THE SUPREME DIGITAL DIVIDE

Mary Graw Leary[*]

"[B]ecause of the role that these devices have come to play in contemporary life, searching their contents implicates very sensitive privacy interests that this Court is poorly positioned to understand and evaluate."[1]

I. INTRODUCTION

Society has long struggled with the meaning of privacy in a modern world.[2] This struggle is not new. With the advent of modern technology and information sharing, however, the challenges have become more complex.[3]

---

* Professor, The Catholic University of America, Columbus School of Law. Many thanks to Steve Young for his outstanding assistance; Katherine Olson and Tina Lee for their research; Arnold Loewy for his commitment to exploring critical Fourth Amendment issues; and the *Texas Tech Law Review* staff for their dedication and patience.

1. Riley v. California, 134 S. Ct. 2473, 2497 (2014) (Alito, J., concurring).
2. *See infra* Part II.
3. *See infra* Part III.B.

Socially, Americans seek to both protect their private lives and also to utilize technology to connect with the world. Commercially, industries seek to obtain information from individuals, often without their consent, and sell it to the highest bidder.[4] As technology has advanced, the ability of other individuals, institutions, and governments to encroach upon this privacy has strengthened.[5] Nowhere is this tension between individual privacy rights and government security interests felt more acutely than within the context of the Fourth Amendment.[6]

Notwithstanding the long duration of this struggle, jurisprudentially, the nation is at a critical point. Traditionally, the touchstone for analyzing the boundaries of Fourth Amendment searches is reasonableness.[7] Quite literally, therefore, the Supreme Court has the task of determining the unanswerable: What is reasonable?[8] This task, combined with the modern realities of rapidly changing technology, increased use of government surveillance, and changing expectations and conceptions of privacy, as well as differing perspectives of privacy in a heterogeneous society, becomes an even further complicated endeavor.[9]

One of the significant realities in play at this critical juncture lies within the Court itself. This Article asserts that there is a new, different form of the digital divide—the divide between the perspective of the Court and twenty-first century realities—which has the potential to negatively impact Fourth Amendment jurisprudence.[10] This Article focuses on two specific aspects of that gap, arguing that this gap in experience and perspective contributes to false presumptions by the Court, which then leads to less than optimal opinions.[11] Such an approach creates a veritable house of cards in which the opinions themselves are weakened and eroded over time.[12] The potential of the Court to add crucial guidance in the area of privacy law in contemporary society is immense.[13] That being said, any constructive impact

---

4. *See generally* Mary Graw Leary, Katz *on a Hot Tin Roof–Saving the Fourth Amendment from Commercial Conditioning by Reviving Voluntariness in Disclosures to Third Parties*, 50 AM. CRIM. L. REV. 341, 343–44 (2013) [hereinafter Leary, Katz *on a Hot Tin Roof*] (discussing entities that collect data online about individuals); Mary G. Leary, *The Missed Opportunity of* United States v. Jones*: Commercial Erosion of Fourth Amendment Protection in a Post-Google Earth World*, 15 U. PA. J. CONST. L. 331, 333 (2012) [hereinafter Leary, *Missed Opportunity*] (discussing commercial technologies that eliminate expectations of privacy).

5. *See infra* Parts II–III.

6. *See infra* Part II.

7. *E.g.*, Bailey v. United States, 133 S. Ct. 1031, 1048 (2013) (Scalia, J., concurring) (quoting Kentucky v. King, 131 S. Ct. 1849, 1856 (2011)); Brigham City v. Stuart, 547 U.S. 398, 403 (2006).

8. *See infra* Part II.

9. *See infra* Part III.B.

10. *See infra* Part III.

11. *See infra* Part III.

12. *See infra* Part III.

13. *See infra* Part VI.

is compromised when the validity of the opinions precludes their ability to withstand the test of time.[14]

Parts II and III of this Article discuss the gap generally, with specific attention paid to the divide between the Court and technological realities, and the gap between the Court and the realities of modern policing and pressures on law enforcement. These Parts specifically argue that these divides result in opinions purporting to determine what is reasonable in modern life, but which rest upon a set of inaccurate presumptions. Part IV illustrates this phenomenon by analyzing *Riley v. California*, in which the Court held that the police may not dispense with the warrant requirement to search arrestees' cell phones incident to arrest.[15] Part IV also examines three inaccurate presumptions made in *Riley*, arguing that they contribute to a failed jurisprudence in this critical area. Part V discusses the significance of this approach by the Court. Finally, Part VI explores ways to reform this approach in the future.

II. THE ROLE OF THE SUPREME COURT IN DEVELOPING FOURTH AMENDMENT PROTECTIONS

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[16] This clause, referred to as the "Reasonableness Clause" of the Fourth Amendment, requires the Court to determine which government searches are reasonable and which are not, thereby violating the Fourth Amendment.[17] The Court's history of developing a workable framework for this analysis is somewhat inconsistent. While originally utilizing a trespass–property law framework, the Court moved from that approach in 1965 in *Katz v. United States*, adopting a "reasonable expectation of privacy" analysis.[18] In so doing, the Court explicitly stated that property law was no longer the Court's approach.[19] More recently, however, the Supreme Court reverted back to a property analysis in *United States v. Jones*, when it concluded that

14. *See infra* Part V.

15. *See* Riley v. California, 134 S. Ct. 2473, 2485 (2014).

16. U.S. CONST. amend. IV.

17. *See* City of Los Angeles v. Patel, 135 S. Ct. 2442, 2451–53 (2015) (discussing the Fourth Amendment's reasonableness requirement).

18. Katz v. United States, 389 U.S. 347, 352–53, 361 (1967).

19. *Id.* As the Court noted in *Katz*, "The premise that property interests control the right of the Government to search and seize has been discredited." *Id.* at 353 (quoting Warden, Md. Peni. v. Hayden, 387 U.S. 294, 304 (1967)); *see also* Oliver v. United States, 466 U.S. 170, 177, 183–84 (1984) (applying the *Katz* test and the open fields doctrine to conclude that, although there was a trespass, there was no Fourth Amendment violation).

the *Katz* approach supplemented the trespass–property framework, but did not replace it.[20]

Notwithstanding this somewhat inconsistent and convoluted history,[21] the Court has not retreated from its repeated assertion that "the ultimate touchstone of the Fourth Amendment is 'reasonableness.'"[22] This inquiry does not require a determination of what is reasonable to the Court;[23] rather, the *Katz* inquiry defines the reasonable expectation of privacy test as a two-pronged approach.[24] The test (originally from Justice Harlan's concurrence) demands, absent an exception to the warrant requirement, a search warrant if the government examines an area in which an individual has a reasonable expectation of privacy.[25] The reasonableness of this expectation is determined by establishing the following: (1) the individual exhibited an actual expectation of privacy in the location searched (the subjective prong); and (2) that expectation is one that society is prepared to accept as reasonable (the objective prong).[26] As such, a fundamental role of the Court in determining the meaning of the Fourth Amendment is determining reasonableness.

III. THE JUDICIAL DIGITAL DIVIDE

The term *digital divide* is one that traditionally refers to the divide between different segments of the population regarding access to technology and the Internet. It references the divide between "information rich" and "information poor."[27] It has also been used to refer to the technological divide between affluent and more impoverished communities "based on race, income, ethnicity, education, profession, and gender,"[28] as well as the

---

20. United States v. Jones, 132 S. Ct. 945, 949 (2012); *id.* at 954 (Sotomayor, J., concurring); *id.* at 964 (Alito, J., concurring).

21. *Id.* at 959–60 (Alito, J., concurring) (disputing this revisionist history regarding *Katz*). For a full discussion of the dubious mischaracterization of *Katz* by the *Jones* majority, see Leary, *Missed Opportunity*, *supra* note 4, at 342.

22. Heien v. North Carolina, 135 S. Ct. 530, 536 (2014) (quoting Riley v. California, 134 S. Ct. 2473, 2482 (2014)); *see also* Rodriguez v. United States, 135 S. Ct. 1609, 1617 (2015) (Thomas, J., dissenting) (citing Brigham City v. Stuart, 547 U.S. 398, 403 (2006)).

23. *E.g.*, Minnesota v. Carter, 525 U.S. 83, 97 (1988) (Scalia, J., concurring) (arguing, as a longtime critic of the *Katz* test, that one of the problems with the reasonable expectation of privacy test is that judges tend to only assess what is reasonable to them).

24. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

25. *Id.*

26. *Id.* at 360.

27. *E.g.*, Gerald Doppelt, *Equality and the Digital Divide*, 24 HASTINGS COMM. & ENT. L.J. 601, 601 (2002).

28. *Id.*; *see also* Amir Hatem Ali, Note, *The Power of Social Media in Developing Nations: New Tools for Closing the Global Digital Divide and Beyond*, 24 HARV. HUM. RTS. J. 185, 188 (2011) (defining "digital divide" as describing unequal distribution of communication technology).

different uses and approaches to technology between digital natives and digital immigrants.[29]

Another divide exists, however. This divide, labeled here the "judicial digital divide," is between the Court and the reality of modern life for both the public as well as for law enforcement.[30] Such a divide is one with far reaching consequences, given the role of the Supreme Court in determining what is reasonable.[31] This is particularly true within the context of technology because three phenomena occur simultaneously.

Technology is playing an increasing role in the public's life. Individuals are using technology in their vehicles, with their cell phones, through the Internet, even in their eyewear and watches.[32] They do so to bank, date, and engage in other activities traditionally thought to be personal.[33] In so doing, individuals, often unknowingly, create numerous pieces of information, thereby exposing themselves to infinite opportunities to be monitored and have information collected about them.[34] An entire industry has developed around the collection of this data and its unauthorized use by third parties.[35] The government is no different, and in certain situations, seeks to obtain this information in its law enforcement and anti-terrorism efforts.[36] The use of technology is also manifested in law enforcement advancements themselves.[37] Law enforcement increasingly uses technology to become more efficient, accurate, and effective. Whether it is DNA collection, license plate readers, or video monitoring, the government seeks to advance its mission through use of technology. Finally, technology affords criminals new avenues to victimize people. Whether it be through exploitation, identity theft, financial crimes, or otherwise, criminals use technological tools to

---

29. *E.g.*, Kari Mercer Dalton, *Bridging the Digital Divide and Guiding the Millennial Generation's Research and Analysis*, 18 BARRY L. REV. 167, 167 (2012); Mary Graw Leary, *Reasonable Expectations of Privacy for Youth in a Digital Age*, 80 MISS. L.J. 1035, 1039 (2011).

