Richmond Journal of Law and Technology

Volume 21 | Issue 1 Article 2

2014

Riley v. California: The New Katz or Chimel?

Adam Lamparello

Charles MacLean

RILEY V. CALIFORNIA: THE NEW *KATZ* OR *CHIMEL*?

Adam Lamparello & Charles MacLean*

"To declare that in the administration of the criminal law the end justifies the means—to declare that the Government may commit crimes in order to secure the conviction of a private criminal—would bring terrible retribution. Against that pernicious doctrine this Court should resolutely set its face."[1]

Cite as: Adam Lamparello & Charles MacLean, *Riley v. California: The New Katz or Chimel?*, 21 RICH. J.L. & TECH. 1 (2014), http://jolt.richmond.edu/v21i1/article1.pdf.

I. INTRODUCTION

[1] In *Olmstead v. United States*,[2] Justice Louis Brandeis dissented from a 5–4 ruling that allowed law enforcement officers to obtain private wiretapped telephone conversations without a warrant and use them as evidence.[3] Justice Brandeis' words foreshadowed the threats to civil liberties that technology would pose:

> The progress of science in furnishing the Government with means of espionage is not likely to stop with wire-tapping. Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences

* Assistant Professors of Law, Indiana Tech Law School.

[1] Olmstead v. United States, 277 U.S. 438, 485 (1928) (Brandeis, J., dissenting), *overruled by* Katz v. United States, 389 U.S. 347, 353 (1967).

[2] *Olmstead*, 277 U.S. 438.

[3] *See id.* at 466.

> of the home. Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions. "That places the liberty of every man in the hands of every petty officer" was said by James Otis of much lesser intrusions than these. To Lord Camden, a far slighter intrusion seemed "subversive of all the comforts of society." Can it be that the Constitution affords no protection against such invasions of individual security?[4]

[2] Over three-quarters of a century later, privacy is being attacked in a manner that threatens the liberty of every citizen. The Government is tracking the whereabouts of its citizens at any time of the day,[5] recording Internet search history[6] and data stored on a hard drive,[7] and monitoring messages sent by text message or e-mail.[8] As a result, some individuals may unknowingly be on a terror watch list for downloading a video that depicts Al Qaeda sympathizers burning an American flag and threatening an attack larger than September 11, 2001, when hijacked planes toppled

[4] *Id.* at 474.

[5] *See, e.g.*, Klayman v. Obama, 957 F. Supp. 2d 1, 7 (D.D.C. 2013) (describing the information involved in metadata collection).

[6] *See* Glen Greenwald, *XKeyscore: NSA tool collection 'nearly everything a user does on the internet,'* THE GUARDIAN (July 31, 2013, 8:56 AM), http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data, *archived at* http://perma.cc/Y847-C3Q7.

[7] *See* Jason Mick, *Tax and Spy: How the NSA Can Hack Any American, Stores Data 15 Years*, DAILY TECH (Dec. 31, 2013, 12:36 PM), http://www.dailytech.com/Former+FBI+Agent+All+Your+Communications+are+Recorded+Government+Accessible/article31486.htm, *archived at* http://perma.cc/ZWZ4-STDD.

[8] *See* Adam Weinstein, *The Government's Phone, Text, and Email Spying, Explained*, FUSION (Oct. 25, 2013, 6:00 PM), http://fusion.net/abc_univision/story/governments-phone-text-email-spying-explained-22515, *archived at* http://perma.cc/VCC2-CPHP.

New York City's twin towers and took the lives of over 3000 people.[9] The most frightening aspect is that the Government is doing all of this without a warrant. In some cases, the Government has no suspicion whatsoever.[10] In every case, the Fourth Amendment rights of its citizens are being violated.

[3] For these and other reasons, *Riley v. California*,[11] where the Supreme Court unanimously held that warrantless searches of a cell phone incident to arrest were unreasonable and therefore violated the Fourth Amendment,[12] came at the right time. As discussed below, *Riley* marks a new era of privacy protection that does not yield in the face of the broad, McCarthy-esque justifications of "national security" and the "war on terror." Instead, the Court recognized that "protection against such invasions of individual security"[13] supports the conclusion that pre-digital era case law could neither foresee nor protect against these invasions.

