NOTES

UNITED STATES v. MORTON: "CATEGORIES OF CONTENT" AND PRESERVING THE PARTICULARITY REQUIREMENT IN SEARCH WARRANTS FOR CELL PHONES*

I. INTRODUCTION

Cell phones are an integral part of many peoples' daily lives.[1] They allow for constant communication, information, and entertainment access. In creating this convenience, they also store incredible records of each individual's interactions, thoughts, and whereabouts.[2] For law enforcement, access to a suspect's cell phone can offer a treasure trove of evidence and investigative leads.[3] The ability to access so much information in a singular device has created tension between individual citizens' privacy interests and law enforcement interests in investigating crimes. Recognizing the tension this technological advancement placed on established Fourth Amendment doctrine relating to police searches, the United States Supreme Court sought to restore balance in *Riley v. California*[4] by requiring law enforcement to obtain a warrant before searching a cell phone seized incident to an arrest.[5]

Though simple in theory, the application of the search warrant requirement to cell phones has proved challenging in practice.[6] The breadth of information potentially available within a cell phone has conveniently allowed courts to assume some evidence will be found on the phone.[7] Thus, courts have issued broad warrants for cell phone searches even following arrests for minor offenses.[8] Furthermore, unclear requirements

---

* Amanda Wagner, J.D. Candidate, Temple University Beasley School of Law, 2023. Thank you to Professor James Shellenberger for his time and thoughtful guidance throughout the writing process, and to the Temple Law Review editorial board and staff for all of their hard work and attention to detail in editing this Note. Greatest thanks to my family and friends, and especially Matt, for their unwavering support and encouragement.

1. *See Mobile Fact Sheet*, PEW RSCH. CTR. (Apr. 7, 2021), https://www.pewresearch.org/internet/fact-sheet/mobile/ [https://perma.cc/QL5B-2KVX].

2. *See* Riley v. California, 573 U.S. 373, 395–96 (2014).

3. *See id.*

4. 573 U.S. 373 (2014).

5. *See id.* at 389–90.

6. *See infra* Part III.E.

7. *See* LOGAN KOEPKE, EMMA WEIL, URMILA JANARDAN, TINUOLA DADA & HARLAN YU, UPTURN, MASS EXTRACTION: THE WIDESPREAD POWER OF LAW ENFORCEMENT TO SEARCH MOBILE PHONES 42 (2020), https://www.upturn.org/static/reports/2020/mass-extraction/files/Upturn%20-%20Mass%20Extraction.pdf [https://perma.cc/KT5Z-D792] (detailing the broad uses of cell phone search tools by law enforcement).

8. *Id.*

relating to specificity and particularity in warrants issued for cell phones have called into question the admissibility of subsequently uncovered evidence.[9]

For Brian Morton, an arrest for simple drug possession led to the issuance of two warrants to search his cell phones, ultimately uncovering child pornography.[10] On appeal, the Fifth Circuit vacated and reversed his conviction, holding that the warrants for the cell phones were fatally broad and unsupported by the facts of his arrest.[11] In suppressing the explicit sexual material discovered pursuant to the flawed warrants, the Fifth Circuit announced a new rule requiring search warrants to specifically apply to particular categories of information within a phone.[12] Despite the important step this ruling took in upholding the spirit of Fourth Amendment protections in the digital age, the Fifth Circuit swiftly vacated and reheard the case.[13] After nearly a year, the Fifth Circuit issued a new holding that sidestepped the complex questions raised in the initial appellate decision; instead, the court affirmed the district court's determination that the officers' reliance on warrants was sufficient to avoid suppression under the good-faith exception to the Fourth Amendment exclusionary rule.[14]

This Note begins with the factual background of the *Morton* case before moving to a discussion of relevant Fourth Amendment doctrine and an analysis of the Fifth Circuit's holdings in *United States v. Morton* (*Morton I*)[15] and *United States v. Morton* (*Morton II*).[16] This Note argues that the new rule presented by the Fifth Circuit in *Morton I*, its 2021 vacated opinion, was a moderate and necessary attempt to reconcile Fourth Amendment protections with law enforcement objectives.

II. FACTS AND PROCEDURAL HISTORY

On September 1, 2018, Brian Morton was stopped for speeding by the Texas Department of Public Safety (DPS) in Palo Pinto County, Texas.[17] During the stop, the officers smelled marijuana, then received consent to search Morton's van.[18] A search of Morton's person uncovered an Advil bottle in his pocket containing sixteen ecstasy pills,[19] and the search of the van uncovered "one small bag of marijuana, and a glass pipe," in addition to "children's school supplies, a lollipop, [fourteen] sex toys, [one

9. *See, e.g.*, United States v. Morton (*Morton I*), 984 F.3d 421 (5th Cir. 2021), *rev'd en banc*, 46 F.4th 331 (5th Cir. 2022); Commonwealth v. Snow, 160 N.E.3d 277 (Mass. 2021); Taylor v. State, 260 A.3d 602 (Del. 2021).

