Pocket-Sized Privacy: The Supreme Court's Coming Clash Over Digital Searches

David A. Lord*

ABSTRACT

Lower courts are deeply divided over how the Fourth Amendment's particularity requirement applies to search warrants for cell phones and other electronic devices. Some courts grant law enforcement broad latitude, permitting searches of cell phones with minimal restrictions. Others demand strict constraints on the execution of searches, imposing limitations such as temporal filters and app-specific boundaries. Without intervention, this legal dispute threatens to undermine privacy protections in the digital age and sow doctrinal confusion in the lower courts.

This Article argues that the Supreme Court will soon need to reconcile these divergent approaches and proposes a framework for doing so. While some scholars have called for either sweeping restrictions or broad deference to law enforcement, these approaches fail to anchor their proposals in the Court's own Fourth Amendment jurisprudence.

DOI: https://doi.org/10.15779/Z38BC3T06R

* David A. Lord is a career prosecutor and adjunct professor in criminal procedure. He has been a prosecutor for the City of Alexandria, Virginia, for 20 years and currently supervises that office's violent crimes unit. He also teaches criminal procedure at George Mason University's Antonin Scalia Law School and serves as a contract instructor for law enforcement officers and prosecutors through Justice3D. He previously published four law review articles that examine prosecutorial ethics in prosecutorial discretion, plea negotiations, trial advocacy, and exculpatory evidence. The author is grateful to his husband, Greg Parks, and to his accountability partner, Jared Asch, for their constant encouragement, support, and insistence on excellence.

By contrast, this Article draws on the Supreme Court's efforts to adapt traditional Fourth Amendment principles to emerging technologies and identifies three essential standards for any new rule: (1) consistency with the philosophical rationales underlying traditional Fourth Amendment doctrines; (2) preservation of the level of privacy protection that existed at the time of the Fourth Amendment's adoption; and (3) doctrinal workability in the face of rapid technological change. Applying these standards, the Article surveys the Supreme Court's particularity and good-faith reliance cases, analyzes the existing split among lower courts, and offers a set of model rules for resolving these conflicts. This framework provides a roadmap for a coherent, principled, and practically enforceable particularity doctrine in the digital era.

INTRODUCTION

Fourth Amendment litigation has moved squarely into the digital world. Whether the crime is drug possession or homicide, cell phones provide the prosecutor with a mountain of potential evidence, but in a way that clearly impacts the privacy interests of the person charged with the offense. Location data, text messages, internet search histories, and the use of ubiquitous cellular apps like Uber provide volumes of investigative leads that police can follow in cases and evidence that prosecutors can use to obtain a conviction. Our lives are so intertwined with technology that if the government has full access to our phones, there is virtually no component of our personal life that is not exposed. Financial transactions, political viewpoints, immigration status, sexual orientation, gender identity, who we talk to, and where we go, are all contained in this small device that everyone keeps in their pocket.

An issue that criminal courts are increasingly forced to address is whether there should be limitations on where or how the government can search for evidence of a crime when they have obtained a search warrant for a cellphone or other electronic device. Can law enforcement officers read all a suspect's emails and text messages? Can prosecutors rummage through every photograph and application on the defendant's cellphone in the hunt for evidence to use against them? Or does the particularity requirement of the Fourth Amendment, requiring a warrant to be supported by an affidavit "particularly describing the place to be searched, and the persons or things to be seized,"[1] create guardrails that limit how far the government can search within an electronic device when investigating a crime?

The resolution of these questions is of vital importance as more of our lives move online and our phones and computers store ever-increasing amounts of information about us. As a result of this digital transition, law enforcement officers and prosecutors continue to increasingly rely on the searches of electronic devices to find evidence. Whether and how those efforts are constrained will shape criminal investigation and prosecution in the future. So far, the Supreme Court has not squarely answered the question of whether the particularity requirement in the Fourth Amendment limits how intrusive a law enforcement officer's search of an electronic device can be. This has resulted in inconsistent rulings by the lower courts.

It is not the case that the Supreme Court has fallen entirely behind the times or is failing to address any criminal procedure cases that implicate new

1. U.S. CONST. amend. IV.

technology. In fact, three cases in the last 25 years, *Riley v. California*,[2] *Carpenter v. United States*,[3] and *Kyllo v. United States*,[4] demonstrate the Court's understanding that traditional Fourth Amendment jurisprudence faces limits when it comes to the digital world and must evolve with modern times. Moreover, the manner in which the Court resolved these cases offers insight into how it might answer the question of whether the particularity requirement constrains the reach of search warrants for electronic devices.

Part One of this law review article will examine the Court's rulings in *Riley*, *Carpenter*, and *Kyllo* to understand the constraints of traditional criminal procedure doctrine on the digital world, and to look for clues about how the Court approaches rules that apply to the Fourth Amendment and technological advances. This section will also examine the Supreme Court's language from a fourth case, *City of Ontario v. Quon*,[5] to gain an understanding of why the Court is sometimes slow to accept and resolve criminal cases involving new technology. From these four cases, I derive three standards that I believe the Supreme Court would require any rule governing the applicability of the particularity requirement to the search of electronic devices to satisfy. Part Two of the article will explore the jurisprudential history of the particularity requirement. Part Three will address how lower courts have applied the particularity requirement when it comes to the search of electronic devices and where the disputes between those opinions lie. Part Four will address how the Supreme Court could approach this issue and rule in a way that is consistent with the three-standard framework distilled from its earlier case law.

I. HOW *RILEY*, *CARPENTER*, *KYLLO*, AND *QUON* ILLUMINATE THE SUPREME COURT'S APPROACH TO NEW TECHNOLOGY AND THE FOURTH AMENDMENT

Riley, *Carpenter*, and *Kyllo* demonstrate that the Supreme Court understands that traditional Fourth Amendment doctrines have limits when it comes to their applicability in a digital world and need to be reimagined, while still sustaining the philosophical rationale that led to the creation of the doctrines in the first place. However, the reason the Court is hesitant to dive deeper into these issues is explained by its method of resolving a fourth case, *Quon*. This section will examine each of these cases in turn and derive three standards that the Supreme Court will expect a rule governing the applicability of the particularity requirement to the search of electronic devices to satisfy. Specifically, (1) consistency with the philosophical rationales underlying traditional Fourth Amendment doctrines; (2) preservation of the level of privacy protection that existed at the time of the Fourth Amendment's adoption; and (3)

2. 573 U.S. 373 (2014).
3. 585 U.S. 296 (2018).
4. 533 U.S. 27 (2001).
5. 560 U.S. 746 (2010).

doctrinal workability in the face of rapid technological change. In the discussion of *Riley*, *Carpenter*, and *Kyllo*, I begin by explaining the traditional Fourth Amendment doctrine at issue in the case and then illustrate how new technology rendered the traditional application of that doctrine problematic.

A. The "Search Incident to Arrest Doctrine" and Riley v. California

The first standard that the Supreme Court will expect of any rule governing the applicability of the particularity requirement to the search of electronic devices is consistency with the philosophical rationale that underlies traditional Fourth Amendment doctrines. In other words, as will be illustrated in this section, if the application of a traditional doctrine from outside of the digital world is applied to the search of an electronic device, it should not result in a disconnect with the principles that led the Court to create the doctrine in the first place. *Riley* provides a great illustration of this concept by taking a traditional Fourth Amendment doctrine (search incident to arrest), applying it in a digital context (the search of a smartphone on an arrestee's person), and seeing how the rationales that led to the doctrine are not advanced by that application. Moreover, the Supreme Court's unwillingness to simply apply the doctrine in this context for that reason highlights why the standard of philosophical consistency will be applied.

1. Foundational "Search Incident to Arrest" Doctrine Caselaw

One of the earliest references to the "search incident to arrest" doctrine was a 1913 case, *Weeks v. United States*.[6] In that case, the defendant was convicted of using the mail system to transport shares of a lottery.[7] Police arrested the defendant at his place of work, and later obtained evidence against him by searching his home without a warrant.[8] While *Weeks* is frequently cited as a jurisprudential underpinning to the exclusionary rule,[9] its dicta regarding searches incident to arrest is illuminating. The Court noted that part of what

6. 232 U.S. 383 (1913).
7. *Id.* at 386.
8. *Id.* at 387.
9. The exclusionary rule curtails the use of evidence by the prosecution in a criminal case under certain circumstances, when it was obtained by the police in violation of a defendant's constitutional rights. While *Weeks* established this rule in federal cases when evidence was obtained in violation of a defendant's Fourth Amendment rights, this rule was not initially applied to the states. *See* Wolf v. Colorado, 338 U.S. 25 (1949). This changed approximately two decades later, when the Supreme Court held that the exclusionary rule was binding on the states as well. *See* Mapp v. Ohio, 367 U.S. 643 (1961). The Court also applies the exclusionary rule in cases where police obtain statements in violation of a defendant's Fifth and Sixth Amendment rights. *See e.g.*, Miranda v. Arizona, 384 U.S. 436 (1966); Dickerson v. United States, 530 U.S. 428 (2000); Massiah v. United States, 377 U.S. 201 (1964). The exclusionary rule is not absolute and has numerous exceptions, one of which features prominently in this article. See Part II(B) *infra* (discussing the good faith reliance exception to the exclusionary rule when an officer relies on a magistrate's flawed finding of probable cause to support the issuance of a search warrant).

distinguished this case is that it did not implicate "the right on the part of the government always recognized under English and American law, to search the person of the accused when legally arrested, to discover and seize the fruits or evidence of crime. This right has been uniformly maintained in many cases."[10]

A decade later in *Carroll v. United States*,[11] the Court made clear that this language did not restrict the search of an arrestee to his person, but also included the area "in his control."[12] While subsequent case law vacillated on precisely what this meant, it was given greater direction by the Court in *Chimel v. California*.[13] In that case a defendant was arrested in the interior area of his home.[14] Police then proceeded to search the entire house, including opening drawers in the furniture of the master bedroom.[15] The Court found the search illegal and provided more definitive guidance on the scope of the "search incident to arrest" exception, specifically holding:

> [I]t is entirely reasonable for the arresting officer to search for and seize any evidence on the arrestee's person in order to prevent its concealment or destruction. And the area into which an arrestee might reach in order to grab a weapon or evidentiary items must, of course, be governed by a like rule . . . . There is ample justification, therefore, for a search of the arrestee's person and the area "within his immediate control"—construing that phrase to mean the area from within which he might gain possession of a weapon or destructible evidence.[16]

As a result, prior to *Riley*, law enforcement was provided with vast authority when it came to a search incident to arrest. Law enforcement can conduct a full search of the arrestee's person and the area within their immediate control. Moreover, the motivation for the search is irrelevant. In other words, legally it doesn't matter whether the officer is searching for weapons that could harm them or evidence of a crime. If the person is being custodially arrested, the officer can conduct the search.

---

10. *Weeks*, 232 U.S. at 392.

11. 267 U.S. 132 (1925). This case gives rise to what is traditionally called either the automobile exception, or the *Carroll* doctrine, which upholds the warrantless search of vehicles when there is probable cause to believe they carry contraband of evidence of a crime.

12. *Id.* at 158 (stating, "When a man is legally arrested for an offense, whatever is found upon his person or in his control which it is unlawful for him to have and which may be used to prove the offense may be seized and held as evidence in the prosecution."). The United States Supreme Court has also made clear that in a search conducted incident to arrest, the officer is not limited to merely looking for items that could harm him or her, but is also able to look for evidence of a crime. *See* United States v. Robinson, 414 U.S. 218 (1973).

