# GET A WARRANT: THE SUPREME COURT'S NEW COURSE FOR DIGITAL PRIVACY RIGHTS AFTER *RILEY V. CALIFORNIA*

ALAN BUTLER*

## INTRODUCTION

The Roberts Court will likely be remembered for its decision to uphold the Affordable Care Act, its same-sex marriage-rulings, and its decisions in First Amendment and corporate-speech cases; but this Court should also be remembered for ushering in the era of digital Fourth Amendment rights. The Court has not only addressed how Fourth Amendment standards will apply to changing communications technologies, it has also gone out of its way to learn and understand how new technologies will affect the balance of power between the government and citizens. We have come a long way from Chief Justice Roberts' question during oral argument in *City of Ontario, California v. Quon*: "[M]aybe everyone else knows this, but what is the difference between a pager and e-mail?"[1]



* Senior Counsel, Electronic Privacy Information Center (EPIC.org); J.D., UCLA School of Law; B.A., *magna cum laude*, Economics, Washington University in St. Louis. I am grateful to everyone who has contributed their time and energy to improving this article, including Nicolle Kownacki, the staff at EPIC, and the editorial staff at the *Duke Journal of Constitutional Law & Public Policy*.

1. Transcript of Oral Argument at 29, City of Ontario, Ca. v. Quon, 560 U.S. 746 (2010) (No. 08-1332). We have also moved past the arguments about a "tiny constable" in Justices Scalia's majority opinion and Justice Alito's concurring opinion in United States v. Jones, 132 S. Ct. 945, 958 (2012) (Alito, J., concurring) (arguing that late-18th-century situations are not analogous to modern cases and rejecting Justice Scalia's contention that it might have been possible to "imagine a case in which a constable secreted himself somewhere in a coach and remained there for a period of time in order to monitor the movements of the coach's owner," quibbling that "this would have required either a gigantic coach, a very tiny constable, or both").

In *Riley v. California*[2] the Court answered—in a unanimous, nine-to-zero decision—the question of whether the police must obtain a warrant prior to searching an individual's cell phone incident to a lawful arrest. The Court said, simply and unequivocally, yes, "get a warrant."[3] Moreover, the Court directly addressed the impact of ever-expanding digital storage, the proliferation of smartphones, and the implications of encryption and access to cloud-based services. The opinion reflected the Court's newfound understanding of modern communications technologies and their impact on civil rights. It stands as one of the strongest and clearest proclamations of Fourth Amendment rights in the Court's history.

This article will explore the implications of the *Riley* decision on future Fourth Amendment cases, including cases challenging the bulk collection of telephone metadata. The article will review the background of *Riley* and the search-incident-to-arrest doctrine, and describe the new categorical rule adopted by the Court. The article will then consider how the *Rile*y decision will affect lower court rulings on important Fourth Amendment issues: the scope of the search-incident-to-arrest and border-search exceptions, whether the collection of metadata and location information is a search, and the rules governing seizure of electronic records.

## I. THE COURT'S DECISION IN *RILEY*

On June 25, 2014, the Supreme Court issued a unanimous opinion in companion cases *Riley v. California* and *United States v. Wurie*, written by Chief Justice Roberts with a concurring opinion by Justice Alito. Both cases presented the question of whether "the police may, without a warrant, search digital information on a cell phone seized from an individual who has been arrested."[4] The Court ultimately held that the warrantless search of a cell phone seized during a lawful arrest was unreasonable and violated the Fourth Amendment.

The two cases arose from slightly different factual circumstances. In *Riley v. California*, the defendant, David Leon Riley, was arrested for "possession of concealed and loaded firearms" in his car, uncovered by police during a traffic stop.[5] Riley was searched incident to the arrest and officers seized several items in his possession,

2. 134 S. Ct. 2473 (2014).
3. *Id.* at 2495.
4. *Id*. at 2480.
5. *Id*.

including the cell phone in his pocket.[6] Both sides agreed that Riley's phone was a "smart phone."[7] A detective later "went through" the defendant's cell phone at the police station "looking for evidence" of gang-related activity.[8] Several videos and photographs from the phone were introduced as evidence in a criminal case about an unrelated shooting that took place several weeks earlier.[9] Specifically, the State of California introduced photos and videos taken from the phone as evidence that Riley "committed those crimes for the benefit of a criminal street gang, an aggravating factor that carries an enhanced sentence."[10]

Riley moved to suppress the evidence obtained from his cell phone, arguing that it was the fruit of an unreasonable warrantless search that violated his Fourth Amendment rights.[11] The trial court denied his motion to suppress, and he was subsequently convicted. The California Court of Appeals affirmed the decision, relying on a recent opinion, *People v. Diaz*,[12] from the California Supreme Court, which had held that an officer could search an arrestee's cell phone incident to arrest if the phone was "immediately associated with the arrestee's person."[13] Riley petitioned for review by the California Supreme Court, which was denied, and he subsequently filed a Petition for a Writ of Certiorari to the United States Supreme Court, which was granted on January 17, 2014.[14]

In *United States v. Wurie*, the defendant, Brima Wurie, was arrested after a police officer observed him making "an apparent drug sale from a car."[15] The officers later seized two cell phones from Wurie at the police station.[16] The phone at issue was a "flip phone" and thus did not have the same advanced capabilities as the smart phone at issue in *Riley*.[17] After the officers seized Wurie's phone, they noticed that it was receiving numerous calls from a

6. *Id*.
7. The Court defined this as "a cell phone with a broad range of other functions based on advanced computing capability, large storage capacity, and Internet connectivity." *Id*.
8. *Id*. at 2480–81.
9. *Id*. at 2481.
10. *Id*.
11. *Id*.
12. 244 P.3d 501 (Cal. 2011).
13. *Id*. at 93.
14. 134 S. Ct. 999 (2014) (granting certiorari).
15. *Riley*, 134 S. Ct. at 2481. Both *Riley* and *Wurie* were decided in the same opinion here denominated simply as "Riley v. California."
16. *Id*.
17. *Id*.

contact labeled "my home" according to the external call indicator.[18] The officers opened the phone and went through the call logs and contacts in order to identify the phone number designated as "my home."[19] They also saw a photograph of "a woman and a baby set as the phone's wallpaper."[20] Using an online directory, the officers were able to use the phone number to obtain Wurie's address.[21] Based on that address, officers obtained a warrant to search his apartment, where they discovered drugs, paraphernalia, cash, a firearm, and ammunition.[22]

Wurie was charged with drug and firearm-related crimes, but he moved to suppress the evidence, arguing that it was the "fruit of an unconstitutional search of his cell phone."[23] The district court denied his motion and he was later convicted.[24] A divided panel of the United States Court of Appeals for the First Circuit subsequently reversed the trial court decision, finding that cell phones are "distinct from other physical possessions that may be searched incident to arrest without a warrant."[25] The United States filed a Petition for a Writ of Certiorari, which was granted, along with the Petition in *Riley*, on January 17, 2014.[26]

### *A. The Search-Incident-to-Arrest Exception*

As the Court noted at the outset, the "ultimate touchstone of the Fourth Amendment is 'reasonableness.'"[27] Under the reasonableness standard, a search "undertaken by law enforcement officials to discover evidence of criminal wrongdoing" generally requires "the obtaining of a judicial warrant."[28] A warrantless search is only reasonable "if it falls within a specific exception to the warrant requirement."[29] One such exception is a search "of the accused when legally arrested to discover and seize the fruits or evidences of

18. *Id*.
19. *Id*.
20. *Id*.
21. *Id*.
22. *Id*.
23. *Id*. at 2482.
24. *Id*.
25. *Id*.
26. 134 S. Ct. 999 (2014) (granting certiorari).
27. *Riley*, 134 S. Ct. at 2482 (quoting Brigham City, Utah v. Stuart, 547 U.S. 398, 403 (2006)).
28. *Id.* (quoting Veronia School Dist. 47J v. Acton, 515 U.S. 646, 653 (1995)).
29. *Id*.

crime."[30]

The Court's decision in *Riley* is the most recent in a long line of cases outlining the boundaries of the search-incident-to-arrest exception. The Court previously established the boundaries of this exception in three cases: *Chimel v. California*,[31] *United States v. Robinson*,[32] and *Arizona v. Gant*.[33] In *Chimel*, the Court held that there was "ample justification . . . 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."[34] The justification for this exception was twofold: (1) to protect the arresting officer and prevent escape, and (2) to prevent the concealment or destruction of evidence.[35]

The Court later clarified this rule in *Robinson*, finding that the physical inspection of an object discovered during the search of the arrestee's person is permissible, regardless of "the probability in a particular arrest situation that weapons or evidence would in fact be found upon the person of the suspect."[36] As the Court noted in *Robinson*, this rule was largely pragmatic: "A police officer's determination as to how and where to search the person of a suspect whom he has arrested is necessarily a quick ad hoc judgment which the Fourth Amendment does not require to be broken down in each instance into an analysis of each step in the search."[37] For more than twenty years after *Robinson*, lower courts applied few limitations on the scope of searches within the "zone of immediate control" of an arrestee.[38] Then in *Gant*, the Court applied the *Chimel* rule to the search of a vehicle and found that police could search a vehicle under the exception "only when the arrestee is unsecured and within reaching distance of the passenger compartment at the time of the search."[39] However, the Court found that a separate exception would

30. *Id*. (quoting Weeks v. United States, 232 U.S. 383, 392 (1913)).
31. 395 U.S. 752 (1969).
32. 414 U.S. 218 (1973).
33. 556 U.S. 332 (2009).
34. *Chimel*, 395 U.S. at 762–63.
35. *Id.*
36. *Robinson*, 414 U.S. at 235.
37. *Id*.
38. The Court clarified in *Chadwick* that the *Robinson* rule did not apply to physical containers that were not "immediately associated with the person of the arrestee." United States v. Chadwick, 433 U.S. 1, 15 (1977) (holding a locked footlocker could not be searched incident to arrest).
39. Arizona v. Gant, 556 U.S. 332, 343 (2009).

allow for the search of a vehicle "when it is 'reasonable to believe evidence related to the crime of arrest might be found in the vehicle.'"[40]

Prior to *Riley*, lower courts applying the *Chimel* and *Robinson* rules were split over whether the exception permitted officers to search photos, call logs, messages, and other data stored on a cell phone. Some courts viewed this as a straightforward application of *Robinson*—any phone found within the arrestee's zone of control could be searched and inspected without further justification.[41] But other courts disagreed, finding that the *Chimel* justifications were not applicable to the search of digital files stored on a cell phone—those files did not pose a threat to the officer and there was no risk of loss of evidence once the phone had been secured.[42] The Court in *Riley* was faced with a clear question: should modern cell phones be treated differently than other objects in the search-incident-to-arrest doctrine and, if so, why?

