Nebraska Law Review

Volume 99 | Issue 2 Article 6

2020

Suspects Use Cell Phones, but So Do We: State v. Goynes and the Constitutional Dangers of Boilerplate Search Warrants

Shayna Bartow
University of Nebraska College of Law

Note*

Suspects Use Cell Phones, but So Do We: *State v. Goynes* and the Constitutional Dangers of Boilerplate Search Warrants

TABLE OF CONTENTS

* Shayna Bartow, J.D. candidate, 2021, University of Nebraska College of Law.

I would like to thank my family and friends who have cheered me on through my law school journey. I would also like to extend a big thank you to the entire *Nebraska Law Review* team for their support and hard work as we prepared this Note for publication.

I. INTRODUCTION

In *Riley v. California*, the United States Supreme Court held that a warrant is generally required for law enforcement to search a cell phone seized incident to a suspect's arrest.[1] Although this mandate seems clear,[2] the Court did not outline what law enforcement must include in a cell phone search warrant to comport with the probable cause and particularity requirements of the Fourth Amendment.[3] As a result, state courts are left to determine when cell phone search warrants satisfy the Fourth Amendment.[4] In applying *Riley* and analyzing the validity of cell phone search warrants, the Nebraska Supreme Court has tried to balance law enforcement's need for evidence against citizens' privacy interests in an increasingly digital age.[5] Unfortunately, in its most recent case on this issue, *State v. Goynes*, the court failed to properly balance these conflicting interests.[6]

In *Goynes*, a criminal defendant challenged the district court's refusal to suppress evidence that police recovered from a search of his cell phone, arguing the authorizing search warrant violated the Fourth Amendment.[7] Despite the shortcomings of the warrant, the Nebraska Supreme Court affirmed the district court's admission of the cell phone evidence, holding the warrant was supported by probable cause and sufficiently particular.[8]

This Note aims to articulate the shortcomings of the court's decision in *Goynes* and the impact it has on Fourth Amendment protections in Nebraska. Part II of this Note will discuss the increased presence of cell phones in American society and rising privacy con-

1. Riley v. California, 573 U.S. 373, 401 (2014).
2. *Id.* at 403 ("Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant.").
3. U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.").
4. *See* William Clark, *Protecting the Privacies of Digital Life:* Riley v. California*, the Fourth Amendment's Particularity Requirement, and Search Protocols for Cell Phone Search Warrants*, 56 B.C. L. REV. 1981, 1997 (2015) (discussing the limited scope of the Court's holding in *Riley v. California* and the responsibility of state courts to determine when cell phone search warrants comply with the Fourth Amendment).
5. *See* State v. Henderson, 289 Neb. 271, 289, 854 N.W.2d 616, 633 (2014) (analyzing the sufficiency of a cell phone search warrant for the first time post-*Riley v. California* and noting that "the privacy interests at stake in a search of a cell phone" require searches to be "sufficiently limited in scope" according to the Fourth Amendment).
6. State v. Goynes, 303 Neb. 129, 927 N.W.2d 346 (2019).
7. *Id.* at 131, 927 N.W.2d at 349.
8. *Id.* at 144, 927 N.W.2d at 357.

cerns as cell phones become more advanced.[9] Additionally, Part II will discuss how the law governing search warrants has developed over time and the ongoing difficulty courts have had in applying traditional Fourth Amendment principles to advancing technology.[10] Finally, Part II will discuss *State v. Goynes*, the Nebraska Supreme Court's most recent failure regarding cell phone search warrants.[11] Part III will discuss how the decision in *Goynes* established a dangerous precedent for lower courts to authorize broad, boilerplate cell phone search warrants that will expose Nebraska citizens to unreasonable searches in direct violation of the Fourth Amendment.[12] Part III will also offer an alternative approach to evaluating cell phone search warrants.[13]

II. BACKGROUND

A. Cell Phone Use & Consumers' Expectations of Privacy

Cell phones have become a staple of the American lifestyle. Approximately 96% of Americans own a cell phone, as compared to just 84% of Americans in 2008.[14] The overwhelming majority of these individuals own smartphones.[15] As technology advances, the frequency at which individuals use their cell phones and the amount of sensitive information they store and access on their cell phones is also exponentially increasing.[16]

---

9. *See infra* section II.A.
10. *See infra* section II.B.
11. *See infra* section II.C.
12. *See infra* section III.A.
13. *See infra* section III.B.
14. *Mobile Fact Sheet*, PEW RES. CTR. (June 12, 2019), https://www.pewinternet.org/f/mobile/ [https://perma.unl.edu/YP76-R6CE].
15. *Id.* (finding that of the 96% of Americans who owned cell phones in 2019, 81% of those individuals owned a smartphone).
16. *See* CTIA, ANNUAL SURVEY HIGHLIGHTS 1, 2–3 (2019), https://api.ctia.org/wp-content/uploads/2019/06/2019-Annual-Survey-Highlights-FINAL.pdf [https://per.unl.edu/3KFL-5X56] (finding that U.S. wireless data use is up over seventy-three times since 2010, and that from 2017 to 2018 alone there was an 82% growth in mobile data use, a 9.6% growth in the number of minutes consumers spent talking on their mobile devices (totaling 2.4 trillion minutes), and a 15.8% growth in the number of text messages exchanged (totaling 5.5 billion texts sent per day)); Monica Anderson, *6 Facts About Americans and Their Smartphones*, PEW RES. CTR.: FACT TANK (Apr. 1, 2015), https://PewResearch-org-preprod.go-vip.co/fact-tank/2015/04/01/6-facts-about-americans-and-their-smartphones/ [https://perma.unl.edu/Z2KK-CET2] (concluding that in as early as 2014, smartphone users were using their cell phones accordingly: 97% for text messaging, 92% for voice/video calls, 88% for email, 75% for social networking, 60% for taking pictures/videos, 62% to get information about a health condition, and 57% to do online banking).

In *Riley*, the Court explained that a standard sixteen gigabyte device can hold millions of text messages and documents.[17] In the six years since *Riley* was decided, cell phone storage capabilities have drastically increased—with the top-selling cell phone of 2018 having up to 256 gigabytes of storage—allowing consumers to store even more private data on their devices.[18] The amount of private information accessible from a smartphone is even greater as more individuals use "the Cloud,"[19] which allows the user—and police—to access data that is not stored directly on the cell phone from the device.[20] In addition to their massive storage capacities, cell phones have become so intertwined with human existence that some philosophers and cognitive researchers argue smartphones are actually an extension of an individual's mind worthy of protection from intrusion.[21] One researcher concluded that "unlocking our devices is not simply like unlocking our house" but "is more like opening up our minds," and therefore, forcing individuals to do so without proper safeguards is a breach of mental autonomy.[22]

17. Riley v. California, 573 U.S. 373, 394 (2014) ("The current top-selling smart phone has a standard capacity of 16 gigabytes (and is available with up to 64 gigabytes). Sixteen gigabytes translates to millions of pages of text, thousands of pictures, or hundreds of videos."). The Court in *Riley* also acknowledged that "data on the phone can date back for years." *Id.* at 375.
18. *See* Jeb Su, *The iPhone X Was the World's Best Selling Smartphone in Q1 2018*, FORBES (June 13, 2018, 2:29 PM), https://www.forbes.com/sites/jeanbaptiste/2018/06/13/the-iphone-x-was-the-worlds-best-selling-smartphone-in-q1-2018/#2589cbd77d2f [https://perma.unl.edu/M3Z3-FP3V]; *iPhone X - Technical Specifications*, APPLE (Aug. 9, 2019), https://support.apple.com/kb/sp770?locale=EN_US [https://perma.unl.edu/3HYU-N33A] (showing the iPhone X is available with either 64 or 256 gigabytes of storage capacity).
19. Cisco Systems, *Forecast Number of Personal Cloud Storage Consumers/Users Worldwide from 2014 to 2020*, STATISTA (Oct. 28, 2016), https://www.statista.com/statistics/499558/worldwide-personal-cloud-storage-users/ [https://perma.unl.edu/3MEQ-XS24] (estimating that approximately 1.8 billion people worldwide would use cloud storage in 2017 with that number continuing to grow into 2020).
20. *See Riley*, 573 U.S. at 397–98 (acknowledging that cell phones can be used to "access data located elsewhere" with the use of "cloud computing," providing another reason for heightened privacy protections when it comes to cell phone searches); *see also What Does iCloud Backup Include?*, APPLE (Jan. 16, 2020), https://support.apple.com/en-us/HT207428#targetText=your%20iPhone%2C%%2C%20and%20iPod%20touch%20backup%20only%20include%20information,you%20store%20in%20iCloud%20Drive [https://perma.unl.edu/9M9Y-WW] (explaining iCloud backup and what data from a cell phone can be backed up to the Cloud, including app data, text messages, photos, videos, etc.).
21. *See, e.g.*, Karina Vold, *Is Your Smartphone an Extension of Your Mind?*, VICE (Mar. 2, 2018, 9:00 AM), https://www.vice.com/en_us/article/qvemgb/is-your-smartphone-an-extension-of-your-mind [https://perma.unl.edu/ZR6M-Z8Z4].
22. Michael Lynch, *Leave My iPhone Alone: Why Our Smartphones Are Extensions of Ourselves*, GUARDIAN (Feb. 19, 2016, 5:29 PM), https://www.theguardian.com/technology/2016/feb/19/iphone-apple-privacy-smartphones-extension-of-ourselves [https://perma.unl.edu/KVU4-V7C8].

In light of these technological developments, debates about cell phones and privacy rights have catapulted into the center of the national stage. Most famously, a court case about how much power law enforcement should have to force providers and manufacturers like Apple to unlock encrypted cell phones[23] exploded into a controversy that divided the nation.[24] This debate illustrated the rise of an underlying national sentiment: cell phone data is so private that the government should not be able to access or monitor it, even for anti-terrorism efforts.[25] Cell phone privacy concerns have also resulted in citizens seeking technological protections to prevent law enforcement from searching their phones, and some major cell phone manufacturers have answered this call.[26] It is with this information about cell phone storage capabilities, along with the understanding of just how important citizens believe cell phone privacy to be, that the legal community must approach the discussion of cell phone search warrants.