13. 395 U.S. 752 (1969).

14. *Id.* at 753-54.

15. *Id.*

16. *Id.* at 763.

2. Riley v. California

Fast forward to the 21st century and the Court's landmark holding in *Riley v. California*. In *Riley*, the Supreme Court substantially reduced the reach of the "search incident to arrest" doctrine. In this case the defendant was pulled over for operating his vehicle with expired tags.[17] During the traffic stop, law enforcement officers discovered that Riley's license was suspended and, in line with department policy, impounded and inventoried his vehicle.[18] This search resulted in the discovery of firearms and evidence that the defendant was associated with a gang.[19] On his person, Riley had a smartphone.[20] While searching the contents of the cell phone, the officer found content that he believed was indicative of gang affiliation.[21] The officer searched the entirety of the phone's contents on the theory that gang members frequently take pictures of themselves with firearms.[22] Police found a video of young men engaged in a fight while someone was shouting "Blood," the name of the street gang to which the defendant was alleged to be affiliated.[23] They also found a photograph of Riley standing in front of a car associated with a prior shooting.[24] Riley was ultimately charged with several offenses related to that crime, including a sentencing enhancement based on the State's allegation that Riley committed the crimes for the benefit of a street gang.[25] The trial court denied the defendant's motion to suppress the evidence found on his phone, a ruling that was upheld on appeal, based on the "search incident to arrest" exception.[26]

The Supreme Court granted certiorari to determine the applicability of the "search incident to arrest" doctrine to cell phones. It began with a nod to the ubiquity of cell phones in modern life, remarking that "the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[27] Of additional import to the Supreme Court's analysis was its definition of the device on Riley (a smartphone), as, "a cellphone with a broad range of other functions based on advanced computing capability, large storage capacity, and internet connectivity." Acknowledging that cell phones, and especially

17. *Riley*, 573 U.S. at 378. It should be noted that a second case was part of the *Riley* decision and involved a defendant with a less sophisticated cellphone. *Id.* at 380-81. However, a separate discussion of those facts will not significantly contribute to the analysis of this article.

18. *Id.* When law or policy requires or permits police officers to impound a vehicle, they are permitted to inventory the contents of the vehicle without a search warrant to protect the police from false claims of theft, to remove any items from the car that could harm people, and to protect the contents of the vehicle. *See* South Dakota v. Opperman, 428 U.S. 364, 369 (1976).

19. *Riley*, 573 U.S. at 378.

20. *Id.* at 379.

21. *Id.*

22. *Id.*

23. *Id.*

24. *Riley*, 573 U.S. at 378.

25. *Id.*

26. *Id.* at 380.

27. *Id.* at 385.

smartphones, would have been technologically inconceivable at the time cases like *Chimel* were decided, the Court held that the traditional justifications underpinning the "search incident to arrest" exception do not apply in the context of a cell phone.[28]

Riley had acknowledged that the police could have seized the phone and then later obtained a search warrant for its content.[29] The government argued that while this would stop the defendant from deleting the contents of the phone, it could still be "wiped" remotely by a third party who was "not present at the scene of the arrest."[30] The Court dismissed this argument for two reasons. First, cases advancing the "search incident to arrest" exception have historically been concerned with the *arrestee* destroying evidence, not a third party.[31] Additionally, not only did the Court find little evidence to support the argument that remote wiping of devices was a real issue, but it pointed out that because of password protection, few arresting officers would be able to execute a search of the device so quickly as to prevent this harm from happening anyway.[32] Additionally, the officer could take steps to frustrate the possibility of remote wiping by either turning the phone off and removing its battery, or placing it in a container that would prevent remote signals from reaching it.[33] The Court's reasoning here opened the door to the possibility that if police could show they were truly in a "now or never" situation, they might be able to rely on the exigent circumstances exception to the search warrant requirement to justify the search.[34]

The Court then turned its analysis to how cell phones present a different challenge to another assumption underlying the "search incident to arrest" doctrine—namely, that arrestees have lesser expectation of privacy in their person and the items on themselves than members of the general public.[35] The Court found that cell phones are materially different from other items traditionally found on an arrestee's person, such as a cigarette packet, a wallet,

28. *Id.* at 386.
29. *Riley*, 573 U.S. at 388.
30. *Id.* at 389.
31. *Id.*
32. *Id.* at 389-90.
33. *Riley*, 573 U.S. at 390-91. The Court noted that police have devices commonly called "Faraday Bags" that are "essentially sandwich bags made out of aluminum foil. . . ." *Id*. While the Court acknowledged that these are not a complete answer to the problem, they provide a "reasonable response" and many police departments already encourage their use. *Id.*
34. *Id.* at 391. An additional exception to the search warrant requirement applies when "'the exigencies of the situation' make the needs of law enforcement so compelling that [a] warrantless search is objectively reasonable under the Fourth Amendment." Kentucky v. King, 563 U.S. 452, 460 (2011) (alteration in original) (quoting Mincey v. Arizona, 437 U.S. 385, 394 (1978)). Exigent circumstances can include providing emergency assistance to the occupant of a home. Michigan v. Fisher, 558 U.S. 45 (2009). Exigency can also exist when law enforcement are engaged in "hot pursuit" of a fleeing suspect. United States v. Santana, 427 U.S. 38, 42-43 (1976). The exemption can also justify warrantless police action intended to "prevent the imminent destruction of evidence." Missouri v. McNeely, 569 U.S. 141, 149 (2013).
35. *Riley*, 573 U.S. at 391-92.

or a purse.[36] The Court noted that modern cell phones should really be understood as mini-computers that are also capable of making a phone call.[37] To the Court, having a cell phone on one's person is like being able to carry around every piece of mail one has received, or every article or book one has read in the last several months.[38] Moreover, when considering expectations of privacy, the Court pointed out that a phone might store such sensitive information as addresses, notes, bank records, and browsing history.[39] The Supreme Court summarized this point well, saying, "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."[40] Moreover, the applications on a phone can potentially reveal even more details about one's private life, such as one's political views, substance use, prayer, requests, pregnancy status, and romantic life.[41] Based on these factors, the Court found that in general, law enforcement must first obtain a warrant in order to search a cell phone found on an arrestee's person at the time of the arrest.[42]

The *Riley* decision highlights a disconnect between the rationale underpinning the "search incident to arrest" exception and the application of that rationale to the search of electronic devices. The *Chimel* concerns that are served by the exception, to prevent the destruction of evidence and protect the physical safety of officers during an arrest, are not advanced by allowing the exception to apply to cell phone searches. *Riley* thus demonstrates the first standard that any rule regarding the application of the particularity requirement to the search of an electronic device must satisfy. If a constitutional doctrine from outside of the digital world is applied to the search of an electronic device, it should not result in a disconnect between the government action and the rationale that led the Court to create the doctrine in the first place.

B. Third-Party Doctrine and Carpenter v. United States

The second standard that the Supreme Court will expect of any rule applying the particularity requirement to the search of electronic devices is that it preserves the level of privacy protection that existed at the time of the Fourth Amendment's adoption. Just as *Riley* recognized that modern technology created limits on the "search incident to arrest" doctrine, *Carpenter* had the same effect on a separate Fourth Amendment concept—the third-party doctrine. Moreover, the Supreme Court's decision in *Carpenter* places an emphasis on not

36. *Id.* at 393.
37. *Id.*
38. *Id.* at 393-94.
39. *Riley*, 573 U.S. at 394.
40. *Id.*
41. *Id.* at 396.
42. *Id.* at 401.

compromising the privacy protections as they existed at the time of the Constitution's adoption.

1. Foundational Third-Party Doctrine Caselaw

One of the foundational cases in Fourth Amendment law is *Katz v. United States*.[43] This case asserted that the Constitution's protection against unreasonable searches and seizures is about something greater than protecting an individual's property interest from unlawful trespass by law enforcement officers and protects those areas where an individual has an expectation of privacy that society considers reasonable.[44] While *Katz* is widely understood as expanding the reach of the Fourth Amendment, one line in the opinion has given rise to a doctrine that significantly constrains protection in this area: "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[45] This raises the question of whether an individual retains a reasonable expectation of privacy when turning over information or documents to a third party. Two cases, *United States v. Miller*[46] and *Smith v. Maryland*[47] create a judicial rule that individuals do not generally have a reasonable expectation of privacy in their records as a customer and thus cannot have the evidence of those records suppressed on the mere grounds that they were obtained by government investigators through means short of a search warrant.

Miller involved a defendant who was charged with possessing an unregistered still that resulted in the government being defrauded of owed duties on a whiskey tax.[48] At issue in the case were his bank records, which were obtained by the government through a defective subpoena *duces tecum*.[49] While

43. 389 U.S. 347 (1967). This case involved a defendant charged with a form of gambling using the telephone. *Id.* at 348. Part of the evidence against him involved a federal agent testifying to the defendant's conversations that had been captured through the use of a listening and recording device that had been attached to a public telephone booth. *Id*. In challenging earlier property-focused jurisprudence, the Court noted that, "the Fourth Amendment protects people, not places." *Id.* at 351. Previous case law required a defendant seeking to suppress evidence on Fourth Amendment grounds to demonstrate that the government committed an unlawful trespass of his property in order to prevail. *Id.* at 353. The *Katz* test for assessing whether government conduct that resulted in the discovery of evidence implicates the Fourth Amendment is best articulated in a concurrence by Justice Harlan. This is a two-part test that asks whether the suspect manifested a subjective expectation of privacy in the area examined by law enforcement and whether that expectation is one that society would deem reasonable. *Katz*, 389 U.S. at 361. In this case the Court found that utilizing the listening device to record the defendant's conversation violated the defendant's reasonable expectation of privacy and was completed without a warrant and accordingly vacated his conviction. *Id.* at 359.

44. *Id.* at 353.

45. *Id.* at 351.

46. 425 U.S. 435 (1976).

47. 442 U.S. 735 (1979).

48. *Miller*, 425 U.S. at 435-56.

