RILEY V. CALIFORNIA: PRIVACY STILL MATTERS, BUT HOW MUCH AND IN WHAT CONTEXTS?

Adam Lamparello and Charles E. MacLean[*]

"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."[1]

INTRODUCTION

Privacy still matters. The question is how much, and in what contexts, 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.[2] 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[3]—supported warrantless searches of arrestees' cell phones.[4] Chief Justice Roberts's majority opinion flatly rejected the Court's rationale in *United States v. Robinson*,[5] which had expanded law enforcement's power to conduct warrantless searches to an unprecedented degree.[6] The *Riley* Court also declined to extend the search incident to arrest standard found in *Arizona v. Gant*[7]—and for good reason. As the Court recognized, cell phones are used by millions of individuals to store the "papers[ ] and

---

[*] Assistant Professors of Law, Indiana Tech Law School.

[1] Riley v. California, 134 S. Ct. 2473, 2495 (2014).

[2] *Id.* at 2493–94.

[3] Chimel v. California, 395 U.S. 752, 762–63 (1969) (holding in 1969 that two justifications—officer safety and the preservation of evidence—framed the limits of the search incident to arrest doctrine).

[4] *See Riley*, 134 S. Ct. at 2484–86 (citing *Chimel*, 395 U.S. at 762–63).

[5] *Id.* at 2484–85 (citing United States v. Robinson, 414 U.S. 218, 235 (1973)).

[6] *See* Derik A. Scheurer, *Are Courts Phoning It In? Resolving Problematic Reasoning in the Debate over Warrantless Searches of Cell Phones Incident to Arrest*, 9 WASH. J.L. TECH. & ARTS 287, 294–95 (2014) ("*Robinson* significantly departed from Supreme Court precedent on the search-incident-to-arrest exception" because it "effectively severed the search-incident-to-arrest exception from a fact-based analysis." Although "[p]rior cases required either an evidentiary link that tied the object of the search to the basis for the arrest or an evident threat to police safety[,] . . . the *Robinson* Court removed such factual considerations from the equation.").

[7] *Riley*, 134 S. Ct. at 2492 (citing Arizona v. Gant, 556 U.S. 332, 343 (2009).

effects"[8] that have historically been protected from warrantless—and suspicionless—intrusion by the Government.[9]

In short, times have changed. Private information is no longer stored only in homes or other areas traditionally protected from warrantless intrusion.[10] The private lives of many citizens are contained in digital devices no larger than the palms of their hands—and carried in public places.[11] But that does not make the data within a cell phone any less private, just as the dialing of a phone number does not automatically waive an individual's right to keep her call log or location private.[12] One should keep in mind these are not individuals suspected of committing violent crimes. The Government is monitoring 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.[13] The Government also has the power to know where

---

[8] 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.").

[9] *See Riley*, 134 S. Ct. at 2484 (noting that "[a] smart phone of the sort taken from Riley was unheard of ten years ago[,]" but that "a significant majority of American adults now own such phones"); *id.* at 2488–89 (rejecting the Government's argument that items subject to search under *Robinson* and *Chimel*—a billfold, address book, wallet, and purse—are analogous to modern cell phones and stating that "[a] conclusion that inspecting the contents of an arrestee's pockets works no substantial additional intrusion on privacy beyond the arrest itself may make sense as applied to physical items, but any extension of that reasoning to digital data has to rest on its own bottom.").

[10] *Id.* at 2490–91.

[11] *See id.* at 2489–90 (noting that "[t]he term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone" and stating that while "[m]ost people cannot lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read[,]" modern cell phones allow individuals to carry around such information in "a container the size of the cigarette package in *Robinson*").

[12] *See id.* at 2492–93 ("We also reject the United States' final suggestion that officers should always be able to search a phone's call log, as they did in Wurie's case. The Government relies on *Smith v. Maryland*, which held that no warrant was required to use a pen register at telephone company premises to identify numbers dialed by a particular caller. The Court in that case, however, concluded that the use of a pen register was not a 'search' at all under the Fourth Amendment. There is no dispute here that the officers engaged in a search of Wurie's cell phone. Moreover, call logs typically contain more than just phone numbers; they include any identifying information that an individual might add, such as the label 'my house' in Wurie's case." (citations omitted)).

[13] *See* Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 HARV. J.L. & PUB. POL'Y 757, 871 (2014) (noting that Government officials have acknowledged that the National Security Agency ("NSA") monitors phone calls made through Verizon, AT&T, and Sprint, which "means that every time the average U.S. citizen

you are and even record the numbers you are calling.[14] Unless the Government has a good reason for using it—often referred to as probable cause or reasonable suspicion[15]—this practice should have no place in a society that values civil liberties.