30. *See infra* Part III.

31. *See supra* note 22 and accompanying text.

32. *See* Adam D. Thierer, *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns Without Derailing Innovation*, 21 RICH. J.L. & TECH. no 2., 2015, at 1, 6, http://jolt.richmond.edu/v21i2/article6.pdf; Aaron Smith, *U.S. Smartphone Use 2015*, PEW RES. CTR. (Apr. 1, 2015), http://www.pewinternet.org/2015/04/01/us-smarthphone-use-in-2015/ (documenting the effect smartphones have on all aspects of modern life).

33. *See* Susannah Fox, *51% of U.S. Adults Bank Online*, PEW RES. CTR. (Aug. 7, 2013), http://www.pewinternet.org/2013/08/07/51-of-u-s-adults-bank-online/; Amanda Lenhart, *Dating & Mating in the Digital Age*, PEW RES. CTR. (Apr. 26, 2014), www.pewinternet.org/2014/04/26/dating-mating-in-the-digital-age.

34. *See* Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1092–95 (2002).

35. Leary, Katz *on a Hot Tin Roof*, *supra* note 4.

36. *See* Solove, *supra* note 34, at 1106.

37. *See id.*

victimize others. As such, law enforcement is expected to engage on this additional battlefield in its efforts to prevent and respond to crime.[38]

Thus, the opportunity for government evidence collection through technology is growing exponentially, and any divide between the Court and reality regarding technology potentially has significant implications. This divide manifests itself most clearly in two aspects: (1) in the chasm between the Court's understanding of technology and how it is used by people in everyday life; and (2) the chasm also exists between the Court and the realities of modern policing.

A. The Ivory Tower Concept Is Not Novel

The Court has long suffered the critique that it functions in an "ivory tower" far separated from the experience of everyday Americans.[39] This reality has been observed in many different contexts.

Significant scholarship has addressed these criticisms in the arena of race and police interaction with minority communities. Professor Donna Coker insightfully commented that "[i]n the Court's Fourth Amendment jurisprudence, 'there is a tendency . . . to pretend that the world we all know is not the world in which law enforcement operates.'"[40] Others have commented upon the individual Justices' lack of experiences common to most people. For example, much was made about the implication by Justice Roberts that he has never been subjected to a police traffic stop.[41] Similarly, the Court has been criticized for its statement that donating large sums of money to candidates is unrelated to corruption and for failing to understand that it is impossible for a victim of sexual discrimination to file a complaint of discrimination until she is actually made aware of a salary disparity between herself and her male co-workers.[42] These critiques share a common theme: a gap between the experiences of the members of the Court and the experiences of the public. This gap seems to affect the decisions of the Court, which has the potential to cause harm when the Court is trying to determine what is reasonable to the common person.

---

38. *See id.*

39. *See infra* note 42 and accompanying text.

40. Donna Coker, *Foreword: Addressing the Real World of Racial Injustice in the Criminal Justice System*, 93 J. CRIM. L. & CRIMINOLOGY 827, 827 (2003) (quoting Stephen A. Saltzburg, *The Supreme Court, Criminal Procedure and Judicial Integrity*, 40 AM. CRIM. L. REV. 133, 133 (2003)).

41. Cristian Farias, *The Chief Justice Has Never Been Pulled Over in His Life*, SLATE (Feb. 11, 2015, 9:36 AM), http://www.slate.com/articles/news_and_politics/jurisprudence/2015/02/chief _justice_john_roberts_has_never_been_pulled_over_rodriguez_v_united.html.

42. Mougambi Jouet, *Is the Supreme Court Disconnected from the Real World?*, HILL (Apr. 22, 2014, 1:00 PM), http://thehill.com/blogs/congress-blog/judicial/203982-is-the-supreme-court-disconnected-from-the-real-world (discussing critiques of the Supreme Court for its reasoning in both *Citizens United v. Fed. Elec. Comm'n*, 558 U.S. 310 (2010), and *Ledbetter v. Goodyear Tire & Rubber Co.*, 550 U.S. 618 (2007)).

B. The Divide Is Magnified When It Relates to Technology

When it comes to technology, the gap is even more significant. Some better known examples of the disconnect between the Court and the everyday use of technology in America illustrate this point. For example, Justice Kagan's remarks have been interpreted as stating that the Court is "basically clueless when it comes to technology," conceding the Justices were not well versed in email—in 2013.[43] Chief Justice Roberts rather famously asked during oral argument what the difference was between a pager and email.[44] In *Riley*, Chief Justice Roberts illustrated the disconnect between his experience and that of many Americans by aggressively challenging an advocate's representation that many people not engaged in criminal activity have more than one cell phone on their person.[45] The Court further displayed an equal ignorance in *Quon* when it asked about what would happen when two texts were sent at the same time.[46]

Unfortunately, the media has covered these events with an almost quaint tone. They are humorously presented as though they were vignettes from one's cousin in a foreign country unfamiliar with local customs.[47] However, there is little humorous about a lack of understanding of everyday life in America by the body charged with determining what a reasonable American expects or what a reasonable officer does.

This judicial digital divide raises some serious questions regarding an institution whose average age of retirement is 78.7 years and whose average age of membership is nearly 70 years old, and the Court's ability to measure the reasonableness expected in modern everyday life.[48] This is not to say that people over any certain age are unable to understand technological changes. That is certainly not the case or the basis for this Article's argument. Indeed, Justice Sotomayor's concurring opinion and Justice Alito's opinion concurring in judgment in *Jones* both reflect insight into the changing

---

43. *E.g.*, Will Oremus, *Elena Kagan Admits Supreme Court Justices Haven't Quite Figured Out Email Yet*, SLATE (Aug. 20, 2013), http://www.slate.com/blogs/future_tense/2013/08/20/elena_kagan_supreme_court_justices_haven_t_gotten_to_email_use_paper_memos.html.

44. Transcript of Oral Argument at 29, City of Ontario v. Quon, 130 S. Ct. 2619 (2010) (No. 08-1332).

45. Transcript of Oral Argument at 50, United States v. Wurie, 728 F.3d 1 (2014) (No. 13-212).

46. Transcript of Oral Argument, *supra* note 44, at 44.

47. *See, e.g.*, Oremus, *supra* note 43.

48. Steven G. Calabresi & James Lindgren, *Justice for Life? The Case for Supreme Court Term Limits*, WALL ST. J. (Apr. 10, 2005), http://web.archive.org/web/20050414061240/http://www.opinionjournal.com/editorial/feature.html?id=110006539; Lawrence Hurley, *In U.S., When High Tech Meets High Court, High Jinks Ensue*, BUS. INSIDER (May 9, 2014), http://www.businessinsider.com/r-in-us-when-high-tech-meets-high-court-high-jinks-ensue-2014-09 (calculating the average age of Supreme Court Justices at just over 68).

technological landscape.[49] Justice Alito calls for a legislative response to questions regarding digital surveillance, arguing that the legislature is indeed better equipped to measure societal expectations.[50] For her part, Justice Sotomayor has expressed a willingness to revisit basic Fourth Amendment doctrines, such as the third-party doctrine, in light of their unworkability in a modern technological age.[51]

Notwithstanding these periodic insights, there is a tension between a Court that experiences a different reality than most of society, combined with its intentional, slow movement deciding issues regarding a rapidly changing aspect of life.[52] In addition to technology-induced changes, there can be no doubt that society's expectations of privacy are changing rapidly and becoming more complex. The Pew Research Center reports that "the majority of adults . . . feel that their privacy is being challenged along such core dimensions as the security of their personal information and their ability to retain confidentiality."[53] The fluidity of these perceptions is problematic as the Court attempts to discern the public's privacy expectations.[54] As the public's expectation shifts, so too must the Court's reflection of it.

The issue of privacy is critical to contemporary life. It is also an evolving and complex issue due to the role technology plays in daily life, perpetrating crime, and government surveillance.[55] Within this complicated landscape, the Court is charged with determining what is reasonable. However, the judicial digital divide is problematic in this regard. It results in the Court making inaccurate presumptions and resting opinions on them. This is detrimental not only because the opinions are not strong, but also because it creates an untenable legal situation. This is an area in the law in need of solid jurisprudence. When the Court's opinions are flawed due to false presumptions, the entire system suffers. Thus, the judicial digital divide undermines the value of the Court's opinions, as well as its ability to offer

---

49. United States v. Jones, 132 S. Ct. 945, 945 (2012) (Sotomayor, J., concurring); *id.* at 957 (Alito, J., concurring).

50. *Id.* at 957 (Alito, J., concurring); Riley v. California, 134 S. Ct. 2473, 2497 (2014) (Alito, J., concurring).

51. *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring).

52. City of Ontario v. Quon, 130 S. Ct. 2619, 2629 (2010) ("The Court must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment . . . . The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear.").

53. MARY MADDEN ET AL., PEW RES. CTR., PUBLIC PERCEPTIONS OF PRIVACY IN THE POST SNOWDEN ERA 2 (2014), http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf.

54. *See supra* Part II.