49. *Id.* at 436. The records were argued to be defective because they were issued by a United States Attorney rather than a court and were ordered returnable on a date when the Grand Jury was not in session. *Id*. at 438-39.

under federal law this would generally result in suppression of the evidence, the Court declined to do this, holding that the defendant did not have a reasonable expectation of privacy in the records and thus could not object to how they were obtained.[50] The Court started its analysis with the premise that the bank's records were not the defendant's private papers.[51] In other words, the defendant could assert neither ownership nor possession of the papers at issue.[52] While the defendant sought to rely on *Katz's* expansion of the area protected by the Fourth Amendment by arguing that the records were personal in nature and a copy was made available to the bank for a limited purpose, the Court considered dispositive the above quoted language in *Katz*, that someone is not entitled to suppress the evidence of record, whose information they exposed to the public.[53] The Court stated that the bank records contained information that the defendant had provided to the bank's employees in the course of conducting business.[54] The defendant took the risk in exposing that information to a third party that the other party would give it to the government.[55] Accordingly, he had no Fourth Amendment interest in the bank's records that he was entitled to "vindicate."[56]

Smith applied this concept in the context of the records of a phone company. In this case, a woman had been robbed and, after she reported the matter to police, she began to receive threatening phone calls.[57] The nature of the phone calls gave rise to the inference that the caller had been involved in committing the robbery.[58] After the police identified the defendant as a suspect, they asked the local telephone company to install a pen register at its office, so that they could record all of the phone numbers that the defendant called.[59] While the register was installed without a warrant, it allowed police to collect information that the defendant had contacted the victim of the robbery, which was in turn used to obtain a search warrant for his home.[60]

The Court framed its analysis using the *Katz* test.[61] While acknowledging that a defendant might subjectively expect that the phone numbers they dialed would remain private, this is not an expectation that society would recognize as reasonable. The Court found that it was not reasonable to have an expectation of privacy in the numbers they dialed since customers should understand that they had provided that information to the telephone company.[62] The Court stated that

50. *Id.* at 437.
51. *Id.* at 440.
52. *Miller*, 425 U.S. at 440.
53. *Id.* at 442.
54. *Id.*
55. *Id.* at 443.
56. *Id.* at 445.
57. *Smith*, 442 U.S. at 737.
58. *Id.*
59. *Id.* at 737.
60. *Id.*
61. *Id.* at 739-41.
62. *Smith*, 442 U.S. at 742.

an individual would understand that the phone company logged all customers' phone calls in order to accurately bill long-distance charges.[63] Building on *Miller*, the Court reasoned that even if the defendant had his own subjective expectation of privacy in these records, it would not be deemed reasonable by society because he had voluntarily conveyed the information to a third party during the course of their conducting business.[64] Customers assume the risk that the company will disclose the information to others, so it is unreasonable for them to expect that the information will remain private.[65] Because the defendant had no expectation of privacy in the records, the Fourth Amendment was not implicated through the use of the pen register.[66]

2. United States v. Carpenter

Like the decision in *Riley*, which illustrated that a traditional Fourth Amendment doctrine (search incident to arrest) was deficient in addressing new technology, *United States v. Carpenter*[67] illustrates the same challenge that new technology presents to third-party doctrine. Chief Justice Roberts's opinion in *Carpenter* starts with a discussion of how cell phones have changed the world, noting that the number of cell phones in the United States exceeds the country's population.[68] Roberts noted that cell phones operate by utilizing a nearby cell site and, when this happens, the information gets recorded in the company's records.[69] This use of cell sites is not limited to when a call is made, but also occurs when text messages are sent or there is a routine data connection, resulting in a vast quantity of precise information about the cell phone's location at particular times.[70]

In this case, a suspect was arrested for robbery.[71] He provided the police with information regarding other robberies that he and his codefendants had committed and also provided the police with his coconspirators' phone numbers.[72] Law enforcement employed a federal statute to obtain one of those conspirators' (Carpenter's) cell site location data from the time of the various robberies, utilizing a statute that only required demonstrating that the records were "relevant and material to an ongoing investigation."[73] The government used the defendant's cell site location data to show that his cell phone was physically near where the robberies had happened at the time they occurred.[74]

63. *Id.*
64. *Id.* at 744.
65. *Id.*
66. *Id.* at 745-46.
67. *See* 585 U.S. 296 (2018).
68. *Id.* at 300.
69. *Id.* at 300-01.
70. *Id.* at 301.
71. *Id.*
72. *Carpenter*, 585 U.S. at 301.
73. *Id.* at 302.
74. *Id.* at 302-03.

In its opinion, the Court acknowledged the way in which *Katz* had expanded the areas that were provided Fourth Amendment protection by the courts.[75] The opinion also noted that as technology progresses, the Court must find ways to uphold the values of the founding generation in its Fourth Amendment jurisprudence.[76] This includes concepts like excluding the "privacies of life" from arbitrary power and placing obstacles in the way of permeating police surveillance.[77] In trying to figure out how to categorize cell site location data, the Court noted that it sat at the intersection of its case law examining government tracking of a person's movement and its third-party doctrine jurisprudence.[78] The Court noted how the records could theoretically fall into either legal doctrine. On the one hand, the cell site location data facilitates the government tracking a defendant's location in a detailed, encyclopedic, and effortless manner, similar to the use of a GPS tracker on their vehicle, which the Court had previously prohibited without a warrant.[79] By contrast, the Court acknowledged that an individual using a cell phone reveals their location to the cell phone company, which could facially implicate *Smith* and *Miller*.[80]

In declining to extend third-party doctrine to cell site location data, the Court noted that, at the point these cases were decided, no one could have conceptualized a world where a person's telephone travels with them all the time.[81] In reaching this conclusion, the Court harkened back to the basic premise of *Katz*, stating that just because someone ventures into the public sphere, does not mean that they have surrendered their reasonable expectation of privacy.[82] To the Court, society would clearly not countenance a scenario where the government could secretly monitor and catalogue the movements of an individual over an extended period of time.[83] But, much like the use of a GPS device on a car, cell site location data does precisely that. In this case, the government had over 100 days of time-stamped data about the defendant's movements.[84] The Court also noted that while people sometimes will leave their car (limiting the tracking of an installed GPS device), they generally still take their cell phone with them.[85] Tellingly, the Court emphasized that any limitations on the geographic reach of cell site location data was shrinking in the light of new technology.[86]

---

75. *Id.* at 304.
76. *Id.* at 305.
77. *Carpenter*, 585 U.S. at 305 (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)).
78. *Id.* at 306-08.
79. *See* United States v. Jones, 565 U.S. 400, 412 (2012).
80. *Carpenter*, 585. U.S. at 309.
81. *Id.*
82. *Id.* at 310.
83. *Id.*
84. *Id.* at 311.
85. *Carpenter*, 585. U.S. at 311.
86. *Id.* at 313. For example, one newer method of plotting an individual's location based on their cell data is called timing advance and is similar to sonar. *See* Destin Watkins, *A Cops Guide to Cellular*

This analysis is vital to understanding how the Court might apply a traditional legal doctrine to new technology. When there is a "seismic shift" in technology that creates a "world of difference" in the outcome, it is not appropriate to mechanically apply the structure of an old test when doing so fails to support the underlying constitutional norm.[87] For example, consider our earlier conversation of *Riley* and the search incident to arrest. If the Court merely applied the structure of the existing doctrine, the search would have been upheld. After all, the phone that Riley had in his pants pocket was clearly property that was on his person or in his control. Historically, when law enforcement arrested an individual, they could search the arrestee's person, and it did not matter why. Nonetheless, if the Court had upheld the search in *Riley*, it would compromise the defendant's privacy interest in a way that was never conceptualized by the original doctrine by handing the government information about every aspect of his life.

The Court applies similar reasoning here. If the third-party doctrine was applied, the government would have prevailed. But the advent of new technology would mean that the government would be receiving far more data about a person's private life and movements than what was conceptualized when the doctrine was created. Allowing that to happen without a warrant would undermine the core constitutional principles that seek to protect an individual's privacy interest from government overreach. This idea points to a second standard for how the Court should approach the particularity requirement and the search of cell phones. The Court should be focused on how the fundamental privacy interests at the time of the founding are impacted by what the government sought to do in this case. Any rule applying the particularity requirement to the search of electronic devices must protect the privacy interests as understood at the time of the adoption of the Fourth Amendment.

C. Kyllo v. United States

In *Kyllo*, an inspector with the Department of the Interior came to suspect that the defendant was growing marijuana inside his home.[88] Knowing that growing marijuana inside a home typically requires the use of high-intensity lamps, the agent used a thermal imager to scan the home.[89] The agent used the device while seated in his own cruiser, parked across the street from the defendant's home.[90] This scan revealed that the garage, as well as a wall on one

Network Investigations, WARRANTBUILDER.COM (Oct. 30 2023) https://warrantbuilder.com/cellular-network-investigations/. This method can track the cell phone's activity within a 10-meter arc. *Id.* In explanation, "[t]he telecom provider knows exactly how long it take[s] for a signal to travel. Because the speed is known, when the response signal is received by the tower the telecom will know exactly how far from the tower the handset is. *Id*.

87. *Carpenter*, 585. U.S. at 313-14.
88. *Kyllo*, 533 U.S. at 29.
89. *Id.*
90. *Id.* at 30.

side of the defendant's home, was warmer than the rest of the residence.[91] Combined with other evidence, this information formed the basis for obtaining a search warrant for the defendant's residence, where police eventually found 100 marijuana plants.[92]

The Supreme Court's analysis of this problem acknowledges the difficulty that the new technology presented to existing Fourth Amendment jurisprudence. At one level, visual surveillance of a home is not normally understood as a search, which the government would be required to justify either by the existence of a search warrant or an exception to the warrant requirement.[93] However, the Court went on to write, "It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology."[94] Just as the development of aerial surveillance meant that more of an individual's property could be observed without triggering a search, the Court had to address whether this newer technology changed that equation.[95]

In ruling that this technology did constitute a search, there are three components of the Court's decision that are worth considering. First, the Court found persuasive the fact that this technology exposed to the police information about the interior of the home that otherwise would have required a physical intrusion into a constitutionally protected area.[96] Second, this intrusion occurred through the use of technology that is not otherwise in general use by the public.[97] "Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search'. . . ."[98] Third, the Court took into consideration the evolving nature of technology when formatting its rule and reasoning in this case. The Court noted, for example, that the technology utilized by the police in this case was not so advanced that the Court could not have limited its holding by acknowledging that the surveillance was technically of radiated heat, not direct exposure to what was happening in the home.[99] "While the technology used in the present case was relatively crude, the rule we adopt must take account of the more sophisticated systems that are already in use or in development."[100] This starts to point to the standard of workability. Meaning, when the Supreme Court develops a general rule, it needs to do so in

91. *Id.*
92. *Id.*
93. *Kyllo*, 533 U.S. at 31-32.. The Supreme Court has also held that aerial surveillance of a home and surrounding area does not constitute a search under the Fourth Amendment. *See* California v. Ciraolo, 476 U.S. 207, 215 (1986); Florida v. Riley, 488 U.S. 445 (1989).
94. *Kyllo*, 533 U.S. at 33-34.
95. *Id.* at 34.
96. *Id.*
97. *Id.*
98. *Id.* at 40.
99. *See Kyllo*, 533 U.S. at 40.
100. *Id.* at 36.

a way that allows the lower courts to apply the rule with some degree of certainty, even if technology evolves in the years after the case is decided. As the next section will demonstrate, part of the Court's reluctance to get involved in these cases too quickly is that, as technology rapidly evolves, the Court wants to make sure that its rules are well suited to address that evolution. The quotation just provided from *Kyllo* and the accompanying discussion manifest a desire not just to look at the impact that the decision will have based on the technological capacity of the specific device in front of the Court, but to have a sense of how the ruling will be interpreted for other existing technologies or new frontiers in technology. When the Court resolves how the particularity requirement interacts with the search of electronic devices, the third standard is it must be a workable rule that can be broadly applied by lower courts regardless of the specifics of the device at issue. Put directly, the rule created by the Court needs to "provide a workable accommodation between the needs of law enforcement and the interests protected by the Fourth Amendment."[101] This forms the third standard that the Supreme Court will expect from any rule applying the particularity requirement to the search of electronic devices.