10. *Morton I*, 984 F.3d at 424.

11. *Id.* at 423.

12. *Id.* at 426–27. At the outset, it should be noted that the court does little to clarify precisely what is meant by "categories of information"—also discussed as "categor[ies] of content" or "cell phone features"—and how this new requirement should be implemented in practice. *Id.* For the purposes of this Note, this author will use the phrase "categories of information" in an attempt to accurately reflect the holding of *Morton I*. For additional discussion of the potential ramifications of the vagueness of this language, see *infra* Section V.

13. *See* United States v. Morton (*Morton II*), 46 F.4th 331 (5th Cir. 2022) (en banc).

14. *Id.* at 339–40.

15. 984 F.3d 421 (5th Cir. 2021), *rev'd en banc*, 46 F.4th 331 (5th Cir. 2022).

16. 46 F.4th 331 (5th Cir. 2022) (en banc).

17. Factual Resume at 3, United States v. Morton, No. 4:19-CR-017-O (N.D. Tex. Mar. 14, 2019).

18. *Morton I*, 984 F.3d 421, 424 (5th Cir. 2021), *rev'd en banc*, 46 F.4th 331 (5th Cir. 2022).

19. Appellant's Initial Brief at 2, *Morton I*, 984 F.3d 421 (5th Cir. 2021) (No. 19-10842).

hundred] pairs of women's underwear," and three cell phones.[20] The officers became concerned that Morton might be a pedophile[21] and arrested him for drug possession.[22] On more than one occasion, the officers inquired as to whether Morton had child pornography on his cell phones, and Morton denied consent to search the phones.[23] Several days later, the officers applied for warrants to search each of the three cell phones discovered during the search of Morton and his van.[24] However, the affidavits provided in support of the search warrants did not communicate the concerns regarding child sexual exploitation and, instead, only explicitly sought additional evidence relating to Morton's drug activity.[25] Specifically, the affidavit sought contact information, communications, photographs, digital images, and multimedia files contained in the cell phones, which might have helped to identify others involved in the illicit drug trade and any profits derived from the sale of illicit drugs.[26]

A judge issued the search warrants for the cell phones without any limitations regarding the scope of the authorized search.[27] An initial search revealed sexually explicit images of children, and law enforcement obtained additional search warrants issued specifically to search the phones for child pornography.[28] The subsequent searches uncovered 19,270 sexually explicit images of minors.[29] Having been released from state custody while his charges were pending, Morton was arrested on federal charges in violation of 18 U.S.C. §§ 2252(a)(2) and (b)(1)—receipt of a visual depiction of a minor engaged in sexually explicit conduct—and was subsequently indicted by a federal grand jury.[30] The Government pursued the federal child pornography charges only, having dropped the state charges relating to Morton's drug possession, and Morton moved to suppress the pornographic evidence.[31]

In Morton's motion to suppress, he argued two points: "(1) the good-faith exception [to the exclusionary rule] did not apply because the search warrant affidavits for the initial cell phone searches were pretextual in nature; and (2) the officers lacked probable

20. *Morton I*, 984 F.3d at 424.

21. Appellant's Initial Brief, *supra* note 19, at 2 (stating that Corporal Blue asked Mr. Morton whether he was a crossdresser or pedophile, to which Mr. Morton replied that the sex toys and underwear belonged to him and his wife).

22. *Morton I*, 984 F.3d at 424.

23. *See* Appellant's Initial Brief, *supra* note 19, at 3.

24. *Id.* at 3–4 (following consultation with a DPS Criminal Investigations Division Special Agent with extensive training and experience in conducting child pornography and human trafficking investigations).

25. *Morton I*, 984 F.3d at 423–24 (relying on Morton's possession and admissions regarding the drugs and the officer's "generalized allegations about the behavior of drug traffickers" based on their training and experience as a drug recognition expert); *see also* Appellant's Initial Brief, *supra* note 19, at 3–4 (noting there was no mention of child sexual exploitation in the affidavits for the warrants despite the assistance of a Criminal Investigations Division special agent with extensive training and experience in conducting child pornography and human trafficking cases).

26. Appellant's Initial Brief, *supra* note 19, at 3–4.

27. *Morton I*, 984 F.3d at 424.