Do the Government's surveillance practices make us safer? Maybe.[16] Should that matter? No. Assurances that we are "safer" come at too high a price if the cost is our personal freedom. Surveillance 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.[17] If the Court were to permit these and other warrantless intrusions into a person's private life, the Fourth Amendment's place in the constitutional hierarchy might be just a notch above the Third Amendment's prohibition against the quartering of soldiers,[18] or slightly below the often-discussed but never-

---

makes a telephone call, the NSA is collecting the location, the number called, the time of the call, and the length of the conversation").

[14] *See* Joseph D. Mornin, Note, *NSA Metadata Collection and the Fourth Amendment*, 29 BERKELEY TECH. L.J. 985, 985–86, 985 n.4 (2014) ("Metadata includes information about a phone call—who, where, when, and how long—but not the content of the conversation."); John Yoo, *The Legality of the National Security Agency's Bulk Data Surveillance Programs*, 37 HARV. J.L. & PUB. POL'Y 901, 911–12 (2014) (noting the Foreign Intelligence Surveillance Court held the Government's collection of metadata for "billions of innocent calling records" is justified "'[b]ecause known and unknown international terrorist operatives are using telephone communications, and because it is necessary to obtain the bulk collection of a telephone company's metadata to determine those connections between known and unknown international terrorist operatives as part of authorized investigations'" (quoting *In re* FBI for an Order Requiring the Production of Tangible Things from [Redacted], No. BR 13-109, at 18 (FISA Ct. Aug. 29, 2013), *available at* http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf).

[15] *See* Christopher Slobogin, *Cause to Believe What? The Importance of Defining a Search's Object—Or, How the ABA Would Analyze the NSA Metadata Surveillance Program*, 66 OKLA. L. REV. 725, 729–30 (2014).

[16] *Compare* John McLaughlin, Editorial, *Misplaced Fear of the NSA*, WASH. POST, Jan. 3, 2014, at A13 (contending that congressional oversight of the NSA makes private information safer in the hands of the Government than private companies), *with* Editorial, *Bad Times for Big Brother*, N.Y. TIMES, Dec. 22, 2013, at SR10 (contending that citizens need both physical security from terrorist attacks and mental security from the fear of being watched by the Government).

[17] *See, e.g.*, PEW RESEARCH CTR., PRIVACY AND DATA MANAGEMENT ON MOBILE DEVICES 6 (2012), http://pewinternet.org/Reports/2012/Mobile-Privacy.aspx (finding that 57% of cell phone app users have uninstalled an app or refused to install an app due to overriding privacy concerns).

[18] *See* Thomas L. Avery, *The Third Amendment: The Critical Protections of a Forgotten Amendment*, 53 WASHBURN L.J. 179, 179 (2014) ("The U.S. Supreme Court has never had occasion to apply or interpret the Third Amendment, and only once has a federal court directly addressed a Third Amendment claim on the merits. Indeed, the Third Amendment is the least litigated Amendment in the Bill of Rights." (footnote ommitted)).

used Privileges and Immunities Clause.[19] Simply put, *Riley* came at the right time, and hopefully it 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.[20] The Court's analysis also suggests that it will balance an individual's privacy interests against the Government's interest in crime prevention.[21] The Court, however, did not address whether the Fourth Amendment applies to *remote* intrusions of a cell phone, such as the collection of metadata.[22] 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, thereby permitting otherwise prohibited searches such as those performed incident to arrest.

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[23]—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—as they should. Cell phones and other digital data contain "'the privacies of life,'"[24] and a search of their contents would "typically

---

[19] *See* Bryan H. Wildenthal, *The Lost Compromise: Reassessing the Early Understanding in Court and Congress on Incorporation of the Bill of Rights in the Fourteenth Amendment*, 61 OHIO ST. L.J. 1051, 1116 (2000) ("Right up to the present day, only one extant (and very recent) Supreme Court decision has ever upheld a claim under the [Privileges and Immunities] Clause . . . ."); *see also, e.g.*, Thomas H. Burrell, *Privileges and Immunities and the Journey from the Articles of Confederation to the United States Constitution: Courts on National Citizenship and Antidiscrimination*, 35 WHITTIER L. REV. 199 (2014); Lori Johnson, *Within Her Sphere: Determining a Woman's Place in the Constitutional Order Under the Privileges and Immunities Clause*, 79 MISS. L.J. 731 (2010); Douglas G. Smith, *The Privileges and Immunities Clause of Article IV, Section 2: Precursor of Section 1 of the Fourteenth Amendment*, 34 SAN DIEGO L. REV. 809 (1997).