[4] The Court's decision suggests that cellular telephones, particularly smartphones, along with laptop computers and other digital devices, are the twenty-first century's private 'homes,' where individuals store the "papers and affects" traditionally accorded Fourth Amendment protection. The unanswered question, however, is whether *Riley* is the beginning of a principled, *Katz*-driven jurisprudence that focuses on privacy protection[14]

[9] *See* Jeremy Scahill & Ryan Devereaux, *The Secret Government Rulebook for Labeling You a Terrorist*, THE INTERCEPT (July 23, 2014, 2:45 PM), https://firstlook.org/theintercept/2014/0/23/blacklisted/, *archived at* http://perma.cc/4FPY-A344; *see also Watchlisting Guidance*, U.S. NAT'L COUNTERTERRORISM CENTER (Mar. 2013) (detailing government qualifications for putting people on a terrorist watchlist).

[10] *See* Scahill & Devereaux, *supra* note 9.

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

[12] *See id.* at 2493.

[13] *Olmstead*, 277 U.S. at 473–74.

[14] *See* Katz v. United States, 389 U.S. 347, 350-51 (1967) (focusing on an individual's right to be left alone rather than determining what geographic areas are constitutionally protected).

or a muddled jurisprudence that immerses itself in the many hyper-technicalities that characterized the post-*Chimel* era.[15] This essay argues that *Riley* is the new *Katz*, and marks the beginning of increased protections for privacy in the digital age.

II. THE NEW *KATZ*: PRIVACY FOR THE DIGITAL AGE

[5] In *Riley*, the Court held that the original justifications for warrantless searches incident to arrest under *Chimel*—officer safety and the preservation of evidence—were not implicated in cell phone searches.[16] Writing for a unanimous court,[17] Justice Roberts correctly held

[15] *See* Chimel v. California, 395 U.S. 752, 762–63 (1967); *see also* Arizona v. Gant, 556 U.S. 332, 342 (2009); New York v. Belton; *and* United States v. Robinson, 414 U.S. 218, 235 (1973) (highlighting the hyper-technicalities that characterized this post *Chimel* world). In *Chimel*, the Court created the search-incident-to-arrest doctrine, which allows warrantless searches of an arrestee's person to protect officer safety and preserve evidence:

> When an arrest is made, it is reasonable for the arresting officer to search the person arrested in order to remove any weapons that the latter might seek to use in order to resist arrest or effect his escape. Otherwise, the officer's safety might well be endangered, and the arrest itself frustrated. In addition, it is entirely reasonable for the arresting officer to search for and seize any evidence on the arrestee's person in order to prevent its concealment or destruction. . . . There is ample justification, therefore, for a search of the arrestee's person and the area "within his immediate control"—construing that phrase to mean the area from within which he might gain possession of a weapon or destructible evidence.

Chimel, at 762-63.

In the years following *Chimel*, the Court expanded *Chimel* to allow virtually all warrantless searches incident to arrest, even if safety and evidence preservation were not implicated. *See, e.g.*, *Belton*, 453 U.S. at 460 (1981) (expanding *Chimel* to hold that law enforcement officers may search the passenger compartment of an arrestee's vehicle).

[16] *See Riley*, 134 S. Ct. at 2484–85.

[17] *Id.* at 2480.

that cell phones could not be used as weapons[18] and that the likelihood of evidence destruction was remote.[19] Thus, absent exigent circumstances law enforcement could not search an arrestee's cell phone without a warrant and probable cause.[20] Several aspects of the Court's opinion suggested that the Government's days of relying on case law from an era of rotary telephones, eight-track tapes, and crumpled cigarette packs is over.[21] Specifically, in distinguishing cell phones from physical objects such as plastic containers, wallets, and address books, the Court recognized that "[c]ell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person."[22]

A. The *Quantity* of Information in Cell Phones

[6] Justice Roberts' opinion recognized that cellular phones, particularly smartphones, are not really "phones" in a traditional sense.[23] Justice Roberts wrote:

> The 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. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.[24]

[18] *See id.* at 2485.

[19] *See id.* at 2486–87.