55. *See infra* notes 29–38 and accompanying text.

clarity to individuals and law enforcement. An example of this phenomenon is the Court's analysis in *Riley v. California*.[56]

IV. *RILEY V. CALIFORNIA*

A. The Opinion

The judicial digital divide is very clearly demonstrated in *Riley v. California*, which held that the search incident to arrest exception to the warrant requirement did not apply to cell phones, and police must generally obtain a warrant before conducting a search.[57] The opinion itself involved two cases in which the police performed some form of a search on an arrestee's cell phone.[58] In *Riley*, the police searched the arrestee's smartphone incident to his arrest and later at the police station, observing information related to gang activity.[59] The government used that information against Riley for charges related to a gang shooting.[60] In the companion case, *United States v. Wurie*, police examined incoming calls and the phone log of a "flip" cell phone, which helped them determine the arrestee's address and locate narcotics stored there.[61]

The Court acknowledged some of the basic characteristics of the modern cell phone, noting that modern-day cell phones are different than other types of items that may be seized from an arrestee.[62] The Court paid specific attention to the ability of a cell phone to store vast quantities of information.[63] But it further recognized it is not just the amount of information that can be accessed, but the type of information, which includes financial records, records of purchases, internet searches, and GPS information, that makes cell phones unique.[64]

The Court began its analysis by noting that the search incident to arrest exception to the warrant requirement rests on two justifications: officer safety and concerns about the destruction of evidence.[65] The Court found that the data on the phone was not a danger to police and, therefore, did not justify a search of the phone without a warrant.[66] The *Riley* Court further held that

---

56. *See generally* Riley v. California, 134 S. Ct. 2473 (2014) (discussing the reasonableness of a warrantless search of the defendant's cell phone during a search incident to arrest).

57. *See id.* at 2485. While the majority opinion discussed several aspects of *Riley*, this Article will briefly summarize its framework.

58. *Id.* at 2480–82.

59. *Id.* at 2480.

60. *Id.* at 2481.

61. *Id.* at 2481–82.

62. *Id.* at 2488–90.

63. *Id.* at 2489.

64. *Id.* at 2490.

65. *Id.* at 2485 (citing Chimel v. California, 395 U.S. 752, 762–63 (1969)).

66. *Id.*

concerns regarding evidence destruction raised by the prosecution, namely encryption and data wiping, were not persuasive because such action would be effectuated by third parties or the ordinary functioning of the phone.[67] Therefore, the Court reasoned that such occurrences were not implicated by *Chimel v. California*'s concern that an arrestee himself will destroy evidence due to arrest.[68] A main concern was that the data, either alone or in combination with other pieces of information, has the potential to reveal highly personal information.[69] Furthermore, the data is not analogous to the type of information an individual would traditionally have on his person when arrested or even in his home.[70] Thus, the Court concluded that both the quantity and quality of data on a cell phone distinguished the cell phone from other items found on an arrested person.[71] The Court recognized the growing reality that viewing cell phones as containers similar to other containers on an arrestee is problematic due to society's evolving uses of cell phones.[72]

Moreover, cell phone technology continues to evolve. Increasingly, cell phones are not saving data on the devices themselves, but instead act as portals to information stored remotely.[73] Although the Government conceded that searches incident to arrest could not access information on the cloud, the Court rejected the Government-suggested solution of implementing protocols for such searches.[74] As the Court put it rather bluntly, "[t]he Founders did not fight a revolution to gain the right to government agency protocols."[75]

B. Presumptions

The purpose of this Article is not necessarily to critique *Riley*'s ultimate holding that the police must obtain a warrant prior to examining a cell phone found on an arrestee. Given the distinction between cell phones and other devices often possessed by individuals at the time of arrest, this holding is with merit. It is a legitimate conclusion that the privacy interests of an individual in his cell phone outweigh the government's interest in searching the phone. The focus of this Article is to analyze the framework and approach of the Court in *Riley*.

The specific concerns examined here are the presumptions the *Riley* Court made in its discussion, which formed the basis for its decision. The

---

67. *Id.* at 2486–87.
68. *Id.* at 2486–88.
69. *Id.* at 2490.
70. *Id.*
71. *Id.* at 2490–91.
72. *Id.*
73. *See id.* at 2491.
74. *Id.*
75. *Id.*

Court's presumptions focused upon in this Article all have to do with technology or law enforcement, and are arguably flawed. When the Court's jurisprudence in such an important area is flawed, it undermines the law. As the Court mentioned in *Riley*, it has a "general preference to provide clear guidance."[76] Guidance cannot be clear if the basis for that guidance is compromised due to a lack of an appreciation of certain realities.

The following is a discussion of three presumptions in the *Riley* opinion that are arguably flawed. This Article submits that this pattern of presumptions can compromise the positive impact the Court can have on the difficult questions presented by modern-day privacy expectations.

1. Presumption 1: The Threat of Remote Wiping Is Invalid

Remote wiping, also known as a mobile kill switch, is the ability of a person to remotely remove data, apps, or even the operating system from a cell phone.[77] *Riley* discussed the Government's main argument that the possibility of a seized cell phone being remotely wiped created a true threat of evidence destruction.[78] The Court rejected this argument, stating that "once law enforcement officers have secured a cell phone, there is no longer *any risk* that the *arrestee himself* will be able to delete incriminating data from the phone."[79] Embedded within this presumption are two faulty grounds. First, it limits the Court's concern to situations in which the arrestee himself could remotely wipe the phone.[80] Second, the presumption erroneously concludes that there is "no risk" that the phone will be wiped.[81]

The first point, that the Court should only be concerned with whether the arrestee himself can remotely wipe the phone, is not based on reality. The *Riley* Court correctly noted that the *Chimel* decision itself was concerned with the actions of an arrestee.[82] However, the Court has since broadened that approach. *Riley*'s deviation from that path, and its failure to recognize both the realities of cell phone use and the interconnectedness of people generally, benefits criminals.

In *Maryland v. Buie*, the search incident to arrest standard was modified to respond to a situation in which an individual is arrested within a home.[83] Recognizing that arrests can be dangerous situations, the Court affirmed the police's ability to search for people in closets or other adjoining spaces from

---

76. *Id.*

77. *Definition of Remote Wipe*, PC MAG, http://pcmag.com/encyclopedia/term/66274/remote-wipe (last visited Oct. 11, 2015).

78. *Riley*, 134 S. Ct. at 2486.

79. *Id.* (emphasis added).

80. *Id.*

81. *Id.* at 2496 (Alito, J., concurring).

82. *Id.* at 2485–88 (majority opinion) (citing Chimel v. California, 395 U.S. 752, 763–64 (1969)).

83. *See* Maryland v. Buie, 110 S. Ct. 1093, 1098 (1990).

which an attack could be launched.[84] Although this expansion was based on officer safety, not on evidence destruction, it demonstrates that the Court is not only concerned with the actions of an arrestee, but also with the potential actions of others.

This reasoning is worth considering in today's interconnected world. People are more connected with one another than ever—often remaining in constant contact via their devices.[85] It is also well documented that offenders utilize cell phones and other technologies to remain in contact with each other.[86] Furthermore, in certain types of cases, such as domestic violence, prostitution, and human trafficking, offenders may use cell phones to remain in contact with their victims.[87] In either scenario, when an offender is arrested, there may be information on the offender's cell phone that the offender or others want to remain undiscovered by police. While the search incident to arrest exception is aimed at the desperate arrestee who may hide or destroy evidence within his reach due to the arrest, given the interconnectedness of people, criminal actors, and victims, it is misplaced to not acknowledge that a desperate cohort may take the same action, triggered by the same event: the arrest.

More concerning, however, is the *Riley* Court's statement that remote wipes are not "prevalent."[88] Even at the time of the opinion's drafting, this issue was well documented in the lower courts and in mainstream media.[89] While there were differing opinions among the lower courts on the relevance of the ability to remotely wipe, some courts did justify cell phone searches

---

84. *Id.* at 1098–99.

85. *See* AARON SMITH, PEW RES. CTR., AMERICANS AND TEXT MESSAGING 3 (2011), http://pewinternet.org/files/old-media/files/Reports/2011/Americans%20and%Text%20Messaging.pdf (finding that 83% of Americans own cell phones, 73% of cell phone owners text, and young adults receive an average of 109.5 texts per day); *Global Digital Communication: Texting, Social Networking Popular Worldwide*, PEW RES. CTR. (Feb. 29, 2012), http://www.pewglobal.org/2011/12/20/global-digital-communication-texting-social-networking-popular-worldwide ("[I]n 19 out of 21 countries, a majority of mobile phone owners regularly send text messages.").

86. *See* United States v. Lazcano-Villalobos, 175 F.3d 838, 842–844 (10th Cir. 1999); People v. Nottoli, 130 Cal. Rptr. 3d 884, 890–91 (Cal. Ct. App. 2011); EOGHAN CASEY & BENJAMIN TURNBULL, DIGITAL EVIDENCE ON MOBILE DEVICES, *in* EOGHAN CASEY, DIGITAL EVIDENCE AND COMPUTER CRIME ch. 20 (3d ed. 2011), www.booksite.elsevier.com/9780123742681/Chapter_20_Final.pdf; David Décary-Hétu & Carlo Morselli, *Gang Presence in Social Network Sites*, 5 INT'L J. CYBER CRIMINOLOGY 876, 878–80 (2011).

87. MARK LATONERO, THE RISE OF MOBILE AND THE DIFFUSION OF TECHNOLOGY-FACILITATED TRAFFICKING 10 (2012), http://technologyandtrafficking.usc.edu/files/2012/11/USC-Annenberg-Technology-and-Human-Trafficking-2012.pdf; Aarti Shahani, *Smartphones Are Used to Stalk, Control Domestic Abuse Victims*, NPR (Sept. 15, 2014, 4:22 PM), http://www.npr.org/sections/alltech considered/2014/09/15/346149979/smartphones-are-used-to-stalk-control-domestic-abuse-victims.

88. *See* Riley v. California, 134 S. Ct. 2473, 2486 (2014).

89. *See* Mat Honan, *Break Out a Hammer: You'll Never Believe the Data 'Wiped' Smartphones Store*, WIRED (Apr. 1, 2013), www.wired.com/2013/04/smartphone-data-trail; Bob Segall, *Cell Phone Warning: Deleted Personal Information Often Left Behind*, WTHR.COM (Mar. 11, 2013, 3:18 PM), www.wthr.com/story/21419450/cell-phone-warning-deleted-information-often-left-behind.

because of this capability.[90] Similarly, in 2012, mainstream media documented that "[a]ll of the major smartphone platforms have some kind of remote erase capability."[91] Various media sources list the types of phones with remote wiping capability, including all major phones such as iPhone, Android, Blackberry, and Microsoft.[92] Not only do the phones have this capability, but mainstream media and manufacturers also documented step-by-step instructions on how to wipe the devices, estimating that the time required to do so is approximately five minutes.[93] Therefore, at the time of the *Riley* opinion, the Court's notion, that the capability to remotely wipe a cell phone was not prevalent, was misplaced.