[20] *Riley*, 134 S. Ct. at 2495 ("The fact that technology now allows an individual to carry [private] information in his hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant.").

[21] *See id.* at 2484, 2488 ("The search incident to arrest exception rests not only on the heightened Government interests at stake in a volatile arrest situation, but also on an arrestee's reduced privacy interests upon being taken into police custody.").

[22] *See infra* notes 75–77 and accompanying text.

[23] *Riley*, 134 S. Ct. at 2482 ("'[T]he ultimate touchstone of the Fourth Amendment is "reasonableness."'" (quoting Brigham City v. Stuart, 547 U.S. 398, 403 (2006))).

[24] *Id.* at 2495 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

expose to the government far *more* than the most exhaustive search of a house."[25]

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."[26] Simply put, 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."[27]

I. CHIEF JUSTICE ROBERTS'S MAJORITY OPINION—DISTINGUISHING THE PHYSICAL AND VIRTUAL WORLDS

Chief Justice Roberts's majority opinion recognized that the "'touchstone of the Fourth Amendment is "reasonableness"'"[28] 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.'"[29]

Answering this question in the affirmative—and holding that warrantless cell phone searches incident to arrest are *per se* unreasonable[30]—the Court explained that neither the *Chimel* justifications,[31] nor the expansive view of law enforcement authority embraced in *Robinson*,[32] nor the *Gant* standard[33] could justify the warrantless search of information that the Founders—and the Court—historically considered private.[34]

---

[25] *Id.* at 2491.

[26] U.S. CONST. amend. IV; *see also* Donohue, *supra* note 13, at 871–72 (noting that the NSA collects call metadata on "hundreds of millions of people").

[27] *Riley*, 134 S. Ct. at 2495.

[28] *Id.* at 2482 *(*quoting *Stuart*, 547 U.S. at 403).

[29] *Id.* at 2485 (quoting Arizona v. Gant, 556 U.S. 332, 343 (2009)).

[30] *Id.* at 2495.

[31] Chimel v. California, 395 U.S. 752, 762–63 (1969) (officer safety and preservation of evidence).

[32] *See* Scheurer, *supra* note 6, at 295 ("With *Robinson*, the Court effectively severed the search-incident-to-arrest exception from a fact-based analysis. As long as an officer executes a lawful arrest, he or she may conduct a 'full' search of the arrestee and, by the implication of *Chimel*, the area within the arrestee's 'immediate control.'").

[33] *Riley*, 134 S. Ct. at 2484 (citing *Gant*, 556 U.S. at 343).

[34] *See id.* at 2484–85 (declining to extend the categorical rule found in *Robinson*); *id.* at 2485–87 (rejecting both *Chimel* justifications); *id.* at 2492 (rejecting a standard based on *Gant*); *id.* at 2491 (stating that the Founders established protections for citizens' private items).

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 into which the arrestee may reach for a weapon.[35] A cell phone cannot be used as an offensive weapon or escape mechanism, and police are authorized to seize the phone upon arrest.[36] As Chief 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.[37]

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."[38]

2. The Preservation of Evidence Is Not Implicated

The Government argued that warrantless searches were justified to prevent the destruction of potentially incriminating evidence, through either "remote wiping [or] data encryption."[39] Remote wiping happens "when a third party sends a remote signal or when a phone is preprogrammed to delete data upon entering or leaving certain geographic areas."[40] Encryption allows individuals to protect cell phone data in a manner that "renders a phone all but 'unbreakable' unless police know the password."[41]

The Court found that neither of these possibilities presented a serious risk that the contents of a cell phone would be destroyed.[42] Indeed, "[r]emote wiping can be fully prevented by disconnecting a phone from the

---

35 *Chimel*, 395 U.S. at 762–63.
36 *Riley*, 134 S. Ct. at 2485.
37 *Id.*
38 *Id.*
39 *Id.* at 2486.
40 *Id.*
41 *Id.*
42 *Id.*

network."[43] With respect to data encryption, "[l]aw enforcement officers are very unlikely to come upon [a password-protected] 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."[44]

B. The Focus on Privacy, Not Trespass

Perhaps more importantly, the Court held that individuals have a reasonable expectation of privacy in data stored in cell phones because the information is fundamentally different than that which is typically stored in physical objects.[45] 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*."[46] Likewise, the Court did not extend the 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."'"[47] As Chief Justice Roberts wrote in the majority opinion, the *Gant* standard would "prove no practical limit at all when it comes to cell phone searches."[48]

1. Cell Phones Cannot Be Analogized to Cigarette Packs or Containers

At the outset, "[o]ne of the most notable distinguishing features of modern cell phones is their immense storage capacity."[49] This distinguishes the search of a cell phone from the search of a person, which is "limited by physical realities and tend[s] as a general matter to constitute only a narrow intrusion on privacy."[50] Chief 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

---

43 *Id.* at 2487.