### *B. The New Digital Rule*

The Court's unanimous opinion in *Riley* answered the narrow question as clearly and forcefully as possible: yes, cell phones must be subject to different rules than other physical objects within the search-incident-to-arrest exception.[43] Whereas the default rule for inspection of physical objects under *Robinson* had been that no warrant is required for a physical search incident to arrest,[44] the default rule for searches of cell phones under *Riley* is "get a warrant."[45] But what is most interesting about *Riley* is the Court's

40. *Id*. (citing Thornton v. United States, 541 U.S. 615, 632 (2004) (Scalia, J., concurring in the judgment)).

41. Three courts prior to *Riley* had held that cell phone searches incident to arrest were categorically permitted under the *Robinson* rule. *See* United States v. Murphy, 552 F.3d 405, 411–12 (4th Cir. 2009); United States v. Finley, 477 F.3d 250, 259–60 (5th Cir. 2007), *cert. denied*, 549 U.S. 1353 (2007); People v. Diaz, 244 P.3d 501, 510 (Cal. 2011), *cert. denied*, 132 S. Ct. 94 (2011). Three other courts had ruled that certain files on a cell phone could be searched incident to arrest, without reaching the question of whether other types of files could be subject to search. *See* United States v. Flores-Lopez, 670 F.3d 803 (7th Cir. 2012) (search to obtain the phone number of the seized cell phone); Commonwealth v. Phifer, 979 N.E.2d 210, 216 (Mass. 2012) (search of recent call list); Hawkins v. State, 723 S.E.2d 924, 926 (Ga. 2012) (search of text messages limited in scope).

42. *See*, *e.g.*, United States v. Wurie, 728 F.3d 1, 11 (1st Cir. 2013); Smallwood v. State, 113 So. 3d 724, 735–36 (Fla. 2013); State v. Smith, 920 N.E.2d 949, 956 (Ohio 2009), *cert. denied*, 131 S. Ct. 102 (2010).

43. *Riley*, 134 S.Ct. at 2490–91.

44. *Robinson*, 414 U.S. at 235.

45. *Riley*, 134 S. Ct. at 2495.

clear articulation of the important differences between Fourth Amendment protections for digital devices, as opposed to physical objects, because this reasoning will likely be applied to evaluating searches affecting a wide range of new technologies.

At the outset, the Court acknowledged that the application of the search-incident-to-arrest doctrine to cell phones is significant because these devices "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[46] The Court went on to recognize the evolution and widespread adoption of cell phones and more sophisticated smartphones that are "based on technology nearly inconceivable just a few decades ago, when *Chimel* and *Robinson* were decided."[47]

As a result of these technological changes, the Court found it necessary to evaluate the cell phone search issue as a possible new exception to the warrant requirement. Rather than applying Robertson directly, the Court approached the issue "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 interests."[48] As the Court noted, the balancing of interests in *Robinson* favored a "categorical rule" exempting all physical searches conducted incident to arrest, but "neither of its rationales has much force with respect to digital content on cell phones."[49] The Court proceeded to describe the key difference between the physical and digital search cases: "Cell phones, however, place vast quantities of personal information literally in the hands of individuals. A search of information on a cell phone bears little resemblance to the type of brief physical search considered in *Robinson*."[50]

46. *Id*. at 2484.

47. *Id*. This is a key point: the Court's old precedents, adopted prior to the development of this new technology, are not directly applicable to the current situation.

48. *Id*. (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999)).

49. *Id*. Specifically, the Court was not convinced that, absent an immediate, warrantless search of cell-phone content, that officer safety would be threatened, or that digital evidence would be destroyed. *Riley*, 134 S. Ct. at 2485–88.

50. *Riley*, 134 S. Ct. at 2485.

### *C. Strong Privacy Interests in Digital Data*

After reviewing the governmental interests at stake in the search-incident-to-arrest context, the Court went on to consider the privacy interests at stake when officers search an arrestee's cell phone.[51] The Court found that cell phones are different "both in a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person."[52] The Court also recognized that most modern devices "are in fact minicomputers that also happen to have the capacity to be used as a telephone."[53] In sum, the "immense storage capacity" of the devices combined with their multifunctional nature fundamentally alters the privacy interests at stake. This portion of the Court's opinion in *Riley*, more than any other, will likely be remembered as a foundational invocation of digital Fourth Amendment rights.

To support its conclusion that digital devices are fundamentally different than physical objects, the Court first addressed the practical limits of physical searches. Those searches had traditionally been "limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy."[54] But unlike physical containers, cell phones can contain "millions of pages of text, thousands of pictures, and hundreds of videos."[55] Phones can also store unique data, such as internet browsing history, that never exists in physical form. The Court also predicted that "this gulf between physical practicability and digital capacity will only continue to widen in the future."[56]

The Court went on to address the "interrelated consequences for privacy" of the increasing storage capacity of mobile devices.[57] The Court found it significant that increased storage capacity enables the consolidation of many different types of information, which could "reveal much more in combination than any isolated record."[58] The Court also noted that the aggregation of photos or other files, along

51. *See id*. at 2489 (noting 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").
52. *Id*.
53. *Id*.
54. *Id*.
55. *Id*.
56. *Id*.
57. *Id*.
58. *Id*.

with timestamps and associated metadata, would reveal a great deal more than individual physical items ever could.[59] Similarly, the archival nature of stored data, providing a record that traces back to the purchase of the phone and potentially beyond, makes a search of the digital device much more invasive than a search of a physical object.[60] And finally, the Court concluded that the pervasiveness of modern cell phones, which most users now carry with them at all times, means that the privacy cost of allowing routine searches of cell phones is much greater than the cost of "allowing them to search a personal item or two in the occasional case."[61]

The Court went on to emphasize that highly sensitive records are now routinely stored on mobile phones, and that these records are "qualitatively different" from what would have been available during a physical search. The Court found that the highly sensitive data includes "Internet search and browsing history," "[h]istoric location information," "transaction records," as well as data from a variety of new mobile "apps" that relate to private activities and interests.[62] Cell phones contain such a wealth of data, the Court reasoned, that "a cell phone search would typically expose the government to far *more* than the most exhaustive search of a house."[63] Cell phones also provide access to sensitive personal information stored on remote servers, and law enforcement would have no clear way to distinguish between locally and remotely stored data.[64]

59. *Id*. ("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.").

60. *Id*.

61. *Id*. at 2490.

62. *Id*. ("Mobile 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. There are apps for Democratic Party news and Republican Party news; apps for alcohol, drug, and gambling addictions; apps for sharing prayer requests; apps for tracking pregnancy symptoms; apps for planning your budget; apps for every conceivable hobby or pastime; apps for improving your romantic life.").

63. *Id*.

64. *Id*. at 2491. *See also* Brief of Amicus Curiae Electronic Privacy Information Center (EPIC) And Twenty-Four Technical Experts And Legal Scholars In Support Of Petitioner at 12–14, 20, Riley v. California, 134 S. Ct. 2473 (2014) (Nos. 13-132, 12-212), 2014 WL 975497 at *12–14, 20 [hereinafter EPIC Amicus Brief].

### *C. General Warrants and the Broad View of Fourth Amendment Rights*

Before reaching its final conclusion, the Court considered the various "fallback" positions offered by the United States and California.[65] The Court rejected these alternative standards because it found that they would impose no meaningful limitations on cell phone searches and would be impractical to administer. In this regard, the Court preferred to adopt a rule "done on a categorical basis—not in an ad hoc, case-by-case fashion by individual police officers."[66]

The Court concluded by addressing the likely impact of its decision and the importance of the underlying constitutional interest that it will serve.[67] The Court acknowledged that its decision "will have an impact on the ability of law enforcement to combat crime,"[68] but also that, "[p]rivacy comes at a cost."[69] The warrant requirement is "not merely 'an inconvenience to be somehow weighted against the claims of police efficiency.'"[70] Rather, the Court recognized, the Fourth Amendment is a critical safeguard, "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."[71]

If there was any question about the breadth of the Court's opinion in *Riley*, it was answered by the Court's sweeping quotation of *Boyd v. United States*[72] in the final paragraphs of the opinion.[73] The Court noted that opposition to warrantless searches "was in fact one of the

65. *Id*. at 2491–93. The United States proposed that the Court adopt the "*Gant* standard" and allow officers to search cell phones "whenever it is reasonable to believe that the phone contains evidence of the crime of arrest." *Id*. at 2492. The United States alternatively proposed an officer should be allowed to search the phone when she "reasonably believes that information relevant to the crime, the arrestee's identity, or officer safety will be discovered." *Id*. And finally, the United States suggested that officers should at least be allowed to search an arrestee's cell phone "call log." *Id*. at 2492–93. California suggested "a different limiting principle, under which officers could search cell phone data if they could have obtained the same information in a pre-digital counterpart." *Id*. at 2493.