That presumption is even more incorrect today. In recent years the extent of government surveillance has captured the attention of the media.[94] In the wake of revelations by Edward Snowden of the government's massive data collection efforts, specifically the collection of data from phone calls, the public's concern regarding access to data has increased.[95] Moreover, with the rise of smartphones came a rise in the theft of these valuable devices.[96] As such, there is an increased consumer demand for the ability to wipe the data from one's phone.[97] Phone manufacturers responded by advertising and

---

90. *E.g.*, United States v. Valdez, No. 06-CR-336, 2008 WL 360548, at *3 (E.D. Wis. Feb. 8, 2008) (concluding that a search of a cell phone's address book and call history was reasonable because, among other reasons, testimony from law enforcement indicated that the cellular provider enabled customers to remotely delete all of the information located on the cell phone); United States v. Young, No. 5:05CR63-01-02, 2006 WL 1302667, at *13 (N.D. W. Va. May 9, 2006) (holding that exigent circumstances justified searching a cell phone for text messages when the cell phone had an option for auto deleting messages after one day).

91. Jamie Lendino, *How to Remotely Disable Your Lost or Stolen Phone*, PCMAG.COM (Apr. 12, 2012), www.pcmag.com/article2/0,2817,2352755,00.asp; *see also Smartphone Remote Wiping Feature Thwarts Secret Service, Law Enforcement,* HOMELAND SECURITY NEWS WIRE (May 19, 2010), http://www.homelandsecuritynewswire.com/smartphone-remote-wiping-feature-thwarts-secret-service-law-enforcement ("Smartphones such as Blackberry and iPhone offer a remote-wipe feature: if your phone is lost or stolen, you can remotely erase all the data stored on the phone; this feature protects one's privacy, but it also allow the accomplices of criminals and terrorists captured by law enforcement remotely to erase all incriminating and intelligence-relevant data from the suspect's phone before the police can access it.").

92. *See* Lendino, *supra* note 91; *Perform a Remote Wipe on a Mobile Phone*, MICROSOFT TECHNET, https://technet.microsoft.com/en-us/library/Aa998614(v=EXCHG.150).aspx (last modified Feb. 6, 2013).

93. *See, e.g.*, Jerry Hildenbrand, *Hands-on With the Android Device Manager Remote Wipe Feature*, ANDROIDCENTRAL (Aug. 7, 2013, 4:12 PM), www.androidcentral.com/hands-android-device-manager-remote-wipe-feature; Lendino, *supra* note 91; *iCloud: Erase Your Device*, APPLE, https://support.apple.com/kb/PH2701?locale=en_US (last modified Aug. 26, 2015).

94. *See* Bruce Schneier, *What's Next in Government Surveillance*, ATLANTIC (Mar. 2, 2015), www.theatlantic.com/international/archive/2015/03/whats-next-in-government-surveillance/385667/.

95. MADDEN ET AL., *supra* note 53.

96. *See, e.g.*, Dana Hedgpeth, *iPhone 'Snatch and Grab' Thefts on Metro Rise*, WASH. POST (Mar. 25, 2014), www.washingtonpost.com/blogs/dr-gridlock/WP/2014/03/25/thefts-of-electronic-devices-on-metro-rise.

97. *See* Donna Tapellini, *Smart Phone Thefts Rose to 3.1 Million in 2013*, CONSUMER REPS. (May 28, 2014, 4:00 PM), www.consumerreports.com/org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year.htm.

marketing this feature.[98] Not surprisingly, reports of smartphones being remotely wiped while in police custody followed.[99] Therefore, the notion that this capability is not prevalent or even a valid issue is misplaced.

The Court in *Riley* suggests that one reason remote wiping is not a problem is because of law enforcement's ability to protect cell phones from remote wiping by the use of a Faraday bag or another similar product that can prevent the cell phone from receiving a signal.[100] While the Court is correct that Faraday bags provide a technological advantage, the Court's overreliance on the existence of such technologies to dismiss legitimate concerns reflects a gap between the Court's experience and the realities facing law enforcement.

A Faraday bag or cage is a container in which law enforcement can place a cell phone after seizing to prevent it from receiving a signal from a phone network or Bluetooth.[101] These bags are designed to prevent remote access.[102] They are manufactured by several companies and marketed to law enforcement to combat cybercrime and retain evidence.[103] They vary in size, quality, and capability.[104]

After presuming that remote wiping was not prevalent, the Court in *Riley* went on to assert that, even if it were, the police could overcome it by simply either disconnecting the cell phone or using a Faraday bag, which it referred to as a "cheap" and "easy" solution.[105] The many sub-assumptions in this analysis underscore the gap between the pressures on today's law enforcement and the Court's perception of their capabilities.[106]

The Court's suggestion that law enforcement disconnect the cell phone ignores the obligations on law enforcement to avoid compromising the integrity of the evidence.[107] Disconnecting or turning off the cell phone may indeed alter it in ways that compromise its integrity.[108]

---

98. *See* sources cited *supra* note 93.

99. *See* Brief for Respondent at 9–10, Riley v. California, 134 S. Ct. 2473 (2014) (No. 13-132) (documenting cases of phones being wiped after arrest); Zack Whittaker, *Smartphones 'Remotely Wiped' in Police Custody, as Encryption vs. Law Enforcement Heats Up*, ZDNET.COM (Oct. 9, 2014), www.zdnet.com/article/smartphones-remotely-wiped-in-police-custody-as-encryption-vs-law-enforcement-heats-up.

100. *See Riley*, 134 S. Ct. at 2487.

101. *See* United States v. Flores-Lopez, 670 F.3d 803, 809 (7th Cir. 2012) (citing Department of Justice, Computer Crime and Intellectual Property Section, "Awareness Brief: Find My iPhone"); United States v. Lustig, 3 F. Supp. 3d 808, 815 (S.D. Cal. 2014).

102. *See Lustig*, 3 F. Supp. 3d at 815.

103. *See Riley*, 134 S. Ct. at 2487.

104. *See, e.g.*, *Faraday Pouches and Bags*, ARROWHEAD FORENSICS, www.crime-scene.com/store/faraday.shtml (last visited Oct. 11, 2015) (selling Faraday containers from $21.00 to $250.00); *Faraday Bags*, EDEC, https://www.edecdf.com/product-category/faraday-bags/ (last visited Oct. 11, 2015).

105. *Riley*, 134 S. Ct. at 2487.

106. *See id.* at 2486–89.

107. *See id.* at 2487.

108. *See, e.g.*, United States v. Flores-Lopez, 670 F.3d 803, 809 (7th Cir. 2012); RICK AYERS ET AL., NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T. OF COMMERCE, GUIDELINES ON MOBILE DEVICE

More importantly, the Court's characterization of the Faraday bag as a foolproof solution is misplaced. While certainly a positive technological development, the Court's reliance on Faraday bags as a flawless solution and dismissal of criticism is of concern.[109] While some Faraday bags are large and allow police to work on and manipulate the cell phone while it remains inside the bag or box by using a clear window, others are not.[110] Generally, a Faraday bag is only useful so long as a cell phone is within it.[111] A targeted remote wipe by an offender's ally, who could be constantly searching for the phone's signal to take advantage of its briefest removal from the bag, is possible. Even if the cell phone is inside of a Faraday bag, the risk of improperly sealing the container is real and could lead to cell phone access to a cell network.[112] Additionally, "Faraday containers . . . [do] not necessarily eliminate [radio signals] completely, allowing the possibility of communications being established with a cell tower, if in its immediate vicinity."[113]

The Court did not consider further information, which undermines its conclusions that the arrestee himself is not a threat and that Faraday bags resolve any real threat of remote wiping.[114] Some wiping of data occurs internally.[115] For instance, a person may alter the data on their phone through a so-called logic bomb.[116] A logic bomb is an alteration that is internally set up on a cell phone to activate if certain conditions are not met.[117] For example, a logic bomb may require the entry of a certain sequence of numbers into a cell phone at specific time intervals.[118] If that condition does not occur, the cell phone will destroy its own internal data.[119] Some cell phones are configured with "geo-fencing" that will automatically wipe the data when the phone leaves a certain geographic area.[120] A Faraday bag may not prevent the use of this technique, which the arrestee himself would cause.[121] Additionally, Faraday bags do nothing to prevent preprogrammed

---

FORENSICS (DRAFT) 30 (2013), http://www.nist.gov/forensics/research/upload/draft-guidelines-on-mobile-device-forensics.pdf.

109. *See Riley*, 134 S. Ct. at 2487.

110. *See* sources cited *supra* note 104.

111. *See Riley*, 134 S. Ct. at 2487.

112. AYERS ET AL., *supra* note 108.

113. *Id.*; *see* ERIC KATZ, A FIELD TEST OF MOBILE SHIELD DEVICES 1–2 (2010), http://docs.lib.purdue.edu/techmasters/33/.

114. *See Riley*, 134 S. Ct. at 2487.

115. *See* Eamon P. Doherty, *The Need for a Faraday Bag*, DFI NEWS (Feb. 21, 2014, 9:44 AM), www.forensicmag.com/articles/2014/02/need-faraday-bag.

116. *Id.*

117. *Id.*

118. *Id.*

119. *Id.*

120. AYERS ET AL., *supra* note 108, at 31.

121. *Id.* at 30–31.

deletions such as those associated with Snapchat and TigerText.[122] Furthermore, when a cell phone is in a Faraday bag, its battery life decreases because it is constantly searching for a network.[123] Continued failure to connect to a network "may cause certain mobile devices to reset or clear network data that otherwise would be useful if recovered."[124]

Moreover, the Court's presumption that Faraday bags are "cheap" is not as simple as it may seem.[125] Such a label turns on quality.[126] While it is true that some Faraday bags cost a few dollars on the Internet, some exceed $500.00.[127] The cost of professional Faraday bags aimed at law enforcement markets can range from approximately $58.00 to hundreds of dollars.[128] Concluding that Faraday bags are a viable solution for modern law enforcement presupposes a number of facts.