44 *Id.*

45 *Id.* at 2488–89.

46 *Id.* at 2483 (emphasis added) (quoting United States v. Robinson, 414 U.S. 218, 235 (1973)).

47 *Id.* at 2484 (quoting Arizona v. Gant, 556 U.S. 332, 343 (2009)).

48 *Id.* at 2492.

49 *Id.* at 2489.

50 *Id.*

> phone book, and so on. We expect that the gulf between physical practicability and digital capacity will only continue to widen in the future.[51]

Indeed, "[c]ell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person."[52]

2. Cell Phones Contain Private Information

The Court also recognized that the storage capacity issue produces "several interrelated consequences for privacy"[53] 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."[54] Chief Justice Roberts noted that "Internet search and 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."[55] In other words, the thousands of photographs found on a cell phone, which contain dates, locations, and descriptions, reveal an individual's private life, while a simple wallet photograph provides no such insight.[56]

As a result, "a cell phone search would typically expose to the government far more than the most exhaustive search of a house" because a cell phone "contains a broad array of private information never found in a home in any form—unless the phone is."[57] 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"[58] does not "make the information any less worthy of the protection for which the Founders fought."[59] As Chief 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."[60] Indeed, it is ludicrous to say that carrying a cell phone in a public place somehow makes the information it

---

51 *Id.* (citations omitted).

52 *Id.*

53 *Id.*

54 *Id.*

55 *Id.* at 2490.

56 *Id.* at 2489.

57 *Id.* at 2491.

58 *Id.* at 2490.

59 *Id.* at 2495.

60 *Id.* at 2490. 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 that "every search 'is acceptable solely because a person is in custody.'" *Id.* at 2488 (quoting Maryland v. King, No. 12-207, slip op. at 26 (U.S. June 3, 2013)).

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.

Although the Court ultimately recognized that its decision would "have an impact on the ability of law enforcement to combat crime,"[61] it also noted that "[p]rivacy comes at a cost,"[62] particularly when the privacy intrusion of a cell phone search extends far beyond that of a physical search.[63] 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."[64]

II. 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.[65] Additionally, an individual's expectation of privacy in her cell phone does not change simply because she is in a public place.[66] 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,"[67] the *Riley* Court established a categorical bright-line rule that provides guidance to law enforcement and safeguards basic privacy rights.[68] Moreover, by basing its analysis on the Fourth Amendment's reasonableness standard,[69] 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.[70]

---

[61] *Id.* at 2493.

[62] *Id.*

[63] *Id.* at 2489.

[64] *Id.* at 2494.

[65] *See id.* at 2484 (noting that the application of the search-incident-to-arrest exception to cell phones is a question of first impression because the technology behind Riley's phone was "nearly inconceivable just a few decades ago, when *Chimel* and *Robinson* were decided").

[66] *See id.* at 2490 ("Today . . . it 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." (citation omitted)).

[67] Thornton v. United States, 541 U.S. 615, 625 (2004) (Scalia, J., concurring).

[68] *Riley*, 134 S. Ct. at 2494–95.

[69] *Id.* at 2482.

[70] *Id.* at 2484 ("[W]e 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

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.[71] Technology, however, has also become an "important tool[] in facilitating coordination and communication among members of criminal enterprises."[72] Additionally, the information on cell phones can "provide valuable incriminating information about dangerous criminals,"[73] and modern technology, more generally, can be an important investigatory tool for the Government, both domestically and internationally.[74]

Accordingly, what remains unknown is how weighty an individual's privacy interest will be outside of the arrest context, where the intrusion is less significant, or where the Government's interest is more substantial.[75] The Court did not, for example, indicate whether an individual's privacy interests in a cell phone's contents 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.[76] Furthermore, the Court did not indicate whether collecting

---

promotion of legitimate governmental interests.'" (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999)).

[71] *Id.* at 2489 (discussing the extensive storage capacity of modern cell phones).

[72] *Id.* at 2493.