28. *Id.*

29. *Id.*

30. Appellee's Brief at 5, *Morton I*, 984 F.3d 421 (No. 19-10842).

31. *Morton I*, 984 F.3d at 424.

cause to search the cell phones for any purpose."[32] In particular, Morton argued that the officers failed to establish probable cause relating to Morton's alleged drug activities to support the initial search of the cell phones.[33] The Government disputed this analysis and argued that there was sufficient probable cause for the search and that, in the absence of probable cause, the good-faith exception to the exclusionary rule should apply.[34] The district court ruled in favor of the Government at the motion to suppress hearing, determining the good-faith exception allowed for the admission of the evidence.[35]

On March 7, 2019, Morton entered a guilty plea for count one of the indictment, Receipt of a Visual Depiction of a Minor Engaged in Sexually Explicit Conduct under 18 U.S.C. § 2252(a)(2), pursuant to a conditional plea agreement.[36] At this time, he stipulated to the knowing receipt of a visual depiction of a minor engaged in sexually explicit conduct by use of the internet and a cellular phone[37] and was eventually sentenced to nine years in prison.[38] As part of the conditional plea agreement, Morton reserved the right to appeal the district court's suppression decision and subsequently filed an appeal in the Fifth Circuit challenging the admission of the evidence found on his cell phones.[39]

On January 5, 2021, the Fifth Circuit Court of Appeals reversed the district court's denial of Morton's motion to suppress, vacated Morton's conviction and sentence, and remanded the case to the district court.[40] The court held that (1) the good-faith exception could not salvage the warrants because the officers' reliance on the defective warrants in authorizing a search of Morton's photographs was objectively unreasonable, and (2) the officers' affidavits did not provide the magistrate with a substantial basis for determining that probable cause existed for the photographs on Morton's cell phones and, therefore, the search constituted a violation of his Fourth Amendment rights.[41] Because the second set of warrants relied on the information obtained in the first set of unconstitutional searches, the evidence found during the subsequent searches was tainted as "fruit of the poisonous tree" and inadmissible.[42]

The United States Attorney's Office for the Northern District of Texas responded with a petition for a rehearing en banc.[43] The petition alleged that the Fifth Circuit sidestepped the central issue of the appeal—whether the officers' pretextual affidavits to search Morton's cell phone precluded the application of the good-faith exception to avoid the suppression of evidence.[44] The Government claimed the court instead created a new

32. Appellant's Initial Brief, *supra* note 19, at 5.

33. *Morton I*, 984 F.3d at 424.

34. *Id.*

35. *Id.*

36. Plea Agreement at 1, United States v. Morton, No. 4:19-CR-017-O (N.D. Tex. Mar. 14, 2019).

37. Factual Resume, *supra* note 17, at 2.

38. *Morton I*, 984 F.3d at 424.

39. *Id.*

40. *Id.* at 431.

41. *Id.* at 423, 431.

42. *Id.* at 431 (citing United States v. Martinez, 486 F.3d 855, 864 (5th Cir. 2007)).

43. Petition of the United States for Rehearing En Banc, *Morton II*, 46 F.4th 331 (5th Cir. 2022) (No. 19-10842).

44. *Id.* at 6.

rule for cell phone searches, requiring a distinct probable cause determination for each discrete location on a cell phone, which ignored established precedent regarding the good-faith exception.[45] A court order granting the petition for rehearing en banc was issued on May 18, 2021.[46] More than a year later, a new decision was issued affirming the district court's suppression determination that the evidence uncovered pursuant to the cell phone searches was admissible due to the officers' good-faith reliance on search warrants.[47] Unfortunately, the new decision did not address the constitutionality of the scope of the searches authorized by the warrants.[48]

III. PRIOR LAW

The Fourth Amendment generally protects individuals from unreasonable searches and seizures.[49] It contains two clauses: the Reasonableness Clause and the Warrant Clause.[50] While the Reasonableness Clause simply requires government searches and seizures to be reasonable, the Warrant Clause incorporates two additional provisions: any warrant issued must (1) be supported by probable cause and (2) particularly describe the places to be searched or the persons or things to be seized.[51]

Traditionally, the Fourth Amendment protected individuals only from conventional understandings of trespass by the government.[52] However, in *Katz v. United States*,[53] the Court clarified that the Fourth Amendment "protects people, not places,"[54] and, more specifically, provides protections against government intrusions into an individual's reasonable expectation of privacy.[55] The rapid proliferation of new technologies has further complicated traditional notions regarding Fourth Amendment protections.[56] For example, in *Kyllo v. United States*,[57] the Court recognized that the use of surveillance equipment to gather information that previously required a physical intrusion may

45. *Id.* at 7.

46. On Petition for Rehearing En Banc, *Morton II*, 46 F.4th 331 (No. 19-10842).

47. *Morton II*, 46 F.4th at 339–40.

48. *Id.* at 335.

49. U.S. CONST. amend. IV.

50. *Id.*; 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, 1986 (2015).

51. U.S. CONST. amend. IV; Clark, *supra* note 50, at 1986.

52. CLARE GARVIE, ALVARO M. BEDOYA & JONATHAN FRANKLE, GEO. L. CTR. ON PRIV. & TECH., THE PERPETUAL LINE-UP: UNREGULATED POLICE FACE RECOGNITION IN AMERICA 33 (2016), https://www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%20121616.pdf [https://perma.cc/DL53-FSXG].

