
Adam Lamparello, Indiana Tech Law School
RILEY v. CALIFORNIA: WHAT IT MEANS FOR METADATA, BORDER SEARCHES, AND THE FUTURE OF PRIVACY

BY ADAM LAMPARELLO

“Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is … simple—get a warrant.”

INTRODUCTION

Privacy still matters. The question is how much, and in what context, it matters.

In Riley v. California, Chief Justice Roberts wrote for a unanimous Court, holding that law enforcement officers could seize but not search an arrestee’s cell phone incident to arrest without a warrant or absent exigent circumstances. The Court rejected the Government’s argument that concerns for officers’ safety and the preservation of evidence—the initial, pre-digital era justifications for searches incident to arrest—supported warrantless searches of an arrestee’s cell phone. Chief Justice Roberts’ majority opinion flatly rejected the Court’s rationale in United States v. Robinson and Arizona v. Gant, which had expanded to an unprecedented degree law enforcement’s power to conduct warrantless searches. And for good reason. As the Court recognized, cell phones are used by millions of individuals to store the “papers … and effects” that have historically been protected from warrantless—and suspicionless—intrusion by the Government.

1 Assistant Professor of Law, Indiana Tech Law School.


3 Id.


7 See infra Part II.

8 See U.S. const., amend. IV (“The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized”).
In short, times have changed. Private information is no longer stored only in homes or other areas traditionally protected from warrantless intrusion. The private lives of many citizens are contained in a digital device no larger than the palm of their hand—and carried in public places. But that does not make the data within a cell phone any less private, just as the dialing of a phone number does not voluntarily waive an individual’s right to keep their call log or location private. Remember that we are not talking about individuals suspected of committing violent crimes. The Government is recording the calls and locations of citizens who have done nothing wrong, who are driving to work while talking to their spouses, or who are using their cell phones to call a loved one in the hospital. And the Government has the power to know where you are—and record the numbers you are calling. Unless it has a good reason for doing so—often referred to as probable cause or reasonable suspicion—this practice should have no place in a society that values civil liberties.

Do the Government’s surveillance practices make us safer? Maybe. Should that matter? No. Assurances that we are ‘safer’ come at too high a price if the cost is to our personal freedom. That may make us safer, but it also makes every citizen less secure—and a little hesitant before dialing a number or downloading a YouTube video. If the Court were permit these and other warrantless intrusions into a person’s private life, the Fourth Amendment’s place on the constitutional hierarchy might be just a notch above the Third Amendment’s prohibition against the quartering of soldiers, or slightly below the often-discussed by never-sued Privileges and Immunities Clause. Simply put, Riley came at the right time, and hopefully is the beginning of enhanced protections for privacy rights.
What we know after Riley is that law enforcement’s power to rummage through an individual’s private life is not unlimited. The Court’s analysis also suggests that it will balance an individual’s privacy interests against the Government’s interest in crime prevention. What we do not know, however, is whether the Fourth Amendment protects from warrantless searches \textit{all} of the data stored in a cell phone, or whether it is limited to information traditionally considered private, such as private emails and confidential documents. We also do not know whether the Fourth Amendment applies to \textit{non-physical} intrusions of a cell phone, such as in the collection of metadata. Finally, we do not know the context within which the Government’s interest in crime-prevention may outweigh or diminish an individual’s expectation of privacy and thereby permit searches that, as in the search incident to arrest context, would otherwise be prohibited.

