decision in *Gant* has only exacerbated the inconsistency. Meanwhile, people have been storing massive amounts of data in relatively small digital devices since the personal computer first became widely available in the late 1970s, but for thirty-five years, most courts have been treating computers and other digital storage devices as "containers" that are no different from backpacks or footlockers.[65]

In the 2010 case of *City of Ontario v. Quon*,[66] the Supreme Court decided a case involving the privacy interest in information transmitted by pagers—hardly a cutting-edge technology at the time. The case would have been a perfect opportunity for the Court to address the third-party doctrine of *Smith v. Maryland* and either revise or simply discard the doctrine as outdated. Instead, the Court ducked the issue and decided the case on narrower grounds. As the majority explained:

> Prudence counsels caution before the facts in this case are used to establish far-reaching premises that define the existence, and extent, of privacy expectations of employees using employer-provided communication devices.
>
> Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior.[67]

The Court appears to have followed this advice in *Riley* as well, using the "rapid changes in the dynamics of communication and information transmission" as a reason to avoid taking major steps forward. But major steps could bring

---

[63] *Id.* at 809.

[64] *Id.*

[65] *See, e.g.*, United States v. Andrus, 483 F.3d 711, 718 (10th Cir. 2007).

[66] 560 U.S. 746 (2010).

[67] *Id.* at 759.

clarity and are sometimes necessary to update vestigial legal principles. The law would have been better served had the *Riley* Court followed the recommendation of Justice Scalia in his concurrence in *Quon*:

> Applying the Fourth Amendment to new technologies may sometimes be difficult, but when it is necessary to decide a case we have no choice. The Court's implication that where electronic privacy is concerned we should decide less than we otherwise would (that is, less than the principle of law necessary to resolve the case and guide private action)—or that we should hedge our bets by concocting case-specific standards or issuing opaque opinions—is in my view indefensible. The-times-they-are-a-changin' is a feeble excuse for disregard of duty.[68]

Unfortunately neither Justice Scalia nor the rest of the Court followed this advice in *Riley*, and therefore lower courts and law enforcement will have to live with the resulting ambiguity, at least until the next case comes along.

---

[68] *Id.* at 768 (Scalia, J., concurring).