D. City of Ontario v. Quon

Although smartphones have existed for years and the Court's decision in *Riley v. California* demonstrates awareness of their capabilities and widespread use, it may seem surprising that the Court has yet to address how the Fourth Amendment's particularity requirement applies to searches of cell phones. Examining how the Court resolved issues with an earlier technology case helps explain its delay in entering this dispute. *City of Ontario v. Quon* addressed whether a government employer could review text messages sent and received on a government-issued pager.[102] In this case, Quon was a police sergeant who was a member of a city's SWAT force and was issued a pager capable of sending and receiving text messages.[103] Each device had a character limit that could be used before incurring an additional fee.[104] While the City had a written computer, internet, and email policy that warned employees that they should have no personal expectation of privacy in these government devices, the policy did not directly include pagers.[105] A police lieutenant did tell the officers at a meeting (at which Quon was a participant), that this policy applied to the pagers as well.[106] Quon initially exceeded his allotted use on his pager and he just paid the department for the added cost.[107] When this continued to happen, his supervisor wanted to ascertain if the character limit was too low, so an audit of Quon's

101. *Id.* at 38.
102. *Quon*, 560 U.S. at 750.
103. *Id.*
104. *Id.* at 750-51.
105. *Id.* at 751.
106. *Id.* at 751-52.
107. *Quon*, 560 U.S. at 751-52.

messages was conducted.[108] This led to the discovery of text messages that were sexual in nature and not work-related.[109] Quon was disciplined as a result and sued.[110]

At first glance, this case seems like it could be easily resolved by simply holding that a government employee does not have an expectation of privacy in a government-owned communication device. Instead, the Court utilized the special needs analytical framework to explain why it was unnecessary for the government employer in this case to have a warrant before looking at the text messages.[111] Nonetheless, the Court did explain why it did not analyze the question of whether Quon had a reasonable expectation of privacy in the text messages on the pager and, in the process, offered good insight on their reluctance to get involved too quickly in Fourth Amendment cases involving new technology.

In addition to noting that this would have required resolving a factual dispute between the parties, the Court reasoned that in this area of the law it needed to move slowly because, "[t]he judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."[112] The Court acknowledged that there are rapid changes in the dynamics of communication and the technology itself that warrant prudence before the Court gets involved.[113] The Court understood that it would have trouble predicting, as technology advanced, how individuals' expectations of privacy are shaped and the degree to which those expectations would be deemed reasonable by the Court.[114] The Court worried that a broader holding could have implications for future cases that couldn't be anticipated in the present.[115] The Court noted that if it simply assumed *arguendo* that Quon had a reasonable expectation of privacy in the text messages, the special needs doctrine could dispose of the legal issue without requiring the Court to substantively weigh in on that more difficult (and potentially evolving) question.[116]

---

108. *Id.* at 752.
109. *Id* at 753.
110. *Id.*
111. The Court has recognized a category of exceptions to the search warrant requirement that are identified as "special needs" and are situations where the warrant and probable cause requirement are impractical. O'Connor v. Ortega, 480 U.S. 709, 732 (1987). When evaluating whether to apply the special needs doctrine, the Court balances the "nature and quality of the intrusion on the individual's Fourth Amendment interests against the importance of the governmental interests alleged to justify the intrusion." *Id*. at 719 (quoting United States v. Place, 462 U.S. 696, 703 (1983). Examples of the use of this doctrine include administrative searches to ensure compliance with housing or safety codes. *See e.g.*, Michigan v. Clifford, 464 U.S. 287 (1984); Camara v. Mun. Court of City & Cty. of S.F., 387 U.S. 523 (1967). Police checkpoints are another example of the application of this doctrine. *See e.g.*, United States v. Martinez-Fuerte, 428 U.S. 543 (1976); Mich. Dep't. of State Police v. Sitz, 496 U.S. 444 (1990).
112. *Quon*, 560 U.S. at 759.
113. *Id.*
114. *Id.*at 759-60.
115. *Id.* at 760.
116. *Id.* at 760-61.

At one level, this echoes a principle that we saw in the discussion of *Kyllo*. Specifically, the Court wants to ensure that it creates workable rules that can be broadly applied by other courts without creating problems as soon as technology continues to change. It may very well be that the Supreme Court has not gotten involved in resolving the dispute between the particularity requirement and the search of electronic devices for the same reason that it avoided answering whether Quon had a reasonable expectation of privacy in his pager—the Court wants to make sure that when it announces a rule, the rule will be practical, useful, and easily applied by the lower courts.

In summary, *Riley*, *Carpenter*, and *Kyllo* offer a three-part structure for testing any rule that the Court applies when answering the question at the heart of this article. First, instead of rigidly applying traditional Fourth Amendment doctrines to new technology, we should assess whether the principles and concerns underlying these doctrines are consistent with the proposed government action. Second, we must ensure that the privacy interests protected by the Fourth Amendment at the time of its adoption are adequately covered by the proposed rule. Third, the rule that is created must provide workable and clear guidance to the lower court seeking to implement it and must be sufficiently fluid to translate into new situations as technology changes.

II. THE PARTICULARITY REQUIREMENT HISTORICALLY AND ITS RELATIONSHIP TO THE DOCTRINE OF GOOD FAITH RELIANCE

To understand the dispute at issue in this article, it is important that we turn next to addressing what the particularity requirement in the Fourth Amendment is and how it has been applied by the Supreme Court outside the context of electronic device searches. I will also overview the doctrine of good faith reliance and its intersections with the particularity requirement, as this is frequently addressed by courts when issuing rulings regarding the search of cell phones.

A. The Particularity Requirement

The text of the Fourth Amendment states, *inter alia*, "no warrants shall issue, but upon probable cause, supported by oath of affirmation, and *particularly describing the place to be searched, and the persons or things to be seized*."[117] One of the first Supreme Court cases to address the particularity requirement was a Prohibition-Era case involving the seizure of illegal whiskey.[118] In that case, an agent asked for a warrant to search any building attached to a garage located at a particular address where he believed that he had seen illegal activity take place.[119] One of the issues challenged was that the

117. U.S. CONST. amend. IV (emphasis added).
118. Steele v. United States, 267 U.S. 498 (1925).
119. *Id.* at 500.

building that was searched had two addresses associated with it.[120] Against a challenge that the warrant failed to state with particularity the place to be searched, the Court held that it was "enough if the description is such that the officer with a search warrant can, with reasonable effort ascertain and identify the place intended."[121]

At first glance, this might seem inapplicable to the issue of searching an electronic device. After all, law enforcement can be exceedingly specific in identifying a device by a serial number. However, the particularity requirement also mandates a specific description of the things to be seized.[122] For example, in one case involving the communism scare in the 1960s, the Court dealt with a challenge where a Texas law enforcement officer had obtained a search warrant to look for "books, records, pamphlets, cards, receipts, lists, memoranda, pictures, recordings and other written instruments concerning the Communist Party of Texas. . . ."[123]

The Court ruled that the warrant was invalid because it was a "general warrant," which sits at the heart of what the Fourth Amendment seeks to prohibit.[124] A general warrant was connected to the old English writ of assistance, which would allow the government official to search wherever they pleased.[125] The particularity requirement in the Fourth Amendment aimed to protect the people from the "whim of the officers charged with executing the warrant" by requiring a level of "scrupulous exactitude" in describing what is to be seized.[126] More specifically, "[t]he requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant."[127]

Another 1960s case gives additional context that helps us understand how these principles might translate to an electronic device.[128] In that case, search warrants were authorized to deploy two eavesdropping devices to further an investigation into suspected bribery of the New York State Liquor Authority.[129] In striking down the New York statute that authorized the warrant for the eavesdropping device, the Supreme Court contrasted how an earlier case compared to what the New York statute would allow. In the earlier case where the Court allowed the installation of a device to record conversations between a

120. *Id.* at 502.
121. *Id.* at 503.
122. *See* Stanford v. Texas, 379 U.S. 476, 485 (1965).
123. *Id.* at 477-78.
124. *Id.* at 480.
125. *Id.* at 481.
126. *Id.* at 485.
127. *Stanford*, 379 U.S. at 485 (quoting Marron v. United States, 275 U.S. 192, 196 (1927)).
128. *See* Berger v. New York, 388 U.S. 41 (1967).
129. *Id.* at 44-45.

suspect and a particular named other individual, there was a detailed affidavit that alleged a specific criminal offense, the order restricted what conversations could be listened to, the officers couldn't listen to unauthorized conversations, and the officers couldn't use the order as a "passkey to further search."[130]

By contrast, in the New York case there were no limiting factors. For example, the statute's "failure to describe with particularity the conversations sought gives the officer a roving commission to 'seize' any and all conversations."[131] Additionally, while the statute appeared to constrain officer discretion by requiring the warrant to name the person being recorded, there was no constraint based on the type of conversations.[132]

This begins to illustrate the framework that defense attorneys are starting to use to attack search warrants for electronic devices. In my experience the way this argument is framed is by asserting that the search warrant is akin to a general warrant and thus violates the particularity provision of the Fourth Amendment. First, the defense attorney might argue that the police do not have evidence that a cell phone was directly used in the commission of the crime, nor do they have reason to believe that the phone will have evidence on it. But if the warrant is far-reaching and allows the search of the entire device without limitation, the defense attorney can also argue that it is a general warrant that allows police to search through the digital equivalent of a person's entire life at their discretion, without any guideposts or substantive restrictions. This, the attorney will argue, violates the particularity requirement.

That lack of specificity would be similar to a problem identified with the search warrant in *Groh v. Ramirez*.[133] In that case, while the affidavit supporting the warrant said that police were looking for specific weapons and records, the warrant itself was silent on what could be seized from the home.[134] The Court held that the failure to state with specificity what was to be seized caused the warrant to be facially invalid because it did not identify the "type of evidence sought."[135] This is where a defense attorney might see problem with a warrant for the search of an electronic device. If law enforcement does not have specific information that the device was used in the commission of a crime, then at some level the police are speculating (even if it is rational speculation based on common sense) that the suspect has a cell phone and that the phone will contain evidence of a crime. Speculative thinking of that nature may lead to law enforcement using general language about what they are searching for such as "text messages or other communication about the crime." While these types of

130. *Id.* at 56-57 (citing Osborn v. United States, 385 U.S. 323 (1966)).

131. *Id.* at 59.

132. *Id.* at 59 (stating, "But this does no more than identify the person whose constitutionally protected area is to be invaded rather than 'particularly describing' the communications, conversations, or discussions to be seized"),

133. 541 U.S. 551 (2004).

134. *Id* at 554.

135. *Id.* at 557.

warrants can be differentiated from the deficient warrant in *Groh*, defense attorneys or proponents of civil liberties may see an analogous problem. When law enforcement officers are allowed to provide less specificity—either in the details that support a finding of probable cause or in what evidence they are looking for—it shifts authority from the neutral judge or magistrate onto the officer. It does so by allowing the search to be conducted with less evidence and with less oversight on what can be seized. This is of concern not just to a defense attorney, but to those supporting civil liberties in general.

The manner in which a lack of specificity can create unfettered discretion for law enforcement was illustrated in a 1970s obscenity case where the search warrant failed to identify specifically what could be taken as evidence of the crime.[136] "Based on the conclusory statement of the police investigator that other similarly obscene materials would be found at the store, the warrant left it entirely to the discretion of the officials conducting the search to decide what items were likely obscene and to accomplish their seizure. The Fourth Amendment does not permit such action."[137] A defense attorney might see a warrant that reasons "they probably used a cell phone to communicate about the crime, so search for evidence of communication about the crime" to have little difference from a warrant that says, "if there is some obscene material at this store, there is probably more, so go seize whatever is obscene."