[20] *See id.* at 2493.

[21] *See Riley* 134 S. Ct. at 2485, 2488–89.

[22] *Id.* at 2489.

[23] *See id.*

[24] *Id.*

[7] Furthermore, cell phones can hold "millions of pages of text, thousands of pictures, or hundreds of videos [and] . . . [e]ven the most basic phones that sell for less than $20 might hold photographs, picture messages, text messages, Internet browsing history, a calendar, [and] a thousand-entry phone book."[25]

[8] Additionally, 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."[26] As Justice Roberts explained, this information implicates privacy in a manner that physical objects do not:

> [A] cell phone's capacity allows even just one type of information to convey far more than previously possible. 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. Third, the data on a phone can date back to the purchase of the phone, or even earlier. A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a phone.[27]

Justice Roberts also emphasized the "element of pervasiveness that characterizes cell phones but not physical records, [holding that] . . . [p]rior to the digital age, people did not typically carry a cache of sensitive

[25] *Id.*

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

[27] *Id.*

personal information with them as they went about their day." [28] Comparing cell phones to physical objects was "like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together."[29]

B. The Quality of Information in a Cell Phone

[9] Most importantly, the Court held that cell phones store uniquely private information.[30] For example, "Internet search and browsing history . . . 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."[31] In addition, "application software on a cell phone, or 'apps,' offer a range of tools for managing detailed information about all aspects of a person's life."[32] In fact, quoting Learned Hand, Justice Roberts held that the quantity and quality of private information stored on a cell phone is even greater than that stored in a home:

> In 1926, Learned Hand observed . . . that it is "a totally different thing to search a man's pockets and use against him what they contain, from ransacking his house for everything which may incriminate him." If his pockets contain a cell phone, however, that is no longer true. Indeed, a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many

[28] *Id.* at 2490 ("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.").

[29] *Id.* at 2488.

[30] *Id.* at 2473.

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

[32] *Id.*

> 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.[33]

[10] Furthermore, through the use of cloud computing, some of "the data a user views on many modern cell phones may not in fact be stored on the device itself . . . [due to] the capacity of Internet-connected devices to display data stored on remote servers."[34]

III. THE SIGNIFICANCE OF *RILEY* AND ITS APPLICATION TO OTHER CASES

[11] *Riley* is a landmark decision and marks the beginning of the end of the Government's intrusion into the private digital lives of its citizens.

A. Pre-Digital Case Law is Easily Distinguishable and Therefore No Longer Controls

[12] The Court recognized that pre-digital era case law could not be applied to digital-era problems.[35] First, Justice Roberts found unpersuasive the Government's reliance on *United States v. Robinson*, where the Court upheld, under *Chimel*, the warrantless search of a crumpled up cigarette pack.[36] The Court's decision in *Robinson* significantly expanded *Chimel* by holding that "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."[37] Thus, under *Robinson* it did not

[33] *Id.* at 2490–91 (quoting United States v. Kirschenblatt, 16 F.2d 202, 203 (2d Cir. 1926)).

[34] *Id.* at 2491.

[35] *See Riley*, 134 S. Ct. at 2484, 2494.

[36] *See* United States v. Robinson, 414 U.S. 218, 225–26 (1973).

[37] *Id.* at 235.

matter whether the original justifications under *Chimel*—officer safety or evidence preservation—were implicated.[38] The *Riley* Court rejected the reasoning in *Robinson* and, although the Court did not directly overturn *Robinson's* holding that *Chimel's* dual objectives "are present in all custodial arrests," it found that there "are no comparable risks when the search is of digital data."[39]

[13] Additionally, although the *Robinson* Court "regarded any privacy interests retained by an individual after arrest as significantly diminished by the fact of the arrest itself," the same could not be said in the cell phone context.[40] Indeed, cell phones "place vast quantities of personal information literally in the hands of individuals," a search of which "bears little resemblance to the type of brief physical search considered in *Robinson*."[41] Furthermore, "[t]he possibility that a search might extend well beyond papers and effects in the physical proximity of an arrestee is yet another reason that the privacy interests here dwarf those in *Robinson*."[42] Put differently, depending on the privacy interests at stake, "[n]ot every search 'is acceptable solely because a person is in custody.'"[43]

[14] The Court also rejected the Government's reliance on *Arizona v. Gant*,[44] which "added . . . 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.'"[45] Importantly, however, *Gant* relied on "circumstances unique

[38] *See id.* at 235.