---

23. *See* Jack Nicas, *Apple to Close iPhone Security Hole that Law Enforcement Uses to Crack Devices*, N.Y. TIMES (June 13, 2018), https://www.nytimes.com//06/13/technology/apple-iphone-police.html [https://perma.unl.edu/64DU-R5] (discussing the infamous case where Apple, in efforts to preserve its customers' privacy, refused to help the F.B.I. unlock the iPhone of a man suspected of killing fourteen people in a mass shooting). Apple's resistance eventually led to the F.B.I. dropping its legal action and paying a private third-party $1.3 million to unlock the phone, causing Apple to pursue new features to prevent future government hacking. *Id.*; *see also* Associated Press v. FBI, 265 F. Supp. 3d 82, 89–90 (2017) ("After initially commencing legal action against the phone's manufacturer, Apple, to compel its assistance in accessing the phone, the FBI moved to stay the proceedings in March 2016 when an 'outside party demonstrated to the FBI a possible method for unlocking Farook's iPhone.'" (citations omitted)).

24. *See CBS News Poll: Americans Split on Unlocking San Bernardino Shooter's iPhone*, CBS NEWS (Mar. 18, 2016, 8:24 PM), https://www.cbsnews.com/news/cbs-news-poll-americans-split-on-unlocking-san-bernardino-shooters-iphone/ [https://perma.unl.edu/2BGJ-UCAY].

25. *See, e.g.*, *Most Americans Think the Government Could Be Monitoring Their Phone Calls and Emails*, PEW RES. CTR.: FACT TANK (Sept. 27, 2017), https://www.pewresearch.org/fact-tank/2017/09/27/most-americans-think-the-gov-be-monitoring-their-phone-calls-and-emails/ [https://perma.unl.edu/-C23A] (finding that 70% of Americans believe their phone calls and emails are likely being monitored by the government and that 54% of Americans "disapprove[ ] of the government's collection of telephone and internet data as a part of anti-terrorism efforts").

26. *See* April Glaser, *The Next iOS Update Has a Feature to Prevent Cops from Searching Your iPhone*, SLATE (Aug. 18, 2017, 2:06 PM), https://slate.com//2017/08/the-new-iphone-update-will-help-prevent-cops-from-searchin-locked-device.html [https://perma.unl.edu/QZP8-HRQ2] (discussing new technology that allows users to disable fingerprint access to their cell phone, preventing police from forcing them to unlock their cell phones with their fingerprints); Nicas, *supra* note 23.

B. Fourth Amendment Overview & Evolution of Search Warrant Requirements in Response to Technology

Both the Fourth Amendment of the United States Constitution and the first Article of the Nebraska Constitution provide that:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[27]

The Founding Fathers' motivation for including this language in the Constitution is clear—citizens need to be protected from "general warrants" which would allow the government to engage in exploratory rummaging of an individual's possessions.[28] Modern courts emphasize this policy rationale when analyzing Fourth Amendment issues.[29] To protect against exploratory rummaging, searches conducted by police without a warrant "are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions."[30]

The second clause of the Fourth Amendment provides that warrants must meet two requirements: (1) warrants must be supported by probable cause, and (2) warrants must be sufficiently particular in describing "the place to be searched, and the persons or things to be seized."[31] In applying these Fourth Amendment requirements, the Nebraska Supreme Court has held: "Probable cause sufficient to justify issuance of a search warrant means a fair probability that contraband or evidence of a crime will be found."[32] Affidavits alleging facts

27. U.S. CONST. amend. IV; NEB. CONST. art. I, § 7; *see also* State v. Baker, 298 Neb. 216, 226, 903 N.W.2d 469, 477 (2017) (reinforcing the long-standing practice of construing "the Nebraska Constitution in lockstep with the U.S. Supreme Court's construction of the U.S. Constitution").

28. *Amdt. 4.1 Fourth Amendment: Historical Background*, CONST. ANNOTATED, https://constitution.congress.gov/browse/essay/amdt4-1/ALDE_00000774/ [https://perma.unl.edu/3SZX-F7XV] (last visited Sept. 14, 2020) (discussing the history of general warrants executed in furtherance of the King of England's reign and the influence of such incidents on the development of Fourth Amendment).

29. *See, e.g.*, Payton v. New York, 445 U.S. 573, 583–86 (1980); *Baker*, 298 Neb. at 227–28, 903 N.W.2d at 477–78; State v. Sprunger, 283 Neb. 531, 539, 811 N.W.2d 235, 243 (2012).

30. Katz v. United States, 389 U.S. 347, 357 (1967) (footnotes omitted); *accord* Riley v. California, 573 U.S. 373, 381–82 (2014); *see also* 2 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 4.1(b) (5th ed. 2018) (outlining the primary exceptions to the per se requirement of a search warrant including consent to the search, searches incident to arrest, exigent circumstances, and the automobile exception).

31. U.S. CONST. amend. IV.

32. *Sprunger*, 283 Neb. at 537, 811 N.W.2d at 242; *see also* State v. Prahin, 235 Neb. 409, 418–19, 455 N.W.2d 554, 561 (1990) (holding that to establish probable cause "there must 'be a nexus between the item to be seized and criminal behavior'" (quoting Warden v. Hayden, 387 U.S. 294, 307 (1967))).

from police investigations are used to establish probable cause.[33] When evaluating if an affidavit provides sufficient probable cause to support a warrant, "[t]he question is whether, under the totality of the circumstances illustrated by the affidavit, the issuing magistrate had a substantial basis for finding that the affidavit established probable cause."[34]

As for particularity, the U.S. Supreme Court[35] and the Nebraska Supreme Court have held that "[a] warrant satisfies the particularity requirement if it leaves nothing about its scope to the discretion of the officer serving it" in order to prevent "overseizure and oversearching."[36] Courts, however, have not taken literally the requirement that a warrant leave "nothing" to the officer's discretion. Instead, this language is widely interpreted to mean that "a warrant must be sufficiently particular to prevent the officer from having unlimited or unreasonably broad discretion in determining what items to seize."[37] Therefore, when analyzing particularity and the officers' discretion, courts must always circle back to the question of whether the description of the things to be seized is so broad that it "constitutes a general exploratory warrant."[38]

Although probable cause and particularity are distinct requirements, the two are closely related.[39] In describing this relationship, the Nebraska Supreme Court held that "[a]warrant may be sufficiently particular even though it describes the items to be seized in broad or generic terms if the description is as particular as the supporting evidence will allow, but the broader the scope of a warrant, the stronger the evidentiary showing must be to establish probable cause."[40]

Applying these Fourth Amendment principles to advancing technology—particularly cell phones—has proven to be a difficult task. One of the earliest and most primitive questions the United States Supreme Court addressed in *Olmstead v. United States* was how, if it

33. State v. Edmonson, 257 Neb. 468, 476, 598 N.W.2d 450, 457 (1999) ("To be valid, a search warrant must be supported by an affidavit establishing probable cause." (citing State v. Johnson, 256 Neb. 133, 589 N.W.2d 108 (1999))).
34. *Sprunger*, 283 Neb. at 537, 811 N.W.2d at 242.
35. Marron v. United States, 275 U.S. 192, 196 (1927).
36. State v. Henderson, 289 Neb. 271, 289, 854 N.W.2d 616, 633 (2014).
37. State v. Baker, 298 Neb. 216, 228–29, 903 N.W.2d 469, 478 (2017); *see also* LAFAVE, *supra* note 30, at § 4.6(a) (discussing particularity and how the Supreme Court's requirement that "nothing" be left to the discretion of officers is not to be read literally).
38. *See* LAFAVE, *supra* note 30, at § 4.6(a).
39. *Sprunger*, 283 Neb. at 540, 811 N.W.2d at 243 ("The requirement of particularity for a search warrant is closely related to the requirement of probable cause."); *see also* LAFAVE, *supra* note 30, at § 4.6(a) (discussing the intertwined analysis when assessing probable cause and particularity).
40. *Baker*, 298 Neb. at 228, 903 N.W.2d at 478.

all, the Fourth Amendment would extend to protect against unreasonable searches of telephone communications.[41] The Court held that intercepting an individual's telephone calls (wiretapping) was not a search that required a warrant under the Fourth Amendment because the government did not physically invade the individual's effects or curtilage.[42] This decision was later overruled by *Katz v. United States*, in which the Court held the Fourth Amendment protects "people rather than places;" therefore, the warrantless interception of Katz's conversation, even in a public phone booth, was unreasonable and violated the Constitution.[43]

Although seizing a cell phone and searching its contents is more clearly a physical intrusion of an effect than intercepting a phone call, these cases represent an important leap in the Court's reasoning as it began to grapple with citizens' "reasonable expectation of privacy" in relation to technology and non-tangible data.[44] The holding in *Katz*—departing from former precedent to find that an individual's expectation of privacy evolves and can be defeated by an electronic invasion[45]—was also a call on the judicial system to continually question and determine the application of the Fourth Amendment in cases involving advancing technology.[46]

41. Olmstead v. United States, 277 U.S. 438 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967).

42. *Id.* at. 466.

43. *Katz*, 389 U.S. at 351, 353. The Court's analysis in this case illustrates the early tension that arose when determining how to apply Fourth Amendment principles to emerging technology. Previously, the Fourth Amendment was exclusively invoked by the Court to protect citizens from physical intrusions (or trespasses) of protected areas such as homes, barns, and effects. *Id.* at 352–53; s*ee also* United States v. Jones*,* 565 U.S. 400, 405–06 (2012) (discussing the Fourth Amendment's deep connection to physical property rights and common-law trespass).

44. *See Katz*, 389 U.S. at 360–62 (Harlan, J., concurring) (explaining that whether the Fourth Amendment provides protection from search and seizure in a particular situation depends on whether "a person have [sic] exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable'"; further, "reasonable expectations of privacy may be defeated by electronic as well as physical invasion"); s*ee also Jones,* 565 U.S. at 406–09 (discussing the reasonable expectation of privacy standard formulated in *Katz* and how it "added to" the common-law trespassory test to recognize invasions prohibited by the Fourth Amendment that extend past physical property invasions).

45. *See supra* note 44 and accompanying text.

46. *See* Christopher Michels, *What's in the Box? Re-Conceptualizing Computers as Containers, Metadata as Contents of that Container, and Applying Fourth Amendment Protections*, 3 CRIM. L. PRAC. 5, 30–32 (2016) ("As technology changes, the reasonable expectation of privacy using technology will likely change as well."); Erica L. Danielsen, Note, *Cell Phone Searches After* Riley*: Establishing Probable Cause and Applying Search Warrant Exceptions*, 36 PACE L. REV. 970, 973–74 (2016) (discussing how technology has evolved citizens' reasonable expectation of privacy and arguing that "the United States judicial system is

Since *Katz*, state courts have struggled to answer this call and determine how the Fourth Amendment applies to technological advancements. Initially, state courts categorized cell phones—specifically early generation cell phones—as "containers" of electronic information and, using the Supreme Court's decision in *United States v. Robinson*, upheld warrantless searches of such cell phones as lawful "searches incident to arrest."[47] As cell phones began storing more data, however, a circuit split, as well as a contentious legal debate, emerged as to whether cell phones and containers were truly analogous.[48] Eventually, the Supreme Court granted certiorari in *Riley v. California* to address this split and decide whether warrantless searches of cell phones incident to arrest were, in fact, constitutional.[49] The Court's

obligated to continue to interpret and adapt the Fourth Amendment to conform to the advancements in society").