66. *Id*. at 2492 (quoting Michigan v. Summers, 452 U.S. 692, 705 n.19 (1981)).

67. *Riley*, 134 S. Ct. at 2493–94.

68. *Id*. at 2493.

69. *Id*.

70. *Id*. (quoting Coolidge v. New Hampshire, 403 U.S. 443, 481 (1971)).

71. *Id*. at 2494.

72. 116 U.S. 616, 625 (1886) (quoting John Adams's account of James Otis's speech, "'Then and there,' said John Adams, 'then and there was the first scene of the first act of opposition to the arbitrary claims of Great Britain. Then and there the child Independence was born'").

73. *See Riley*, 134 S. Ct. at 2494.

driving forces behind the [American] Revolution," and that John Adams had described a speech by James Otis decrying writs of assistance as "the first scene of the first act of opposition to the arbitrary claims of Great Britain. Then and there the child Independence was born."[74] The Court then emphasized that, "Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life.'"[75] The Court's decision in *Riley* is based on a recognition that these digital devices are as deserving of protection as our homes and private spaces, if not more so.

The *Riley* decision will have important implications for future Fourth Amendment cases, especially search-incident-to-arrest cases, electronic-search-and-seizure cases, and metadata cases. The effects of the Court's decision will be immediate and most substantial in search-incident-to-arrest cases, but could support significant doctrinal changes in electronic-search-and-seizure as well as metadata-surveillance cases. In particular, *Riley* could influence the outcome of two major Fourth Amendment issues being considered by state and federal courts: whether (1) the collection of location records or (2) the bulk collection of call detail records constitute a "search" under the Fourth Amendment.

## II. SEARCH-INCIDENT-TO-ARREST CASES POST-*RILEY*

The Court's decision in *Riley* will have the most obvious and immediate impact on future search-incident-to-arrest cases. Lower courts were previously divided over the question presented in *Riley*,[76] but now the Supreme Court has made clear that officers must obtain a warrant, absent exigent circumstances, prior to searching a cell phone that is seized during an arrest.[77] However, there are still several related issues that lower courts will have to sort out in future cases.[78]

First, lower courts will have to decide whether there are exigent circumstances that would justify an officer's failure to obtain a warrant prior to searching an arrestee's cell phone. Several of the

74. *Id*. (quoting *Boyd*, 116 U.S. at 625).
75. *Id*. at 2494–95 (quoting *Boyd*, 116 U.S. at 630).
76. *See* cases cited *supra* notes 41–42.
77. *Riley*, 134 S. Ct. at 2493.
78. This article will not discuss the application of the good faith exception in post-*Riley* cases. For a discussion of the good faith exception, *see generally* Susan Freiwald, *The Davis Good Faith Rule and Getting Answers to the Questions Jones Left Open*, 14 N.C. J. L. & TECH. 341 (2013).

hypothetical concerns outlined by the State of California and the Solicitor General in their briefs before the Court might be reframed as exigent circumstances if they have a factual basis in a particular case. These include: threat of the destruction of data and risks to officer safety due to an arrestee's communications with an accomplice. However, the Court was quick to dismiss these arguments in *Riley* due to their lack of factual basis, and there is currently no evidence showing that these concerns are present in real world cases. It would be difficult for an officer to establish some real threat of injury or loss of evidence in most cases.

Second, lower courts will likely have to apply the *Riley* rule in search incident to arrest cases involving the seizure of computers and other electronic devices. This will be the most straightforward application of the *Riley* decision. The Court's opinion made clear that modern phones are computers, and provided no basis to distinguish between different types of digital devices.[79] The Court also explicitly adopted a categorical rule, rejecting the government's proposal for a case-by-case approach to evaluating searches incident to arrest involving digital devices.[80] And even before the Court issued its decision in *Riley*, lower courts had been treating cell phones and computers as indistinguishable for the purposes of the search-incident-to-arrest analysis.[81] Thus, any court considering a search incident to arrest involving a computer or other digital device will almost certainly apply the *Riley* categorical rule.

Thirdly, lower courts will also likely consider the implications of *Riley* in cases involving exceptions to the warrant requirement that are similar, but not identical to, the search-incident-to-arrest exception. In particular, lower courts will have to decide how *Riley* impacts border search and seizure cases involving digital devices. Under the border search doctrine, as established by the Court in *United States v. Ramsey*,[82] a warrant is typically not required for a search conducted at the border, and such searches have been deemed

79. *Riley*, 134 S. Ct. at 2489.

80. *Id*. at 2491–92.

81. *See*, *e.g.*, United States v. Flores-Lopez, 670 F.3d 803, 805–06 (7th Cir. 2012) ("Judges are becoming aware that a computer (and remember that a modern cell phone is a computer) is not just another purse or address book."); United States v. Phillips, 9 F. Supp. 3d 1130, 1141 (E.D. Cal. Mar. 25, 2014) ("A modern cell phone is a computer . . . ." (quoting *Wurie*, 728 F.3d at 8)); Smallwood v. State, 113 So. 3d 724, 735 (2013) ("[T]he search of Smallwood's computer-like device violated the Fourth Amendment.")).

82. United States v. Ramsey, 431 U.S. 606 (1977).

"reasonable simply by virtue of the fact that they occur at the border."[83] However, the Ninth Circuit recently held in *United States v. Cotterman*[84] that a "forensic examination" of a digital device at the border requires reasonable suspicion.[85] But some courts have not embraced this standard.[86] The Court's reasoning in *Riley*, that searches of digital devices implicate significant privacy interests, could provide a basis for lower courts to adopt the *Cotterman* rule in future border search cases.

For example, in *United States v. Saboonchi*,[87] the United States District Court for the District of Maryland considered the impact of the *Riley* decision on its earlier ruling on the scope of Fourth Amendment protections for cell phones and other devices at the border. In the earlier holding, the court adopted a *Cotterman*-like rule that "forensic" searches of cell phones and other devices at the border can only be conducted based on reasonable suspicion.[88] The court's definition of a "forensic search,"[89] differed somewhat from the definition in *Cotterman*, but the rule it adopted was essentially the same. The defendant in *Saboonchi* moved for a reconsideration of that decision after *Riley*, arguing that the court should adopt a categorical warrant requirement for searches of cell phones at the border.[90] The court in *Saboonchi* ruled that its "forensic search" rule was supported by the Court's findings in *Riley*, about the increased privacy interests in digital data, but that the *Riley* decision did not overturn the "long history of the border search doctrine" cases that have declined to impose any standard higher than reasonable suspicion.[91] This ruling is consistent with the view that the Court's

83. *Id*. at 616.

84. United States v. Cotterman, 709 F.3d 952 (9th Cir. 2013).

85. *Id*. at 967–68.

86. *See* Abidor v. Napolitano, 990 F. Supp. 2d 260, 282 (E.D.N.Y. 2013) ("I would agree with the Ninth Circuit that, if suspicionless forensic computer searches at the border threaten to become the norm, then some threshold showing of reasonable suspicion should be required. Now, however, 'locking in a particular standard for searches would have a dangerous, chilling effect as officer's often split-second assessments are second guessed.'").

87. United States v. Saboonchi, No. PWG–13–100, 2014 WL 3741141 (D. Md. Jul. 28, 2014) [*Saboonchi II*].

88. United States v. Saboonchi, 990 F. Supp. 2d 536, 569 (D. Md. 2014).

89. *Id*. ("I also do not define a forensic search in terms of the amount of data that is recovered, thereby leaving the status of a given search to be resolved later by Customs officers. *Cf. Cotterman,* 709 F.3d at 967. A forensic search is a different procedure, fundamentally, from a conventional search. It occurs when a computer expert creates a bitstream copy and it analyzes it by means of specialized software.").

90. *Saboonchi II*, 2014 WL 3741141 at *4.

91. *Id*.

reasoning in *Riley* supports the adoption of a reasonable suspicion standard for forensic searches at the border, similar to the rule articulated by the Ninth Circuit in *Cotterman*.

Finally, lower courts will face cases where searches incident to arrest lead to the seizure of unique physical objects and quasi-digital devices. The application of *Riley* in those cases could prove difficult. For example, the federal district court for the Northern District of Illinois recently analyzed the reasonableness of Drug Enforcement Agency (DEA) searches following an initial stop and seizure of the defendant's vehicle in *United States v. Correa*.[92] The court in *Correa* considered whether the recent Supreme Court decisions in *United States v. Jones*[93] and *Florida v. Jardines*[94] provided a basis to find that the use of seized garage door openers and keys to identify the defendant's apartment was a "search" under the Fourth Amendment.[95]

In *Correa*, the officers "discovered a bag on the front passenger seat" of the defendant's vehicle "containing four garage door openers, three sets of keys, and four cell phones."[96] The officers subsequently drove through the surrounding neighborhood testing the garage door openers until one of the devices opened the garage of an apartment building.[97] The officers then used the key fob from the bag to gain access to the lobby of the apartment building and tested the keys from the bag on various mailboxes until they found one that matched.[98] The officers searched the apartment with the defendant's consent, and discovered contraband and other evidence that was ultimately used to convict him.[99]

In analyzing the defendant's motion to suppress the evidence found in the apartment, the court considered whether the use of electronic garage door openers to identify the defendant's apartment building constituted a search. In a prior decision (pre-*Jardines*), the court in *Correa* had denied the motion and found that the facts were

92. United States v. Correa, No. 11-cr-0750, 2014 WL 1018236 (N.D. Ill. Mar. 14, 2014). The search of the defendant's vehicle in *Correa* was technically a consent search, but the circumstances were similar to a search incident to arrest.