First, the Court assumes adequate funding exists to equip police officers to carry such bags on their person and immediately place a recovered cell phone into the bag upon arrest. Although it is recommended that law enforcement use such devices, the presumption that every police department can do so may be overly optimistic.[129] Most police departments are small and underfunded, not large, well-funded operations with the money to purchase Faraday bags for the 13.5 million arrests that take place annually in the United States.[130] Furthermore, most of those arrests take place in small police departments.

Notwithstanding the image of police departments projected by the media, approximately one-half (49%) of local law enforcement agencies employ less than ten officers, 24% employ less than five officers, and 4.9% have just one officer.[131] While the correlation is not perfect, it would stand to reason that small police departments perform several million arrests

---

122. Adam M. Gershowitz, *Seizing a Cell Phone Incident to Arrest: Data Extraction Devices, Faraday Bags, or Aluminum Foil as a Solution to the Warrantless Cell Phone Search Problem*, 22 WM. & MARY BILL RTS. J. 601, 608 (2013); Sean Gallagher, *Update: Boeing's Black—This Android Phone Will Self-Destruct*, ARS TECHNICA (Feb. 26, 2014, 3:01 PM), http://arstechnica.com/information-technology/2014/02/boeings-black-this-android-phone-will-self-destruct/.

123. AYERS ET AL., *supra* note 108.

124. *Id.*

125. *See* Riley v. California, 134 S. Ct. 2473, 2487 (2014).

126. *See Black Hole Data Bag*, EDEC, https://www.edecdf.com/promo/vector-bags/index.php (last visited Oct. 11, 2015).

127. *Id.*; *Faraday Pouches and Bags*, *supra* note 104.

128. *Faraday Pouches and Bags*, *supra* note 104; *Black Hole Data Bag*, *supra* note 126.

129. AYERS ET AL., *supra* note 108.

130. *Crime in the United States, 2009*, U.S. DEP'T JUST., https://www2.fbi.gov/ucr/cius2009/data/table_29.html (last updated Sept. 2010).

131. BRIAN A. REAVES, U.S. DEP'T OF JUST., LOCAL POLICE DEP'TS, 2013: PERSONNEL, POLICIES, AND PRACTICES 2 (May 2015), www.bjs.gov/content/pub/pdf/lpd13ppp.pdf. Fifty-seven percent of sheriffs' offices employ less than twenty-five sworn personnel, and twenty-five percent employ less than ten deputies. ANDREA M. BURCH, U.S. DEP'T OF JUST., SHERIFFS' OFFICES, 2007—STATISTICAL TABLES 2 (Dec. 2012), www.bjs.gov/index/cfm?ty=pbdetail&iid=4555.

annually. Although some small police departments encourage the use of Faraday bags, it is not likely that all small departments receive funding for enough Faraday bags of the requisite quality, and it is even less likely that these departments have a forensic department to examine the device.[132] Many police departments have to apply for federal funding to obtain equipment such as bulletproof vests.[133] The ability to buy Faraday bags and cages would likely be less of a priority.[134] Some rural departments report that this requirement will strain their budgets, and instead are trying to improvise with microwaves.[135] While the *Riley* Court indicated the use of aluminum foil as a viable replacement for Faraday bags, this too presents some challenges.[136]

There is little doubt that Faraday bags are a technological advancement. Compelling cases have been made that their use by law enforcement can provide a way in which cell phones can be preserved prior to obtaining a warrant.[137] This Article's concern is more on the Court's overreliance on these bags to dismiss any concerns and to draw sweeping conclusions.

---

132. *See* Lucian McCarty, *Forensic Frenzy: Higher Demand Being Placed on State Crime Labs*, SARATOGIAN (May 11, 2013, 12:01 AM), http://www.saratogian.com/general-news/20130511/forensic-frenzy-higher-demand-being-placed-on-state-crime-labs. If history is any lesson, police departments of all sizes struggle to keep up with the technical demands placed upon them. *See id.* For example, forensic examinations of computers take time and examiners. *Id.* The nation experienced a significant backlog in keeping up with them, and even the FBI experienced a significant backlog in processing its forensic evidence. *See* OFF. INSPECTOR GEN., U.S. DEP'T OF JUST., THE FEDERAL BUREAU OF INVESTIGATION'S EFFORTS TO COMBAT CRIMES AGAINST CHILDREN 29 (2009), https://oig.justice.gov/reports/FBI/a0908/final.pdf [hereinafter U.S. DEPT. OF JUST., CRIMES AGAINST CHILDREN] (finding hundreds of digital evidence cases waiting for processing and a nine-month delay); OFF. INSPECTOR GEN., U.S. DEP'T OF JUST., AUDIT OF THE FEDERAL BUREAU OF INVESTIGATION LABORATORY'S FORENSIC DNA CASE BACKLOG I (2012), https://oig.justice.gov/reports/2012/a1239.pdf (indicating a total of 403 backlogged forensic DNA cases). This is due to several obstacles, many of which have to do with funding. Even when local or more rural departments can benefit from a state-wide lab, the backlog can be lengthy due to cost. *See, e.g.*, McCarty, *supra*. The same is true for the examination of rape kits, with an estimated 400,000 of them never examined. Nora Caplan-Bricker, *The Backlog of 400,000 Unprocessed Rape Kits Is a Disgrace*, NEW REPUBLIC (Mar. 9, 2014), http://www.newrepublic.com/article/116945/rape-kits-backlog-joe-biden-announces-35-million-reopen-cases. While many local police departments rely on federal supplemental funding, that has also been the subject of budget cuts. *See generally* NAT'L CRIMINAL JUST. ASS'N & VERA INST. OF JUST., THE IMPACT OF FEDERAL BUDGET CUTS ON STATE AND LOCAL PUBLIC SAFETY (2012), http://www.ncja.org/sites/default/files/documents/NCJA-VERA-Summar-of-Sequestration-Survey-2012.pdf (indicating decreased federal funding to criminal justice stakeholder organizations).

133. *See* Paige Kelton, *JSO Was Denied Federal Grant to Buy Bulletproof Vests*, ACTIONNEWSJAX (Dec. 8, 2014, 10:15 PM) (noting that even larger police departments do not receive funds for vests).

134. *See id.*

135. *See* George Graham, *Greenfield Police Turn to Microwave Ovens as Improvised Faraday Cages as Department Adjusts to U.S. Supreme Court Ruling Requiring Warrants for Cell Phone Searches*, MASSLIVE (July 11, 2014, 3:09 PM), http://www.masslive.com/news/index.ssf/2014/07/greenfield_police_turn_to_micr.html.

136. *See* KATZ, *supra* note 113, at 32 (discussing shielding issues); Gershowitz, *supra* note 122, at 609 (arguing foil is a viable alternative).

137. Gershowitz, *supra* note 122.

The Court's presumption differs significantly from reality. This is not to say that Faraday bags are irrelevant. They certainly are an advantage for law enforcement and an important method to preserve evidence. It is the Court's overreliance on them to dismiss valid concerns that is troubling. This presumption that remote wiping is not a threat, or that Faraday bags resolve all the issues, reflects a lack of understanding of the technical uses of cell phones, as well as the real demands of modern policing.

2. Presumption 2: The Threat of Encryption Is Not a Significant Threat to Evidence Preservation

Distinct from remote wiping, encryption is a method of making data unreadable by others.[138] Many forms of encryption exist, but the *Riley* Court used it to describe situations beyond password protection when a phone locks and its "data becomes protected by sophisticated encryption that renders a phone all but 'unbreakable' unless police know the password."[139] The *Riley* Court did note that the arguments regarding encryption were not made in the lower courts, but went on to indicate that encryption was not a significant problem due to two factors.[140] First, the Court again assumed it was not a prevalent practice; it recognized that the capability could be found only on "some modern" cell phones.[141] Second, it concluded that the problem can be "fully prevented" by a Faraday bag or disabling the feature before it locks the device.[142] The Court again asserted that data encryption is not an action of the arrestee, but the "ordinary operation of a phone's security features" and, therefore, is not relevant to the search incident to arrest scenario.[143]

As with remote wiping, this concern about active evidence destruction is misplaced, as is the Court's narrow focus only on spontaneous (as opposed to pre-planned) active efforts to destroy evidence.[144] *United States v. Robinson* made clear that the search incident to arrest exception to the warrant requirement needed no further justification.[145] Police need not believe that the arrestee is actively destroying evidence to conduct a search incident to arrest.[146] It is only the risk that destruction could occur that allows police to search. Therefore, the fact that police do not see arrestees actively

---

138. United States v. Lustig, 3 F. Supp. 3d. 808, 816 (S.D. Cal. 2014).

139. Riley v. California, 134 S. Ct. 2473, 2486 (2014) (citing Brief for United States as Amicus Curiae Supporting Respondent at 11, *Riley*, 134 S. Ct. 2473 (No. 13-132), 2014 WL 1389032).

140. *Id.* at 2486–87.

141. *Id.* at 2486.

142. *Id.* at 2486–87.

143. *Id.* at 2486.

144. *See id.* at 2486–87.

145. *See* United States v. Robinson, 414 U.S. 218, 235 (1973).