[73] *Id.*

[74] *See, e.g.*, Bert-Jaap Koops, *Law, Technology, and Shifting Power Relations*, 25 BERKELEY TECH. L.J. 973, 978–79 (2010) (noting that although "increasingly sophisticated technology enables criminals to protect their communications from police surveillance and store incriminating electronic evidence[,] . . . technology also facilitates criminal investigation by supplying unprecedented surveillance tools"); Caitlin T. Street, Note, *Streaming the International Silver Platter Doctrine: Coordinating Transnational Law Enforcement in the Age of Global Terrorism and Technology*, 49 COLUM. J. TRANSNAT'L L. 411, 420–24 (2011) (discussing the "sophisticated surveillance and weapons technology" that is "critical in countering the international terrorism threat").

[75] *See Riley*, 134 S. Ct. at 2493–94 ("Our holding, of course, is not that the information on a cell phone is immune from search; it is instead that a warrant is generally required before such a search . . . . [E]ven though the search incident to arrest exception does not apply to cell phones, other case-specific exceptions may still justify a warrantless search of a particular phone. . . . [These include] the need to prevent the imminent destruction of evidence in individual cases, to pursue a fleeing suspect, and to assist persons who are seriously injured or are threatened with imminent injury.").

[76] *See id.* at 2490 ("Although the data stored on a cell phone is distinguished from physical records by quantity alone, certain types of data are also qualitatively different."). *But cf. id.* at 2493 ("[A]t oral argument California suggested a different limiting principle, under which officers could search cell phone data if they could have obtained the same information from a pre-digital counterpart. . . . The fact that someone could have tucked a paper bank statement in a pocket does not justify a search of every bank statement from the last five years. And to make matters worse, such an analogue test would allow law enforcement to search a range of items contained on a phone, even though people would be

all information from a cell phone, whether directly or through remote monitoring, will be considered a "search" for Fourth Amendment purposes.[77]

Riley also did not address how this more generalized privacy interest applies in other contexts, including where the Government's conduct is arguably less invasive and the privacy interest less pronounced, such as in the collection of metadata,[78] or where the Government's interest in crime prevention is heightened, such as in the searches of laptops at the border.[79] In other words, it is unclear whether all, or merely some, of the information collected from a cell phone, directly or through remote monitoring, may in some cases be outside of Fourth Amendment protections.

Furthermore, it is unclear how *Riley*'s focus on privacy can be reconciled with the trespass theory that the Court relied on in *United States v. Jones*,[80] in which the Court 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.[81] In a 5-4 decision, the majority based its decision on the fact that the physical installation of the device on the car constituted a trespass[82] but did not expressly consider under *Katz v. United States*[83] whether the intrusion violated the

---

unlikely to carry such a variety of information in physical form. . . . In addition, an analogue test would launch courts on a difficult line-drawing expedition to determine which digital files are comparable to physical records. Is an e-mail equivalent to a letter? Is a voicemail equivalent to a phone message slip? It is not clear . . . ." (citations omitted)).

77 *Cf. id.* at 2492–93 (distinguishing *Smith v. Maryland*, 442 U.S. 735 (1979), which had allowed the telephone company's collection of numbers dialed by a certain caller because that collection "was not a search" (internal quotation marks omitted)).

78 *See* United States v. Davis, No. 12-12928, slip op. at 23 (11th Cir. June 11, 2014) ("[W]e hold that cell site location information is within the subscriber's reasonable expectation of privacy. The obtaining of that data without a warrant is a Fourth Amendment violation."), *vacated & reh'g en banc granted*, No. 12-12928, 2014 WL 4358411, at *1 (11th Cir. Sept. 4, 2014); Klayman v. Obama, 957 F. Supp. 2d 1, 41 (D.D.C. 2013) ("[P]laintiffs have a substantial likelihood of showing that their privacy interests outweigh the Government's interest in collecting and analyzing bulk telephony metadata and therefore the NSA's bulk collection program is indeed an unreasonable search under the Fourth Amendment.").

79 *See* United States v. Cotterman, 709 F.3d 952, 966 (9th Cir. 2013) ("We recognize the important security concerns that prevail at the border. The government's authority to protect the nation from contraband is well established and may be 'heightened' by 'national cris[e]s,' such as the smuggling of illicit narcotics, the current threat of international terrorism and future threats yet to take shape." (alteration in original) (quoting United States v. Montoya de Hernandez, 473 U.S. 531, 538 (1985))), *cert. denied*, No. 13-186, 2014 WL 102985, at *1 (U.S. Jan. 13, 2014).

80 United States v. Jones, 132 S. Ct. 945, 949 (2012).

81 *Id.* at 948–49.

82 *See id.* at 947, 949 (5-4 decision).