47. In *United States v. Robinson*, 414 U.S. 218, 226 (1973) (citations omitted), the Supreme Court held that "[w]hen an arrest is made, it is reasonable for the arresting officer to search the person arrested in order to remove any weapons that the latter might seek to use in order to resist arrest or effect his escape" and that it is also "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." Applying this standard, the Court held the officers were authorized to search a container (specifically, a cigarette carton) found in the arrestee's pocket without a warrant or additional probable cause. *Id.* at 235–36. The Court in *New York v. Belton*, 453 U.S. 454, 460 (1981) (footnotes omitted) extended the parameters of lawful searches incident to arrest holding that "when a policeman has made a lawful custodial arrest of the occupant of an automobile, he may . . . examine the contents of any containers found within the passenger compartment." Soon, courts across the country began relying on *Robinson* and *Belton* to find warrantless searches of cell phones and their digital contents to be lawful searches incident to arrest, analogizing cell phones as "containers" of electronic information. *See, e.g.*, People v. Diaz, 244 P.3d 501, 507–08 (2011) (alteration in original) ("[T]ravelers who carry sophisticated cell phones have no greater right to conceal personal information from official inspection than travelers who carry such information in 'small spatial container[s].' . . . [D]iffering expectations of privacy based on the amount of information a particular item contains should also be irrelevant."), *abrogated by* Riley v. California, 573 U.S. 373 (2014); *see also* Adam M. Gershowitz, *The iPhone Meets the Fourth Amendment*, 56 UCLA L. REV. 27, 38–40 (2008) (discussing lower court cases that relied on *Robinson* and *Belton* to hold that warrantless searches of cell phones were lawful searches incident to arrest).

48. *See* Adam M. Gershowitz, *The Post-*Riley *Search Warrant: Search Protocols and Particularity in Cell Phone Searches*, 69 VAND. L. REV. 585, 595 (2016) (discussing the circuit split that emerged "among federal courts and a handful of state courts" concerning warrantless searches of cell phones incident to arrest); Charles E. MacLean, *But, Your Honor, a Cell Phone Is Not a Cigarette Pack: An Immodest Call for a Return to the* Chimel *Justifications for Cell Phone Memory Searches Incident to Lawful Arrest*, 6 FED. CTS. L. REV. 41, 43–44 (2012) (discussing the small circuit split concerning whether cell phones could be constitutionally searched incident to arrest and arguing that the Supreme Court should find cell phones are not analogous to containers).

49. *Riley*, 573 U.S. 373. In this case, the Court addressed two separate appeals both dealing with warrantless searches of cell phones incident to arrest. In the first

decision was unanimous and unequivocally clear: "Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant."[50]

In coming to this conclusion, the Court explained that cell phones are vastly different from other objects or containers that may be found on an arrestee, especially since modern cell phones are much less like a telephone and much more like a "minicomputer."[51] Accordingly, the Court asserted that searching the contents of an individual's cell phone, on most occasions, would reveal more personal information than a search of one's entire home.[52] Since cell phones hold these "privacies of life," the Court acknowledged that in many cases citizens have a reasonable expectation of privacy when it comes to their cell phones.[53] The Court's decision to protect cell phone privacy was met with widespread support from individuals in the legal profession[54] and in the media.[55]

---

case, the defendant was stopped for a traffic violation and the incident ended in police arresting him for a weapons charge. In a search incident to his arrest, police discovered a cell phone in his pants pocket which they seized and later searched. Evidence uncovered from the cell phone, including photos and videos, led to the State charging the defendant in connection with an unsolved shooting. The State also sought an enhanced sentence based on evidence of gang membership that was uncovered during the search of the cell phone. The defendant filed a motion to suppress the evidence retrieved from the cell phone which the trial court denied. The California Court of Appeal upheld the decision, and the Supreme Court granted certiorari. In the second case, police arrested the defendant for participating in a drug sale. In a search incident to his arrest, police uncovered a cell phone and observed incoming calls from a contact named "my house." Police then traced the number to find his home address and executed a warrant to search the premises. Police found drugs and firearms in the home, and the defendant was arrested for possession of those items. The defendant challenged the trial court's admission of the evidence obtained from his cell phone. *Id.* at 373.

50. *Id.* at 403.

51. *Id.* at 393 ("[Cell phones] could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.").

52. *Id.* at 396–97 ("[A] cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.").

53. *Id.* at 403 (quoting Boyd v. United States, 116 U.S. 616, 625 (1886)).

54. *See, e.g.*, Richard M. Re, *Symposium: Inaugurating the Digital Fourth Amendment*, SCOTUSBLOG (June 26, 2014, 12:37 PM), http://www.scotusblog.com/2014/06/symposium-inaugurating-the-digital-fourth-amendment [https://perma.unl.edu/QX3T-6KLG] (asserting that "*Riley* will be remembered as the inauguration of a new era of Fourth Amendment doctrine" and that the decision is "the privacy gift that keeps on giving").

55. *See, e.g.*, Ben Goad, *Court on Cellphone Search: 'Get a Warrant*,' HILL (June 25, 2014, 8:34 PM), https://thehill.com/regulation/court-battles/210518-roberts-court-on-cell-phone-searches-get-a-warrant [https://perma.unl.edu/CWG8-XC9F] (noting that the *Riley* case was being described "as a 'revolutionary' victory for pri-

Despite early applause for the Court's decision,[56] it quickly became apparent that the seemingly unambiguous mandate—that law enforcement must have a warrant to search a cell phone—was difficult to implement without a methodology for lower courts to use when determining whether a cell phone search warrant is supported by probable cause and sufficiently particular.[57] As courts have struggled with these questions, various approaches and standards have emerged, many of which do not provide the privacy protections called for in *Riley* to shield citizens from "general warrants."[58]

The Nebraska Supreme Court first analyzed what is necessary to establish probable cause[59] and satisfy the particularity requirement[60] in a cell phone search warrant post-*Riley* in *State v. Henderson*.[61] In this case, police were called to the scene after reports of a shooting.[62] Witnesses told police they saw two men shooting at the victims, and police, after observing two men "running from the scene," initiated a foot chase and apprehend Henderson.[63] A search incident to his arrest uncovered a handgun and a cell phone.[64] Officer Schneider requested a warrant to search the contents of Henderson's cell phone. "As grounds for the issuance of the warrant, Schneider asserted that Henderson was a suspect in a shooting and that the cell phone was in Henderson's possession when he was arrested."[65] The county court for

---

vacy rights and a powerful check against the prying eyes of government"); Adam Liptak, *Major Ruling Shields Privacy of Cellphones*, N.Y. TIMES (June 25, 2014), https://www.nytimes.com/2014/06/26/us/supreme-court-cellphones-search-privacy.html [https://perma.unl.edu/TS3W-EE47] (describing *Riley v. California* as a "sweeping victory for privacy rights in the digital age").

56. *See* Gershowitz, *supra* note 48, at 587 (discussing the widespread support for the *Riley* decision among scholars after nearly a decade of calling on the Supreme Court to ban warrantless cell phone searches incident to arrest and noting that scholars believed the *Riley* decision was "recalibrating the balance between privacy and the needs of law enforcement").
57. *See* State v. Henderson, 289 Neb. 271, 290, 854 N.W.2d 616, 633–34 (2014) ("The parameters of how specific the scope of a warrant to search the contents of a cell phone must be will surely develop in the wake of *Riley v. California*."); *see also* Gershowitz, *supra* note 48, at 600–01 (providing an initial overview of the issues courts are having post-*Riley* with narrowing the scope of cell phone search warrants); Danielson, *supra* note 46, at 971–72 (explaining that "the *Riley* decision fails to address what should be stated in a warrant application" to establish probable cause and be sufficiently particular).
58. Clark, *supra* note 4, at 1983–84 (outlining the inconsistent, and in some cases, inadequate standards that have emerged in the lower courts as they grapple with the proper way to limit cell phone search warrants post-*Riley*).
59. *See supra* note 32 and accompanying text.
60. *See supra* notes 36–40 and accompanying text.
61. *Henderson*, 289 Neb. 271, 854 N.W.2d 616.
62. *Id.* at 287, 854 N.W.2d at 631.
63. *Id.*
64. *Id.*
65. *Id.* at 277, 854 N.W.2d at 625.

Douglas County issued the warrant, and Henderson filed a motion to suppress the evidence obtained from the search of his cell phone on the grounds that the warrant "did not contain sufficient information to establish probable cause to believe a crime or evidence of a crime would be found on [Henderson's] cellular telephone."[66]

Before the district court ruled on Henderson's motion to suppress, police submitted a revised affidavit and obtained a second search warrant for the cell phone from the county court.[67] Again, Henderson filed a motion to suppress the cell phone evidence on the same grounds.[68] The district court agreed that the affidavit in support of the first warrant was not sufficient to establish probable cause because it "did not sufficiently state why a search of the cell phone would produce evidence relevant to the crimes for which Henderson was arrested."[69] However, because *Riley* had not yet been decided by the Supreme Court, the district court held that the invalidity of the warrant did not require suppression of the cell phone evidence; the search of the cell phone was a valid warrantless search incident to arrest.[70] The jury found Henderson guilty on multiple charges, including first degree murder, and he was sentenced to life imprisonment.[71] In appealing his conviction, Henderson claimed the district court erred in overruling his motion to suppress and admitting the evidence obtained from the search of his cell phone.[72]

Henderson's appeal was pending when the United States Supreme Court decided *Riley*. Accordingly, the Nebraska Supreme Court applied the new *Riley* standard for cell phone search warrants.[73] In do-

66. *Id.* at 277, 854 N.W.2d at 626 (alteration in original).

67. *Id.* at 277–78, 854 N.W.2d at 626. To prevent suppression of the evidence, officer Schneider submitted a revised affidavit in attempt to more concretely establish probable cause that evidence of a crime would be found on Henderson's cell phone. In the revised affidavit, there was additional language stating:

> In Affiant Officers [sic] experience and training as a detective it is known that suspects that we have had contact with use cell phones to communicate about shootings that they have been involved it [sic], before, during, and afterwards. The communication can be though [sic] voice, text, and social media, to name a few.