B. Good Faith Reliance—Leon

In the next section, I will be turning to look at how lower courts have been tackling the challenge of applying the particularity requirement in the context of searches of electronic devices. However, to understand that case law in its entirety, it is important to look at another Fourth Amendment concept—good faith reliance—and how this interacts with the particularity requirement.

Good faith reliance was established as a doctrine in the seminal case of *United States v. Leon*.[138] This case involved a narcotics investigation where law enforcement obtained a search warrant but the trial court invalidated the search, noting that while it was a "close one," the search warrant was not supported by probable cause.[139] On review to the Supreme Court, the prosecution did not challenge the finding that there was no probable cause, but argued that if law enforcement relied in good faith on the warrant, that evidence obtained pursuant to the search should not be suppressed.[140]

In siding with the prosecution, the Court started out with the premise that because a search warrant "provides the detached scrutiny of a neutral magistrate, which is a more reliable safeguard against improper searches than the hurried

136. Lo-Ji Sales v. New York, 442 U.S. 319 (1979).
137. *Id.* at 325.
138. 468 U.S. 897 (1984).
139. *Id.* at 902-03.
140. *Id.* at 905.

judgment of a law enforcement officer . . . ," it is always preferred to conducting a warrantless search.[141] And, because reasonable minds can disagree on what constitutes probable cause, great deference should be given to the magistrate's conclusion when issuing the original search warrant.[142] The *Leon* decision recognized three exceptions to this: (1) when an officer lies in the affidavit or shows reckless disregard for the truth; (2) when the magistrate abandons their neutral and detached function; and (3) when the affidavit does not provide the magistrate with a substantial basis for determining the existence of probable cause.[143]

It is that third exception (and a variation I will discuss momentarily) that is relevant to the consideration of the issue at the heart of this article. The Court noted within that context that if an officer obtains a search warrant in good faith and acts within its scope, even if it later proves to be the case that the warrant was not supported by probable cause, there is no police misconduct to dissuade by excluding the evidence.[144] The Court expressed the test for the third exception to good faith reliance as arising when, "an affidavit [is] 'so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable.'"[145]

As will be illustrated in the next section, *Leon*'s good faith reliance will almost always have to be assessed by an appellate court assessing the applicability of the particularity requirement to a search of an electronic device. In other words, somewhere in the process, a judge or magistrate has made a finding of probable cause to justify the search. The *Leon* decision helps explain the relationship between the third exception to good faith reliance and the particularity requirement with the following statement. "Finally, depending on the circumstances of the particular case, a warrant may be so facially deficient—i.e., in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid."[146] This is where a defense attorney must rest their argument. In other words, in order for the defense to prevail in arguing that the search of the electronic device fails the particularity requirement, they must demonstrate that the warrant is so facially deficient that it was unreasonable for the officer to have relied on it.

III. HOW LOWER COURTS ARE ADDRESSING THE APPLICATION OF THE PARTICULARITY REQUIREMENT TO THE SEARCH OF CELL PHONES

In this section I will examine lower court cases that have disfavored broad search warrants for the contents of electronic devices and then look at cases

141. *Id.* at 913-914.
142. *Id.* at 914.
143. *Leon*, 468 U.S. at 914-15.
144. *Id* at 920.
145. *Id.* at 923 (citing *Brown v. Illinois*, 422 U.S. 590, 610-611 (1975)).
146. *Id.* (White, J., concurring).

where the courts have taken the opposite position. From these cases, I identify three areas where lower courts disagree, likely necessitating resolution by the Supreme Court.

A. Case Law Disfavoring Broad Search Warrants for Cell Phones

In a Texas state-level appellate decision, the court examined a search warrant related to a cell phone seized in the investigation of a robbery, where the gunmen shot and killed the victim.[147] The defendant was detained in a traffic stop and was driving a vehicle similar to one seen in surveillance video from near the crime scene.[148] A cell phone was found during the traffic stop and police obtained a search warrant for its contents.[149] In agreeing that the warrant was fatally flawed, the court opined that there were simply no facts that established a connection between the cell phone and the crime, and the affidavit, "include[d] only generic recitations about the abstract use of cellphones."[150] The court held that generic boilerplate language that a suspect might communicate about his plans did not satisfy probable cause.[151] The court was concerned that, without requiring proof of a connection between the phone and the crime, searching a suspect's cell phone would be warranted any time a person is arrested.[152]

Another traditional Fourth Amendment problem addresses what law enforcement can do when they are searching for evidence of a specific crime and, in the process, come across evidence of a crime that was not under investigation.[153] This issue arises in a digital context as well. In an Oregon case, a state appellate court analyzed that issue when law enforcement officers were searching a cell phone for evidence related to a robbery and came across images related to child pornography.[154] In that case, the victim of the robbery was the former girlfriend of the defendant. Prior to the robbery, the defendant had communicated with the victim through Instagram and text messages.[155] But the investigator's search warrant was far broader than text messages and Instagram communication and talked in more general terms about how files like photographs and call logs can further an investigation.[156] The court found unpersuasive the idea that text messages can contain photographs and, therefore,

147. State v. Baldwin, 614 S.W.3d 411, 413 (Tex. App. 2020).
148. *Id.* at 413-14.
149. *Id.* at 414.
150. *Id.* at 417.
151. *Id.*
152. *Baldwin*, 614 S.W.3d at 418.
153. The plain view exception to the search warrant requirement permits police under certain circumstances to seize evidence without a warrant that is in plain view. *See* Coolidge v. New Hampshire, 403 U.S. 443 (1971). If officers are lawfully in place where they observe something that is immediately apparent to constitute incriminating evidence, the officer may seize it without a warrant. Horton v. California, 496 U.S. 128, 142 (1990).
154. State v. Vesa, 324 Or. App. 674, 676 (2023).
155. *Id.* at 676.
156. *Id.* at 677.

that allowing the search of photographs created, modified, or deleted during the timeframe at issue satisfied the particularity requirement.[157]

This opinion frames well the core dispute that frequently arises between the prosecution and the defense when it comes to the search of electronic devices. In this case, there was undisputed evidence that a cell phone was used in the commission of a crime. But that evidence showed the phone was used in very specific ways (Instagram and text messages) and during a particular date range. A defense attorney, armed with that information, might argue that the particularity requirement mandates that the search be limited to examining where and when the probable cause supports that there may be evidence of a crime. By contrast, the prosecution, looking at the fact that an electronic device was used in the commission of an offense, may argue that electronic evidence in a phone is intermingled. Consider this analogy to a more traditional search in a non-digital space. We can imagine a scenario where a witness told the police that they saw the defendant put stolen property in the closet of a particular room in a house where multiple people lived. If those were the limited relevant facts in the affidavit, it seems unlikely that a court would uphold a search warrant for an entire house, its garage, and the shed in the backyard. But the defense would likely have to acknowledge that if the search was more geographically limited to where the evidence was known to be, the warrant could also permit the seizure of "indicia of occupancy" that would support the prosecutor's argument that the defendant lived in or controlled the room (and its closet) where the stolen property was located.

When it comes to electronic devices, the government would argue that indicia of ownership of the phone at issue could be located anywhere, from photographs (which might include the owner's "selfies"), to text messages and emails (sent from and to the owner), to social media accounts on the phone. As one judge wrote, "[a]s a practical matter the only way for law enforcement to identify who owned each phone, or if a particular phone is one identified in the warrant, is through some manner of a search."[158] For the prosecution, the apt analogy would be a search warrant issued for a filing cabinet containing evidence of a crime, which would surely allow the police to look through every file in the cabinet itself.[159] But to the defense attorney, allowing all parts of the phone to be

157. *Id.* at 684.

158. United States v. Boyd, No. 24-cr-4-pp, 2025 U.S. Dist. LEXIS 69476, at *20 (E.D. Wis. Apr. 11, 2025) (alteration in original).

159. *Id.* at *29 (stating "[t]he government reiterates the Seventh Circuit's analogy between cell phones and a filing cabinet, in which the incriminating evidence could be found on any phone, or in any file or folder. The government states, '[I]f the warrant "cabins the things being looked for by stating what crime is under investigation," it is enough.') (citations omitted). The Seventh Circuit has noted that just as a search warrant to find drugs in a home would allow police to look anywhere in the home where the drugs could be hidden, so too it is permissible for a search warrant to authorize police to look everywhere on a phone to see what evidence fits within the scope of the warrant. *See* United States v. Bishop, 910 F.3d 335, 336-37 (7th Cir. 2018). Similarly, the Sixth Circuit has upheld a broad search of a cellphone's contents because, "[a]t the time of the seizure, however, the officers could not have known

searched when the evidence related to the crime is of a limited nature would be more akin to a warrant permitting the police to search the shed for indicia of occupancy of a room in a house. From that perspective, this creates a general warrant with no meaningful limit on where law enforcement can search.

The Second Circuit highlighted that concern by contrasting a normal search warrant for a home where "the physical dimensions of the evidence sought will naturally impose limitations on where an officer may pry: an officer could not properly look for a stolen flat-screen television by rummaging through the suspect's medicine cabinet, nor search for false tax documents by viewing the suspect's home video collection."[160] By contrast, those "limitations are largely absent in the digital realm."[161] From the perspective of the court, this creates a particular danger because any file law enforcement chooses to open is in plain view and could implicate a defendant in a crime not contemplated by the warrant.[162] If that is the case, then every warrant for electronic devices becomes a general warrant.[163] The essential argument here is that if the police look hard enough at someone's computer or cell phone, there is a strong possibility that they will find evidence of some kind of crime. That is akin to the danger of the general warrant that would have allowed the British soldier to go through the house of the colonist, turning everything upside down to find evidence of some crime, even though he had no cause to believe the house would contain evidence of any particular crime. The Second Circuit has also cautioned about how to apply *Leon* good faith reliance in this context by examining whether there is proof that "investigators sought evidence beyond the scope of the one crime that was particularized in the warrant application and for which the application supplied probable cause."[164] If so, the officer is not acting in good faith.[165]

As will be discussed in the next section, some courts believe that a sufficient limiting factor is when the magistrate who issues the warrant specifies that law enforcement can only look for evidence of a particular crime. Not every court agrees with this. For example, the D.C. Circuit Court of Appeals wrestled with a search warrant that allowed for the recovery from a cell phone of all evidence related to a homicide, but where the facts themselves only supported the existence of three particular pieces of electronic evidence: text messages between the defendant and the suspect, a call log establishing the timing of a particular call at issue, and a search of the GPS tracking features on the phone to show the suspect's whereabouts at the time of the crime.[166] But when law

---

where this information was located in the phone or in what format." United States v. Bass, 785 F.3d 1043, 1050 (6th Cir. 2015).

160. United States v. Galpin, 720 F.3d 436, 447 (2d Cir. 2013).

161. *Id.*

162. *Id.*

163. *Id.*

164. *Id.* at 453.