146. *See id.* at 228–29.

destroying the evidence on their phones upon arrest seems less critical than the Court suggests in *Riley*.[147]

More troubling is the Court's suggestion that encryption is only available on a few phones.[148] This presumption is simply incorrect because virtually all major cell phone models have, or will have, this capability. "Content encryption capabilities are offered as a standard feature in many mobile devices or may be available through add-on applications."[149] This was the case for most cell phones for several years. For example, Android phones have had this feature since 2011.[150] Apple's products have been capable of encryption since 2009.[151] What has changed between 2011 and the present day is twofold. First, encryption features are now a default setting and the capability to wipe cell phones comes standard.[152] Second, in the past, law enforcement could access cell phone data under certain circumstances.[153] It could do so through a so-called back door.[154] This is no longer the case.[155] Moreover, even at the time of *Riley*'s announcement, numerous Internet sites and media outlets offered "simple" instructions on how to encrypt data on one's cell phone.[156]

Not only were the Court's presumptions inaccurate in 2014, the year *Riley* was announced, they are certainly no more true today. In 2015, the Washington Post accurately described the state of the field as follows:

> Both [Apple and Google] have now embraced a form of encryption that in most cases will make it impossible for law enforcement officials to collect evidence from smartphones—even when authorities get legally binding warrants.[157]

This was not an overstatement because all major cell phone companies provide phones with the ability to encrypt data with no back door way that allows access to law enforcement.

In September 2014, Apple announced that its phones and other products would feature such a high level of encryption that Apple itself will "lack the

147. *Riley*, 134 S. Ct. at 2486.

148. *See id.*

149. AYERS ET AL., *supra* note 108, at 24.

150. Craig Timberg, *Newest Androids Will Join iPhones in Offering Default Encryption, Blocking Police*, WASH. POST (Sept. 18, 2014), https://www.washingtonpost.com/news/the-switch/wp/2014/09/18/newest-androids-will-join-iphones-in-offering-default-encryption-blocking-police/.

151. AYERS ET AL., *supra* note 108, at 43.

152. *See* Tim Shiesser, *The FBI Slams Smartphone Encryption Because There's No Backdoor*, TECHSPOT (Sept. 26, 2014, 7:30 AM), http://www.techspot.com/news/58204-the-fbi-slams-smartphone-encryption-because-theres-no-backdoor.html.

153. *Id.*

154. *Id.*

155. *Id*.

156. *See supra* note 92 and accompanying text.

157. Timberg, *supra* note 150.

technical ability to unlock the phones or recover data for anyone—whether it be for police or even users themselves."[158] Google followed suit, announcing that its next version of its operating system would require all new phones to have full-disc encryption "enabled by default out of the box" as a standard feature.[159] While Google has not been able to fully implement this vision, it has not been due to a change of priority, but rather, it is due to performance issues.[160] It continues the course to do so.

The significance of these actions is that the most popular operating system in the world (Android) will have this encryption capability.[161] Furthermore, because Apple controls both the hardware and software of its products, it can implement this feature on not only its new products, but also on older products, which updates their operating system to enable them to not only be encrypted, but to have lockable encryption.[162]

Weakening the Court's presumption that few phones have this capability is the reality that not only do these companies offer this feature—they market based on it. For example, Tim Cook, CEO of Apple, wrote an open letter to Apple users stating that Apple "respect[s] your privacy and protect[s] it with *strong encryption*, plus strict policies."[163] Apple has further advertised itself as actively thwarting government efforts to obtain data, noting on its website that "[i]n its latest Who Has Your Back? report, the [Electronic Frontier Foundation] awarded Apple 5 out of 5 stars for our commitment to standing with our customers when *the government seeks access to their data*."[164]

Not surprisingly, this has caused great concern among law enforcement and national security figures.[165] In response to Apple's announcement of the data encryption in iOS 8, the Federal Bureau of Investigation (FBI) expressed that it was "'very concerned' about new steps Silicon Valley tech giants were taking to strengthen privacy protections on mobile devices."[166] While FBI Director, James Comey, has acknowledged the valid concern regarding protecting phones from being compromised, he has objected strongly to the

158. Timberg, *supra* note 150.

159. Andrew Cunningham, *Google Quietly Backs Away from Encrypting New Lollipop Devices by Default*, ARS TECHNICA (Mar. 2, 2015, 11:00 AM), http://arstechnica.com/gadgets/2015/03/google-quietly-backs-away-from-encrypting-new-lollipop-devices-by-default/.

160. *See id.*

161. *See* Timberg, *supra* note 150.

162. *See id.*

163. *Apple's Commitment to Your Privacy*, APPLE, http://www.apple.com/privacy (last visited Oct. 11, 2015) (emphasis added).

164. *Privacy: Government Information Requests*, APPLE, http://www.apple.com/privacy/government-information-requests/ (last visited Oct. 11, 2015) (emphasis added).

165. *See* Igor Bobic & Ryan J. Reilly, *FBI Director James Comey 'Very Concerned' About New Apple Google Privacy Features*, HUFFINGTON POST (Sept. 25, 2014), http://www.huffingtonpost.com/2014/09/25/james-comey-apple-encryption_n_5882874.html (quoting FBI Director James Comey).

166. *Id.*

aforementioned marketing techniques, which he characterized as advertising "something expressly to allow people to place themselves beyond the law[,] . . . market[ing] a closet that could never be opened."[167]

Similarly, Michael Rogers, head of the National Security Agency, has also acknowledged a legitimate concern about privacy, but openly criticized a "no back door" approach.[168] He advocates as a compromise that companies create a key that can open any system to access pictures or texts, but divide the key into pieces, such that no one entity could access all of the data.[169] He argues not for a "back door," but for a "front door" with multiple, strong locks that will protect individuals but also allow access for the government when needed.[170] This "split-key approach" has been the subject of debate in the public sphere with many identifying potential weaknesses, including some vulnerability to hackers and issues regarding key storage.[171]

This debate is a real one occurring in the public sphere. The ability of cell phone encryption and the complete inability of law enforcement to access cell phone data are well documented. "[I]n the wake of widespread government surveillance and increasingly serious privacy breaches by people with malicious intent, it looks like tech companies will continue to close down ways to access private data, even if that means shutting off access from law enforcement agencies."[172]

Yet the Court incorrectly presumes that encryption is a minor problem for law enforcement on only a small number of cell phones.[173] Such a presumption was incorrect at the time it was made, and has become even more misplaced as technologies develop.[174] Thus, the presumption underlying *Riley*'s rejection of this concern undermines the outcome of the case.

The same is true for the Court's suggestion that Faraday bags, although an incomplete solution, are a reasonable response.[175] It is difficult to imagine how a Faraday bag will preserve data if the encryption is automatic and there is no way to break the code. Furthermore, the *Riley* opinion is rather circular on this point. On the one hand, the Court advocates for obtaining access to the phone and disabling the encryption feature prior to its activation.[176] On the other hand, the Court notes that a search incident to arrest is not a solution

---

167. *Id.*

168. Ellen Nakashima & Barton Gellman, *As Encryption Spreads, U.S. Grapples with Clash Between Privacy, Security*, WASH. POST (Apr. 11, 2015), https://www.washingtonpost.com/world/national-security/as-encryption-spreads-us-worries-about-access-to-data-for-investigations/2015/04/10/7clc7518-d401-11e4-a62f-ee745911a4ff_story.html.

169. *See id.*

170. *See id.*

171. *See id.*

172. Shiesser, *supra* note 152.

173. *See* Riley v. California, 134 S. Ct. 2473, 2486–87 (2014).

174. *See* Shiesser, *supra* note 152.

175. *Riley*, 134 S. Ct. at 2487.

176. *Id.* at 2486–87.

to encryption because there is simply not enough time to pay attention to a cell phone during the heat of an arrest.[177]

Finally, the Court suggests that much of the information will be saved to the cloud and is thus available for access via a warrant.[178] However, one merely need not have their phone set up to back up to the cloud—not an unreasonable action for a criminal—to circumvent that solution. This brings one to the final presumption discussed in this Article, which regards warrants.

3. Presumption 3: "Just Get a Warrant"

The *Riley* Court concludes its decision with the following statement: "Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant."[179] Embedded within this "simple" statement is the presumption that obtaining a warrant is possible. The Court notes that obtaining a warrant is easier today than it was previously due to the use of technology to speed along the process.[180] But this quip invites the obvious questions: A warrant for what? A warrant served upon whom?

If the warrant is to search the cell phone, what is the utility of the warrant if the concern was remote wiping? In that scenario, there is nothing to search. Similarly, no one, including the manufacturer or law enforcement, can access an encrypted phone.[181] Indeed, as Tim Cook advertised to Apple users, one of the very purposes of encrypting its cell phones is to thwart government access.[182] Therefore, a warrant for an encrypted phone is equally as anemic and ineffectual. While in Great Britain there may be a law that requires a suspect to disclose his password, the Fifth Amendment precludes this from being the case in the United States.[183] Thus, routine remote wiping of cell phones can create a measurable effect on the most legitimate methods of evidence collection.

Even if law enforcement could establish that information was actually available, the next obstacle would be identifying on whom they should serve the warrant.[184] As discussed previously, many cell phone manufacturers and operating system developers have taken steps to actively thwart law

---

177. *Id.* at 2487.

178. *Id.* at 2491–92.

179. *Id.* at 2495.

180. *See id.* at 2493.

181. *See supra* text accompanying notes 158–63.

182. *See supra* text accompanying note 165.

183. *See* United States v. Kirschner, 823 F. Supp. 2d 665, 669 (E.D. Mich. 2010) (indicating that the government cannot compel a defendant to reveal his password because it would "communicate[a] factual assertion to the government and thus, is testimonial").

184. FED. R. CRIM. P. 41(e)(2)(a) (discussing that after a judge issues a warrant, the warrant must identify the person or property to be searched).

enforcement efforts.[185] They actually advertise their inability to comply with a law enforcement request:

> Unlike our competitors, Apple cannot bypass your passcode and therefore cannot access this data. So it's not technically feasible for us to respond to government warrants for the extraction of this data from devices in their possession running iOS 8.[186]

Although much of the data could stay on the iCloud and be accessible through a warrant, programming the cell phone to not back up to the iCloud easily prevents such access.[187] The reality is that a warrant will not assist law enforcement if the information sought is not accessible.[188]

V. SIGNIFICANCE

The Supreme Court has made a determination of what is a reasonable search incident to an arrest and concluded, in this instance, that it is reasonable for law enforcement to obtain warrants.[189] However, the Court based this conclusion in some part on incorrect or flawed presumptions—either due to its own gap between reality and experience, or the inability of any judicial institution to keep pace with rapidly changing technologies.[190] While the *Riley* holding itself may not be incorrect (it may be that the level of intrusion outweighs the government interest), it exemplifies an approach to solving complicated issues that occur at the intersection of the Fourth Amendment, privacy, and technology that is problematic.[191] The Court's approach is problematic because it precludes the evolution of long-term jurisprudence in an area of the law that critically needs guidance. This development is hindered in the same way a house built on sand can never be sturdy. The *Riley* decision will not withstand the test of time, as its basis is compromised from the beginning.