Id. at 278, 854 N.W.2d at 626 (alteration in original).

68. *Id.*

69. *Id.*

70. *Id.* Because the court held no warrant was needed, it also did not address whether the revised affidavit in support of the second warrant was sufficient to establish probable cause to search the cell phone; the issue was moot. *Id.* However, after Henderson filed a motion to reconsider the ruling on the motion to suppress, the court held the second search warrant was "properly issued and executed" because the additional language in the affidavit "established probable cause to search the cell phone." *Id.* at 279, 854 N.W.2d at 626.

71. *Id.* at 282, 854 N.W.2d at 628.

72. *Id.* at 282, 854 N.W.2d at 628–29.

73. *Id.* at 285, 854 N.W.2d at 630.

ing so, it held the district court's ruling—that the search of Henderson's cell phone was a valid warrantless search incident to arrest—was erroneous and, consequently, evaluated the validity of the search warrant.[74]

First, the court analyzed whether the affidavits submitted by police were sufficient to establish probable cause for the searches.[75] The court held that the first warrant[76] was supported by probable cause because the affidavit alleged that (1) Henderson was a suspect in a shooting; (2) Henderson was apprehended by police near the scene of the crime after witnesses said two men shot at the victim; and (3) police found a cell phone in his pocket when he was arrested.[77] Based on these facts, the court held that the first warrant established probable cause to search Henderson's cell phone—it "established a fair probability that Henderson was involved in the shootings" and that "Henderson was working with at least one other person to commit the shootings, [so] it is reasonable to infer that the cell phone that was in his possession was used to communicate with others regarding the shootings before, during, or after they occurred."[78] In other words, the court found the first warrant established probable cause to search the cell phone, even without the additional allegations presented in the second affidavit that "cell phones are used in relation to crimes."[79]

Once the court established the warrants were supported by probable cause, it analyzed whether the warrants were sufficiently particular.[80] The court ultimately held the warrants were not sufficiently particular because they did not state "the specific crime being investi-

74. *Id.* at 286, 854 N.W.2d at 631 ("[U]nder the U.S. Supreme Court's holding in *Riley*, the district court erred when it concluded that the search of Henderson's cell phone was justified or necessitated as a search incident to arrest. Because a search of the contents of Henderson's cell phone required a warrant, we must consider whether the evidence Henderson sought to be suppressed was obtained in a search that was supported by a valid warrant."). In holding a valid warrant was required to search Henderson's cell phone per *Riley*, the court noted there were no exigent circumstances that would have authorized police to search the contents of Henderson's cell phone without obtaining a warrant. *Id.* at 285–86, 854 N.W.2d at 631. This was an important and necessary determination because the *Riley* Court held that, while warrantless searches of cell phones incident to arrest were unconstitutional, warrantless searches of cell phones could be valid where there were compelling, exigent circumstances that made the search by law enforcement objectively reasonable. Riley v. California, 573 U.S. 373, 401–02 (2014).

75. *Henderson*, 289 Neb. at 286–88, 854 N.W.2d at 631–32.

76. *See supra* text accompanying note 65.

77. *Henderson*, 289 Neb. at 286–88, 854 N.W.2d at 631–32.

78. *Id.* at 287–88, 854 N.W.2d at 632.

79. *Id.*; *see also supra* note 67. It naturally followed that the second warrant, which was supported by an affidavit with these additional allegations, was also supported by probable cause. *Id.*

80. *Henderson*, 289 Neb. at 288–90, 854 N.W.2d at 632–34.

gated" nor did they sufficiently state "the type of information encompassed by their authorization."[81] Both warrants "listed types of data, such as cell phone calls and text messages," however, "they concluded with a catchall phrase stating that they authorized a search of 'any other information that can be gained from the internal components and/or memory Cards.'"[82] By including this catchall phrase, the warrants were effectively general warrants that allowed law enforcement to conduct a search that was limited in scope only by the discretion of the officer serving the warrant (as opposed to being limited to content that was related to the probable cause which justified the search as required by the Fourth Amendment).[83]

In finding that the "any and all" catchall language violated the particularity requirement, the court relied in part on its decision in *State v. Sprunger*,[84] which addressed the validity of a warrant to search a computer.[85] In that case, a citizen reported that a fraudulent purchase was made online with his credit card, and police traced the IP address used to make the purchase back to the defendant.[86] When the defendant refused to let police take his computers, the police obtained a warrant authorizing them to search for and seize "[a]ny and all computer equipment."[87] After seizing the computers and learning some additional facts, the police applied for, and the county court issued, a second warrant to search the computers for "evidence of child pornography."[88] Police ultimately found child pornography on the

81. *Id.* at 289–90, 854 N.W.2d at 633; *see also* Gershowitz, *supra* note 48, at 599–600 (discussing the primary reasons lower courts sustain particularity challenges for cell phone search warrants, which include (1) "when the search warrant does not state on its face what crime the search is being conducted to find evidence of," and (2) "when the search warrant contains overbroad, catch-all language"). The court in *Henderson*, therefore, fell in line with other courts when it said the warrants failed the particularity requirement on both of these grounds.

82. *Henderson*, 289 Neb. at 290, 854 N.W.2d at 633.

83. *Id.* at 289–90, 854 N.W.2d at 633–34 ("In the present case, because the search warrants allowed a search of '[a]ny and all' content, their scope was clearly not sufficiently particular and therefore the warrants did not meet the Fourth Amendment particularity requirement and were invalid for this reason." (alteration in original)).

84. State v. Sprunger, 283 Neb. 531, 811 N.W.2d 235 (2012).

85. *Henderson*, 289 Neb. at 288–89, 854 N.W.2d at 632–33 ("Given the privacy interests at stake in a search of a cell phone as acknowledged by the Court in *Riley* and similar to our reasoning in *Sprunger*, we think that the Fourth Amendment's particularity requirement must be respected in connection with the breadth of a permissible search of the contents of a cell phone.").

86. *Sprunger*, 283 Neb. at 533, 811 N.W.2d at 239.

87. *Id.* at 534, 811 N.W.2d at 240 (alteration in original).

88. *Id.* During the execution of the first warrant, the defendant asked police if he could delete things off of his computer before they were taken. Based solely on this statement, police asked the defendant if he had child pornography on his computer. Even though he replied that he did not, police still stated their suspicions were raised. A few days later, police received a call from the defendant's

computer, and, after the district court denied the defendant's motion to suppress this evidence, Sprunger was convicted for possession of child pornography.[89]

In reviewing the validity of the warrants, the *Sprunger* court held both warrants were invalid because they lacked probable cause and particularity.[90] Ultimately, the court emphasized that in the age of advancing technology, it is "all the more important" that police particularly describe what they are looking for and establish probable cause that what they are looking for could be found on the device.[91] Defending this assertion, the court stated:

> "[T]he modern development of the personal computer and its ability to store and intermingle a huge array of one's personal papers in a single place increases law enforcement's ability to conduct a wide-ranging search into a person's private affairs." It thus makes the particularity and probable cause requirements all the more important.[92]

Relying on this strong statement about the importance of protecting computers from general searches, the court in *Henderson* held that the particularity requirement must be equally respected and enforced to limit the scope of cell phone search warrants, espeically since cell phones function as "'a digital record of nearly every aspect of their [owners'] lives,' and their ability to 'access data located elsewhere.'"[93] Therefore, the warrants in Henderson's case, which authorized law enforcement to search "any and all" information, violated the particularity requirement—they were not "sufficiently limited in scope to allow a search of only that content that is related to the probable cause that justifies the search."[94]

---

lawyer. The lawyer stated that his client had told him his computers were taken by police to search for child pornography. It was these facts that police used in their affidavit for the second warrant to assert there was probable cause child pornography would be found on the computer. *Id.*

89. *Id.* at 535–36, 811 N.W.2d at 240–41.

90. *Id.* at 540–41, 811 N.W.2d at 243–44 ("Based only on the fact that Sprunger wanted to delete some files, the deputies could never say with particularity what it was that they wanted to seize. They had no idea what files Sprunger might have wanted to delete. How could the deputies have had probable cause to believe that what they were looking for would be found on his computers when they did not even know what they were looking for? . . . Summed up, the call from Sprunger's attorney to the deputies established nothing more than that the deputy had made an offhand remark that led Sprunger to believe he was being investigated for child pornography. And Sprunger's desire to delete some files does not mean that any particular evidence would be found. Taken together, there was no probable cause to support the warrant.").

91. *Id.* at 540–41, 811 N.W.2d at 244.

92. *Id.* (alteration in original) (footnote omitted) (quoting Mink v. Knox, 613 F.3d 995, 1010 (10th Cir. 2010)).

93. State v. Henderson, 289 Neb. 271, 289, 854 N.W.2d 616, 633 (2014) (alteration in original) (quoting Riley v. California, 573 U.S. 373, 375, 397 (2014)).

94. *Id.* at 289, 854 N.W.2d at 633.

Despite finding that the search warrants for Henderson's cell phone were invalid, the court upheld the search of his cell phone under the good faith exception.[95] "[T]he warrants were carried out in good faith," so "the district court did not err when it overruled the motions to suppress or when it admitted evidence obtained from the search over Henderson's Fourth Amendment objections."[96] Problematically, the court did not outline what police need to include in future cell phone search warrants to comply with the particularity requirement. As a result, the court provided law enforcement with guidance on what an invalid warrant looked like but did not outline what was required for cell phone search warrants to be sufficiently particular under the Fourth Amendment.[97]

C. Nebraska's Current Approach to Cell Phone Search Warrants: *State v. Goynes*

After *Henderson*, the Nebraska Supreme Court did not hear another constitutional challenge to a cell phone search warrant until

95. The exclusionary rule may keep evidence out when the Fourth Amendment is violated, however, "[t]he Fourth Amendment contains no provision expressly precluding the use of evidence obtained in violation of its commands." *Id.* at 291, 854 N.W.2d at 634. "The good faith exception provides that evidence seized under an invalid warrant need not be suppressed when police officers act in objectively reasonable good faith in reliance upon the warrant." *Id.* Whether the officers' actions were objectively reasonable depends on "'whether a reasonably well-trained officer would have known that the search was illegal despite a magistrate's authorization.'" *Id.* (quoting *Sprunger*, 283 Neb. at 542, 811 N.W.2d at 245). Since there was no indication that the officers in Henderson's case "would reasonably have known of the defects in the warrants as authorized" and the police did not use "the warrant to conduct a search for evidence other than that related to the shootings investigation," the court held it was executed in good faith. *Id.* at 291–92, 854 N.W.2d at 634–35. The court recognized the warrants were not sufficiently particular; however, since they "contained references to specific items," they were not "so facially deficient" that reasonably well-trained officers would have known they violated the particularity requirement. *Id.* at 292, 854 N.W.2d at 635.