Thus, although Riley is a victory for individual privacy rights and a signal to law enforcement that its investigative powers are not without limits, the critical question is: how much does privacy matter? This article argues that if the guiding principle in Riley—the reasonableness of the search—governs the Court’s analysis in upcoming cases, then other warrantless intrusions on individual privacy, such as the collection of cell phone metadata or forensic searches of laptops at the border, may end or be limited. And they should. Cell phones and other digital data contain the “privacies of life,”\textsuperscript{9} and a search of their contents would “typically expose to the government far \textit{more} than the most exhaustive search of a house.”\textsuperscript{10}

Ultimately, the Government’s indiscriminate, widespread, and suspicionless collection of information, even if it only involves call records and identifies a user’s location cannot be reconciled with the “right of the people to be secure in their … papers and effects.”\textsuperscript{11} Simply put,

\footnotesize
\textsuperscript{9} 2014 WL 2864483 at *20.  
\textsuperscript{10} \textit{Id.} at *16 (emphasis in original).  
\textsuperscript{11} U.S. Const., amend. IV, \textit{supra} note 8.
with respect to the search of cell phone metadata, laptops, and other digital devices, the answer to what the Government must do before searching these items should also be simple: “get a warrant.”

II.

CHIEF JUSTICE ROBERTS’ MAJORITY OPINION—DISTINGUISHING THE PHYSICAL AND VIRTUAL WORLD

Chief Justice Roberts’ majority opinion recognized that the “touchstone of the Fourth Amendment is ‘reasonableness,’” and focused on “whether application of the search incident to arrest doctrine to this particular category of effects would ‘untether the rule from the justifications underlying the Chimel exception.’”

Answering this question in the affirmative—and holding that warrantless cell phone searches incident to arrest are per se unreasonable—the Court explained that neither the Chimel justifications nor the expansive view of law enforcement authority embraced in Robinson and Gant could justify the warrantless search of information that the Founders—and Court—had historically considered private.

---

12 2014 WL 2864483 at *20.
13 Id. at *6.
14 Id. at *9 (quoting Gant, 556 U.S. at 343).
15 Id. Chief Justice Roberts stated as follows:

Robinson regarded any privacy interests retained by an individual after arrest as significantly diminished by the fact of the arrest itself. Cell phones, however, place vast quantities of personal information literally in the hands of individuals. A search of the information on a cell phone bears little resemblance to the type of brief physical search considered in Robinson.
A. THE SEARCH INCIDENT TO ARREST DOCTRINE DOES NOT AUTHORIZE WARRANTLESS CELL PHONE SEARCHES

1. CELL PHONES ARE NOT WEAPONS

The Court’s decision in Chimel recognized that the threats posed to officer safety during an arrest permit a limited search of the arrestee’s person and areas within which the arrestee may reach for a weapon.16 Cell phone data, however, “cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee's escape.”17 Also, a cell phone cannot be used as a weapon because police are authorized to seize the phone upon arrest.18 As Justice Roberts explained, whatever threat that may conceivably exist is eliminated by the seizure:

Digital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee's escape. Law enforcement officers remain free to examine the physical aspects of a phone to ensure that it will not be used as a weapon—say, to determine whether there is a razor blade hidden between the phone and its case. Once an officer has secured a phone and eliminated any potential physical threats, however, data on the phone can endanger no one.19

Thus, although “unknown physical objects may always pose risks … during the tense atmosphere of a custodial arrest … [n]o such unknowns exist with respect to digital data.”20

2. THE PRESERVATION OF EVIDENCE IS NOT IMPLICATED

The Government also argued that warrantless searches were justified to prevent the destruction of potentially incriminating evidence, either through remote wiping or data encryption.21 Remote wiping occurs “when a third party sends a remote signal or when a phone

---

16 Chimel, 395 U.S. at 762-63.
17 2014 WL 2864483 at *14.
18 Id. at *10.
19 Id.
20 Id.
21 Id. at *11.
is preprogrammed to delete data upon entering or leaving certain geographic areas."22 Encryption allows individuals to protect cell phone data in a manner that “renders a phone all but “unbreakable” unless police know the password.”23

The Court found that neither of these possibilities presented a serious risk that the contents of a cell phone would be destroyed.24 Indeed, “remote wiping can be fully prevented by disconnecting a phone from the network.”25 With respect to data encryption, “[l]aw enforcement officers are very unlikely to come upon such a phone in an unlocked state because most phones lock at the touch of a button or, as a default, after some very short period of inactivity.”26