[39] *Riley*, 134 at 2484–85.

[40] *Id.*

[41] *Id.* at 2485.

[42] *Id.*at 2491.

[43] *Id.* at 2488 (quoting Maryland v. King 133 S. Ct. 1958, 1979 (2013)).

[44] *See id.* at 2492.

[45] *Riley*, 134 S. Ct. at 2484 (quoting Arizona v. Gant, 556 U.S. 332, 343 (2009)).

to the vehicle context" to endorse a search solely for the purpose of gathering evidence.[46] Relying on Justice Scalia's concurring opinion in *Thornton v. United States*,[47] Justice Roberts explained that the unique circumstances in *Gant* are "'a reduced expectation of privacy' and 'heightened law enforcement needs' when it comes to motor vehicles."[48] Searches of cell phones, however, "bear neither of those characteristics."[49]

[15] Most importantly, Justice Roberts recognized that the standard adopted in *Gant* "would prove no practical limit at all when it comes to cell phone searches,"[50] stating as follows:

> In the vehicle context, *Gant* generally protects against searches for evidence of past crimes. In the cell phone context, however, it is reasonable to expect that incriminating information will be found on a phone regardless of when the crime occurred. Similarly, in the vehicle context *Gant* restricts broad searches resulting from minor crimes such as traffic violations. That would not necessarily be true for cell phones. It would be a particularly inexperienced or unimaginative law enforcement officer who could not come up with several reasons to suppose evidence of just about any crime could be found on a cell phone. Even an individual pulled over for something as basic as speeding might well have locational data dispositive of guilt on his phone. An individual pulled over for reckless driving might have evidence on the phone that shows whether he was texting while driving. The sources of potential pertinent

[46] *Gant*, 556 U.S. at 343.

[47] Thornton v. United States, 541 U.S. 615, 628–32 (2004) (Scalia, J., concurring).

[48] *Riley*, 134 S. Ct. at 2492 (quoting *Thornton*, 541 U.S. at 631).

[49] *Id.* at 2492.

[50] *Id.*

> information are virtually unlimited, so applying the *Gant* standard to cell phones would in effect give "police officers unbridled discretion to rummage at will among a person's private effects."[51]

The Court also rejected the Government's reliance on *Smith v. Maryland*,[52] which upheld the use of pen registers to monitor outgoing calls from a suspect's private residence.[53] In doing so, the Court rejected the Government's argument that searches can be limited to call logs, as they "typically contain more than just phone numbers; they include any identifying information that an individual might add."[54] Finally, the Court refused to permit searches of cell phone data "if [law enforcement] could have obtained the same information from a pre-digital counterpart."[55] In fact, Justice Roberts made it a point to distance the Court from applying pre-digital era case law to digital age technology:

> [T]he fact that a search in the pre-digital era could have turned up a photograph or two in a wallet does not justify a search of thousands of photos in a digital gallery. 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 unlikely to carry such a variety of information in physical form.[56]

---

[51] *Id.* (quoting *Gant*, 556 U.S. at 345).

[52] *See id.*, 134 S. Ct. at 2492–93.

[53] *See* Smith v. Maryland, 442 U.S. 735 at 745–46 (1979).

[54] *Riley*, 134 S. Ct. at 2492–93.

[55] *Id.* at 2493.

[56] *Id.*

[16] Indeed, "a significant diminution of privacy" would result if law enforcement could search all areas of a cell phone merely to locate information that could be stored in a pre-digital era physical object.[57] Furthermore, the Government's argument that law enforcement could "'develop protocols to address' concerns raised by cloud computing," was unpersuasive because "the Founders did not fight a revolution to gain the right to government agency protocols."[58] They fought to ensure that the Government could not run roughshod over the privacy rights of its citizens—even if its citizens might be safer as a result.