165. *Id.*

166. Burns v. United States, 235 A.3d 758, 774 (D.C. Cir. 2020).

enforcement looked at the internet search history on the phone, they recovered searches that illustrated the killing was premeditated and not an act of self-defense.[167] The court set out an exacting standard for the search of electronic evidence that is among the most favorable to defendants as examined in this article:

> It is not enough for police to show there is probable cause to arrest the owner or user of the cell phone, or even to establish probable cause to believe the phone contains some evidence of a crime. To be compliant with the Fourth Amendment, the warrant must specify the particular items of evidence to be searched for and seized from the phone and be strictly limited to the time period and information or other data for which probable cause has been properly established through the facts and circumstances set forth under oath in the warrant's supporting affidavit.[168]

No other decision, particularly from a federal court, has provided that breadth of protection to a defendant in this context. The court was critical that a broad warrant for the search of any evidence related to the homicide had been issued based on the assertion of a detective that it was his "belief" that there was probable cause to believe that evidence related to the homicide could be found in other areas of the phone such as the subscriber and owner information, call logs, contact lists, voice mail and text messages, videos, photographs, and tweets.[169] To the court, these were bare-bones assertions that were the equivalent of conjecture that the items related to the crime under investigation existed.[170]

This decision also addressed how this type of issue came about, attributing it to the use of a template where the detective acknowledged that he had used the same language in the warrant at issue in the last twenty-five cell phone search warrants he had obtained.[171] In my experience as a prosecutor, the use of templates is ubiquitous in everything from traffic to homicide investigations. When a patrol officer is investigating an allegation of drunk driving and wants to obtain a sample of the suspect's blood, the officer doesn't want to waste the time and resources recreating the same basic structure of probable cause that accompanies every case of this nature. Accordingly, the officer relies on a template and just changes the facts to match the case at hand. This approach is used when it comes to electronic devices where the affidavits supporting the search warrant may be dozens of pages long and include voluminous information on how cell phones operate, how they can be searched, how they are typically used in the commission of a crime, etc. And while this decision is highly dismissive of the template, a prosecutor would argue that the facts contained in

167. *Id.* at 770 (including searches such as "'what does it feel like to kill someone'" and "'how does it feel when you kill someone for the first time'" made before the homicide itself).

168. *Id.* at 773.

169. *Id.* at 774.

170. *Burns*, 235 A.3d at 774-75.

171. *Id.* at 775.

the document are necessary to establish probable cause and typically do not change from case to case. In this case, the court felt the more appropriate approach would have been to use the template as a starting point and then for the officer to tailor it to what he had probable cause to search for, rather than allowing the "exploratory search" that it did.[172]

The court acknowledged that this decision runs contrary to decisions in other courts but stated that it found those decisions unpersuasive.[173] This disagreement highlights why Supreme Court intervention is becoming increasingly both likely and necessary. Courts appear to be deeply divided. Some view the citation of an offense as a limiting factor on discretion, while others see that as creating no restraint at all.[174] Some see broad searches for the digital equivalent of "indicia of occupancy" as highly analogous to what is permitted in ordinary physical search warrants, while other courts see that as allowing the government to look through the entirety of someone's life without constraint. Some courts have insisted on the imposition of temporal or application-based limitations in a search, while others note that police do not necessarily know when and where the evidence was created or stored.

B. Case Law Supporting Broad Search Warrants for Cell Phones

The Second Circuit, in response to some of the cases cited in the above section, cautioned against confusing the breadth of a warrant with a lack of particularity.[175] For example, in the non-digital context, if there is evidence that a drug dealer's home contains evidence of narcotics, a warrant can be issued to search the entire home because drugs can fit anywhere.[176] Similarly, when criminal activity "pervades an entire business," seizure of all records of the business is appropriate and does not offend the particularity requirement.[177] If a suspect uses a computer to commit a crime, a broad search might be warranted.

In a federal case in Puerto Rico, a defendant charged with being a felon in possession of a firearm, along with possession of a machine gun, argued that the search warrant for his phone failed to comply with the particularity requirement because it allowed for the recovery of firearms records that predated his felony conviction and were thus attenuated from the crime, and because the warrant failed to explain how the location information related to the possession of a firearm charge.[178] In denying the defendant's motion, the court noted that

172. *Id.*

173. *Id.* at 776.

174. *See* United States v. Dawkins, No. 17 Crim. 684, 2019 U.S. Dist. LEXIS 91534, at *7 (holding that when the target crimes are identified and the data to be seized is related to the target crime, it is sufficient to satisfy particularity).

175. United States v. Ulbricht, 858 F.3d 71, 102 (2d Cir. 2017).

176. *Id.*

177. *Id.*

178. United States v. Torres-Diaz, No. 23-410, 2025 U.S. Dist LEXIS 117857, at *2 and *12 (D.P.R. June 20, 2025).

frequently, broad warrants are authorized when it comes to electronic devices because it is difficult for law enforcement to know what evidence will be found and its location in the device.[179] Moreover, the court noted that the defendant's argument failed because evidence outside of an offense date frequently has relevance to conduct within those dates.[180] Additionally, location data on a phone can often demonstrate circumstantially who possessed the phone.[181] This indicia of ownership would be relevant evidence to which the government would be entitled.[182]

In a federal case in Connecticut, a defendant objected to evidence recovered from four cell phones during the course of a narcotics investigation.[183] Using precedent from jurisdictions outside of his own, he argued that the particularity requirement should impose limitations on which applications law enforcement should be allowed to open on his devices.[184] The court declined to adopt this kind of rule, holding that there is no way to ascertain the content of an electronic file without opening it, and files containing evidence can be intermingled with innocuous ones, which necessitates a broad search.[185] This is all the more true because law enforcement cannot necessarily anticipate how a suspect will store evidence and files.[186] The defendant also took issue with the fact that the warrant lacked temporal limitations on the data seized.[187] The court noted that even data on the phone not connected to the offense date helped demonstrate that the defendant was the owner of the phone, a relevant fact for the government to prove.[188] Finally, the court opined that even if the defendant were correct about the lack of temporal limitation rendering the warrant defective, *Leon's* good faith

179. *Id.* at 13.
180. *Id.* at 14.
181. *Id.* at 14-15.
182. *Id.* In my experience as a prosecutor, search warrants that are issued for a physical location usually include, among the items to be seized, documents that show an "indicia of ownership." This assists prosecutors in connecting the evidence that was obtained to the defendant. "We have upheld warrants authorizing the seizure of items which establish the identity of persons in control of premises." United States v. Whitten, 706 F.2d 1000, 1009 (9th Cir. 1983). Where multiple individuals were suspected to utilize a premise, it is reasonable for the arresting officers to search for evidence showing who occupied and controlled the property. *Id.* The same challenge is applicable in a cellular phone. The phone at issue may have great evidence of a crime on it, but it is still incumbent on the prosecution to show that the phone belonged to or was used by the defendant. While sometimes this could be accomplished by showing that the phone was on the defendant's person or was being used by that individual, that will not always be the case. The ownership of a phone can also be demonstrated through indicia of possession/control based on factors like who the registered owner of accounts on the phone are, whose pictures and emails are on the phone, etc.
183. United States v. Salaman, 742 F. Supp. 3d 221, 225 (D. Conn. 2024).
184. *Id.* at 233-34.
185. *Id.* at 234.
186. *Id.*
187. *Id.* at 235
188. *Salaman*, 742 F. Supp. 3d at 235.

reliance would mean that exclusion of the evidence was not the appropriate remedy.[189]

Another case out of Illinois similarly analyzed the issue of whether the particularity requirement necessitated either temporal limitations on the data recovered from a phone or mandated particular procedures for how the phone should be searched.[190] This case involved financial crimes arising from a narcotics investigation.[191] The court acknowledged that the presence of temporal limitations was a factor in ascertaining whether the warrant sufficiently spelled out what was to be searched for, but also held that it was not dispositive.[192] After all, it is sometimes difficult to know how far back criminal conduct may go and, in that case, specifying the conduct at issue is sufficient to satisfy the particularity requirement.[193] This case also rejected the defendant's objection to a two-step process of executing the search where the contents of the phone were duplicated and then sifted through to determine what fell within the strictures of the warrant and what did not.[194] The court opined that this was an oft-used method of executing a search warrant for an electronic device and the warrant's specification of the categories of data to be seized was sufficient to constrain the discretion of law enforcement.[195]

IV. HOW THE SUPREME COURT'S METHODOLOGICAL APPROACH IN *RILEY*, *CARPENTER*, AND *KYLLO* PREDICTS THE OUTCOME OF THIS ISSUE

Reviewing these differing trial and appellate court decisions, three main disputed issues arise regarding electronic device searches that lower courts do not agree about:

- Probable Cause Assessment: Does a search warrant affidavit for a cell phone need specific evidence connecting the device to the crime, or can general language based on typical law enforcement experience about the use of cell phones more broadly suffice?
- Restrictions on the Method of Searching: Is the specification that law enforcement is looking for evidence related to a particular crime a sufficient limiting factor to satisfy the particularity requirement? If not, should courts impose time-based limitations, application-based limitations, or other procedural restrictions on how the search is conducted regarding what kind of evidence or files police can examine or seize when searching a cell phone?

189. *Id.*
190. *See* United States v. Kim, 707 F. Supp. 3d 751 (N.D. Ill. 2023).
191. *Id.* at 753.
192. *Id.* at 757.
193. *Id.*
194. *Id.*
195. *Kim*, 707 F. Supp. 3d at 756-57.

- Under what circumstances does the *Leon* good faith exception fall to a facially deficient warrant for the search of a cellular device?

This section of the paper will examine rules that the Supreme Court could articulate for the search of electronic devices that would address each of these disputes among the lower courts. To ensure that these suggested solutions are grounded in the Supreme Court's jurisprudence on how it handles searches and new technology, as discussed in Section I, I will return our focus to three standards that were established there. First, as illustrated in *Riley*, if a constitutional doctrine from outside of the digital world is applied to the search of an electronic device, it should not result in a disconnect between the government action and the rationale that led the Court to create the doctrine in the first place. Second, as illustrated in *Carpenter*, the scope of what the Court permits the government to do must be consistent with how fundamental privacy interests were understood at the time of the adoption of the Fourth Amendment. Third, as illustrated in *Kyllo*, the rules created by the Court must be workable and be capable of being broadly applied by lower courts without regard to the specifics of an electronic device or minor changes in technology.

A. The Assessment of Probable Cause

In reading the decisions of lower courts, one can imagine two extremes of how a law enforcement officer could write an affidavit seeking to obtain a search warrant for an electronic device. In a world of extreme deference to the police, the officer would merely establish probable cause that a crime occurred and who the suspect is. To establish a reason for believing a cell phone exists and that it would contain evidence of a crime, the officer would rely on generic language that reasons as follows: first, virtually everyone has a cell phone and they use it for practically everything. Second, because cell phones are now used in almost every aspect of our lives, there will be some evidence of crime on the phone. The suspect will surely have told someone about it, taken pictures of the crime's aftermath, performed an internet search on the crime itself or how to get away with it. If all else fails, phones have great evidence of where their owners were at any point in time, which is almost always helpful to the government as they seek to place the defendant at the scene of the crime. This generic recitation in turn could become boilerplate language that could be copied and pasted from affidavit to affidavit, with little regard to the underlying crime. The officer would have to do nothing more than insert a few facts about this particular offense. And *voila*, the officer gets a warrant for the suspect's cell phone. Moreover, in this reality, police could acquire a warrant for a cell phone for virtually any crime, so the only limitation would be the resources the police are willing to spend obtaining the warrant and extracting and searching the contents of the phone.

On the opposite end of the spectrum, law enforcement would be held to a far more exacting standard. The courts would prohibit the officer from reaching

and using generic conclusions about life and instead require the facts in the warrant to be particularized to the case at hand. In other words, the officer would be required to have specific evidence not only that a phone was used in the commission of the crime, but also about the way it was used and specifically how the recovery of that data would advance the investigation and prosecution of the crime.