93. 132 S. Ct. 945 (2012).

94. 133 S. Ct. 1409 (2013).

95. *Correa*, 2014 WL 1018236 at *3.

96. *Id*. at *1.

97. *Id*.

98. *Id*. at *2.

99. *Id*.

analogous to those considered by the Seventh Circuit in *United States v. Concepcion*.[100] The officers in *Concepcion* used keys seized from the defendant to enter his apartment building and tested the keys on various doors until they found a match to his apartment.[101] The court in *Concepcion* concluded that the use of the key to test the defendant's apartment door was a "search," but that "the privacy interest at issue was so small, the agents did not need a warrant (or even probable cause) to conduct the search."[102] The court in *Correa* rejected the defendant's argument that the use of the garage door opener was meaningfully different from the use of the key in *Concepcion* or the use of other investigative techniques to identify the defendant's apartment building.[103]

The court specifically rejected the defendant's argument in *Correa* that the use of the garage opener was equivalent to a digital "trespass," which would make it a search under *Jones* and *Jardines*.[104] The court distinguished the facts in *Correa* from those cases on the grounds that the garage door opener had been lawfully seized incident to arrest, citing the Seventh Circuit's recent cell phone search incident to arrest case.[105]

> In Correa's case, even if [the DEA Agent] "searched" the garage door openers by pressing their buttons to see if they worked, he did so after lawfully seizing the garage door openers as evidence. For that reason, this case is much more like *United States v. Flores–Lopez* . . . a case decided by the Seventh Circuit after *Jones,* and on facts more analogous to Correa's case.[106]

But the Supreme Court rejected that premise in *Riley*, finding that the categorical rule used by the Seventh Circuit and other courts was not valid in the context of digital devices.[107] The question now is would *Riley* support a different outcome in cases like *Correa*? One portion of the Court's opinion in *Riley* seems to indicate that it might.

---

100. United States v. Correa, No. 11-cr-0750, 2013 WL 5663804, at *5–6 (N.D. Ill. Oct. 17, 2013) (citing United States v. Concepcion, 942 F.2d 1170, 1172–73 (7th Cir. 1991)).

101. *Concepcion*, 942 F.2d at 1171.

102. *Id*. at 1173.

103. *Correa*, 2014 WL 1018236 at *6. The court also noted in a footnote that although the defendant did not challenge the use of the electronic key fob to enter the apartment building, they saw "no real distinction between the use of a metal key and an electronic one." *Id*. at *5 n.1.

104. *Id*. at *3.

105. *Id*.

106. *Id*. (citing United States v. Flores-Lopez, 670 F.3d 803 (7th Cir. 2012)).

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

As the Court noted in *Riley*, the search of an arrestee's cell phone is necessarily broader than the search of physical objects found on his person because cell phones now routinely provide access to remotely stored files.[108] Allowing the officer to search remote files from the phone, the Court noted, would be "like finding a key in a suspect's pocket and arguing that it allowed law enforcement to unlock and search a house."[109] Yet that is almost exactly what the lower courts allowed in *Correa* and *Concepcion*. The question for future courts will be whether the combination of *Jones*, *Jardines*, and *Riley* prohibits the use of electronic keys and other devices in ways that reach to the level of "trespass."

## III. THE IMPACT OF *RILEY* ON THE NSA METADATA CASES

Perhaps the most interesting and controversial question raised after the Court's decision in *Riley* is what impact, if any, the decision will have on pending challenges to the National Security Agency's (NSA) bulk collection of telephone call records under section 215 of the USA PATRIOT Act[110] (the metadata cases). Plaintiffs in the metadata cases have already argued that the *Riley* decision supports the adoption of a new Fourth Amendment rule governing the collection of call detail records and other metadata, including cell phone location data.[111] The government's primary argument in these cases has been that the collection of non-content information held by third party telephone providers is not a "search" under the Fourth Amendment, based on the Supreme Court's ruling in *Smith v. Maryland*.[112] Courts must now decide whether *Smith*, a case decided in the pre-digital era, provides a basis for rejecting privacy interests in phone and internet metadata in the present day. The Supreme Court's decision in *Riley* did not directly address that question,[113] but the Court's reasoning provides strong support for a new approach to analyzing metadata searches under the Fourth Amendment.

---

108. *See id*. (citing EPIC Amicus Brief, *supra* note 64, at 12–14, 20).

109. *Id*.

110. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-58, 2001, § 215, 115 Stat. 272, 287–88 (2001) (codified at 50 U.S.C.A. § 1861).

111. *See*, *e.g.*, Appellant's Opening Brief, Smith v. Obama, No. 14-35555, at 30–31 (9th Cir. filed Sept. 2, 2014).

112. 442 U.S. 735 (1979).

113. *See Riley,* 134 S. Ct. 2473.

### *A. The DOJ Argument in Favor of Bulk Metadata Collection*

There are three major cases arising from challenges to the NSA's bulk collection of telephone metadata currently pending before federal appellate courts: *Klayman v. Obama* (D.C. Circuit),[114] *American Civil Liberties Union v. Clapper* (2nd Circuit),[115] and *Smith v. Obama* (9th Circuit).[116] The NSA Metadata Program, at issue in these cases, is conducted pursuant to orders by the Foreign Intelligence Surveillance Court (FISC).[117] These FISC orders have been issued based on applications filed by the Federal Bureau of Investigation (FBI) for "Certain Tangible Things for Investigations to Protect Against International Terrorism."[118]

Under section 215 of the PATRIOT Act,[119] the FBI may apply for an order for "the production of business records and tangible things" when it has "reasonable grounds to believe that the tangible things are relevant to an authorized investigation" to protect against international terrorism.[120] The Business Record (BR) Orders issued by the FISC in the metadata cases require telephone companies to conduct "ongoing daily production to the [NSA] of certain call detail records or 'telephony metadata' in bulk."[121] Call detail records include the time, duration, and numbers dialed and received for every call, as well as other identifying and routing information.[122] These FISC BR Orders have been issued to major telephone carriers on an ongoing basis since at least 2006.[123] Plaintiffs in all three cases are Verizon

114. No. 14-50005 (D.C. Cir. filed Jan. 9, 2014).

115. No. 14-42 (2nd Cir. filed Jan. 6, 2014).

116. No. 14-35555 (9th Cir. filed Jul. 1, 2014).

117. *See* In re Application of the FBI for an Order Requiring the Production of Tangible Things from [REDACTED], No. BR 13-109, 2013 WL 5741573 (FISC Aug. 29, 2013) [hereinafter Eagan Opinion].

118. These applications are filed pursuant to 50 U.S.C.A. § 1861(a) (West 2014).

119. Codified at 50 U.S.C.A § 1861 et seq.

120. 50 U.S.C.A. § 1861(b)(2)(A). The FBI can also seek an order for tangible things relevant to "obtain foreign intelligence information not concerning a United States person" or to protect against "clandestine intelligence activities." *Id.*

121. Eagan Opinion, *supra* note 117, at *1.

122. As the FISC defines it, "telephony metadata" includes "comprehensive communications routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number, International Mobile station Equipment Identity (IMEI) number, International Mobile Subscriber Identity (IMSI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call." *Id.* at *2 n.2.

123. *See*, *e.g.*, Eagan Opinion, *supra* note 117. In June of 2013, an unredacted BR Order was published by the Guardian, revealing that Verizon Business Network Services was a recipient of one of these BR Orders in 2013. *See* Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN (June 6, 2013),

customers[124] who allege that their call detail records have been collected under this program in violation of their Fourth Amendment rights.

In response, the Government has argued that (1) plaintiffs lack standing to challenge the bulk collection of domestic telephone records by the NSA, (2) federal district courts do not have the authority to override the FISC determination that the FBI applications satisfied the statutory requirements of 50 U.S.C. § 1861, and (3) the plaintiffs' challenges are foreclosed by the Supreme Court's decision in *Smith v. Maryland*.[125] It is the last argument that is most likely to be impacted by the Court's recent decision in *Riley*.

The Government's Fourth Amendment arguments are essentially the same in the three metadata cases[126]: collection of domestic call detail records pursuant to FISC BR Orders does not violate plaintiffs' Fourth Amendment rights because (1) under *Smith v. Maryland* plaintiffs have no "reasonable expectation of privacy" in call data sent to a phone company; (2) the telephone metadata records collected by the NSA do not contain sensitive information; and (3) the post-collection use limitations imposed by the FISC are sufficient to protect user privacy interests.[127] But the Court's decision in *Riley* undercuts all three of these arguments.

---

http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order. Senator Diane Feinstein later confirmed that Verizon, AT&T, and Sprint have all received BR Orders on an ongoing basis since 2006. Dan Roberts & Spencer Ackerman, *Senator Feinstein: NSA Phone Call Data Collection in Place 'Since 2006'*, THE GUARDIAN (June 6, 2013), http://www.theguardian.com/world/2013/jun/06/court-order-verizon-call-data-dianne-feinstein.

124. The Plaintiffs in *Klayman* and *Smith* are Verizon Wireless customers, which complicates matters somewhat because the FISC BR Order disclosed last year was directed to Verizon Business Network Services, a subsidiary of Verizon Communications that was acquired during the 2006 acquisition of MCI. *See Company Overview of Verizon Business Network Services*, BLOOMBERG BUSINESSWEEK, http://investing.businessweek.com/research/stocks/private/snapshot.asp?privcapid=4259068 (last visited Jan. 20, 2015). The Government has already argued in the *Smith* case that the plaintiff cannot prove her metadata was collected. *See* Brief of the United States, Smith v. Obama, No. 14-35555, at 38 (9th Cir. filed Oct. 2, 2014) ("But there is no evidence in the record that the government has acquired metadata from Verizon Wireless under the Section 215 program, let alone that it would do so in the imminent future.").