[17] Ultimately, Justice Roberts' opinion suggests that the Government will now be required to provide a digital-era justification to search the "papers and effects" that are stored in cell phones.[59] At the heart of Justice Roberts' opinion was a desire to prevent law enforcement from conducting the types of broad, non-particularized searches, which was "one of the driving forces behind the Revolution itself," and led the Founders to adopt the Fourth Amendment.[60] Indeed, "the Fourth Amendment was the founding generation's response to 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."[61]

B. Rejecting an *Ad Hoc*, Case-By-Case Jurisprudence

[18] In a noticeable departure from its Fourth Amendment jurisprudence, the Court emphasized the importance of creating bright-line rules to govern searches of private cell phone data.[62] Justice Roberts

[57] *Id.*

[58] *Id.* at 2491.

[59] *Id.* at 2493.

[60] *Riley*, 134 S. Ct. at 2494.

[61] *Id.*

[62] *See id.* at 2491–92.

wrote that "if police are to have workable rules, the balancing of the competing interests . . . 'must in large part be done on a categorical basis—not in an ad hoc, case-by-case fashion by individual police officers.'"[63] Otherwise, the Court would be thrust into an uncertain jurisprudence that would raise more questions than it would answer:

> [A]n 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 how officers could make these kinds of decisions before conducting a search, or how courts would apply the proposed rule after the fact. An analogue test would "keep defendants and judges guessing for years to come."[64]

[19] The Court may have recognized the difficulties that arose in the years after *Chimel*, where the Court's *ad hoc* jurisprudence was often based on hyper-technicalities that resulted in a muddled, uncertain, and unworkable jurisprudence.[65] Indeed, after *Robinson*,[66] *Gant*,[67] and *New York v. Belton*,[68] law enforcement had nearly unfettered authority to conduct warrantless searches incident to arrest, even where officer safety

[63] *Id.* at 2491–92 (quoting Michigan v. Summers, 452 U.S. 692, 705 n.19 (1981)).

[64] *Riley*, 134 S. Ct. at 2493 (quoting Sykes v. United States, 131 S. Ct. 2267, 2287 (2011) (Scalia, J., dissenting)).

[65] *See* Arizona v. Gant, 556 U.S. 332, 345–47 (2009).

[66] United States v. Robinson, 414 U.S. 218, 235 (1973) (holding a custodial arrest based on probable cause is a reasonable intrusion under the Fourth Amendment and requires no additional justification to conduct a search incident to arrest).

[67] *Gant*, 556 U.S. at 342 (expanding *Chimel* to allow warrantless searches of vehicles when the passenger is unsecured and within reaching distance of the vehicle, and when there is reason to believe evidence relevant to the crime of arrest may be found within).

[68] New York v. Belton, 453 U.S. 454, 459 (1981) (holding that upon arrest, law enforcement may search a vehicle's passenger compartment).

and evidence preservation rationales were non-existent. Simply put, for many years the warrant requirement ceased to exist the moment law enforcement slapped handcuffs on a suspect.

C. Support for an Internet Neutrality Doctrine

[20] Although it is a Fourth Amendment case, the majority's reasoning in *Riley* reflects a fundamental truth: the world has changed, and to protect basic civil liberties, the law must change as well. This is particularly true with respect to the Internet, which is the digital age equivalent of traditional public and limited purpose public forums (e.g., public sidewalks and town halls), just as cellular telephones are similar to a private home for search and seizure purposes.[69] The Internet enables the free flow of information between networks, including speech on matters of political, social, and commercial importance. Importantly, however, through pricing and "traffic shaping,"[70] which involves "slowing down some forms of traffic, like file-sharing, while giving others priority,"[71] Internet service providers have the ability to discriminate against users based on the content of their message, and thus thwart public debate and stifle competition. These practices are the equivalent of allowing the Boy Scouts to march in the public square, while relegating flag burners to desolated areas, remote deserts, or dark alleys.[72] Consequently, the Court should embrace a net neutrality doctrine for the same reason it invalidated warrantless cell phone searches in *Riley*: technology has ushered civil liberties into the virtual world, and the law must adapt by providing legal protections to individuals who speak, assemble, and associate in that world.