B. FOCUSING ON PRIVACY, NOT TRESPASS

Perhaps more importantly, the Court held that individuals have a reasonable expectation of privacy data stored in cell phones because the information is fundamentally different than that which is typically stored in physical objects. In so holding, the Court refused to apply Robinson, which held that the “custodial arrest of a suspect based on probable cause [was] a reasonable intrusion under the Fourth Amendment …[such that] a search incident to the arrest requires no additional justification.”27 Likewise, the Court rejected its rationale in Gant, which sanctioned “an independent exception for a warrantless search of a vehicle's passenger compartment “when it is ‘reasonable to believe evidence relevant to the crime of arrest might be found in the vehicle.””28 As Justice Roberts wrote in the majority opinion, the Gant standard would “prove no practical limit at all when it comes to cell phone searches”29

22 Id.
23 Id.
24 Id.
25 Id.
26 Id.
27 Robinson, 414 U.S. at 235 (emphasis added).
28 Gant, 556 U.S. 332 at 350.
29 2014 WL 2864483 at *17.
1. **Cell Phones Cannot Be Analogized to Cigarette Packs or Containers**

   a. **Storage Capacity**

   To begin with, “[o]ne of the most notable distinguishing features of modern cell phones is their immense storage capacity,” which is not “limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy.”  

   Indeed, not only do cell phones have the capability “to store to millions of pages of text, thousands of pictures, or hundreds of videos.” Justice Roberts explained as follows:

   The current top-selling smart phone has a standard capacity of 16 gigabytes (and is available with up to 64 gigabytes). Sixteen gigabytes translates to millions of pages of text, thousands of pictures, or hundreds of videos … Cell phones couple that capacity with the ability to store many different types of information: Even the most basic phones that sell for less than $20 might hold photographs, picture messages, text messages, Internet browsing history, a calendar, a thousand-entry phone book, and so on … We expect that the gulf between physical practicability and digital capacity will only continue to widen in the future.

   Simply stated, “cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person.”

   b. **Cell Phones Contain Private Information**

   The Court also recognized that storage capacity for cell phones has “several interrelated consequences for privacy,” because a cell phone “collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record.” Justice Roberts noted that “Internet search and

---

30 Id.
31 Id. at *14.
32 Id.
33 Id.
34 Id.
35 Id.
browsing history, for example, can be found on an Internet-enabled phone and could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD.”

In other words, “the sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet.”

As a result, a “cell phone search would typically expose to the government far more than the most exhaustive search of a house, and contains a broad array of private information never found in a home in any form—unless the phone is.” Furthermore, the fact that, “[p]rior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day,” did not “make the information any less worthy of the protection for which the Founders fought.” As Justice Roberts noted in the majority opinion, today it is “the person who is not carrying a cell phone, with all that it contains, who is the exception.” Indeed, to say that carrying a cell phone in a public place somehow makes the information it contains less private, or to equate it with someone standing naked in front of a large window in their home who then complains of an invasion of privacy when stunned onlookers peer into the window.

Ultimately, therefore, while recognizing that its decision would “have an impact on the ability of law enforcement to combat crime” but noted that “privacy comes at a cost,”

36 Id.
37 Id.
38 Id.
39 Id. at *15.
40 Id. at *20.
41 Id. Furthermore, even though an arrestee has a reduced expectation of privacy upon arrest, “diminished privacy interests [do] not mean that the Fourth Amendment falls out of the picture or mean that every search ’is acceptable solely because a person is in custody.’” Id. at *13 (quoting Maryland v. King, 569 U.S. ——, ——, 133 S.Ct. 1958, 1979) (2013)).
42 2014 WL 2864483 *19.
43 Id.
particular where “the possible intrusion on privacy is not physically limited in the same way when it comes to cell phones.”

Indeed, warrantless searches of an arrestee’s cell phone would resemble “the reviled “general warrants” and “writs of assistance” of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity.”

III.