125. *See* Brief for the Appellees, Smith v. Obama, No. 14-35555 (9th Cir. filed Oct. 2, 2014); Government Appellants' Opening Brief, Klayman v. Obama, Nos. 14-4004, 14-5005, 14-5016, 14-5017 (D.C. Cir. filed July 14, 2014); Brief for Defendants-Appellees, ACLU v. Clapper, No. 14-42 (2nd Cir. filed Apr. 10, 2014), 2014 WL 1509706.

126. *See* cases cited *supra* notes 115–117. All three briefs use the same structure (the language in the *Smith* brief is slightly different, but the substance is the same).

127. *See*, *e.g.*, Brief for Defendant-Appellees at 41–47, ACLU v. Clapper, No. 14-42 (2nd Cir. Filed Apr. 10, 2014), 2014 WL 1509706 at *41–47.

### *B. Application of Riley in the Metadata Cases*

The Court in *Riley* did not directly address whether the collection of telephone metadata in bulk from a service provider would constitute a "search" under the Fourth Amendment. In fact, in the soon-to-be-infamous Footnote 1, the Court explicitly noted that it had *not* addressed that issue in *Riley*.[128] But the Court's reasoning may very well prove persuasive to lower courts deciding the metadata cases. In each of these cases the courts will consider (1) whether the "third party" rule established in *Smith v. Maryland* still applies in the context of modern telecommunications networks, (2) whether the type of metadata generated and collected today is sensitive enough to trigger increased privacy interests, and (3) whether post-collection rules limiting the use of collected metadata alter the Fourth Amendment analysis.

#### 1. *Smith v. Maryland*, like *Robinson*, Could Be Overturned Because of Changes in Technology.

Lower courts faced with this question may very well depart from the *Smith v. Maryland* doctrine based on changes in technology, using the same reasoning as the Court in *Riley*. The Court's opinion made clear that digital communications devices implicate broader privacy interests than do physical objects and other traditional types of records.[129] In particular, the Court found that data stored on cell phones is both quantitatively and qualitatively different from the types of physical objects found on an arrestee's person.[130] The Court also found that the pervasive use of modern cell phones implicates broader privacy interests because allowing access to that data would impact the privacy rights of all Americans.[131]

Similarly, both the type and volume of communications records at issue in the metadata cases are fundamentally different from the pen register[132] records at issue in *Smith v. Maryland*. In *Smith*, the Court considered whether law enforcement's use of a device to record the numbers dialed on the defendant's phone line without a warrant

128. Riley v. California, 134 S. Ct. 2473, 2489 n.1 (2014).
129. *Id*. at 2491.
130. *Id*. at 2489.
131. *Id*. at 2490.
132. The "pen register" used in *Smith v. Maryland* was a "mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released. It does not overhear oral communications and does not indicate whether calls are actually completed." *Smith*, 442 U.S. at 736 n.1.

violated his Fourth Amendment rights.[133] The Court emphasized the "limited capabilities" of the pen register and the limited scope of what it could collect, which was a significant factor in determining whether the defendant had a legitimate expectation of privacy in that information.[134]

Indeed, a law enforcement official could not even determine from the use of a pen register whether any conversation took place. These devices do not hear sound. They disclose only the telephone numbers that have been dialed—a means of establishing the connection. Pen registers in the 1970s did not disclose the purport of any communication between the caller and recipient, their identities, or even whether the call was completed.[135]

The Court concluded that most individuals must be aware they "convey" the phone numbers they dial to the phone company, which may record logs of their calls for billing or other business purposes.[136] But the evolution of communications technologies since 1979 has dramatically expanded both the type of information collected about users by their service providers and the privacy interests at stake in the collection of that data.[137]

2. The Pen Registers Analyzed in *Smith v. Maryland* Collected a Very Limited Amount of Call Data

In order to understand the difference between the call data currently collected by phone companies and the phone records at issue in *Smith v. Maryland*, it is helpful to unpack the Court's accepted definition of pen register in 1979. The Court in *Smith* provided a definition of a pen register in its first footnote, relying on two prior opinions issued in 1977 and 1974.[138] The first was *United States v. New York Telephone Company*,[139] a case arising out of a telephone company's refusal to provide a "leased line" to the FBI in order to facilitate the off-site monitoring of a target phone line via pen register.[140] The telephone company argued that a pen register could

133. *Id*. at 739.
134. *Id*. at 741.
135. *Id*.
136. *Id*. at 742.
137. *See generally* Brief of Amici Curiae Electronic Privacy Information Center (EPIC) and Thirty-Three Technical Experts and Legal Scholars in Support of Appellant, Smith v. Obama, No. 14-35555 (9th Cir. filed on Sept. 9, 2014), 2014 WL 4678192.
138. *Smith*, 442 U.S. at 736 n.1.
139. United States v. N.Y. Tel. Co., 434 U.S. 159 (1977).
140. *Id*. at 161–64.

only be authorized under a Title III Wiretap Order[141] because the use of a pen register would involve "intercepting" wire communications.[142] The Court rejected this contention because it found that pen registers "disclose only the telephone numbers that have been dialed."[143] The Court emphasized that, "[n]either the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers."[144]

The Court's understanding of pen registers in *Smith v. Maryland* and *New York Telephone Co.* was derived from an earlier case, *United States v. Giordano*,[145] a criminal wiretap case where the Court ruled that the evidence should be suppressed because the Attorney General did not properly execute the wiretap applications.[146] Four justices[147] filed an opinion concurring in part, but dissenting regarding the suppression of evidence gathered using a pen register on the grounds that the use of a pen register device was "not governed by Title III."[148] In Justice Powell's dissenting opinion, he described a pen register as a device that "records on a paper tape all numbers dialed from" a target telephone line, but stressed that "[i]t does not identify the telephone numbers from which incoming calls originated, nor does it reveal whether any call, either incoming or outgoing, was completed."[149] Justice Powell noted that the pen register device and its "mechanical complexities" had been described by the district court below.[150]

---

141. Title III, which governs wiretapping and electronic surveillance, was first enacted as part of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C.A. §§ 2510–20 (West 2014), and later modified by the Electronic Communications Privacy Act, 18 U.S.C.A. §§ 2701–2710 (West 2014). Under Title III, certain federal and state agents may apply for an order authorizing the interception of wire or oral communications, and a judge may grant an interception order as provided in 18 U.S.C.A. § 2518. *See generally* WAYNE R. LAFAVE, JEROLD H. ISRAEL, & NANCY J. KING, CRIMINAL PROCEDURE § 4.2 (10th ed. 2000).

142. *N.Y. Tel. Co.*, 434 U.S. at 165–66.

143. *Id*. at 167.

144. *Id*.

145. United States v. Giordano, 416 U.S. 505 (1974).

146. *Id*. at 533.

147. Justice Powell, Chief Justice Berger, Justice Blackmun, and Justice Rehnquist.

148. Giordano, 416 U.S. at 503–04 (Powell, J., concurring in part and dissenting in part).

149. *Id*. at 549 n.1 (Powell, J., concurring in part and dissenting in part). Other lower court decisions also emphasize the fact that a pen register was not designed to detect whether or when a call had been completed. *See*, *e.g.*, United States v. Caplan, 255 F. Supp. 805, 807 (E.D. Mich. 1966) ("With reference to incoming calls, the pen register records only a dash for each ring of the telephone but does not identify the number from which the incoming call originated. The pen register cuts off after the number is dialed on outgoing calls and after the ringing is concluded on incoming calls without determining whether the call is completed or the receiver is answered.").

150. *Id*. (Powell, J., concurring in part and dissenting in part). The district court opinion is United States v. Focarile, 340 F. Supp. 1033 (D. Md. 1972).

As the lower court described, a pen register device at that time was nothing more than a "decoder" used to detect and translate the electronic tones that are generated by a phone during its dialing operation.[151] When a number is dialed on a rotary dial phone, like the one used in the *Giordano* case, "a switch is opened and closed a corresponding number of times to the digit dialed which in turn interrupts the direct current on the line and causes the voltage of the electrical current to rise or fall the corresponding number of times."[152] The pen register is installed on the phone line and "counts the number of pulses in the electrical energy caused by the changes in voltage, and causes the digit dialed on the telephone to be printed in Arabic numerals corresponding to the number of electric pulses."[153] The mechanism for decoding touch-tone phone dialing was slightly more sophisticated, but the result was the same.[154]

With that in mind, imagine the situation considered by the Court in *Smith v. Maryland*. Officers were called to investigate a robbery on March 5, 1976, and the victim provided a description of the robber and a vehicle seen near the scene of the crime.[155] Police later spotted a man fitting the description driving a similar vehicle in the victim's neighborhood and, based on the license plate, learned that the car was registered to the defendant.[156] The police contacted the phone company and requested that a pen register be installed on the defendant's home phone line.[157] That same day, the pen register recorded a call made from the defendant to the victim; the defendant was later charged and convicted based on the phone call and other evidence.[158] So the call log would have looked something like:

(555) 555-5555 – dialed – (555) 556-5556 – 12:34:56 PM, March 17, 1976

Plus similar entries for any other calls that were placed from the Defendant's phone while the pen register device was installed.

---

151. United States v. Focarile, 340 F. Supp. 1033, 1039–40 (D. Md. 1972).

152. *Id*. at 1039.