---

[69] *See, e.g.*, Perry Educ. Ass'n v. Perry Local Educators' Ass'n, 460 U.S. 37, 45 (1983) ("A traditional public forum is property that by long tradition or by government that have been devoted to assembly and debate").

[70] Christopher R. Steffe, *Why We Need Net Neutrality Now Or: How I Learned to Stop Worrying and Start Trusting the FCC*, 58 DRAKE L. REV. 1149, 1158 (2010).

[71] *Id.*

[72] *See* Texas v. Johnson, 491 U.S. 397 (1989) (invalidating a statute prohibiting desecration of the American flag).

D. The End of Metadata: Protecting Cell Phones as Objects and Repositories for the Fourth Amendment's 'Papers and Effects'

[21] *Riley* establishes cell phones as the new repository for the "papers and effects" that the Fourth Amendment protects from warrantless searches.[73] Not only did the Court reject the Government's analogies to pre-digital era physical objects, such as plastic containers, wallets, and crumpled cigarette packs, but it also held that cell phone data, both in quantity and quality, contains more private information than can be found in a private home.[74] To be sure, "[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."[75]

[22] In so holding, the Court implicitly recognized that cell phones, to an even greater degree than private homes, engender privacy protections as *objects*, and not merely because of the private data they contain. Thus, just like law enforcement officers cannot enter a home to search for incriminating evidence that might be in plain view *inside* the home, they cannot search *any* area of a cell phone, even though some areas, such as a call log, are less private than, for example, Internet browser history.[76] The point of *Riley* was that cell phones are protected not just for what they contain, but for how they are used in modern society, and for the privacy expectations that millions of individuals have in their phones. Thus,

[73] *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 [w]arrants shall issue, but upon probable cause, supported by [o]ath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized"); *see also Riley*, 134 S. Ct. at 2491.

[74] *See Riley*, 134 S. Ct. at 2490–91.

[75] *Id.* at 2491.

[76] *See id.* at 2489.

individuals have a reasonable expectation of privacy not merely in a cell phone's *contents*, but in the phone itself.[77] This could signal the end to warrantless metadata collection, where the Government used cell phone towers to monitor and collect information such as outgoing calls and physical location. In fact, the Court suggested that this type of information also warrants Fourth Amendment protection, "[d]ata on a cell phone can also reveal where a person has been. Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building."[78]

[23] For purposes of metadata collection, the message is clear: the Supreme Court is likely to hold that Government will not be permitted to indiscriminately collect metadata unless it has, at the very least, reasonable suspicion.[79]

E. The Third-Party Doctrine May be Invalidated

[24] The third-party doctrine is also a product of pre-digital era case law, and holds that individuals who knowingly transmit information through a third party can be found to have waived their expectation of privacy in such information.[80] Essentially, because individuals know that a third party may or will view information that is transmitted via a cell phone, they implicitly consent to its disclosure to additional parties. The

[77] *Id*. at 2494–95 ("Our answer to the question of what police must do before searching a cell phone seized incident to arrest is accordingly simply get a warrant.").

[78] *Id*. at 2490 (citing United States v. Jones, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring) ("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.")).

[79] *See, e.g.*, Terry v. Ohio, 392 U.S. 1, 21 (1968) (establishing the reasonable suspicion standard, which requires law enforcement, "to point to specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant that intrusion").

[80] *See* United States v. Miller, 425 U.S. 435, 442–43 (1976).

problem with the third-party doctrine, however, is identical to the problem the Government faced when trying to equate searches of physical containers with searches of cell phone data. The third-party doctrine was developed in an era when the information in question, *e.g.*, a bank record or paper check, did not implicate the same privacy concerns as are present in the cell phone context. As one commentator notes, "the Supreme Court decisions that established the third-party doctrine are decades old,"[81] and cell phones, just as they are not containers or address books, are unlike "information voluntarily conveyed to banks in the ordinary course of business."[82]

F. *Riley* is *Katz* for the Digital Age

[25] To the extent that questions remain about the scope and significance of *Riley*, they can be put to rest by reading three critical passages in the majority opinion that show beyond doubt that *Riley* is *Katz* for the digital age. Indeed, courts should not repeat the mistakes that occurred in the post-*Chimel* era, where courts created an *ad hoc*, hyper-technical, and muddled jurisprudence that eviscerated *Chimel's* limitations and led to expansive searches regardless of concerns about officer safety and evidence preservation.[83] In fact, *Riley* was the logical result of a jurisprudence that had nearly abandoned the original *Chimel* justifications, and this time the Court signaled that it will not make the same mistake again.