83 *See* Katz v. United States, 389 U.S. 347, 351–52 (1967) (noting that privacy attaches not to a place, but to a person demonstrating his desire for it); *see also* United States

occupant's reasonable expectation of privacy.[84] Thus, it remains uncertain whether the generalized privacy interest in cell phone data will be limited to physical intrusions, whether the expectation of privacy diminishes when the Government remotely tracks information, and whether the duration of the Government's monitoring may turn an otherwise permissible search into a Fourth Amendment violation.[85]

Nonetheless, *Riley* will impact future cases because there are important parallels between the Court's decision and cases that it soon may decide, particularly involving the collection of cell phone (and internet) metadata[86] and searches of laptop computers at the border.[87] Indeed, if reasonableness continues to guide the Court's analysis, law enforcement's sweeping surveillance powers may soon come to an end.[88]

---

v. Miller, 425 U.S. 435, 442–43 (1976) (holding that the defendant had no expectation of privacy in banks' records of his financial activity because they were voluntarily conveyed to the bank and were included in the bank's business records).

[84] *Jones*, 132 S. Ct. at 950.

[85] It is not surprising that Chief Justice Roberts's majority opinion in *Riley* resulted in the relatively limited holding that an arrestee's *diminished* expectation of privacy while in custody does not *extinguish* the arrestee's privacy rights in information that has historically been protected under the Fourth Amendment. As a result of this holding, the Court left many questions unresolved. Narrow rulings are a hallmark of Chief Justice Roberts, who strives for "unanimous or near-unanimous decisions, on the ground that they promote the rule of law" and "lead to narrow, minimalist opinions." *Chief Justice Roberts and Minimalism*, U. CHI. L. SCH. FAC. BLOG (May 25, 2006, 9:52 AM), http://uchicagolaw.typepad.com/faculty/2006/05/chief_justice_r.html. Indeed, Chief 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.'" *Id.*

[86] Recently, a panel of the Eleventh Circuit held that a warrant is required to obtain cell site location data, and the full court granted a rehearing *en banc* soon afterwards. *See* United States v. Davis, No. 12-12928, slip op. at 23 (11th Cir. June 11, 2014), *vacated & reh'g en banc granted*, No. 12-12928, 2014 WL 4358411, at *1 (11th Cir. Sept. 4, 2014). *See also* Colin Campbell, *Antonin Scalia Has a Civil Liberties Debate in Brooklyn*, N.Y. OBSERVER (Mar. 22, 2014, 2:34 PM), http://observer.com/2014/03/antonin-scalia-has-a-civil-liberties-debate-in-brooklyn/ ("Mr. Napolitano then asked if mass surveillance of cellphones and emails would be prohibited by the Fourth Amendment . . . . 'You're getting into the NSA stuff, right?' Mr. Scalia remarked . . . . This may come before the court. And I don't want to get myself recused.'").

[87] Only a few months before deciding *Riley,* the Supreme Court denied certiorari to a case involving a forensic search of a laptop begun at the border. *See* United States v. Cotterman, 709 F.3d 952, 957 (9th Cir. 2013) ("[W]e consider the reasonableness of a computer search that began as a cursory review at the border but transformed into a forensic examination of Cotterman's hard drive."), *cert. denied*, No. 13-186, 2014 WL 102985, at *1 (U.S. Jan. 13, 2014). This kind of case may, of course, come before the Court again.

[88] Ann E. Marimow & Craig Timberg, *Low-Level U.S. Judges Limit Digital Evidence*, WASH. POST, Apr. 25, 2014, at A01 (discussing recent, though pre-*Riley*, magistrate decisions that have limited digital device searches by contrasting law enforcement's sweeping surveillance powers with the Fourth Amendment's "reasonableness" requirement).

A. The Collection of Cell Phone Metadata

In *Smith v. Maryland,* the Court held that law enforcement's installation of a pen register in a suspect's home to record outgoing calls did not constitute a search under the Fourth Amendment.[89] The Court held that the petitioner did not have a "legitimate" expectation of privacy in the numbers he dialed on his phone.[90] The Court stated as follows:

> [P]etitioner 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.[91]

The Court's decision was based in part on the third-party doctrine, which allows the Government to conduct warrantless searches of otherwise-private information when an individual has voluntarily conveyed that information to a third party.[92]

The Government has relied on *Smith* to support its collection of cell phone metadata, which records the user's calls *and* location.[93] Recent case law, however, has rejected the analogy much the same way that the *Riley* Court refused to equate cell phones with physical objects.[94] In *Klayman v. Obama,* for example, the court held that, unlike a pen register, which was "operational for only a matter of days,"[95] the Government metadata collection operation "involves the creation and maintenance of a historical database containing *five years*' worth of data."[96] Furthermore, pen registers "'record the numbers dialed from the [individual's] telephone,'" but metadata collection yields, "*on a daily basis*[,] electronic copies of call detail records" that can reveal the user's location.[97] Indeed, although it is

---

89 442 U.S. 735, 745–46 (1979).