153. *Id*.

154. *See id*. at 1040 ("In the case of a touch tone telephone, the press of a button on the face of the phone activates an electrical oscillator, which generates two alternating electrical currents at frequencies assigned by the telephone company to correspond to the particular button pushed. The TR-12 touch tone decoder detects these electrical currents at the varying frequencies and determines the arabic number to which the various combinations of frequencies of electrical current have previously been assigned by the telephone company.").

155. Smith v. Maryland, 442 U.S. 735, 737 (1979).

156. *Id*.

157. *Id*.

158. *Id*.

But the experience of the officers in the *Smith* case bears no resemblance to that of NSA analysts reviewing the millions of telephone records that are collected each day under the Metadata Program. The pen-register data at issue in *Smith* was very limited—only showing dialed numbers and times without any ability to detect the duration (or even the existence of) a call. Given that background, the Court's holding in *Smith* was based on a narrow set of factual circumstances that are not easily generalizable to new digital metadata records. But the Government now argues that the 1979 holding authorizes the collection of any and all information shared with private companies.[159]

3. Modern Metadata is Different

One key question in the metadata cases will be whether courts find that the NSA's collection of metadata today is fundamentally different from the FBI's use of pen registers in *Smith v. Maryland*. There are several factors that distinguish the NSA program from anything previously considered by the Supreme Court, but the most significant is the sheer volume of data. One expert estimates that the NSA Metadata Program could be generating "140 gigabytes of data" each day, the equivalent of "70 million pages of information every day, and about 25 billion pages of information every year."[160] This is only possible because of the exponential growth in digital storage and the sophistication of modern databases. Over the last thirty years, the capacity of computer storage has increased "at a compound annual growth rate (CAGR) of 60%."[161]

In 1976, the state-of-the-art 5 ¼ inch floppy disk drive had a capacity of 8,000 kilobytes and cost more than $500.[162] Today companies produce memory products that can store 128 gigabytes of

159. *See*, *e.g.*, Brief for the Appellees, *Smith v. Obama*, No. 14-35555 at 37–60 (Oct. 2, 2014).

160. Declaration of Professor Ed Felten at ¶ 11, ACLU v. Clapper, No. 13-3994 (2nd Cir. filed Aug. 26, 2013) [hereinafter Felton Declaration], *available at* https://www.aclu.org/files/pdfs/natsec/clapper/2013.08.26%20ACLU%20PI%20Brief%20-%20Declaration%20-%20Felten.pdf (assuming 3 billion calls are made each day in the United States).

161. E. Eleftheriou, R. Haas, J. Jelitto, M. Lantz, & H. Pozidis, *Trends in Storage Technologies*, INST. ELEC. & ELEC. ENG'RS. COMP. SOC'Y. TECHNICAL COMM. ON DATA ENG., Dec. 2010 at 1, *avialable at* http://sites.computer.org/debull/A10dec/ELE_Bulletin_Dec.pdf.

162. In the Matter of Certain Double-Sided Floppy Disk Drives & Components Thereof at 230–32, Inv. No. 337-TA-215, USITC Pub. 1860 (May. 1986), *available at* http://books.google.com/books?id=mW8aJDLjowsC&lpg=PA230&ots=QVZqm3c7-g&dq=1976%20shugart%20FDD&pg=PP1#v=onepage&q&f=false.

data on an eleven-by-ten-milimeter chip[163] and hard drive disks that can store eight terabytes of data.[164] That means a hard drive today could hold more than a million copies of the data stored on a 5 ¼ inch floppy disk.[165] But even the exponential growth in digital storage rates has not been able to keep up with our ever-expanding demands for storage capacity. In 2007, the amount of information created and replicated surpassed the amount of storage capacity available, and analysts predict that we will see a fifty-fold increase in total data stored from the beginning of 2010 to the end of 2020.[166]

The pen register records in *Smith v. Maryland* were physical files—paper records created by an automated machine—containing a very limited amount of information about calls placed from an individual telephone line. The records collected under the NSA Metadata Program are massive digital files containing comprehensive routing and call log information, including: date, time, target number, trunk identifier, number dialed/calling party number, device identification number, and duration of call (government officials claim that they do not currently collect cell site location information for mobile calls).[167] These files contain data about millions of calls each day, not just the numbers dialed from a single target line. This metadata, like the cell phone data at issue in *Riley*, is both quantitatively and qualitatively different than the physical records at issue in *Smith v. Maryland*.

Modern metadata is qualitatively different because it includes additional fields that provide sensitive information about the caller and the conversation. Firstly, metadata includes the duration of each incoming and outgoing call—information that the Court specifically noted was not present in *Smith v. Maryland* and the other pen register cases. The call duration data indicates whether a conversation

163. *See* Press Release, Toshiba, Toshiba Offers World's Smallest-Class E-Mmc Embedded Nand Flash Memory Products (Oct. 1, 2014), http://www.toshiba.com/taec/news/press_releases/2014/memy_14_725.jsp.

164. Press Release, Segate, Seagate Ships World's First 8TB Hard Drives (Aug. 26, 2014), http://www.seagate.com/about/newsroom/press-releases/Seagate-ships-worlds-first-8TB-hard-drives-pr-master/.

165. There are 1,073,741,824 kilobytes in a terabyte, so an eight terabyte hard drive is roughly 1,073,742 times the size of a 8,000 kilobyte floppy disk.

166. JOHN GANTZ & DAVID REINSEL, THE DIGITAL UNIVERSE IN 2020: BIG DATA, BIGGER DIGITAL SHADOWS, AND BIGGEST GROWTH IN THE FAR EAST, Dec. 2012 at 3, *available at* http://www.emc.com/collateral/analyst-reports/idc-the-digital-universe-in-2020.pdf.

167. *See*, *e.g.*, *Sample Call Detail w/ Cell Sites*, VERIZON WIRELESS LAW ENFORCEMENT RESOURCE TEAM PRESENTATION at slide 23, *available at* http://cryptome.org/isp-spy/verizon-spy.pdf (last visited Dec. 3, 2014).

occurred and can also be used to infer to some degree the nature of that conversation.[168] Secondly, metadata includes the trunk identifier and other routing information that will reveal the general geographic origin of the call.[169] This can reveal not only with whom the user is communicating, but also when and where they were located when that communication occurred. Finally, the metadata for wireless calls includes the unique identification number associated with the phone used.[170] This unique identifier can be used to associate an individual user with a set of calls, as opposed to an entire household who would have typically shared a landline phone at the time the Court ruled in *Smith v. Maryland*. These differences alone are sufficient to alter the privacy analysis, but the aggregation of this data allows for much more invasive techniques.

Modern metadata is also fundamentally different from printed call logs because of how it is collected and processed. Modern communications data is stored in structured datasets that facilitate sophisticated link analysis by data-mining programs.[171] The combination of advanced processing capabilities with nearly limitless storage capacity and access to all the daily call records of major carriers allows for "new ways of exploiting the digital record."[172]

168. *See also* Jonathan Mayer & Patrick *Mutcheler, Metaphone: The Sensitivity of Telephone Metadata*, WEB POL'Y. (Mar. 12, 2014), http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/.

169. *See* Patrick Di Justo, *What the N.S.A. Wants to Know About Your Phone Calls*, NEW YORKER (June 7, 2013), http://www.newyorker.com/tech/elements/what-the-n-s-a-wants-to-know-about-your-phone-calls ("A cellular network is a 'trunked' system: rather than providing a direct radio link between two phones, callers are linked through a series of high-capacity channels, typically existing telephone circuits. The trunk identifier of a cell-phone call can reveal where that call entered the trunk system. This single piece of data can locate a phone within approximately a square kilometer.").

170. There are three different identification numbers that can be associated with a phone or other mobile communications device: IMEI, IMSI, and ESN. The International Mobile Equipment Identity (IMEI) "uniquely identifies an individual mobile station," and consists of "a number of fields totaling 15 digits" with a "range of 0 to 9." GSM ASS'N, IMEI ALLOCATION AND APPROVAL GUIDELINES 5 (v.6 2011), *available at* http://www.gsma.com/newsroom/wp-content/uploads/2012/06/ts0660tacallocationprocessapproved.pdf. The Electronic Serial Number (ESN) is "a unique identification number embedded or inscribed on the microchip in a wireless phone by the manufacturer." *ESN Migration to MEIDs*, TELECOMM'N INDUS. ASS'N, http://www.tiaonline.org/standards/numbering-resources/electronic-serial-numbers-esn-and-meid (last visited Nov. 3, 2014). The International Mobile Subscriber Identity (IMSI) is a "15-digit identifier" that "has always been used by GSM systems" but has also been implemented on other cellular networks across the globe. David Crowe, *Cellular Networking Perspectives*, WIRELESS TELECOM MAG. (2001), *available at* http://www.cnp-wireless.com/ArticleArchive/Wireless%20Telecom/2001Q1WT.html.

171. Felton Declaration, *supra* note 160, at ¶¶ 20–29.

172. *Id*. at ¶ 24.

Furthermore, the aggregation and bulk analysis of metadata poses special risks for privacy and associational rights.[173] The government's use of contact chaining[174] and other relational analysis will necessarily expose private facts that would otherwise be very costly to obtain, and it will provide the government with easy access to that information about millions of innocent individuals who have never been suspected of wrongdoing. Government regulations are not sufficient to protect against such broad access.