---

[81] Jeremy H. Rothstein, Note, *Track Me Maybe: The Fourth Amendment and the Use of Cell Phone Tracking to Facilitate Arrest*, 81 FORDHAM L. REV. 489, 506 (2012).

[82] *Id.* at 506–07 (discussing United States v. Miller, 425 U.S. 435, 442-43 (1976)).

[83] *See generally* Arizona v. Gant, 556 U.S. 332, 342 (2009) (expanding *Chimel* to allow warrantless searches of vehicles when the passenger is unsecured and within reaching a distance of the vehicle, and when there is reason to believe evidence relevant to the crime of arrest may be found within); New York v. Belton, 453 U.S. 454, 459 (1981) (holding that upon arrest, law enforcement may search a vehicle's passenger compartment); *and* United States v. Robinson, 414 U.S. 218, 235 (1973) (holding a custodial arrest based on probable cause is a reasonable intrusion under the Fourth Amendment and requires no additional justification to conduct a search incident to arrest).

[26] First, by holding that there "are no comparable risks [to officer safety and the destruction of evidence] when the search is of digital data,"[84] the Court recognized that digital devices are so fundamentally different from pre-digital era objects that they justified a *categorical* prohibition against warrantless searches.[85] Second, the Court stated in no uncertain terms that cell phones contain a "broad array of private information *never found in a home in any form*—unless the phone is,"[86] and a case-by-case, *Chimel*-type jurisprudence would only threaten to confuse, undermine, and render uncertain the core commitment to protecting privacy.[87] Indeed, phones are not merely a compilation of YouTube videos, Amazon.com purchases, and personal photographs. They house users' thoughts, private expressions, and most intimate and confidential communications.[88] Third, and in recognition of this fact, the Court refused to fashion an "analogue test [that] would launch courts on a difficult line-drawing expedition to determine which digital files are comparable to physical records."[89] Instead, the Court understood that, although the Fourth Amendment remains unchanged from its original purpose, the technology era has changed everything else.[90] With those changes came a reaffirmation of that purpose and a commitment to protect core civil liberties.

[27] Ultimately, the information on a cell phone is so private that the only line to be drawn is precisely where the Court did: "[o]ur answer to the question of what police must do before searching a cell phone seized

[84] *Riley*, 134 S. Ct. at 2485.

[85] *See id.* at 2493.

[86] *Id.* at 2490–91 (emphasis added).

[87] *See id.* at 2484–85.

[88] *See id.* at 2490.

[89] *Riley*, 134 S. Ct. at 2493.

[90] *See id.* at 2490–91.

incident to an arrest is accordingly simple—get a warrant."[91] *Riley* is the new *Katz*, and soon the Government's ability to track metadata, record Internet browser history, apply the third-party doctrine to digital data, and peer into other aspects of our private lives will end—just like pre-digital era case law saw its relevance disappear in *Riley.*

IV. CONCLUSION

[28] Justice Brandeis forecasted that "[t]he progress of science in furnishing the Government with means of espionage is not likely to stop with wiretapping."[92] In the law enforcement and government surveillance context, technological advances have made it possible to store an individual's DNA in a national database, and have made it nearly impossible for that same individual to send an e-mail, download a YouTube video, or transmit a text message without knowing that the government might be watching—without having the slightest degree of suspicion of criminal behavior. In any society that values basic civil liberties, such practices are intolerable—and unconstitutional. In *Riley*, the Court correctly held that, if privacy is to mean anything, it should protect individuals from being monitored without their consent, without a reason, and without a warrant. It is the beginning of principled change and enhanced protections for civil liberties in the digital age.

[91] *Id.* at 2495.

[92] *Olmstead*, 277 U.S. at 474 (Brandeis, J., dissenting).