To be sure, there are some who do not regard this as problematic at all.[192] There are valid criticisms of the notion that the government should have a right to access cell phone data.[193] Indeed, safe manufacturers are not required

---

185. *See supra* notes 164–65.

186. Jay McGregor, *Apple Beefs Up iOS8 Security With Unbreakable Passcode*, FORBES (Sept. 18, 2014, 7:04 AM), http://www.forbes.com/sites/jaymcgregor/2014/09/18/ios8-beefs-up-security-with-unbreakable-passcode (quoting Apple CEO Tim Cook regarding its privacy policy).

187. *See id.*

188. *See id.*

189. *See* Riley v. California, 134 S. Ct. 2473, 2495 (2014).

190. *See supra* Parts III, IV.

191. *See generally Riley*, 134 S. Ct. at 2473 (discussing Fourth Amendment and privacy concerns regarding digital data stored on cell phones).

192. *See* Leary, *Missed Opportunity*, *supra* note 4, at 351.

193. *See* Shiesser, *supra* note 152.

to include in construction a way the government can always use to enter a safe and read the papers stored therein.[194] It is a legitimate argument that cell phone manufacturers should not be made to do so either. Chief Justice Roberts, writing for the majority in *Riley*, quite rightly notes that "[p]rivacy comes at a cost."[195] Moreover, many of the extreme examples of abusive police searches, mentioned in amici and in the majority opinion, could indeed occur in an unrestrained, blanket search of cell phones. However, the Court's approach continues to be problematic on both a practical and philosophical level.

A. Riley *Exemplifies Practical Shortfalls*

Riley demonstrates some of the practical problems that arise from the judicial digital divide. Many cases exist in the middle ground between the two alternatives the Court mentions.[196] The Court dwells on two extremes. First, it expresses concern about the extreme invasion of privacy a nefarious law enforcement official could engage in if he actually sought to violate an individual's privacy.[197] The Court also asserts that no significant harm will result from its ruling because in some cases an exigency will exist that relieves the requirement of a warrant.[198]

Such a perspective further illustrates a gap in the Court's understanding of both the reality of modern policing and the role of some technologies in modern life and criminality.[199] These cases involve neither extreme exigencies, which would merit a warrantless search, nor police abuse. But they do involve a serious type of case in which a cell phone, given its ubiquity in modern life, likely contains available and important evidence. For example, in sex trafficking cases, the offenders are often some of the most brutal: engaging in torture-like tactics to buy and sell women and children into lives of slavery.[200] It is well documented that such offenders stay in contact with and keep control over their victims through digital devices and

194. *See* United States v. Castro, No. 88-3044, 1989 WL 42903, at *1 (9th Cir. Apr. 24, 1989).

195. *See Riley*, 134 S. Ct. at 2493; *see also id.* at 2491 ("[T]he Founders did not fight a revolution to gain the right to government agency protocols.").

196. *See, e.g.*, State v. Robinson, 786 N.W.2d 463, 472 (Wis. 2010).

197. *Riley*, 134 S. Ct. at 2492 ("It would be a particularly inexperienced or unimaginative law enforcement officer who could not come up with several reasons to suppose evidence of just about any crime could be found on a cell phone.").

198. *See id.* at 2487.

199. *See supra* Part III.

200. *See* Michael J. Frank & G. Zachary Terwilliger, *Gang-Controlled Sex Trafficking*, 3 VA. J. CRIM. L. 342, 364 (2015); Press Release, U.S. Attorney Dist. Md., New York Pimp Conviction in Maryland Sex Trafficking and Gun Crimes (May 8, 2013), www.justice.gov/usao-md/pr/new-york-pimp-convicted-maryland-sex-trafficking-and-gun-crimes.

technologies such as GPS, texting, etc.[201] Furthermore, they are often interconnected with other members of their trafficking organization and utilize cell phones to arrange purchases.[202] In a case in which a purchaser or co-trafficker is arrested, the cell phone may be the only lead to the trafficker.[203] While there may be reason to search the phone, there is not an exigency on the level of what Chief Justice Roberts demands in *Riley*.[204] Under the current regime, a regime based on false premises, this criminal's phone cannot be accessed in a timely manner, and perhaps the only avenue to a perpetrator is lost.

B. Riley *Exemplifies and Contributes to a More Profound Problem*

This leads to the philosophical objection to this false-premise approach unaddressed by the Court in *Riley*, notwithstanding that it furthered the current regime. Currently, the very same commercial entities that created a climate in which massive amounts of data are collected, but the government cannot access, are profiting from it.

The atmosphere around digital data has changed. The Edward Snowden leaks revealed previously unknown government surveillance of Americans' data.[205] The public has also learned of several unauthorized hacks into iCloud accounts,[206] corporate databases,[207] and government databases.[208] Consequently, customers and individuals are pushing back against companies that acted in concert with the government during its surveillance efforts.[209] This

---

201. *See Pimp-Controlled Online Advertisement*, POLARIS PROJECT, http://www.polarisproject.org/topics/332-sex-trafficking-pimp-controlled-online-advertisement (last visited Oct. 11, 2015) (documenting how trafficker monitored victim through cell phone).

202. *See* United States v. Nyuon, No. CR. 12-40017-01-KES, 2013 WL 1338192, at *1 (D.S.D. Mar. 29, 2013); Chamberlain v. Marshall, No. SACV 08-1468-AG (MLG), 2009 WL 2392093, at *2 (C.D. Cal. Aug. 4, 2009); LATONERO, *supra* note 87.

203. *Nyuon*, 2013 WL 1338192, at *1.

204. *See* Riley v. California, 134 S. Ct. 2473, 2494 (2014).

205. *See* Lorenzo Franceschi-Bicchierai, *The 10 Biggest Revelations from Edward Snowden's Leaks*, MASHABLE (June 4, 2014), http://mashable.com/2014/06/05/edward-snowden-revelations.

206. *See, e.g.*, James Cook, *Hackers Just Released a Tool That Could Threaten Everyone's iCloud Account*, BUS. INSIDER (Jan. 2, 2015, 7:38 AM), http://businessinsider.com/hacker-tool-for-icloud-account-2015-1.

207. *See, e.g.*, Shelly Banjo, *Home Depot Hackers Exposed 53 Million Email Addresses*, WALL STREET J. (Nov. 6, 2014, 8:03 AM), http://wsj.com/articles/home-depot-hackers-used-password-stolen-from-vendor-1415309252; Charles Riley & Jose Pagliery, *Target Will Pay Hack Victims $10 Million*, CNN MONEY (Mar. 19, 2015, 3:05 AM), http://money.cnn.com/2015/08/19/technology/security/target-data-hack-settlement.

208. *See, e.g.*, Mike Levine, *OPM Hack Far Deeper Than Publicly Acknowledged, Went Undetected for More Than a Year, Sources Say*, ABC NEWS (June 11, 2015, 4:59 PM), http://abcnews.go.com/politics/opm-hack-deeper-publicly-acknowledged-undetected-year-sources/story?id=31689059.

209. *See* Gregory Wallace, *Lawsuits Piling Up on Target Over Hack*, CNN MONEY (Dec. 24, 2013, 11:17 AM), http://money.cnn.com/2013/12/23/news/companies/target-credit-card-lawsuits.

is arguably a positive development for individuals seeking to control their privacy.

The resulting regime, however, is a fiction. The very companies that advertise they protect customer privacy from the government collect personal identifying information and aggregated data on their customers, often without their meaningful, voluntary consent, and sell it to private entities.[210] For example, Apple is a defendant in a class action suit alleging that it collected personal identifying information on some of its customers on one of its commercial platforms.[211] While Apple claims to protect its customers' privacy from the government, its own terms of use state that it "reserve[s] the right to 'make certain . . . information available to strategic partners.'"[212]

Similarly, Google combines information about its customers across services and platforms, and stores the information indefinitely.[213] It has stated that "[w]hen you use our services *or view content provided by Google*, we automatically collect and store certain information in server logs."[214]

The result of such a regime is that these companies play a role in creating this conundrum faced by the courts. They have designed a world in which companies have unrestrained access to information from individuals—often taken without any meaningful consent by the individual. They collect, house, and sell the information so that the only entity without access to it is the government.[215] This sort of legal fiction turns privacy on its head. Not only does privacy come at a cost, as Chief Justice Roberts argues, but it creates an illogical framework.[216] Because the citizenry is pushing back against a loss of privacy, it seems the only manageable target is law enforcement's access to private information. The result is a system in which only law enforcement is precluded from accessing information when the real threat to privacy is commercial entities.

VI. THE FUTURE

A factor driving this perverse world in which individuals have no actual privacy from commercial entities, but these same entities conspire with individuals to preclude an underfunded police department from accessing personal information, is cell phone technology itself. Our technological

---

210. *See* Leary, Katz *on a Hot Tin Roof*, *supra* note 4, at 343–56.

211. *See Apple Customer Data Collection Class Action Lawsuit*, BIGCLASSACTION.COM, http://bigclassaction.com/lawsuit/Apple-data-collection-lawsuit.php (last updated Jan. 22, 2014).

212. *Id.*

213. Mark Milian, *Google to Merge User Data Across its Services*, CNN (Jan. 25, 2012, 8:18 PM), http://www.cnn.com/2012/01/24/tech/web/google-privacy-policy.

214. *Welcome to the Google Privacy Policy*, GOOGLE, www.google.com/policies/privacy (last modified Aug. 19, 2015) (emphasis added).

215. *See* Leary, Katz *on a Hot Tin Roof*, *supra* note 4, at 343–56.