In *Riley*, the Court found that the privacy interests at stake in the search of a cell phone are heightened in part because of the *volume* of data stored—the aggregation of which could "convey far more than previously possible."[175] The Court also found that the type of data stored on cell phones, including call logs and historical location records, would reveal sensitive personal information about the user, and potentially provide access to a "comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[176] The Court also found that the *pervasiveness* of cell phone use means that allowing routine searches of cell phone data "is quite different from allowing them to search a personal item or two in the occasional case."[177] The Court repeatedly emphasized that the practical limitations of physical searches make them inherently different from the collection and analysis of digital data. This was the Court's basis for departing from the well-established categorical rule from *Robinson*—the Court held that digital records are different from physical objects in the Fourth Amendment context.

173. As the Court noted in *Riley*, "[t]he sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions." *Riley*, 134 S. Ct. at 2489.

174. The term "contact chaining" refers to the process of identifying and mapping everyone who is within two steps/hops of an individual of interest. *See* Vladis Krebs, *Contact Chaining*, The Network Thinkers (June 28, 2013), http://www.thenetworkthinkers.com/2013/06/contact-chaining.html. For example, a contact chaining graph of Alice might show that she contacted Betty and Carl, and it might also show that Carl contacted David and Elaine and that Betty contacted Frank and Greg. In that scenario, Alice would be "two hops" from David, Elaine, Frank, and Greg.

175. *Id*.

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

177. *Id*.

The same reasoning that led the Court to reject the application of the search-incident-to-arrest exception to cell phone data in *Riley* would support the rejection of the *Smith v. Maryland* rule for digital communications records.

## IV. OTHER SIGNIFICANT FOURTH AMENDMENT AREAS THAT COULD BE IMPACTED BY *RILEY*

The Court's decision in *Riley* will likely have a lasting impact not only in search-incident-to-arrest cases and in cases challenging the NSA Metadata Program, but also in other major Fourth Amendment cases involving electronic storage and digital communications records. In particular, the *Riley* decision will guide lower courts in cases involving the collection of location data records and in cases involving the search and seizure of data in electronic storage.

### *A. Impact of Riley on Location Data Cases*

One significant unresolved issue is whether the collection of cell phone location data is a search subject to Fourth Amendment protections.[178] Lower courts are currently split over the statutory and constitutional standards applicable to law enforcement requests for location data. And several federal appellate courts are currently considering this issue in light of the Supreme Court's decision in *Jones*.[179] Those courts will now measure the impact of the *Riley* decision.[180]

In 2005, a magistrate judge in the Eastern District of New York issued a rare published opinion following an application for a surveillance order.[181] This opinion revealed for the first time that the

178. *See generally* Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now?: Toward Reasonable Standards for Law Enforcement Access to Location Data That Congress Could Enact*, 27 BERKELEY TECH. L.J. 117 (2013) (discussing the constitutional implications of the collection of cell phone location data.).

179. *See*, *e.g.*, United States v. Davis, 754 F.3d. 1205 (11th Cir. 2014), *reh'g granted*, 573 Fed. Appx. 925, (11th Cir. 2014); United States v. Graham, No. 12-4659 (4th Cir. filed Aug. 22, 2012).

180. *See*, *e.g.*, Supplemental Brief of Appellants, United States v. Graham, No. 12-4659 (4th Cir. filed Jul. 18, 2014).

181. *See* In re Application of the United States for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device & (2) Authorizing Release of Subscriber Info. &/or Cell Site Info., 384 F. Supp. 2d 562, 563 (E.D.N.Y. 2005). *See generally* Kevin Bankston, *Only the DOJ Knows: The Secret Law of Electronic Surveillance*, 41 U.S.F. L. Rev. 589, 608–12 (2007). The DEA had previously obtained real-time location information in a case where they obtained a Title III wiretap. *See* M. Wesley Clark, *Cell Phones as Tracking Devices*, VAL. U. L. REV. 1413, 1415 (2007) (discussing United States v. Forest, 355 F.3d 942 (6th Cir. 2004), *cert. denied*, 543 U.S. 856 (2004)).

DOJ had been routinely seeking authorization to track cell phones in real time under section 2703(d) of Electronic Communications Privacy Act.[182] The judge ruled that section 2703(d) could only authorize the compelled production of "information already in existence" at the time of the application, and could not authorize the ongoing or real-time tracking of a suspect.[183] Courts have subsequently authorized the government to collect historical cell phone location data pursuant to section 2703(d),[184] and at least one federal appellate court has ruled that this construction of the statute does not render it "categorically unconstitutional."[185]

At issue in the location data cases is the government's collection of cell site location information (CSLI). As the Eleventh Circuit described in *Davis*,

> [t]hat location information includes a record of calls made by the providers' customer, in this case Davis, and reveals which cell tower carried the call to or from the customer. The cell tower in use will normally be the cell tower closest to the customer. The cell site location information will also reflect the direction of the user from the tower. It is therefore possible to extrapolate the location of the cell phone user at the time and date reflected in the call record.[186]

That location information is similar, but not identical to the data generated by the tracking device used in *United States v. Jones*. In *Jones*, the Supreme Court held that "the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search'" under the Fourth Amendment.[187] But the majority opinion in *Jones* ruled on the narrower grounds that the government's physical occupation of the defendant's "private property for the purpose of obtaining information" constituted a search, regardless of whether the

182. Bankston, *supra* note 181, at 609.

183. In re Application of the United States for an Order (1) Authorizing the Use of a Pen Register and a Trap and Trace Device, 396 F. Supp. 2d 294, 312–13 (E.D.N.Y. 2005).

184. *See Davis*, 754 F.3d at 1210–11 ("The evidence at issue consists of records obtained from cell phone service providers pursuant to the Stored Communications Act ("SCA"), 18 U.S.C. §§ 2703(c) and (d).").

185. In re Application of the United States, 724 F.3d 600, 615 (5th Cir. 2013). *See also* In re Application of the United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't, 620 F.3d 304, 317–18 (3d Cir. 2010) (holding that a magistrate has discretion under section 2703(d) to require probable cause before issuing an order for location data, but that probable cause is not required under the Fourth Amendment in every case).

186. *Davis*, 754 F.3d at 1210–11.

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

defendant had a "reasonable expectation of privacy" in his location information.[188] The Court in *Jones* did not directly answer whether the collection of location data without the use of a physical tracking device is a "search" under the Fourth Amendment. But two concurring opinions—one by Justice Sotomayor and another by Justice Alito joined by three other justices—reasoned that the long-term monitoring of an individual's location would violate a reasonable expectation of privacy.[189]

The state of Fourth Amendment protection for location data is still uncertain post-*Jones*, but the Court's decision in *Riley* will likely have a significant impact on future decisions. Unlike *Jones* Court, the *Riley* Court spoke with one voice and clearly outlined the important privacy interests in cell phone data. The Court also specifically addressed the sensitivity of location data, invoking the reasoning of Justice Sotomayor's far-reaching concurrence in *Jones*:

> Although the data stored on a cell phone is distinguished from physical records by quantity alone, certain types of data are also qualitatively different. . . . 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.[190]

The Court found that the privacy interest in location data, as well as other cell phone data, was so great that it outweighed the government's interest in gathering evidence during a lawful arrest, overturning the categorical rule previously established in *Robinson*.[191] Defendants in future cases will argue that the *Smith v. Maryland* rule should be similarly rejected in the context of stored location data. And given the Court's findings on the significant privacy interests at stake, it would be difficult for a lower court to conclude that an individual has no "reasonable expectation of privacy" in such sensitive data.

---

188. *Id*. at 950.

189. *Id*. at 956 (Sotomayor, J., concurring); *id.* at 964 (Alito, J., concurring).

190. Riley v. California, 134 S. Ct. 2473, 2495 (2014) (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.")).

191. *Id*. at 2493.

### *B. Impact of Riley on Electronic Search and Seizure Cases*

In a growing number of cases, lower courts must grapple with the question of when and for how long law enforcement officers are allowed to collect, search, and store digital data.[192] Determining the proper scope of digital data searches and the identifying reasonable retention and minimization practices for seized data is a complex problem; lower courts are likely to consider the Supreme Court's analysis in *Riley* when ruling on electronic search issues. Among these issues, first: Is the copying of a digital device's contents a seizure that triggers Fourth Amendment requirements? Second: Are there limits to how long law enforcement officers may store seized digital data—i.e., do they have an obligation to delete the data? And finally, what is the reasonable scope of a digital data seizure or search—how does the "plain view" doctrine apply in the digital context? These are all questions that lower courts will have to answer in future cases; the *Riley* decision will likely inform those answers. In particular, *Riley* supports the conclusion that the retention of electronic data should be subject to different Fourth Amendment rules than those used for handling physical evidence.[193] *Riley* would also support a narrower construction of the "plain view" exception for digital searches.

Lower courts have not yet resolved whether law enforcement investigators have any obligations to delete or minimize seized data. Courts will have to address the scope of Fourth Amendment protections for seized data in cases where officers obtain a copy of a hard drive or other storage device in one case, and later attempt to use evidence gathered from that device in a separate case. For example, in *United States v. Ganias*,[194] the Second Circuit considered "whether the Fourth Amendment permits officials executing a warrant for the seizure of particular data on a computer to seize and indefinitely retain every file on that computer for use in future criminal investigations."[195] The investigators in *Ganias* seized the defendant's hard drives pursuant to a warrant in 2003 as part of an investigation into fraud by two government contractors for whom the defendant performed accounting work.[196] By 2004, the investigators

192. *See generally* Orin Kerr, *Fourth Amendment Seizures of Computer Data*, 119 YALE L. J. 700 (2010) (discussing recent decisions regarding law enforcement seizure of digital data.).

193. *Riley*, 134 S. Ct. at 2489–91.

194. 755 F.3d 125 (2d Cir. 2014).

195. *Id*. at 137.