WHAT RILEY MEANS FOR THE FUTURE

*Riley* is significant in several respects. The Court recognized that pre-digital case law neither confronted nor contemplated the issues raised by rapid technological advances. Additionally, an individual’s expectation of privacy does not change simply because that individual is in a public place. And unlike the *ad hoc*, case-by-case approach characteristic of its earlier Fourth Amendment jurisprudence, which threatened to stretch the doctrine “beyond its breaking point,” the *Riley* Court established a categorical bright-line rule that provided guidance to law enforcement and safeguarded basic privacy rights. Moreover, by basing its analysis on the Fourth Amendment’s reasonableness standard, the Court’s opinion indicates that future cases involving digital privacy rights will involve balancing an individual’s privacy interest against law enforcement’s interest in crime prevention.

---

44 *Id.* at *14.
45 *Id.* at *20.
46 *Id.* at *9-10.
47 *Id.* at *20.
49 2014 WL 2864483 at *20.
50 *Id.* at *6.
51 *Id.* at *9 (holding that “we generally determine whether to exempt a given type of search from the warrant requirement ‘by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interest’”) (*quoting Wyoming v. Houghton*, 526 U.S. 295, 300 (1999)).
After all, technology cuts both ways. It gives individuals the ability to store a virtual treasure trove of information, much of it traditionally considered private under the Fourth Amendment, in an object no larger than the size of their hands, but has also become “[an] important tool[] in facilitating coordination and communication among members of criminal enterprises.”

Additionally, the information on cell phones can “provide valuable incriminating information about dangerous criminals,” and modern technology, more generally, can be an important investigatory tool for the Government, both domestically and internationally.

Thus, what remains unknown is how weighty an individual’s privacy interest in cell phone data will be outside of the arrest context, where the intrusion is less significant or where the Government’s interest is more substantial. The Court did not, for example, indicate whether the privacy interest may vary depending on the specific type of information being searched, such as an individual’s contact list or call log as opposed to confidential bank statements.

In addition, Justice Roberts’ opinion did not suggest whether non-physical and arguably less invasive intrusions, such as in the remote collection of metadata, will trump privacy protections, or whether that interest will be diminished where the Government’s interest in crime prevention is heightened, such as in the searches of laptops at the border.

Thus, it remains uncertain whether the generalized privacy interest in cell phone data will be limited to physical intrusions, whether a diminished expectation will apply when the Government remotely tracks information or has a legitimate interest in the information sought, and whether factors such as the

---

52 2014 WL 2864483 at *19 (brackets added).
duration of the Government’s monitoring may turn an otherwise permissible search into a Fourth Amendment violation.  

Furthermore, it is unclear how Riley’s focus on privacy can (or must) be reconciled with the trespass theory that the Court relied on in United States v. Jones, where it held that using a GPS tracking device to remotely monitor a suspect’s vehicle’s movement for nearly a month constituted a search under the Fourth Amendment. In a 5-4 decision, the majority based its decision on the fact that the actual physical installation of the device on the car constituted a trespass, and did not expressly consider, under Katz v. United States, whether the intrusion violated the occupant’s reasonable expectation of privacy. In Riley, however, privacy, not trespass, controlled.

Nonetheless, there are important parallels between Riley and cases that the Court soon may decide, particularly involving the collection of cell phone (and internet) metadata, and searches of laptop computers at the border, both of which have split the circuit court. Indeed, if