90 *Id.* at 745.

91 *Id.* at 744.

92 *Id.* at 743–44.

93 *See* Donohue, *supra* note 13, at 866–67, 871.

94 *See* Klayman v. Obama, 957 F. Supp. 2d 1, 31 (D.D.C. 2013) ("When do present-day circumstances—the evolutions in the Government's surveillance capabilities, citizens' phone habits, and the relationship between the NSA and telecom companies—become so thoroughly unlike those considered by the Supreme Court thirty-four years ago that a precedent like *Smith* simply does not apply? The answer, unfortunately for the Government, is now.").

95 *Id.* at 32 (distinguishing *Smith*, 442 U.S. at 737).

96 *Id.*

97 *Id.* (quoting *Smith*, 442 U.S. at 737).

reasonable for phone companies to occasionally assist law enforcement,[98] it is an entirely different matter for citizens to "expect all phone companies to operate . . . a joint intelligence-gathering operation with the Government."[99]

Likewise, in *United States v. Davis*, the Eleventh Circuit held that the warrantless collection of cell phone metadata to identify a suspect's location violates the Fourth Amendment.[100] Significantly—and contrary to the Fifth Circuit[101]—the court held that individuals have a reasonable expectation of privacy in data that identifies their whereabouts.[102] The Eleventh Circuit reasoned that such location information is similar to communicative data because "it is private in nature,"[103] and its collection would impermissibly "convert what would otherwise be a private event into a public one."[104] Importantly, the court distinguished *Jones*, which "involved the movements of the defendant's automobile on the public streets and highways,"[105] by holding that *Jones*'s reliance on a trespass theory did not suggest that the *Katz* privacy rationale was no longer applicable.[106]

The Eleventh Circuit's decision creates a circuit split that the Supreme Court may ultimately resolve.[107] Based on the reasoning employed in *Riley*, the Court may very well hold that the Government's metadata collection practices violate the Fourth Amendment. Unlike the analysis in *Jones,* the *Riley* Court's reasoning focused on the privacy

---

[98] *Id.* at 33.

[99] *Id.*

[100] United States v. Davis, No. 12-12928, slip op. at 23 (11th Cir. June 11, 2014), *vacated & reh'g en banc granted*, No. 12-12928, 2014 WL 4358411, at *1 (11th Cir. Sept. 4, 2014).

[101] *See In re* U.S. for Historic Cell Site Data, 724 F.3d 600, 624 (5th Cir. 2013) ("[T]here is substantial doubt as to whether cell phone users have a reasonable expectation of privacy in cell site location information . . . .").

[102] *Davis*, slip op. at 23.

[103] *Id.* at 20.

[104] *Id.*

[105] *Id.* at 19.

[106] *Id.* at 18 ("In light of the confluence of the three opinions in the Supreme Court's decision in *Jones*, we accept the proposition that the privacy theory is not only alive and well, but available to govern electronic information of search and seizure in the absence of trespass.").

[107] *Compare Davis*, slip op. at 23 (holding that a warrant is required to search cell phone location information), *vacated & reh'g en banc granted*, No. 12-12928, 2014 WL 4358411, at *1 (11th Cir. Sept. 4, 2014), *with In re* U.S. for Historic Cell Site Data, 724 F.3d 600, 624 (5th Cir. 2013) (stating that cell phone users likely do not have a reasonable expectation of privacy in their cell location information).

infringement that resulted from searches on an arrestee's cell phone[108] and recognized that cell phones are not analogous to physical objects traditionally subject to post-arrest searches.[109] Although the collection of metadata is arguably less intrusive and occurs from a distance,[110] it records a user's call history and location without even the slightest hint of suspicion.[111] Furthermore, metadata collection is neither limited in duration nor targeted at individuals already suspected of criminal conduct.[112] Under *Riley*'s reasonableness standard, which recognized a generalized expectation of privacy in cell phone data,[113] the Government's indiscriminate and prolonged collection of metadata[114] appears unreasonable.

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

Riley may also affect the Government's ability to conduct intrusive, or "forensic," searches of laptops at the border without any degree of suspicion.[115] 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[116] and the discovery of contraband.[117]

As the *Riley* Court correctly recognizes, however, digital devices contain a vast amount of private information that renders searches of them far more intrusive.[118] Furthermore, just as the justifications for

---

[108] *See Riley*, 134 S. Ct. at 2494–95 (holding that cell phones are protected from warrantless searches because of the privacy interests implicated).