196. *Id*. at 128.

had "isolated and extracted" files relevant to the contractor case, and pursuant to the warrant they were "not permitted to review any other computer records."[197] When the government subsequently expanded their investigation to include "possible tax violations by Ganias," more than twenty months after the initial seizure of the hard drives, they were still maintaining copies of the non-relevant files from their previous search.[198]

The court in *Ganias* ruled that the government's "seizure and retention" of digital filed beyond the scope of their 2003 warrant was unreasonable under the Fourth Amendment.[199] Specifically, the court found that "[w]ithout some independent basis for its retention of those documents in the interim, the Government clearly violated Ganias's Fourth Amendment rights by retaining the files for a prolonged period of time and then using them in a future criminal investigation."[200] The court implied that while the government might be allowed to keep a mirror image of files for the purpose of maintaining its evidentiary chain of custody, there was no justification to use that data for "any other purpose."[201] The court's ruling was clear: when the government obtains a warrant to search an electronic storage device for certain evidence, it must extract that evidence within a reasonable time period, then delete or otherwise prevent the use of all other data from the seized device.

The rule adopted in *Ganias* is consistent with the scope of privacy interests in digital data outlined in *Riley*, and other courts will be more likely to adopt the rule in light of the Supreme Court's decision. The Court emphasized in *Riley* that users have significant privacy interests in the files stored on their digital devices, and that searches of digital devices "would typically expose to the government far *more* than the most exhaustive search of a house."[202] Given the large volume of sensitive records stored on digital devices, it is necessary to establish clear limits on the retention and use of data seized pursuant to a warrant for a specific investigatory purpose.

197. *Id*. at 129.
198. *Id*.
199. *Id*. at 137.
200. *Id*. at 138.
201. *Id*. at 139.
202. Riley v. California, 134 S. Ct. 2473, 2490 (2014) (emphasis in original).

As the search and seizure of stored electronic data has become commonplace in criminal investigations, lower courts have also had to address the application of the "plain view" doctrine to digital searches.[203] The Supreme Court previously held in *Arizona v. Hicks*[204] and *Horton v. California*[205] that "[i]f an article is already in plain view, neither its observation nor its seizure would involve any invasion of privacy."[206] But this rule is problematic when applied to seizures of digital data, as the Ninth Circuit recently discussed in *United States v. Comprehensive Drug Testing* (*CDT*).[207] In *CDT*, the government argued that it could lawfully retain medical records outside the narrow scope of what it was authorized to obtain in the warrant because "that evidence was in plain view once government agents examined" the computer directory.[208] The court in *CDT* rejected this argument because, under that theory, "everything the government chooses to seize will . . . automatically come into plain view. Because the government agents ultimately decide how much to actually take, this will create a powerful incentive for them to seize more rather than less . . . ."[209] Furthermore, the court found that it would "render the carefully crafted safeguards" in the warrant "a nullity."[210]

In *Comprehensive Drug Testing*, the Government obtained a grand jury subpoena for all "drug testing records and specimens" held by CDT pertaining to their administration of Major League Baseball's drug testing program.[211] The company sought to quash the subpoena but the same day the motion was filed the government obtained a warrant to "search CDT's facilities in Long Beach" that was "limited to the records of ten players as to whom the government

203. *See generally* Orin Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531 (2005) (discussing the application of the plain view doctrine to searches of various digital mediums).

204. 480 U.S. 321 (1987).

205. 496 U.S. 128 (1990).

206. *Id*. at 133 (1990) (citing *Hicks*, 480 U.S. at 325). As Professor Kerr points out, "[t]echnically speaking, the plain view doctrine is a limitation on the government's right to seize evidence. It regulates seizures, not searches." Kerr, *Searches and Seizures*, *supra* note 203, at 577 n.200. Thus the plain view doctrine might not apply to "searches" of computer files at all if the court finds no seizure took place, but "no court that has applied the plain view exception to digital evidence has recognized or even acknowledged this point." *Id.*

207. United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1170–71 (9th Cir. 2010) (en banc).

208. *Id*. at 1170.

209. *Id*. at 1171.

210. *Id*.

211. *Id*. at 1166.

had probable cause."[212] However, "[w]hen the warrant was executed . . . the government seized and promptly reviewed the drug testing records for hundreds of players in Major League Baseball (and a great many other people)."[213] The players and CDT successfully moved for return of their property under Federal Rule of Criminal Procedure 41(g), and the government appealed.[214] The court ultimately concluded that the Government had wrongfully accessed data beyond the scope of the original warrant and that, as a result of its intentional wrongdoing, it must return the property to CDT.[215]

The Ninth Circuit's decision in *CDT* and the Second Circuit's recent decision in *Ganias* both show that the application of the plain view exception to the Fourth Amendment warrant requirement should be narrowly construed in the context of seizures of digital data. As Professor Kerr has outlined, there are three main approaches to narrowing the plain view exception in the digital context: first, "narrow the plain view exception based on the circumstances of the search, such as the analyst's subjective intent or the tool used;" second, narrow the exception based on the nature of the evidence discovered, permitting the use of some kinds of evidence while blocking others;" and third, abolish the plain view exception in digital evidence cases."[216] The court in *Ganias* adopted a version of the third approach, following along with the rule outlined by the Ninth Circuit in *CDT*.[217] But recently some courts have declined to extend the same protections to data stored on digital devices that are seized pursuant to a warrant.

For example, in *United States v. Miller*[218] the court considered whether the forensic search of a digital camera that was seized during the lawful execution of a search warrant of the defendant's home violated his Fourth Amendment rights.[219] The officers in *Miller* obtained a warrant to search the defendant's home for evidence related to suspected drug and narcotics sales.[220] During the search, an

212. *Id*.
213. *Id*.
214. *Id*.
215. *Id*. at 1171, 1174.
216. Kerr, *Fourth Amendment Seizures*, *supra* note 192, at 576–77.
217. *See* United States v. Ganias, 755 F.3d 125, 136 (2d Cir. 2014)(citing *CDT*, 621 F.3d at 1171 (9th Cir. 2010) (en banc)).
218. *See*, *e.g.*, United States v. Miller, No. 13-20929, 2014 WL 3671062 (E.D. Mich. July 23, 2014).
219. *Id*. at *1.
220. *Id*.

officer inspected a digital camera that was discovered in the defendant's home.[221] The officer turned on and "examined" the camera, discovering images that he believed to be child pornography.[222] The police subsequently sought separate warrants to search the defendant's house for evidence of child pornography based on the image discovered on the camera.[223] The defendant argued that the detective's examination of the camera was outside the scope of the warrant, but the court ultimately found that the examination was "consistent with an authorized narcotics search."[224]

The court in *Miller* rejected the defendant's argument, made post-*Riley*, that the search of a digital camera is "different" from the search of a photo album or other physical item that the police could lawfully inspect during the search of a home.[225] The court distinguished *Riley* on the grounds that the search of a home pursuant to a warrant involves a "different mode of analysis" from a warrantless search incident to arrest.[226] The court also reasoned that the search of a digital camera is different than the search of a smartphone because cameras only "contain a limited type of data, restricted to image and video files, that do not touch the breadth or depth of information that a cell phone's data offers."[227] The court held that the search of the camera did not violate the defendant's reasonable expectation of privacy because the police "inadvertently discovered Defendant's child pornography," and did not purposefully exceed the scope of the warrant.[228] The court in *Miller* clearly adopted the "intent of the analyst" approach to the plain view doctrine in the context of a digital device seized during the search of a home.[229]

These cases, which seem inconsistent upon first inspection, may in fact fit into a new framework of Fourth Amendment protection for digital data. When investigators obtain copies of digital data, as in *Ganias* and *CDT*, they will be subject to search and retention

221. *Id*.
222. *Id*.
223. *Id*.
224. *Id*. at *2.
225. *Id*. at *3.
226. *Id*.
227. *Id*.
228. *Id*. at *5. The court analogized Miller's case to United States v. Lucas, 640 F.3d 168 (6th Cir. 2011), and distinguished United States v. Carey, 172 F.3d 1268 (10th Cir. 1999).
229. *See* Kerr, *Searches and Seizures*, *supra* note 203, at 576–80 (discussing *Carey*, United States v. Gray, 78 F.Supp.2d 524 (E.D. Va. 2009), and problems with the plain view approach focused on the circumstances of the search).

restrictions based on the scope of the warrant or authorization. This is similar to the heightened standard imposed on "forensic" searches at the border in *Cotterman* and *Saboonchi*. However, when officers discover evidence upon initial inspection of a digital device during an authorized search, that evidence will be admissible even if it is outside the scope of the original search, so long as the discovery was inadvertent or reasonable under the circumstances. This rule would be necessarily limited because it would not extend to more in-depth forensic examinations of the digital devices. Any such examination would require an independent legal justification, similar to the "forensic search" standard applied by courts in the border search context.

## CONCLUSION

The Supreme Court's decision in *Riley* will likely have a significant impact on future Fourth Amendment cases involving new technologies, especially cases involving cell phones and other digital devices. The first major test of post-*Riley* Fourth Amendment standards will likely come in the metadata cases, which are now pending before three federal appellate courts. Judges in the metadata cases could find that the "third party" rule articulated in *Smith v. Maryland* is inapplicable to modern communications metadata in the same way that the search-incident-to-arrest rule established for physical items in *Robinson* is now inapplicable to cell phones. Similarly, judges considering whether the collection of cell phone location information is a "search" could rely on the Court's decision in *Riley* to support the conclusion that individuals have strong privacy interests in their location records. The *Riley* decision will likely also have an impact on border search and electronic search cases. Because of its potentially broad impact on future cases, the *Riley* decision will likely be remembered as a landmark decision for digital Fourth Amendment rights.