---

54 The questions left unresolved by Justice Roberts’ majority opinion, and the relatively narrow ruling that an arrestee’s diminished expectation of privacy while in custody does not extinguish the arrestee’s privacy rights in information historically that protected by the Fourth Amendment, should not be surprising. Narrow rulings are a hallmark of Justice Roberts, who strives for “unanimous or near-unanimous decisions, on the ground that they promote the rule of law … lead to narrow, minimalist opinions.” Indeed, Justice Roberts has stated that “[i]f it is not necessary to decide more to dispose of a case, in my view it is necessary not to decide more.” This view lies at the heart Roberts’ jurisprudence, which reflect a concern with the Court’s institutional legitimacy and avoiding the perception that the Court’s decision are influence by political or ideological considerations. The approach results in carefully-crafted, narrow decisions that lead to incremental changes in the law and leave much to the democratic process. See University of Chicago Law School Faculty blog, Chief Justice Roberts and Minimalism, (May 25, 2006), available at: http://uchicagolaw.typepad.com/faculty/2006/05/chief_justice_r.html.
55 132 S.Ct. 945 (2012)
56 Id.
57 89 U.S. 347 (1967); see also United States v. Miller, 425 U.S. 435 (1976) (holding that the defendant had no expectation of privacy in bank records, including original checks and deposit slips, because they were voluntarily conveyed to law enforcement and the bank’s business records).
58 Jones, 132 S.Ct. at 949-950. In their concurring opinions, however, Justices Alito and Sotomayor suggested that the prolonged monitoring of the vehicle violated the suspect’s reasonable expectation of privacy. Id. at 956-57, 962-64 (Sotomayor, J., concurring) (Alito, J., concurring).
reasonableness continues to guide its analysis, law enforcement’s sweeping surveillance powers may soon come to an end.

A. THE COLLECTION OF CELL PHONE METADATA

In *Smith v. Maryland*, the Court held that law enforcement’s installation of a pen register to record a suspect’s outgoing calls did not constitute a search under the Fourth Amendment. The Court determined that the suspect did not have a “legitimate expectation of privacy regarding the numbers he dialed on his phone,” which the suspect voluntarily “convey[ed] to the telephone company, since it is through telephone company switching equipment that their calls are completed.” The Court stated as follows:

> Petitioner can claim no legitimate expectation of privacy here. When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and “exposed” that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed. The switching equipment that processed those numbers is merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber.

The Court’s decision was predicated on the third-party doctrine, which allows the Government to conduct warrantless searches of otherwise-private information where an individual has voluntarily disclosed that information to a third party.

In the context of metadata collection, which record’s the user’s calls and location, the Government has relied on *Smith* and analogized metadata to pen registers. Recent case law, however, has rejected the analogy much the same way that the *Riley* Court refused to equate cell phones with physical objects. In *Klayman v. Obama*, for example, the court held that, unlike the

---

60 Id. at 745-46.
61 Id.
62 Id. at 742.
63 Id. at 744.
64 Id. at 744, 746.
pen register in *Smith*, which was “operational for only a matter of days,” metadata collection “involves the creation and maintenance of a historical database for five years’ worth of data.” Furthermore, whereas pen registers “record the numbers dialed from the [suspect’s] telephone,” the Government’s collection of metadata occurs “on a daily basis … [retrieves] electronic copies of call detail records … and can reveal the user’s location.” Thus, although it is reasonable for “phone companies to occasionally provide information to law enforcement,” it is an entirely different matter for citizens to “expect all phone companies to operate … a joint intelligence gathering operation.” Just like cell phones are not crumpled up cigarette packs, metadata collection is not a pen register.

In *United States v. Davis*, the Eleventh Circuit reached the same result and unlike the Fifth Circuit, held that individuals have a reasonable expectation of privacy in data that identifies their whereabouts. The Eleventh Circuit Court reasoned that such information is similar to communicative data because “it is private in nature,” and that its collection would impermissibly “convert what would otherwise be a private event into a public one.” The Court also distinguished *Jones*, which “involved the movements of the defendant’s automobile on the public streets and highways,” and held that *Jones*’ reliance on a trespass theory did not suggest that the *Katz* was no longer applicable.