96. *Id.*

97. Since the court in *Henderson* held the catchall language to search "any and all" content on the cell phone failed to satisfy the particularity requirement, law enforcement could not expect to use this language again and rely on the good faith exception to "save" the evidence. Once officers had a ruling from the court that such language was insufficient, it could be easily established that a reasonably well-trained officer would know that a search conducted using such a warrant was illegal despite the magistrate's authorization. The court held in *Henderson* that "[o]fficers are assumed to 'have a reasonable knowledge of what the law prohibits.'" *Id.* at 291, 854 N.W.2d at 634 (quoting *Sprunger*, 283 Neb. at 542, 811 N.W.2d at 245). Therefore, after *Henderson*, officers were assumed to know that a warrant authorizing the search of "any and all" content on a cell phone was invalid but did not have guidance from the court as to what language would make a warrant sufficiently particular.

State v. Goynes.[98] On April 25, 2016, police were dispatched to an Omaha apartment complex after receiving reports that shots had been fired.[99] An investigation ensued and ultimately led to police arresting Michael Goynes five days after the incident.[100] Goynes had a cell phone in his possession when he was taken into custody.[101]

To establish probable cause to search Goynes's cell phone, police submitted an affidavit alleging eyewitnesses had seen Goynes exit a white sedan, fire shots at the victim, and return to the sedan, which then sped off.[102] The witnesses also stated they saw additional parties in the sedan but that none of them exited the vehicle.[103] The witnesses could not definitively state, however, whether Goynes was driving the sedan or was a passenger.[104] The witnesses' recollection of the incident was corroborated by video evidence from the crime scene, but the video was not clear enough to identify the shooter.[105]

In addition to alleging these facts to establish probable cause Goynes was the shooter, police attempted to assert facts that would specifically justify the search of his cell phone and extraction of his electronically stored information.[106] First, the investigating officer "stated his belief that data from the cell phone would assist him in determining the course of events regarding the homicide investigation."[107] The officer's explanation of why he believed evidence of the crime would be found on Goynes's cell phone was similar to the generic language used by officers in the *Henderson* warrant.[108] The warrant stated:

> From training, experience and research Affiant Officer is aware that the data on cell phones can provide invaluable insight for criminal investigations. Cell phones are used for communication, access to information, socialization, research, entertainment, shopping and other functionality. In addition to personal use, cell phones are often used as tools in criminal activity. Affiant Officer is aware of numerous instances where cell phones were used by participants in crimes to communicate via voice and text messaging, occasions

98. State v. Goynes, 303 Neb. 129, 927 N.W.2d 346 (2019).
99. *Id.* at 131, 927 N.W.2d at 349.
100. *Id.* Goynes was charged with "murder in the first degree, use of a deadly weapon (firearm) to commit a felony, and possession of a deadly weapon by a prohibited person." *Id.* at 135, 927 N.W.2d at 351.
101. *Id.* at 131, 927 N.W.2d at 349.
102. *Id.* at 132–34, 927 N.W.2d at 349–51.
103. *Id.* at 132–33, 927 N.W.2d at 350 ("Taylor indicated that he saw additional parties inside the white sedan, but that those individuals did not exit the sedan.").
104. *Id.* at 132–34, 927 N.W.2d at 349–51 (explaining that one eyewitness said the shooter got in "the driver's side of the sedan," another stated that he took cover and did not see Goynes get back into the sedan, and the last eyewitness said she saw Goynes exit from the "rear driver's side seat" but did not specify where he got back in once he was fleeing).
105. *Id.* at 132, 927 N.W.2d at 350.
106. *Id.* at 131, 927 N.W.2d at 349.
107. *Id.*
108. *See supra* note 67 and accompanying text.

> when they took photographs of themselves with weapons and/or illegal narcotics, times when they created videos of their criminal activity and instances when the Internet was used to research crimes they participated in, just to name a few. As such a cell phone can serve both as an instrument for committing a crime, as well as a storage medium for evidence of the crime.
>
> Cell phone data can assist investigators in determining the culpability of participants in criminal investigations. This is because the data can potentially provide a wealth of information that can assist in determining the motivation, method and participants involved in an incident. Information on the devices can provide invaluable insight to the who, what, when, where and why an incident occurred.[109]

In the warrant, officers also listed the types of data to be searched and extracted:

> [C]ell phone information, configurations, calendar events, notes, and user account information which could identify who owns or was using a cell phone; call logs which could establish familiarity between people involved and timelines of an incident; short and multimedia messaging service messages, chat and instant messages, and emails which could provide insight to establish an individual's level of culpability and knowledge of the incident; installed application data which could aid in determining a user's historical geographic location and demonstrate the user's association with investigated people, location, and events; media files such as images, videos, audio, and documents which could provide times and locations, as well as firsthand documentation of the incident; internet browsing history which could demonstrate the planning, desire, and participation in a crime; cell tower connections, global positioning system data, Wi-Fi, Bluetooth, and synchronization logs which could provide information on location in relation to the incident; and user dictionary information which could demonstrate familiarity with the crime being investigated.[110]

Based on this language, Goynes filed a pre-trial motion to suppress "all evidence obtained from the search of his cell phone records," arguing the search violated the Fourth Amendment.[111]

The district court held a hearing on the motion to suppress, and the officer who requested and executed the warrant testified.[112] During cross-examination the officer agreed the following was true:

> [T]he witnesses described in the affidavits did not provide any information or evidence that the shooter was using a cell phone in the minutes immediately preceding or after the shooting, that the shooter communicated about the shooting over his cell phone, that the shooter took photographs or video of the shooting, or that the shooter communicated about the shooting on social media.[113]

The district court overruled Goynes's motion to suppress, holding the warrant was supported by probable cause and was sufficiently particular.[114] During the trial, the prosecution inadvertently offered evi-

109. *Goynes*, 303 Neb. at 134, 927 N.W.2d at 351.
110. *Id.* at 142–43, 927 N.W.2d at 356.
111. *Id.* at 135, 927 N.W.2d at 351.
112. *Id.* at 135, 927 N.W.2d at 351–52.
113. *Id.* at 135–36, 927 N.W.2d at 352.
114. *Id.* at 136, 927 N.W.2d at 352.

dence which showed Goynes did not make any calls, send any text messages, or do any internet browsing shortly before, during, or after the shooting.[115] At the conclusion of the trial, the jury found Goynes "guilty of all counts," and he was sentenced to life in prison.[116]

On appeal, Goynes argued the district court erred in overruling his motion to suppress and admitting the evidence extracted from his cell phone.[117] The court ultimately held that the district court did not err when it overruled Goynes's motion to suppress because the warrant to search his cell phone "was supported by probable cause and met the particularity requirement of the Fourth Amendment."[118] To reach its conclusion that the warrant for Goynes's cell phone was constitutional, the court analyzed two issues. First, the court had to decide whether finding a cell phone on the suspect incident to arrest, coupled with an officer's opinion that cell phones typically have information relevant to criminal investigations, was sufficient to establish probable cause to search the cell phone.[119] Second, the court had to decide if the warrant's extensive list of data and applications to be searched was sufficiently particular.[120]

The court held the warrant to search Goynes's cell phone and seize its content was supported by probable cause.[121] The court applied *Henderson* and noted a similar factual basis that established probable

115. *See id.* ("According to the data contained in these exhibits, Goynes used the internet throughout the morning and early afternoon on April 25, 2016. Notably, Goynes repeatedly accessed Facebook between 3:38 and 4:19 p.m. and then stopped. There were no cell phone calls, text messages, or internet browsing history between 4:19 and 5:08 p.m. that day. At 5:08 p.m., Goynes again began accessing Facebook and, at 5:10 p.m., visited the website of a local television news station and viewed an article about the shooting before returning to Facebook."). The prosecution likely found this gap in his cell phone usage significant since the shooting occurred shortly before 4:25 p.m. on April 25, 2016.

116. *Id.* at 137, 927 N.W.2d at 352 ("Goynes was sentenced to life imprisonment for murder in the first degree, 45 to 50 years' imprisonment for use of a deadly weapon (firearm) to commit a felony, and 20 to 25 years' imprisonment for possession of a deadly weapon by a prohibited person.").

117. *Id.* at 137, 927 N.W.2d at 352–53. In assessing the merit of Goynes's appeal, the court applied a two-part standard of review. "Regarding historical facts, an appellate court reviews the trial court's findings for clear error, but whether those facts trigger or violate Fourth Amendment protections is a question of law that an appellate court reviews independently of the trial court's determination." *Id.* at 137, 927 N.W.2d at 353.

118. *Id.* at 145, 927 N.W.2d at 357; *see also* Aaron Hegarty, *Nebraska Supreme Court: Cellphone Records Used in 2016 Murder Case Were Admissible*, OMAHA WORLD-HERALD (May 17, 2019), https://www.omaha.com/news/courts/nebraska-supreme-court-cellphone-records-used-in-murder-case-were/article_697a6474-90de-5456-b876-4b1f53f14514.html [https://perma.unl.edu/D7W8-BHAA] (discussing the court's ruling and affirmation of Goynes's sentence).

119. *Goynes*, 303 Neb. at 138–41, 927 N.W.2d at 353–55.

120. *Id.* at 141–44, 927 N.W.2d at 355–57.

121. *Id.* at 141, 927 N.W.2d at 355.

cause—in both cases, "there was a fair probability that the defendant . . . was involved in the shootings and . . . he had a cell phone in his possession when he was taken into custody shortly after the shootings."[122] Further, as in *Henderson*, witnesses told police that Goynes was with other individuals during the commission of the crime.[123] These facts, coupled with the officer's assertions that "individuals who committed similar crimes commonly communicate, research, record, and perform other operations on their cell phones that would amount to evidence of the crime," were, according to the court, sufficient to support the finding that probable cause existed to search Goynes's cell phone.[124] The court noted this finding was limited in that "the content of the affidavit pertaining to how suspects use cell phones standing alone may not always be sufficient probable cause."[125]

Next, the court outlined why the warrant was sufficiently particular.[126] The court distinguished *Goynes* from *Henderson*, noting that the *Henderson* warrants were insufficiently particular because (1) they failed to refer to the crime police were investigating, and (2) because "by including such a catchall phrase as 'any other information,' a warrant fails to set parameters for the search of this substantial device and limit the search to only that content that is related to the probable cause justifying the search."[127] The court went on to say that *Henderson* does not prohibit expansive, and in some cases, perhaps even unlimited searches.[128] Contrary to Goynes's objections—that the list of areas to be searched on his phone was virtually a search of any and all information—the court held the warrant was sufficiently particular because, unlike *Henderson*, it stated that police were investigating a homicide and "listed specific areas to be searched within the cell phone."[129] Thus, the court held the warrant met the Fourth Amendment requirements and affirmed the district court's judgment.[130]

122. *Id.* at 140–41, 927 N.W.2d at 354–55.