In order to account for the practicalities of policing without compromising individual liberty, the Supreme Court would be more likely to adopt a rule that allows an officer to employ common sense and their past experiences in creating the affidavit, but still requires (a) some indicia that an electronic device is connected to the facts of the case, and (b) that the common sense and past experiences of the officers be filtered through the actual facts of the offense and not just blindly transferred from affidavit to affidavit.[196]

How would this rule fare against the three standards offered as the progeny of cases like *Riley*, *Carpenter*, and *Kyllo* when it comes to the Fourth Amendment and technology? First, is a constitutional doctrine being employed to the search of an electronic device and does it create a disconnect between the government action and the rationale that led the Court to create the doctrine in the first place? The Court has repeatedly insisted that probable cause is connected to common sense but always as filtered through the specific facts of the case before it. For example, the Court held that when basing probable cause on the alert of a drug-detecting dog, instead of employing a rigid test for assessing the reliability of the dog, a court should view "all the facts surrounding a dog's alert… through the lens of common sense . . . "[197] Moreover the Court has specifically opined that "a police officer may draw inferences based on his own experience in deciding whether probable cause exists" and that what appears innocuous to a lay person might be legitimately suspicious to the police.[198] For example, the Court has noted that if officers arrive at a home that appears vacant and in disarray, their assessment of probable cause can include a reasonable inference that the partygoers inside knew they were not allowed to be there

196. For example, I once prosecuted a homicide that occurred during a mob-style after school fight. On the perimeter of those engaged in fighting were numerous teenagers who were filming the fight that was taking place. In approaching a search for evidence on electronic devices, it is reasonable for a law enforcement officer to lean on the fact that cell phones are broadly used, particularly by high school students and that frequently young people communicate electronically about things that happen or dramatic events that they see. But in this type of scenario, the officer doesn't have to rely merely on common sense because there are facts in the case itself that highlight the use of electronic devices during the crime. Another example might be drug dealing. An officer seeking a search warrant could lean on their experience investigating these types of crimes to talk about the different ways that cellphones are used to set up a drug deal between a buyer and a seller. This goes a step beyond simply asserting that everyone has cell phones and uses them and thus a search should be permitted.

197. Florida v. Harris, 568 U.S. 237, 248 (2013).

198. Ornelas v. United States, 517 U.S. 690, 700 (1996) (noting that, "[t]o a layman the sort of loose panel below the back seat armrest in the automobile involved in this case may suggest only wear and tear, but to Officer Luedke, who had searched roughly 2,000 cars for narcotics, it suggested that drugs may be secreted inside the panel").

because most homeowners do not live in such conditions or permit such conduct.[199] The Court has repeatedly stated that an officer can rely on their experience in assessing probable cause. But what keeps this moored to the underlying doctrine that "probable cause is a flexible, common-sense standard"[200] is when an officer's experience is filtered through the specific facts of the case rather than blanket assumptions about life.

Next, is this test consistent with the fundamental understanding of privacy at the time of the adoption of the Fourth Amendment? The concern at our nation's founding with general warrants or writs of assistance was that they gave the Crown "license to search all places and for everything in a given place, limited only by their own discretion."[201] Allowing an officer to use their experience and common sense to interpret specific facts does not run afoul of the protection against general warrant. It is only when the common sense is unmoored from the facts of the case that it would enable the officer to act with unbridled discretion. And law enforcement officers, like all humans, approach a situation with their own set of biases. If there is no curb on that discretion, it results in a world where the desire to search simply becomes the right to search. After all, at that juncture, we slip into the first hypothetical scenario conceptualized in this section where, when probable cause exists once in one case, it exists always and in every case. Permitting common sense and inferences based on an officer's experience about how cell phones are used in certain crimes but requiring that it be filtered through the lens of the actual case is a check on the general warrant that concerned the founding generation. Officers cannot always seize a cell phone in every case, but if they have reason to believe a cell phone was used in a crime, they can rely on their own experience to help the court understand why the phone is likely to have evidence on it.

Finally, does this create a workable rule that lower courts can apply without being dependent on particular technology or the rule being rendered moot as technology advances? Absolutely. This rule provides clear guidance. When evaluating an officer's affidavit of probable cause, the magistrate or judge should expect to see clear and direct facts in the case itself that illustrate that a phone was used. Additionally, the officer's reliance on their experience or common sense in the affidavit must be directly tied to the facts at issue, rather than broad and unmoored statements about the ubiquitous use of cell phones in everyday life. Those requirements are not inherently connected to any specific technology or electronic device, so changes to technology will not impact the rule itself.

199. District of Columbia v. Wesby, 583 U.S. 48, 49 (2018) (noting that officers can use common sense about human behavior).

200. Texas v. Brown, 460 U.S. 730, 742 (1983).

201. United States v. Matlock, 415 U.S. 164, 180, n.1 (1974) (Douglas, J., dissenting).

B. Restrictions on How the Search is Conducted

Just as was true in the prior section, we can conceptualize two very different scenarios regarding the level of restrictions a court could impose on how a police officer conducts a search of an electronic device. On the side most deferential to law enforcement, as some cases discussed in this article have advocated, the warrant would merely provide that the officer can search for evidence of a particular crime on the phone. And, the officers could almost certainly look anywhere on the phone for that evidence.

By contrast, in the most restricted world, the courts would impose strict temporal limitations on the search, focused on the date of the offense, and would require that the search only extend to those parts of the phone where the probable cause points to the existence of evidence. In other words, if law enforcement can demonstrate that the suspect sent a text message about the crime, they can look in his text messages. If the suspect was seen in a "selfie" holding what appears to be an illegal firearm, then officers can examine his photos, but they do not get to look everywhere in all crimes.

This is the trickiest section for devising rules, because it is where the strongest debate between the lower courts has risen. In this section, I will operate in reverse by looking at the two extreme versions of possible rules to see if we can reverse-engineer the correct rule. As a starting point, I would note that each of the extreme positions appears to significantly run afoul of at least one of the standards established in Part I of this article.

For example, if the Supreme Court adopted a ruling that followed the most permissive line of jurisprudence (from a law enforcement perspective), it would appear to violate both the first and second standards. First, a rule that places virtually no restriction on how law enforcement officers examine the contents of an electronic device could cause a disconnect between the government action and the rationale that led the Court to create the doctrine in the first place in a non-digital context. For example, in this scenario, police are broadly allowed to look anywhere in an electronic device without temporal or application-based restrictions and seize all evidence related to a given crime. However, the problematic implication of this rule from a civil liberties context is that the officers could see an enormous amount of information about other aspects of the suspect's life that are not necessarily under investigation and seize anything that appears to be either contraband or evidence of another crime. This is because of the Supreme Court's plain view doctrine, which holds that when law enforcement officers are in a place they are legally permitted to be, they can seize contraband or evidence they come across without having a warrant for it in advance.[202] The plain view exception to the search warrant requirement has generally been justified by the Supreme Court through several different

202. *See* Coolidge v. New Hampshire, 403 U.S. 443 (1971); and Horton v. California, 496 U.S. 128, 142 (1990).

rationales. First, there is the principle that mere observation does not constitute a search.[203] Second, for a person to have a reasonable expectation of privacy that is protected under the Fourth Amendment, they must take the steps necessary to manifest that expectation—if someone chooses to expose their criminality to the world writ large, they do so at their own risk.

There would be a disconnect between those rationales and what would be permitted if the Supreme Court adopted an unrestricted rule on how law enforcement searches electronic devices. While simply looking or observing may not be understood as a search, an officer rummaging through countless personal files and images has much different privacy implications than the police officer making a passing observation through an open window, from a plane, or when doing a quick walk through the home of an arrestee to make sure there is no one hiding who could harm the police.[204] Second, in the case of an electronic device, the steps an individual takes to manifest an expectation of privacy are different than in other contexts. While the homeowner might pull down the blinds or put items away that they do not want visitors to see, there is no easy analogy in the digital context. Presumably, many people feel that simply by the nature of having the phone on their person, they have sufficiently manifested a desire to keep its contents private from others. Additionally, opening and examining each file on an electronic device to ascertain whether it is contraband or evidence is akin to the constitutionally prohibited act in a physical search of turning an item over to examine its serial number in order to see if is stolen property. And, it is worth noting, the Court has held firm that if an officer is justifying a seizure based on the plain view doctrine, they cannot do anything to manipulate the property at issue to reveal it as contraband or evidence of a crime.[205]

Similarly, an unrestricted rule on how these searches are conducted appears to be discordant with the fundamental understanding of privacy at the time the Fourth Amendment was adopted. To see how this might be the case, it is important to return to the founding generation's concern about general warrants. There was clearly a worry about the idea that an individual would somehow offend the Crown and, as a result, have an officer search through the entirety of their home based solely on a piece of paperwork that provided no meaningful restriction or guidance on what the officer could and could not do. It is difficult

203. *See e.g.*, *Ciraolo*, 476 U.S. at 213 (opining, "[t]he Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares").

204. The Supreme Court has held that a defendant does not have a reasonable expectation of privacy that prevents police form observing his property form a helicopter using their naked eye. *Riley*, 488 U.S. at 456. The Court has also permitted officers to do a protective sweep of a home of an occupant that is being arrested to make sure that no one is hiding who can harm the officer. Maryland v. Buie, 494 U.S. 325 (1990).

205. Arizona v. Hicks, 480 U.S. 321, 324-25 (1987) (holding that an officer's search did not fall within the plain view doctrine when he manipulated a stereo speaker to see its serial number).

not to see a worrisome analogy between that image and a lack of any restriction on how electronic evidence warrants are executed. Having failed both the first and second standards, I believe that this proposed ruling would not be the appropriate outcome based on the expectations from Supreme Court precedent.

Now consider the opposite viewpoint—one that imposes strict temporal and application-based limitations on how law enforcement conducts a search or takes even more restrictive measures that provide technical limitations to how the search is conducted. I believe that this approach would conflict with the first and third standards offered by this article. First, this is a highly formalistic, technical, and constraining approach that appears to be disconnected from much of the Fourth Amendment jurisprudence surrounding the relationship between probable cause and searches. The Supreme Court has repeatedly rejected rules that apply inflexible standards that come across as formalistic, checkbox approaches rather than maintaining flexibility.[206]

Additionally, this approach would violate the third standard because it would not create easily manageable standards that can be applied by the lower courts without respect to changing technology. The ability of police departments to comply with mandates that warrant that officers only look at files from a specific date or a particular application depends on the technological capacity of the police department. There is no reason to assume that all departments, large and small, rural and urban, have the same technology that would facilitate a highly specified method of isolating and extracting only certain data, during a certain time frame, and labelling it in such a way as to prevent inadvertent exposure to prohibited material. Moreover, consider the difficulties of managing an exacting standard. For example, let us assume a scenario where probable cause supported the idea that, on the suspect's phone, there was a single picture of him with the stolen property in a case. If the warrant only provided for the search and recovery of that particular photograph, how would the police possibly identify the image without looking at other pictures? And what would happen if the police inadvertently saw another photograph that had criminal evidentiary value? Would they have to ignore it since it would fall outside the scope of the limited warrant?