---

65 2013 WL 6571596, at *19.
66 Id.
67 Id. [brackets added].
68 Id.
69 Id.
70 See *Davis*, supra note 53, available at: https://www.aclu.org/sites/default/files/assets/q_davis_opinion.pdf.
71 See *In re Application of the United States for Historic Cell Site Data*, 724 F.3d 600 (5th Cir. 2013).
73 Id. at 20.
74 Id.
75 Id. at 19.
76 Id. at 18.
The court’s decision creates a circuit split and may ultimately be decided by the Supreme Court. After Riley, the Court may very well hold that the Government’s metadata collection practices violate the Fourth Amendment. Unlike Jones, the Riley Court’s reasoning rested on privacy, and did not differentiate among the types of data, e.g., call lists and confidential documents that, if considered separately, might not engender the same privacy protections. Furthermore, although the collection of metadata is a non-physical intrusion and arguably less invasive, it records a user’s call history and location without a warrant or, in some cases, even the slightest hint of suspicion. Additionally, metadata collection is not limited in duration, which was the principle factor upon which the Jones Court deemed the Government’s use of a GPA tracking device a search. Thus, under Riley’s reasonableness standard, the Government’s indiscriminate and prolonged collection of metadata appears unreasonable.

B. Laptop Searches at the Border—and in the Home

Riley may also affect the Government’s ability to conduct warrantless searches of a laptop at the border, particularly where border agents conduct forensic searches and therefore examine the laptop’s contents. Of course, border searches of a vehicle’s physical contents have traditionally been justified on grounds relatively similar to the search incident to arrest doctrine—officer safety and the discovery of contraband.

As the Riley Court recognized, however, digital devices contain a vast amount of private information that alters the fundamental nature of the search. Furthermore, and as in Riley, the justifications for warrantless searches of physical containers at the border do not necessarily support warrantless searches of laptops. Like cell phones, laptops are not weapons, and they store a vast array of private information.
Indeed, the Ninth Circuit recently considered this issue and held that border agents must have reasonable suspicion before conducting forensic searches of laptops.\textsuperscript{77} The Eastern District of New York reached the opposite result, holding that such searches are permissible because the “Government’s interest in preventing the entry of unwanted persons and effects is at its zenith at the international border.”\textsuperscript{78} The court did acknowledge, however, that if warrantless forensic searches, which occur rarely, were more routine, reasonable suspicion would be required.\textsuperscript{79}

Ultimately, the Court’s reasoning in Riley supports requiring reasonable suspicion before border agents perform forensic searches at the border. Unlike the probable cause standard, reasonable suspicion only requires law enforcement to have specific and articulable facts “which, taken together with rational inferences from those facts, reasonably warrant that intrusion.”\textsuperscript{80} Thus, it would provide law enforcement with sufficient flexibility while not subjecting motorists to suspicionless searches of intimately personal information. On the other hand, considering the Government’s heightened interests at the border, the Court would likely permit superficial searches of a motorist’s laptop provided that: (1) there is a reason to believe that officer safety is implicated; or (2) the search may reasonably uncover contraband or other evidence of criminal conduct.

\textsuperscript{77} See United States v. Cotterman, 709 F.3d 952 (9th Cir. 2013) (en banc) (emphasis added), cert. denied, ___ S. Ct. ___, No. 13-186, 2-14 WL 102985 (Jan. 13, 2014).
\textsuperscript{78} Abidor v. Napolitano, --F. Supp.2d --, 2013 WL 6912654 (E.D.N.Y. December 31, 2013) (the court dismissed the complaint on standing grounds but nonetheless discussed the border search issue).
\textsuperscript{79} 2013 WL 6912654 at *14
\textsuperscript{80} Terry v. Ohio, 392 U.S. 1, 21 (1967).
CONCLUSION

*Riley* is a landmark decision because of the reasoning, not merely the result. Justice Roberts’ majority opinion focused on reasonableness and recognized that digital devices implicate fundamental privacy concerns. Indeed, *Riley* suggests that the Court will take a more active role in ensuring that the Government’s investigative and surveillance practices do not lead to the modern-day version of the general warrant.

Quite frankly, it is about time. The National Security Agency’s surveillance program has resulted in alarming encroaches by the government into the private lives of its citizens and made any threshold standard of suspicion seem like an inconvenience, not a requirement. Hopefully, *Riley* is the first step toward restoring the proper—and reasonable—constitutional balance.