123. *Id.* at 141, 927 N.W.2d at 355.

124. *Id.*

125. *Id.*

126. *Id.* at 141–44, 927 N.W.2d at 355–57.

127. *Id.* at 143–44, 927 N.W.2d at 356–57.

128. *Id.* at 143, 927 N.W.2d at 356 ("*Henderson* does not stand for the rule that a search of a cell phone cannot be expansive; instead, we held that the unlimited search of the cell phone in that case did not align with the justifying probable cause.").

129. *Id.* at 144, 927 N.W.2d at 357.

130. *Id.* at 145, 927 N.W.2d at 357.

III. ANALYSIS

A. Shortcomings of the *Goynes* Decision

1. Essential Eradication of Probable Cause Requirement

In finding the warrant to search Goynes's cell phone was supported by probable cause, the court held that the police affidavit provided sufficient evidence to establish a fair probability that evidence of the shooting would be on the cell phone.[131] This finding is problematic given the generic nature of the "evidence" provided in the affidavit.[132] Besides noting Goynes was a suspect in the shooting and that he had a cell phone when police arrested him five days after the incident, police did not provide any evidence specific to Goynes that established a fair probability that evidence of the shooting was on his phone.[133] At the motion to suppress hearing, officers admitted they had *no evidence* that Goynes used a cell phone before, during, or immediately after the shooting to plan, discuss, or record the crime.[134] None of the witnesses even reported seeing a cell phone in his possession at the time of the shooting.[135]

Instead, the affidavit relied almost exclusively on the investigating officer's opinion that (1) cell phone data "can *potentially* provide a wealth of information that can assist in determining the motivation, method and participants involved in an incident," and (2) that the officer was aware of "numerous instances" where criminals used cell phones to discuss and document criminal activity.[136] In essence, the officer opined—and the court affirmed—that if someone is suspected of a crime and owns a cell phone, there is a fair probability that evidence of the crime exists on the cell phone (even if there is absolutely no particularized evidence that the suspect used the phone to plan, discuss, or document the alleged criminal activity). Thus, an officer's unsupported suspicion is sufficient to find a nexus "between the item to be seized and criminal behavior."[137] In creating this standard, the court virtually eradicated the requirement for probable cause in cell phone search warrants. This is especially true given the officer's opinion was not that it was *probable* evidence of the crime was on the sus-

131. *Id.* at 139, 927 N.W.2d at 353 ("Probable cause sufficient to justify issuance of a search warrant means a fair probability that contraband or evidence of a crime will be found.").

132. *See supra* text accompanying notes 122–24.

133. *Goynes*, 303 Neb. at 140–41, 927 N.W.2d at 355.

134. *See supra* text accompanying note 113.

135. *Goynes*, 303 Neb. at 132–34, 927 N.W.2d at 349–51.

136. *Id.* at 134, 927 N.W.2d at 351 (emphasis added).

137. *See supra* note 32 and accompanying text.

pect's cell phone, but only that a cell phone can *potentially* provide information useful to investigations.[138]

Likely recognizing this standard was overly broad, the court unsuccessfully attempted to limit the scope of its application. After deciding the warrant was supported by probable cause, the court qualified its statement by noting:

> Although the content of the affidavit pertaining to how suspects use cell phones standing alone may not always be sufficient probable cause, when considered with all of the facts recited above, as we determined in *Henderson*, the affidavit provided a substantial basis to find probable cause existed to search the cell phone data.[139]

However, in *Goynes*, the only fact alleged in addition to the officer's opinion that "suspects use cell phones" (and that Goynes was a suspect with a cell phone) was that witnesses had seen other individuals in the sedan with Goynes before he exited the vehicle and fired shots.[140] Accordingly, the court held that an officer's opinion that "suspects use cell phones" is sufficient to establish probable cause to search a suspect's cell phone in any case where there is evidence that other individuals accompanied a suspect to the crime scene.

In attempt to further justify the lack of facts particular to Goynes necessary to establish probable cause that evidence of the crime existed on his cell phone, the court attempted to analogize its finding with its holding in *Henderson*.[141] The affidavit in *Henderson*, however, alleged significantly different, case-specific facts in addition to the officer's opinion that "suspects use cell phones," creating a stronger (but arguably still insufficient) nexus between the cell phone and the crime. First, in *Henderson*, when police were dispatched to the location where shots had been fired, witnesses stated they saw "two men firing at a victim."[142] One officer noticed "two men running from the scene."[143] While chasing one of the men, later identified as Henderson, the officer saw him throw a gun under a vehicle.[144] When po-

138. *Goynes*, 303 Neb. at 134, 927 N.W.2d at 351; *see also infra* note 175 (explaining that a possibility evidence may exist is not sufficient to establish probable cause).

139. *Goynes*, 303 Neb. at 141, 927 N.W.2d at 355.

140. *Id.* at 140–41, 927 N.W.2d at 355 ("In the instant case, Goynes had the cell phone in his possession at the time he was taken into custody and the affidavit established it was a fair probability that Goynes had committed the shooting. There were additionally witness accounts summarized in the affidavit that described Goynes' [sic] committing the shooting with the aid of one or more other people, and Cahill described how, in his experience as an investigator, individuals who committed similar crimes commonly communicate, research, record, and perform other operations on their cell phones that would amount to evidence of the crime.").

141. *Id.* at 140–41, 927 N.W.2d at 354–55.

142. State v. Henderson, 289 Neb. 271, 287, 854 N.W.2d 616, 631 (2014).

143. *Id.*

144. *Id.*

lice apprehended Henderson, they found a cell phone in his pocket.[145] Given these circumstances, police knew Henderson had the cell phone with him at the time of the shooting and that he had conspired with an accomplice to commit the crime.

These additional facts in *Henderson*—which may indicate a nexus between the cell phone and the crime—were not present in *Goynes*, making the inference that evidence of the crime would be located on Goynes's cell phone much weaker. In *Henderson*, police knew from witness statements that two individuals had shot at the victim.[146] Since it is highly unlikely two individuals coincidentally started firing shots at the same person at the same time, there is some indication that the individuals who fired the guns had planned the shooting *before* it happened. This makes it more likely that cell phone communication occurred between Henderson and the other suspect before, during, or after the shooting.[147]

Conversely, witnesses told police that Goynes was the only person who fired a gun at the victim on the day of the homicide.[148] Without further evidence, it is possible the other individuals in the vehicle with Goynes on the day of the shooting did not know what he intended to do when he exited the vehicle, and that they simply rode off with him afterward out of shock. In other words, there is no evidence Goynes conspired or communicated with these individuals before the incident about his plan to shoot the victim. Neither the witnesses nor the video surveillance provided any insight into who was driving the vehicle, meaning there is also no evidence that someone other than Goynes acted as an accomplice by driving away from the scene of a crime.

Further, since police found the cell phone on Henderson when he was apprehended briefly after the shooting and a short distance from the crime scene, it was reasonable to infer that communications with his alleged accomplice would be found on that cell phone.[149] On the other hand, police did not arrest Goynes until *five days* after the shooting.[150] Therefore, even if Goynes had a cell phone with him on the day of the shooting (which there was no evidence of when the court considered the motion to suppress), there is no evidence that the cell phone seized by police was the one Goynes had with him on the day of the incident. Given these facts, there was not probable cause to believe police would find evidence of the crime on Goynes's cell phone. At most, there was a slight possibility.

---

145. *Id.*
146. *Id.*
147. *Id.* at 288, 854 N.W.2d at 632 ("[I]t is reasonable to infer that the cell phone that was in his possession was used to communicate with others regarding the shootings before, during, or after they occurred.").
148. State v. Goynes, 303 Neb. 129, 132–34, 927 N.W.2d 346, 349–51 (2019).
149. *Henderson*, 289 Neb. at 287–88, 854 N.W.2d at 631–32.
150. *Goynes*, 303 Neb. at 131, 927 N.W.2d at 349.

These distinct factual differences between *Henderson* and *Goynes* emphasize that, without the officer's opinion that suspects use cell phones, the nexus between the cell phone and the crime in Goynes's case was virtually non-existent. The only other facts the court used to conclude there was a fair probability police would find evidence of the shooting on Goynes's cell phone were: (1) Goynes was a suspect; (2) Goynes possessed a cell phone five days after the incident; and (3) Goynes arrived at the scene of the crime with other individuals who did not participate in the commission of the crime.[151] As stated above, if this is all that is necessary to establish probable cause, then courts will be hard-pressed to find a situation where probable cause to search a suspect's cell phone does not exist. This effectively eradicates the probable cause requirement for cell phone search warrants.

Other courts across the country have recognized the danger of allowing an officer's general opinion that "suspects use cell phones" to support a finding of probable cause to search a cell phone. For example, the Supreme Court of Massachusetts held that an officer's opinion—that based on training and experience, evidence of a crime can often be found on a cell phone—was insufficient to establish probable cause, even when the defendant was a suspect in a multi-perpetrator crime and officers knew he owned a cell phone.[152] The court pointed to the fact that officers had "no information that the cellular telephone had been used to plan, commit, or cover up the crime, or that it contained any evidence of the crime."[153] The court reasoned that "it would be a rare case where probable cause to charge someone with a crime would not open the person's cellular telephone to seizure and subsequent search" if these facts alone were sufficient to establish probable cause —a result which is contrary to the significant privacy interests that individuals have in cell phones.[154]

151. *Id.* at 140–41, 927 N.W.2d at 355.

152. Commonwealth v. White, 59 N.E.3d 369, 376 (Mass. 2016) ("Here, prior to seizing the defendant's cellular telephone, police had received information that the robbery and homicide under investigation had been committed by several people, that the defendant likely was one of those people, and that he owned a cellular telephone. They also knew from experience that coventurers often use cellular telephones to communicate with each other, and that these devices may contain evidence of such communications. . . . This, without more, does not satisfy the nexus requirement.").

153. *Id.* at 371. The court concluded that, at most, police *suspected* the defendant had used his phone to plan or communicate about the crime and that was insufficient. *Id.* at 376. The court stated, "While probable cause may be based in part on police expertise . . . such considerations do 'not, alone, furnish the requisite nexus between the criminal activity and the places to be searched.'" *Id.* (citation omitted) (quoting Commonwealth v. Anthony, 883 N.E.2d 918, 928 (Mass. 2008)).