So, what kind of rule might provide the middle ground that would satisfy all three standards? I propose the following: A search warrant for an electronic device must include limitations on its execution that restrict the search to data reasonably likely to exist based on the specific facts of the case and the nature of the alleged crime. Before assessing this rule against this article's three standards,

206. For example, the Supreme Court has struck down formalistic approaches to assessing the reliability of a drug detection dog used by the police in an investigation in favor of utilizing a flexible, totality of the circumstances approach. Florida v. Harris, 568 U.S. 237, 240 (2013). Similarly, the Court eliminated a formal two step approach to assessing probable cause that required independent assessment of an informant's basis of knowledge and reliability by favoring a totality of the circumstances approach that viewed those factors holistically. Illinois v. Gates, 462 U.S. 213 (1983).

it is worth examining the strengths of this approach in addressing some of the concerns raised in the cases previously discussed. First, this test moves law enforcement away from the sweeping "any and all" language that finds its way into many search warrants and sounds akin to a general warrant. Second, it forces law enforcement to rely upon the specific facts of the case and to develop a nexus between those facts and how they will search the electronic device. This too takes aim at sweeping generalizations and focuses on particularization. At the same time, this rule preserves reasonable flexibility and allows law enforcement to rely on their experience as discussed in the prior chapter. For example, one can understand how the likelihood of a phone having evidence on it is heightened when the offense is an ongoing and preplanned crime like drug dealing, rather than a spontaneous "one-off" crime like an assault. This standard allows for flexibility but requires the affiant to go to greater lengths to explain why particular parts of the phone are likely to yield evidence of a crime.

Additionally, when it comes to the more general data that applies in virtually all cases, such as location data and indicia of ownership, this rule recognizes the utility and legitimacy of law enforcement obtaining that evidence. At the same time, it forces law enforcement to articulate how it would obtain that information in a manner that does not result in observing additional information that goes beyond the scope of what is permitted.[207]

Let us now consider how this proposed rule fares under the three standards offered in this article. First, does the application of the doctrine cause a disconnect between the government action and the rationale that led the Court to create the doctrine in the first place in a non-digital context? There is no disconnect. The Supreme Court has frequently connected the assessment of probable cause with the requirement that it be particularized. For example, the Court has opined that "[t]he substance of all the definitions of probable cause is a reasonable ground for belief of guilt and that the belief of guilt must be particularized with respect to the person to be searched or seized."[208] This doctrine re-emphasizes that line of jurisprudence, calling for probable cause to be particularized to the place being searched. Rather than allowing an officer to roam through a device with no limitations in the abstract hope of recovering evidence, this requires some minimal level of connection between the place being searched and the facts at issue, without being so overly restrictive as to render the investigation unworkable.

---

207. As will be discussed in the next section on good faith reliance, there are reasonable measures that can be put in place to ensure that law enforcement doesn't use broad categories of evidence like location data and indicia of ownership as a ruse to see areas of the phone beyond the scope of the warrant in an abstract hope that it might reveal evidence of some other unrelated crime.

208. Maryland v. Pringle, 540 U.S. 366, 371 (2003); *see also* Ybarra v. Illinois, 444 U.S. 85, 91 (1979) (stating, "[w]here the standard is probable cause, a search or seizure of a person must be supported by probable cause particularized with respect to that person. This requirement cannot be undercut or avoided by simply pointing to the fact that coincidentally there exists probable cause to search or seize another or to search the premises where the person may happen to be").

Second, is the rule consistent with the fundamental understanding of privacy at the time of the adoption of the Fourth Amendment? This rule is specifically designed to prevent the specter of a general warrant by ensuring that there are some levels of guardrails that guide the action of law enforcement.

Finally, does this create a workable rule that lower courts can apply without being dependent on particular technology or being quickly rendered moot as technology advances? This rule creates a clear and manageable standard that is not dependent on a particular type of technology. It is flexible and can be applied as technology changes. The lower courts will be looking for a nexus between specific facts and the way law enforcement is seeking to conduct the search.

C. The Circumstances for Applying Leon's Good Faith Reliance

In a sense, good faith reliance looks at both the actions of law enforcement (are they behaving in good faith) and the actions of the magistrate (was the warrant facially valid and arguably supported by probable cause rather than a bare-bones affidavit). At first glance, *Leon* good faith reliance appears to be a deal killer to the overwhelming number of particularity challenges. A warrant will always have been issued in these cases and is considered presumptively valid.[209] Unless a defense attorney can prove either that the police officer was not acting in good faith or the magistrate's or judge's granting of the warrant was so outrageous that the officer should have known better, the prosecution is going to win the motion to suppress.

This brings to mind Justice Brennan's dissent in *Leon* where he argued that if the protections of the Fourth Amendment do not result in the exclusion of evidence, they may just as well not be written down in the Constitution in the first place.[210] It is acting to "grant the right, but in reality to withhold its privilege and enjoyment."[211] Justice Brennan went on to warn:

> Although the Court's opinion tends to overlook this fact, the requirement of particularity is not a mere "technicality," it is an express constitutional command. The purpose of that requirement is to prevent precisely the kind of governmental conduct that the faulty warrant at issue here created a grave risk of permitting–namely, a search that was not narrowly and particularly limited to the things that a neutral and detached magistrate had reason to believe might be found at respondent's home. [212]

Justice Brennan's predictions notwithstanding, it is not the case that good faith reliance is simply the prosecution's ace in the hole that will always sustain the government's case even in the event of a constitutionally defective warrant.

---

209. *See e.g.*, Archer v. Chisholm, 870 F.3d 603, 613 (7th Cir. 2017) (opining, "Searches undertaken pursuant to valid search warrants are presumptively valid . . . ").

210. *Leon*, 468 U.S. at 936 (Brennan, J., dissenting).

211. *Id.* at 940.

212. *Id.* at 947.

Within the context of a search warrant for electronic evidence, I would offer two prongs for assessing this doctrine's applicability. With respect to whether the law enforcement officer is acting in "good faith," I would offer as a test whether there is evidence that the law enforcement officer is attempting to intentionally circumvent the constraints of probable cause in order to go on a "fishing expedition" through a suspect's electronic device.[213] For example, let us consider a situation where the officer's affidavit in support of probable cause provides justification for examining the phone to obtain the suspect's location data at a particular location. The officer could correctly argue that location data could be in numerous parts of a phone since activity on many apps, along with text messages, phone calls, and sending or receiving emails, requires the use of a cell tower that might reveal that individual's location. If obtaining the actual location data from those areas does not require directly looking at the content of images and messages just to see where they were sent from, but the officer still does so under the argument that this was in "plain view" while the officer was examining location information, it would point to disingenuous behavior or bad faith.

As for evaluating whether either the magistrate's finding of probable cause is so outrageous or the warrant is facially invalid such that *Leon* provides no harbor to the government, the best standard is already offered by dicta in *Leon*. Is this a situation where reasonable minds could differ on whether the warrant was supported by probable cause?[214] If the answer is yes, and there is no evidence of bad faith by law enforcement, *Leon* should apply.

How does this test (no evidence of disingenuous behavior by law enforcement coupled with an evaluation of whether reasonable minds could differ on the magistrate's conclusion) hold up to the three standards I offered from *Riley*, *Carpenter*, and *Kyllo*?

First, does the application of the doctrine cause a disconnect between the government action and the rationale that led the Court to create the doctrine in the first place in a non-digital context? *Leon* created the doctrine of good faith reliance under the theory that if there is not improper police conduct to deter in the first place, then the exclusionary rule is not the appropriate remedy to apply.[215] This rule provides examination into the propriety of a law enforcement officer's behavior. If there is no evidence of a disingenuous subterfuge, and there is a question of reasonable legal dispute, then the officer is not punished for having relied on the magistrate's assessment of the situation. This rule's application in the digital context keeps it directly moored to the reason the concept exists in the first place.

213. When used in a case law, a fishing expedition is traditionally understood as a search or action taken, not based on articulable suspicion, but "in the hope that something would turn up." *See e.g.*, Utah v. Strieff, 579 U.S. 232, 242 (2016).

214. *See Leon*, 468 U.S. at 914.

215. *Id.* at 909.

Second, is the rule consistent with the fundamental understanding of privacy at the time of the adoption of the Fourth Amendment? As explained in the preceding section, the rules suggested by this article protect against the concept of the general warrant that was detested by the founding generation. The application of this rule will continue to steer law enforcement to obtain judicial review of their action rather than conducting warrantless searches. Since there are meaningful constraints on the breadth of when the warrant can be issued and what it can be issued for, it is consistent with that original expectation of privacy.

Finally, does this create a workable rule that lower courts can apply without depending on particular technology or being quickly rendered moot as technology advances? As it relates to evaluating whether the officer was behaving disingenuously, at first glance it seems challenging to explore that individual's subjective mindset.[216] But the reality is that the law frequently requires courts to examine circumstantial evidence to determine intent.[217] When there is a disconnect between what the officer argues probable cause supports (i.e., finding location data or indicia of ownership) and what the officer is actually looking at (content of messages), the court can reasonably infer a lack of good faith. One can imagine a world in which looking for indicia of ownership of a phone would permit not just looking at who the registered owner of the phone is and what accounts are associated with it, but also looking at photographs to see who is depicted in images and reading through every text message and email with the nominal purpose of seeing if it points to the phone's user. However, there is a juncture at which the evidence of ownership is so overwhelming that it would strain credulity to believe that the officer was doing anything more than examining every part of the phone they could look at in the bare hope that there might be evidence of wrongdoing.

Asking whether reasonable minds can differ on a legal conclusion is also not a difficult task for lower courts to administer. After all, this article shows many contested views of issues regarding probable cause. Presumably a judge can understand why differing views are entitled to deference even if they do not reflect the reviewing judge's assessment of the situation. This is akin to the "abuse of discretion" standard that is routinely used by courts.[218]

This test is neither tied to particular technology, nor is it likely to be rendered moot with minor technological advancements.

---

216. *See, e.g.*, Whren v. United States, 517 U.S. 806, 813 (1996) (stating, "Subjective intentions play no role in ordinary, probable-cause Fourth Amendment analysis").

217. *See, e.g.*, Foster v. Chapman, 578 U.S. 488, 501 (holding that, "determining whether invidious discriminatory purpose was a motivating factor demands a sensitive inquiry into such circumstantial . . . evidence of intent as may be available").

218. "An abuse of discretion is defined in this circuit as a judicial action which is arbitrary, capricious, or whimsical." Pelican Prod. Corp. v. Marino, 893 F.2d 1143, 1146 (10th Cir. 1990). "Only if the decision 'was made without a rational[] explanation, inexplicably departed from established policies, or rested on an impermissible basis,' will we grant the petition for review." Jimenez-Guzman v. Holder, 642 F.3d 1294, 1297 (10th Cir. 2011) (alteration in original).

CONCLUSION

The question of how the Fourth Amendment's particularity requirement applies to cell phone searches is not a theoretical one—it is a live issue dividing the lower courts and affecting millions of Americans. Some courts have given law enforcement near-limitless discretion to rummage through the digital equivalent of an entire life, while others have imposed demanding restrictions that risk hampering legitimate investigations. This fractured landscape cries out for guidance from the Supreme Court.

This Article has argued that any resolution must satisfy three essential standards: it must remain true to the philosophical foundations of the Fourth Amendment, preserve the level of privacy protection the Framers intended, and provide a workable rule for courts facing ever-changing technologies. The framework proposed here offers a coherent path forward. By adopting clear and principled limits on cell phone searches, the Supreme Court can bring much-needed clarity to the law and ensure that constitutional privacy protections remain meaningful in the digital age.