216. Riley v. California, 134 S. Ct. 2473, 2493 (2014).

environment is rapidly changing, and thus it is difficult for courts to develop rules that are responsive to the realities of the modern day. But the Court's response that law enforcement simply needs to work harder, based on flawed presumptions, seems an inadequate remedy.[217] Conversely, the notion that the government has a right of access to vast quantities of information simply because it exists is equally as problematic.

Chief Justice Roberts correctly notes that "the Founders did not fight a revolution" for the right to protocols.[218] But the Founders also did not fight a revolution to prevent police from effectively investigating crime because their hands are tied by commercial conditioning and courts' misapplied presumptions.

Several suggestions exist to address cell phone search situations. While none are perfect, when analyzed by the Court, they should not be critiqued and ultimately rejected based on false presumptions. For example, the *Riley* Court rejected applying the *Arizona v. Gant* approach to cell phones.[219] In *Gant*, the Court held that police may only conduct a search of a vehicle incident to arrest when either the arrestee is unsecured or there is reason to believe the vehicle holds evidence of the crime of arrest.[220] The *Riley* Court rejected *Gant*'s compromise approach because of the unique characteristics of automobiles, namely the driver's decreased expectation of privacy and the heightened need for prompt law enforcement searches.[221] That presumption, however, was again incorrect. Research of Americans' expectations of privacy reveals that the majority of Americans feel their information is not private from the government or private companies.[222] Similarly, just as in a car search, there is a heightened need for government searches of cell phones because the information is fleeting.

The Court in *Riley* acknowledged the types of information available in a cell phone.[223] Given the aforementioned discussion of encryption and remote wiping, this information is also fleeting.[224] As Chief Justice Roberts reiterated for the majority in *Riley*, the focus of the Court's analysis should be on the data within the phone, not the phone itself.[225] That data, like the evidence in the vehicle in *Gant*'s, is equally fleeting.[226]

---

217. *See id.* at 2495.
218. *Id.* at 2491.
219. *See id.* at 2492.
220. Arizona v. Gant, 556 U.S. 332, 343 (2009).
221. *See Riley*, 134 S. Ct. at 2492.
222. MADDEN ET AL., *supra* note 53.
223. *Riley,* 134 S. Ct. at 2492.
224. *Id.* at 2478.
225. *See id.* at 2478–79 (explaining that cell phone searches paint a broader picture for police than findings of isolated records).
226. *See id.* at 2478.

Therefore, the Court's rejection of the *Gant* approach was again based on a digital divide between the Court's perception of the nature of the information on a cell phone and the reality. Such frameworks do not move Fourth Amendment privacy protections forward.

Other solutions exist. Many of these are imperfect. They include some exceptions to the warrant requirement,[227] but they fall short of the search incident to arrest exception's preference for clear rules and requirement of a warrant. This approach is almost analogous to the automobile exception, which would build upon the fleeting nature of the cell phone evidence.[228] The problem with this approach is that the Court rejected a similar analogy between luggage and automobiles in *Chadwick v. United States*[229] and rejected the automatic, albeit slow, destruction of evidence produced by blood-alcohol dissipation in *Missouri v. McNeely*.[230]

Another possible course for the Court is to follow the suggestion of the majority in *Riley* and loosen exigency restrictions.[231] This approach, however, would lead to unpredictability and a lack of consistency. Others have noted that mirroring phones would solve the problem.[232] But, given the number of police departments without adequate funds, pursuing such a plan poses other negatives.[233] Finally, the Author argues elsewhere that limiting the commercial availability of information may protect people from law enforcement obtaining it.[234]

The proper remedy for cell phone searches incident to arrest exceeds the scope of this Article. This Article focuses on the systemic falterings of the Court's currently flawed approach. That is, the more significant concern is the one with broad effects.

Many social norms change over time. The social norm of privacy, and what is reasonable to expect regarding it, changes rapidly and continuously. Fueled by technological advances, differing experiences, and diverse views of digital life, changes in expectations around privacy are even more complex. In the middle of this ever-transforming world, the Court finds itself tasked with the challenge of determining what is reasonable.[235] This is a challenge that must be answered effectively because individuals, law enforcement, and lower courts need principle-based guidance.

---

227. *Id.*

228. *See* United States v. Jones, 132 S. Ct. 945, 948 (2012).

229. *See* United States v. Chadwick, 433 U.S. 1, 10–16 (1977), *abrogated by* California v. Acevedo, 500 U.S. 565 (1991).

230. *See* Missouri v. McNeely, 133 S. Ct. 1552, 1560–61 (2013).

231. *See Riley*, 134 S. Ct. at 2493–95.

232. *See* United States v. Flores-Lopez, 670 F.3d 803, 809 (7th Cir. 2012).

233. *See* Graham, *supra* note 135 (explaining that the Supreme Court's ruling requiring police to obtain search warrants before searching cell phones strained the police department's budget).

234. Leary, *Missed Opportunity*, supra note 4, at 331.

235. *See* United States v. Jones, 132 S. Ct. 945, 958–64 (2012) (Alito, J., concurring).

While no simple solution exists to this complex problem, steps can be taken. Primary among them is working to address and close the judicial digital divide. This can be done by not only actions of the judiciary, but also by all stakeholders interested in a long-term jurisprudence.

Heeding to the repeated counsel of Justice Alito, who seems to see this challenge most clearly, can address this gap.[236] In *Jones*, he recognized the turbulent landscape that digital advances create and called upon the legislature to act.[237] Regarding technology, he insightfully noted:

> Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes. New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile.[238]

Then in *Riley*, he expanded upon this point:

> In light of these developments, it would be very unfortunate if privacy protection in the 21st century were left primarily to the federal courts using the blunt instrument of the Fourth Amendment. Legislatures, elected by the people, are in a better position than we are to assess and respond to the changes that have already occurred and those that almost certainly will take place in the future.[239]

Therefore, the first step in removing the judicial digital divide is addressing it. One way to address it is to relieve the Court from some of the challenge because it is not well suited as an institution to address these issues.

Legislatures must act. This branch of government is most able to assess privacy considerations and is most equipped to understand the demands and constraints on local law enforcement. As such, legislatures are more likely able to accurately measure a reasonable balance between the two.

Justice Alito astutely notes, however, that the Fourth Amendment is not the best instrument for regulating privacy.[240] Legislatures should also heed this counsel and understand that the failure to regulate private industries' collection and sale of personal data has profound consequences. It creates a climate in which individuals feel they have no privacy and then turn to courts to regain control. But those court cases are often criminal, and the desire for control over privacy can only target the government, not the entities that are the greatest threat to privacy. This nuance leads to the incongruous result that allows private industries to invade privacy and access information

---

236. *See id.*
237. *Id.*
238. *Id.* at 962
239. Riley v. California, 134 S. Ct. 2473, 2497–98 (2014) (Alito, J., concurring).
240. *See id.*

readily available to them, whereas law enforcement—who arguably has a legitimate need to do so at times—is artificially cordoned off from doing so.

Not all issues, however, can be resolved legislatively. In fact, the Fourth Amendment exists so that individuals are not left at the mercy of a government that is insensitive to privacy concerns. Here, other stakeholders can work to close the gap. Litigants must present evidence and expert information regarding the details and capabilities of technology, both current and expected. That is not to say that Fourth Amendment issues should be resolved based on technology. That is not the case. A court can offer principles consistent with Fourth Amendment jurisprudence only after a full understanding of the technology's uses and effects on law enforcement and the government. Therefore, lower courts, faced with busy dockets and numerous motions to suppress, must develop the record in this way for appellate courts.

Appellate courts, and ultimately the Supreme Court, must have full information regarding these issues as part of the cases before them, so that the gap between their experience and modern-day life can close. Some of that responsibility falls upon appellate courts to seek out the creation of a full record. These courts should invite specific amici to develop briefing on the technology and the increasing challenges it brings, as well as the actual abilities of law enforcement to accomplish the tasks faced with these challenges.[241] An understanding of the technology is insufficient if it does not accompany an understanding of how offenders utilize it, how citizens perceive it, and how law enforcement can respond to it. Courts must not wait for amicus parties to come forward. Then the Court is left to sort out the facts based on what others framed the issue to be. Rather, to close the gap, appellate courts, including the Supreme Court, must invite parties to brief on precise issues to gain an unbiased and balanced understanding of technology and its impacts. While litigants must create the factual record for the appellate process, as Justice Black noted, "[m]ost of the cases before this Court involve matters that affect far more people than the immediate record parties."[242] They also affect far more people than those with views expressed by interest groups with the funding and time to inject their interest into a case.

These measures may close the judicial digital divide and the Court's jurisprudence in this area may sit on more solid and long-standing footing. Until that time, privacy will likely continue to erode and law enforcement's efforts to fulfill its function will remain artificially handicapped.

---

241. *Cf.* FED. R. APP. P. 29 (explaining that the United States or a state may file a request for an amicus curiae without the agreement of the parties or leave of court, but any other party requires consent by both parties or by leave of court); Brian P. Goldman, Note, *Should the Supreme Court Stop Inviting Amici Curiae to Defend Abandoned Lower Court Decisions?*, 63 STAN. L. REV. 907, 916–17 (2011) (emphasizing the use of amicus curiae in the 1980s and its popularity among legal officers).

242. Order Adopting Revised Rules of the Supreme Court of the United States, 346 U.S. 945, 947 (1954).

VII. CONCLUSION

The role of technology in everyday life is increasing at every moment. This allows people to utilize technology in new ways, integrating it into the norms of daily living. Technology also allows criminals more access to victims and law enforcement more avenues of investigation. Consequently, when the government is seeking to execute its duties of crime control and investigation, it should take great caution to prevent law enforcement from intruding into private, protected information. Similarly, criminal elements should not be enabled to take advantage of all the benefits this technology creates without law enforcement norms also being adjusted for this new reality.

What is reasonable is a measure for the judiciary to decide when the legislative measure fails. In that capacity, courts must strive to develop a long-lasting jurisprudence based on principles, not technology. To do so, however, they must understand the technology, its uses, and the demands on law enforcement to respond. Only when the judicial digital divide is closed can we hope for consistent guidance for law enforcement, lower courts, and citizenry as a whole.