154. *Id.* at 377.

Other courts have also held that an officer's suspicions are not sufficient to establish probable cause to search a suspect's cell phone.[155] In these cases, as in *Goynes*, the only evidence officers used to establish probable cause was: (1) the defendant was a suspect in a multi-perpetrator crime; (2) the defendant had a cell phone on him when he was arrested; and (3) from officer training and experience, law enforcement had reason to believe evidence of the crime may be found on the suspect's phone.[156] Unlike these courts, however, the Nebraska Supreme Court held these facts created a sufficient nexus between the cell phone and the crime.[157] In doing so, the Nebraska Supreme Court authorized the type of "bare-boned affidavit" other courts have warned against.[158] Based on this precedent, whenever individuals are arrested as suspects in an alleged multi-perpetrator crime, police will have probable cause to search any cell phones in their possession at

155. *See, e.g.*, United States v. Tirado, No. 16-CR-168, 2018 U.S. Dist. LEXIS 65321, at *49–50 (E.D. Wis. Jan. 26, 2018) (holding that a warrant to search cell phones found on a suspect a week after a retail theft incident was not supported by probable cause). The court in this case stated:

> The affidavit establishes that photos from the surveillance video were used to identify Dumas. It also establishes that Dumas was arrested and that when he was arrested he was in possession of the two cell phones. But the bare-boned affidavit woefully fails to connect the two cell phones with the commission of the retail theft and disorderly conduct. Recall that Dumas was arrested one week after the theft. Nothing in the affidavit suggests that he was in possession of the cell phones during the commission of the retail theft and disorderly conduct, or that he used the cell phones during the commission of the offenses. There must be some nexus between the items to be searched and the commission of the crime. A mere boilerplate recitation about the use and features of cell phones is not enough. Otherwise being arrested for anything, including minor violations of the law, would always provide probable cause to search one's cell phone regardless of any connection between the violation arrested for and the cell phone. The law requires more.

Id.; *see also* Buckham v. State, 185 A.3d 1, 17–18 (Del. 2018) (footnotes omitted) ("Buckham is right that many of the allegations in the warrant application are too vague and too general to connect his cell phone to the shooting. Particularly unpersuasive was the statement that 'criminals often communicate through cellular phones' (who doesn't in this day and age?) . . . Nor do we see much significance in the statement that 'Buckham was making posts on social media about getting arrested' while he was at-large. By that time, an arrest warrant had been issued for him; the fact that Buckham may have been using his phone to talk about his impending arrest connects his phone to the arrest warrant, not the underlying crime. Even with the deference we owe to a magistrate's probable cause finding, these sorts of generalized suspicions do not provide a substantial basis to support a probable cause finding.").

156. *See Goynes*, 303 Neb. at 140–41, 927 N.W.2d at 355; *see also supra* notes 152 and 155 and accompanying text (discussing the cases where courts found these facts insufficient to create a nexus between the crime and the cell phone).

157. *Goynes*, 303 Neb. at 140–41, 927 N.W.2d at 355.

158. *See supra* note 155 and accompanying text.

the time of arrest, regardless of any connection between the commission of the crime and the cell phone.

2. *Substituting Particularity for General Searches of Cell Phones*

The court also erred in holding that the search warrant in *Goynes* was sufficiently particular. Even if the court believed there was probable cause to search Goynes's cell phone,[159] this limited probable cause did not justify the expansive scope of the warrant.[160] In finding the warrant in *Goynes* was sufficiently particular, the court attempted to distinguish the warrant language[161] from that in *Henderson*.[162] Specifically, the court relied on the fact that the *Henderson* warrant authorized a search of "any and all" information on the cell phone, while the warrant in *Goynes* "listed specific areas to be searched within the cell phone . . . along with a description of the information they held which would be relevant to the investigation."[163] Goynes contested this distinction, arguing the warrant in his case was comparable in scope to the one rejected by the court in *Henderson*.[164]

The warrant in *Goynes* was not sufficiently limited in scope because "the areas which the warrant permitted to be searched encompassed the entirety of the data contained within the cell phone."[165] Although the warrant did not explicitly state officers could search "any and all" data on the cell phone, which, again, is prohibited by *Henderson*,[166] the laundry list of places to be searched effectively authorized officers to search the entirety of the phone.[167] In fact, the warrant authorized the search of call logs, text messages, chat messages, emails, notes, calendar information, images, videos, audio, documents, internet browsing history, user dictionary information, cell tower connections, GPS data, and "installed applications and their corresponding data."[168] In this way, the court authorized officers to

159. *See supra* subsection III.A.1 (arguing there was no basis for the court to find the warrant was supported by probable cause).
160. *See supra* text accompanying notes 40 and 94.
161. *See supra* text accompanying note 110.
162. *See supra* text accompanying note 81.
163. State v. Goynes, 303 Neb. 129, 144, 927 N.W.2d 346, 357 (2019).
164. *Id.* at 143, 927 N.W.2d at 356 ("Goynes argues the scope of the search authorized in the warrant was too broad and was similar to warrants we determined did not meet the particularity requirement in *Henderson*.").
165. *Id.*
166. State v. Henderson, 289 Neb. 271, 290, 854 N.W.2d 616, 634 (2014).
167. *See supra* text accompanying note 110.
168. *Goynes*, 303 Neb. at 134–35, 927 N.W.2d at 351. Although the warrant affidavit stated that police would search installed application information that could provide insight into the suspect's "historical geographic location and demonstrate the user's association with investigated people, location, and events," the warrant itself did not limit which applications could be searched. *Id.* at 134–35, 142, 927

rely on a technicality—listing every part of the cell phone instead of stating "any and all data"—to skirt the important principles of particularity outlined in *Henderson*.[169] By authorizing a warrant that allowed police to search the entirety of Goynes's cell phone, the court created precedent that allows general searches of cell phones contrary to the Fourth Amendment.

In addition to the areas of the phone listed on the search warrant being exhaustive, there are clearly parts of the phone listed that could not reasonably contain any content related to the probable cause for searching the phone[170] (that Goynes was a suspect in a shooting and possibly planned the shooting with others).[171] Specifically, even if officers knew that "individuals who committed similar crimes commonly communicate, research, record, and perform other operations on their cell phones that would amount to evidence of the crime,"[172] this did not establish a reasonable probability that police could find evidence of the shooting on all of Goynes's applications[173] or in logs of his calls and messages from months or years in the past (which could include

N.W.2d at 351, 355–56. Even if it could be argued the warrant only authorized police to search applications that could track Goynes's geographic data or demonstrate his association with people, that would hardly limit the applications police could search. *See* Jennifer Valentino-DeVries, Natasha Singer, Michael H. Keller & Aaron Krolik, *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. TIMES (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html [https://perma.unl.edu/R4UZ-R378] ("More than 1,000 popular apps contain location-sharing code from such companies, according to 2018 data from MightySignal, a mobile analysis firm."). Additionally, any social or gaming application, such as Facebook, Snapchat, Words with Friends, Candy Crush, etc., could all arguably demonstrate a user's association with certain individuals. Overall, when this board language is taken into consideration with the other areas of the cell phone listed in the warrant, the installed application clause acts as a catchall, ensuring law enforcement can search every part of the phone.

169. *Henderson*, 289 Neb. at 288–89, 854 N.W.2d at 632–33 (holding "the privacy interests at stake in a search of a cell phone" are so important that unfettered searches of cell phone data exceed the permissible scope of a search allowed by the Fourth Amendment).

170. *Id.* at 289, 854 N.W.2d at 633 ("[A] warrant for the search of the contents of a cell phone must be sufficiently limited in scope to allow a search of only that content that is related to the probable cause that justifies the search.").

171. *Goynes*, 303 Neb. at 140–41, 927 N.W.2d at 355.

172. *Id.* at 141, 927 N.W.2d at 355.

173. *See In re* The Search of Premises Known as: A Nextel Cellular Tel. with Belonging to & Seized from, No. 14-MJ-8005-DJW, 2014 U.S. Dist. LEXIS 88215, at *41–42 (D. Kan. June 26, 2014) ("[P]robable cause to believe drug trafficking communication may be found in phone's the [sic] mail application will not support the search of the phone's Angry Birds application. The Fourth Amendment would not allow such a warrant and should therefore not permit a similarly overly broad warrant just because the information sought is in electronic form rather than at a residence.").

conversations with hundreds of different people).[174] Still, all of these areas of the cell phone were within the scope of the warrant.

Given the lack of evidence linking the cell phone to the commission of the crime, there was, at most, a possibility that evidence of the shooting existed in Goynes's call logs and messages between him and those in the sedan. A possibility, however, does not create probable cause.[175] Conversely, based on what police knew, there was *no* indication that evidence of the shooting could be found on Goynes's gaming or social media applications or in his audio recordings, photos, or videos.[176] Since the warrant did not limit the search to areas of the cell phone where officers had probable cause to believe evidence of the shooting could be found, it was facially overbroad and violated the Fourth Amendment's particularity requirement.[177]

B. Alternative Approach to Cell Phone Search Warrants

1. Probable Cause: Case-Specific Nexus Between Crime & Cell Phone

Instead of relying almost exclusively on the officer's opinion that evidence of the shooting could possibly be found on Goynes's cell phone,[178] the court should have looked to its precedent in *Sprunger* and *Prahin* and required a showing of particularized facts demonstrating a nexus between the shooting and the cell phone.[179] Applying this precedent, the *Goynes* court should have held there was no probable cause to support the warrant since there were no particularized facts linking the phone officers found on Goynes five days after the shooting to the shooting itself.[180]

174. *See supra* note 17 and accompanying text.

175. *See* Gershowitz, *supra* note 48, at 609–10 ("[I]t is possible that a person could hide a lawnmower in a bedroom. Yet, the ordinary search warrant for a lawnmower does not extend to bedrooms because while a 'lawnmower could be in the bedroom, [ ] there is no probable cause to believe that it is there.'" (alteration in original) (footnotes omitted) (quoting Long v. State, 132 S.W.3d 443, 453 (Tex. Crim. App. 2004))).

176. *See supra* note 168 and accompanying text.

177. *See* Clark, *supra* note 4, at 2008–10; *see also* Gershowitz, *supra* note 48, at 611–12 (arguing that if police only have probable cause to believe there would be communications between the suspects on the phone, issuing a warrant for other areas of the phone such as photos or videos goes against the particularity requirement).