[109] *Id.* at 2488–89.

[110] *See, e.g.*, *Historic Cell Site Data*, 724 F.3d at 610, 613, 615 (holding that historical cell site data is not subject to a reasonable expectation of privacy because users knowingly expose this information to cell providers).

[111] *See* Donohue, *supra* note 13, at 759–60, 872 (describing the "call detail information" of law-abiding citizens that cell phone service providers must turn over to the NSA).

[112] *See* Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 723–24 (2011) ("The government apparently seeks location information about ostensibly innocent parties regularly. . . . [M]ore than two hundred and ninety million Americans who use cell phones are at risk of location data surveillance.").

[113] *See Riley*, 134 S. Ct. at 2494–95.

[114] Freiwald, *supra* note 112, at 746–47.

[115] *Cf.* United States v. Cotterman, 709 F.3d 952, 962 (9th Cir. 2013) (noting in a border laptop search case that "the comprehensive and intrusive nature of a forensic examination—not the location of the examination . . . is the key factor triggering the requirement of reasonable suspicion here."), *cert. denied*, No. 13-186, 2014 WL 102985, at *1 (U.S. Jan. 13, 2014).

[116] *See* United States v. Brignoni-Ponce, 422 U.S. 873, 880–81 (1975).

[117] United States v. Montoya de Hernandez, 473 U.S. 531, 537 (1985).

[118] *Riley*, 134 S. Ct. at 2489.

searching incident to arrest are not triggered by the mere presence of a cell phone,[119] the justifications for border searches are not necessarily sufficiently implicated by the presence of a laptop to make a search reasonable.[120] Importantly, the Ninth Circuit recently considered this issue and held that border agents must have reasonable suspicion before conducting forensic searches of laptops.[121] However, the Eastern District of New York held 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.' "[122] The court did recognize, however, that if warrantless forensic searches (which occur rarely) were more routine, reasonable suspicion would be required.[123]

The Court's decision in *Riley* provides additional support for requiring reasonable suspicion before border agents perform forensic searches at the border.[124] Given the Government's heightened interests in this context,[125] however, the Court would probably permit more superficial searches of a motorist's laptop, provided they are limited to areas: (1) traditionally deemed searchable in that context;[126] (2) that implicate officer safety or the presence of contraband;[127] or (3) to which no reasonable expectation of privacy attaches.[128]

CONCLUSION

Riley is a landmark decision because of its reasoning, not merely its result.[129] Chief Justice Roberts's majority opinion focused on reasonableness and recognized that digital devices implicate fundamental privacy concerns.[130] Indeed, *Riley* suggests that the Court will take a more

---

[119] *Id.* at 2485–87.

[120] *See Cotterman*, 709 F.3d at 962, 966–68.

[121] *Id.* at 967–68.

[122] Abidor v. Napolitano, 990 F. Supp. 2d 260, 278 (E.D.N.Y. 2013) (quoting United States v. Flores-Montano, 541 U.S. 149, 152 (2004)).

[123] *Id.* at 282.

[124] *Cf. Cotterman*, 709 F.3d at 962.

[125] *Id.* at 966.

[126] *See id.* at 960 (discussing the traditional limits of the border search exception).

[127] *See* United States v. Montoya de Hernandez, 473 U.S. 531, 537 (1985); United States v. Brignoni-Ponce, 422 U.S. 873, 880–81 (1975).

[128] *See* Katz v. United States, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.").

[129] *See Landmark Supreme Court Ruling Protects Cell Phones from Warrantless Searches*, NAT'L L. REV. (June 30, 2014), http://www.natlawreview.com/article/landmark-supreme-court-ruling-protects-cell-phones-warrantless-searches (recognizing that the Court's analysis in *Riley* stemmed from an understanding of "the unique role that cell phones play in modern life").

[130] *Riley*, 134 S. Ct. at 2484–85, 2488–89.

active role in ensuring that the Government's investigative and surveillance practices do not lead to the modern-day version of the general warrant.[131]

Quite frankly, it is about time. The National Security Agency's surveillance program has resulted in alarming encroachments by the Government into the private lives of its citizens and made any threshold standard of suspicion seem like an inconvenience, not a requirement.[132] Hopefully, *Riley* is the first step toward restoring the proper—reasonable—constitutional balance.

---

[131] *Id.* at 2494–95.

[132] *See* Mornin, *supra* note 14, at 1000–02 (discussing the extent of the NSA's monitoring of metadata over time, including individual call and aggregate call analysis).