178. State v. Goynes, 303 Neb. 129, 139–41, 927 N.W.2d 346, 354–55 (2019); *see also* subsection III.A.1 (outlining the lack of case-specific evidence in *Goynes* to establish probable cause and the court's reliance on officers' opinions).

179. *See supra* note 32 and accompanying text (outlining the legal requirement that there be a nexus between the crime and the item to be searched to establish probable cause).

180. *See supra* note 140 and accompanying text.

Moving forward, to uphold the sanctity of privacy and the protections provided by the Fourth Amendment, the Nebraska Supreme Court should only uphold warrants where this nexus exists. For example, in Goynes's case, there could have arguably been a nexus between his cell phone and the shooting if witnesses saw other individuals in the sedan firing at the victim; if a witness saw Goynes talking or texting on his cell phone shortly before or after the shooting; if Goynes made social media posts about committing the shooting; if a witness received a picture from Goynes where he was brandishing a gun matching the description of the one used in the shooting; or if Goynes's alleged co-conspirators told police that they planned or discussed the shooting over calls or texts.[181] These types of particularized facts would likely be sufficient to create a nexus between the phone and the crime being investigated.

Requiring this type of case-specific nexus between the crime and the cell phone is an approach already supported by some judges, including United States Magistrate Judge David Waxse.[182] In fact, some courts have specifically discussed what the nexus between the crime and the cell phone should look like, and the Nebraska Supreme Court could look to these opinions for guidance. The Massachusetts Supreme Court, for example, has a bright-line rule that opinions of officers alone, without knowledge of "particularized evidence" related to the crime, are insufficient to establish probable cause to search a suspect's cell phone.[183] Other courts have followed similar reasoning when holding that a defendant's status as a suspect and the officers'

181. In some cases, there may also be probable cause to search a cell phone for GPS location data. However, in *Goynes*, there were no alleged facts that established a *fair probability* that GPS evidence on Goynes's phone could place him at the location of the shooting. This is because there was no evidence that Goynes had the phone with him at the time of the shooting. *See, e.g.*, United States v. Tirado, No. 16-CR-168, 2018 U.S. Dist. LEXIS 65321, at *50–51 (E.D. Wis. Jan. 26, 2018) (holding there was not probable cause to search the suspect's cell phone for GPS location data where there was no particularized evidence that (1) the defendant had a cell phone on him at the time the robbery occurred, or (2) if he had a cell phone during the robbery, it was the one he had on him when he was arrested weeks later). "[A]lthough the probable cause bar is not high, it is more than an open-ended possibility that a search will yield evidence of the crime under investigation." *Id.*

182. David J. Waxse, *Search Warrants for Cell Phones and Other Locations Where Electronically Stored Information Exists: The Requirements for Warrants Under the Fourth Amendment*, 9 FED. CTS. L. REV. 1, 9 (2016).

183. Commonwealth v. White, 59 N.E.3d 369, 375 (Mass. 2016) ("[P]olice must first obtain information that establishes the existence of some 'particularized evidence' related to the crime. Only then, if police believe, based on training or experience, that this 'particularized evidence' is likely to be found on the device in question, do they have probable cause to seize or search the device in pursuit of that evidence."). The court contrasted this case with, *Commonwealth v. Dorelas*, 43 N.E.3d 306 (Mass. 2016), in which it held there were particularized facts sufficient to create a nexus between the cell phone and the crime.

belief that the suspect's cell phone contains evidence are insufficient to establish a nexus.[184] Although enforcing a particularized nexus standard may require police to gather more information before they can establish probable cause to search a cell phone, this is the type of sacrifice the Fourth Amendment requires.[185]

2. Particularity: Specifying the "Apps" to Be Searched and Content to Be Seized

Even when there is a nexus between the cell phone and the crime sufficient to establish probable cause, the particularity requirement must be strictly applied to ensure searches are limited to areas of the cell phone where evidence related to the crime could actually be located.[186] A warrant like that in *Goynes*, which effectively authorizes police to search every part of a cell phone, does not sufficiently limit the scope of the search to prevent over-searching and over-seizing.[187] The method proposed to resolve overbreadth issues is relatively simple: Courts should only authorize police to search applications in which the particularized evidence articulated in the affidavit could reasonably be located. Further, courts must limit searches of calls logs and messages to an appropriate time frame based on the crime committed and only include communications between the suspect and people who have been specifically connected to the underlying investigation.[188]

For example, if a witness saw Goynes communicating on his cell phone shortly before, during, or after the shooting (which could possibly create probable cause to search his call and message logs), simply listing all call logs and text messages as the places to be searched would not be sufficiently particular. This could include thousands of

184. *See, e.g.*, United States v. Oglesby, No. 4:18- CR-0626, 2019 U.S. Dist. LEXIS 71238, at *12–20 (S.D. Tex. Apr. 26, 2019); United States v. Ramirez, 180 F. Supp. 3d 491, 494–96 (W.D. Ky. 2016).

185. *See, e.g.*, Riley v. California, 573 U.S. 373, 401 (2014) (providing that constitutional requirements must be upheld even if it makes the work of law enforcement more burdensome because "[p]rivacy comes at a cost"); Waxse, *supra* note 182, at 11 ("This might entail more complicated affidavits and more research performed by law enforcement agencies, but the privacy interests and vast amount of information available on these digital devices requires it. The privacy interest in cell phone data is critical.").

186. *See supra* text accompanying note 94.

187. *See supra* subsection III.A.2.

188. *See, e.g.*, Waxse, *supra* note 182, at 10 ("If officers, for example, want to search an individual's cell phone, they should cite the specific phone, specifically his text messages, specifically between himself and a known possible co-conspirator, because they had an independent suspicion about a connection to that other conspirator. Specifying this level of detail prevents law enforcement from seeing the individual's mother's health problems, his marriage issues, his children's problems in school, or his emails back and forth with his attorney.").

calls and text messages dating back years before the shooting, and these communications could be with individuals completely unrelated to the shooting such as Goynes's grandparents, boss, or pastor.[189] Instead, the scope of such a search should be limited to calls and messages exchanged between Goynes and other alleged co-conspirators during a reasonable time period before and after the shooting.

Although some scholars believe it is impossible for police to identify the parts of a cell phone that will contain relevant evidence in advance of the search,[190] cell phones are not like computers, which allow suspects to easily hide evidence anywhere amongst files and folders.[191] Instead, cell phones contain applications that hold specific types of data, and police should be able to identify, based on the particularized evidence sought, where in the phone such evidence could reasonably be located.[192] If this does not uncover the evidence, but instead, reveals other places the data may be, nothing prohibits police from securing a second warrant.[193] Providing a clear answer to *where* in the phone police can search would be a major step forward in preventing overly broad searches while allowing law enforcement to access relevant evidence.[194]

---

189. *See supra* note 17 and accompanying text.

190. *See* Clark, *supra* note 4, at 2011 ("[I]t is impossible at a search's outset to identify the exact part of a cell phone's internal storage containing relevant data . . . .").

191. *See* Andrew D. Huynh, Note, *What Comes After "Get a Warrant": Balancing Particularity and Practicality in Mobile Device Search Warrants Post-*Riley, 101 CORNELL L. REV. 187, 207 (2015) ("[O]ne of the biggest concerns in a traditional computer search is that potentially incriminating evidence may be masked by an innocuous file name or by modifying the file extension. But file names and extensions are not so easily modified on a mobile device, because mobile operating systems are designed for ease of use and do not emphasize user-directed file organization." (footnotes omitted)).

192. *See* Gershowitz, *supra* note 48, at 632–33 (arguing that in cases where probable cause "is limited to certain applications" judges should simply restrict searches to certain applications).

193. *See id.* at 636 ("There is nothing revolutionary about suggesting that officers return to the magistrate to request a broader search warrant. . . . Subsequent warrants are already used with some frequency in traditional computer searches.").

194. The top priority is for the court to adopt these minimal particularity requirements to protect citizens' private data from generalized searches. Once the court departs from the precedent established in *Goynes* and returns to strict enforcement of the probable cause and particularity requirements for cell phone warrants, it may be necessary to evolve these requirements further. This could include permitting courts to provide police officers with search protocols "specifying how the search of digital data should be conducted," as alluded to in *Henderson*. State v. Henderson, 289 Neb. 271, 290, 854 N.W.2d 616, 633 (2014). Search protocols sometimes require law enforcement to provide a detailed methodology to the judge about their data extraction process to ensure police only search evidence related to the crime. For in-depth discussions on the benefits of search protocols, see Clark, *supra* note 4; Gershowitz, *supra* note 48, at 614–29; Huynh, *supra* note 191. Since the constitutionality of such protocols is still widely debated, however, it is critical that the court focus on adopting the protections sug-

IV. CONCLUSION

The Founding Fathers drafted the Fourth Amendment to ensure citizens would be protected from general searches.[195] Although they had invasions of physical property in mind, the Supreme Court has declared, on numerous occasions, that the Fourth Amendment must evolve to protect against unreasonable electronic invasions.[196] With the rapid advancement of cell phone technology and society's ever-increasing reliance on these devices,[197] the Court in *Riley* correctly provided such protection by requiring law enforcement to secure a warrant to search an arrestee's cell phone.[198]

However, the Court's monumental decision in *Riley* can only protect citizens from unreasonable cell phone searches if state courts strictly adhere to Fourth Amendment principles when issuing and upholding warrants.[199] Unfortunately, in *Goynes*, the Nebraska Supreme Court departed from these requirements when it upheld a boilerplate warrant that was deficient of probable cause[200] and insufficiently particular.[201]

This decision does not comply with the Fourth Amendment. Probable cause requires courts to find some nexus between the crime and the cell phone beyond the simple fact that a suspect owns and uses a cell phone.[202] Further, the particularity requirement obligates courts to sufficiently limit a search to areas of the cell phone where evidence of the crime could reasonably be located.[203] Failing to apply these standards to cell phone search warrants renders the Supreme Court's ruling in *Riley* meaningless and leaves the privacy of Nebraska citizens utterly unprotected.

---

gested in this Note that are not only clearly constitutional, but, in fact, necessary for the court to preserve Nebraskans' constitutional protections. For an introduction to the constitutionality debate surrounding search protocols, see Clark, *supra* note 4, at 1992; Gershowitz, *supra* note 48, at 621–23.

195. *See supra* note 28 and accompanying text.
196. *See supra* section II.B.
197. *See supra* section II.A.
198. *See supra* text accompanying note 50.
199. *See supra* section II.B.
200. *See supra* subsection III.A.1.
201. *See supra* subsection III.A.2.
202. *See supra* subsection III.B.1.
203. *See supra* subsection III.B.2.