53. 389 U.S. 347 (1967).

54. *Id.* at 351.

55. *See id.* at 361 (Harlan, J., concurring).

56. *See* Eric Engle, *Digest Comment - New Technologies and the Fourth Amendment*, HARV. J. L & TECH DIGEST (Dec. 29, 2009), https://jolt.law.harvard.edu/digest/digest-comment-new-technologies-and-the-fourth-amendment [https://perma.cc/29CF-THF4].

57. 533 U.S. 27 (2001).

constitute an unreasonable search.[58] Similarly, in *Carpenter v. United States*,[59] the Court found that individuals may retain a reasonable expectation of privacy in the record of their physical movements as preserved in cell-site location records, despite the fact that such records are held by a third party.[60] These technological advancements have spurred calls for a reevaluation of the scope of Fourth Amendment protections as they relate to digital spaces.[61]

This Section details the current law as it relates to warrant requirements, the plain view doctrine, and the search incident to arrest exception. It discusses the remedy for Fourth Amendment violations and the application of the good-faith exception to exclusion when certain constitutional violations are found. Looking specifically at the application of these protections to digital spaces, this Section will conclude with an examination of recent cases that have raised questions regarding the effectiveness of these protections for new technologies, mainly cell phones, under existing jurisprudence.

A. The Warrant Requirement

Pursuant to the Fourth Amendment, "[w]here a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing . . . reasonableness generally requires the obtaining of a judicial warrant."[62] A search warrant must be issued based on affidavits stating probable cause to search, meaning a "fair probability" that criminal evidence will be found in the place to be searched at the time of the search.[63] Unless the circumstances are subject to an exception to the warrant requirement, such a warrant must be supported by an oath or affirmation.[64] In providing affidavits sufficient to support a finding of probable cause, reliance may not be placed on wholly conclusory statements that are, thus, "bare bones."[65] This is because such a bare-boned affidavit lacks the facts and circumstances necessary for the magistrate to independently determine whether probable cause exists.[66]

---

58. *Id.* at 40 ("Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant.").

59. 138 S. Ct. 2206 (2018).

60. *Id.* at 2217, 2223 ("In light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection.").

61. *See* LAURA HECHT-FELELLA, BRENNAN CTR. FOR JUST, THE FOURTH AMENDMENT IN THE DIGITAL AGE: HOW CARPENTER CAN SHAPE PRIVACY PROTECTIONS FOR NEW TECHNOLOGIES 30 (March 18, 2021), https://www.brennancenter.org/our-work/policy-solutions/fourth-amendment-digital-age [https://perma.cc/TWE9-JU5U].

62. Riley v. California, 573 U.S. 373, 382 (2014) (alteration and omission in original) (quoting Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 653 (1995)) (noting that the label "exception" is misleading, as warrantless searches incident to arrest occur more frequently than searches conducted pursuant to a search warrant).

63. Illinois v. Gates, 462 U.S. 213, 238 (1983).

64. U.S. CONST. amend. IV.

65. United States v. Restrepo, 994 F.2d 173, 188 (5th Cir. 1993) (quoting United States v. Pigrum, 922 F.2d 249, 252 (5th Cir. 1991)).

66. *Id.* at 188.

Warrants must also be sufficiently particularized.[67] The requirement that warrants "*particularly describ[e]* the place to be searched, and the persons or things to be seized" is intended to prevent the issuance of general warrants.[68] The Fifth Circuit has explained that "in order for a warrant to meet the particularity requirement of the Fourth Amendment, the warrant itself must, *at a minimum*, contain something more than [an] absolute generality."[69] Therefore, the language contained in the warrant should articulate precise locations and targets so that the "executing officer is left with no discretion to decide what may be seized."[70]

The justification for the particularity requirement, the Court explained in *Maryland v. Garrison*,[71] is to "ensure[] that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit."[72] This objective is accomplished by limiting law enforcement officer discretion through documented restrictions on the search's location and the types of evidence that may be searched for and seized.[73] Such restrictions ensure that the activities conducted pursuant to the warrant are supported by the magistrate's probable cause determination.[74] In searches of digital spaces, this may include detailed parameters for items that may be searched for and seized, including specific time and date limitations, persons involved, or types of content (i.e., text messages, call logs, and photographs).[75]

If particularized details regarding the objects to be searched for and seized are impossible given the circumstances, some ambiguity may be tolerated by courts.[76] However, to determine if the generic language is sufficient, courts will seek to determine whether, in context, the warrant was adequately particularized to the items within the scope of the seizure.[77] This may include consideration of the descriptiveness and

67. U.S. CONST. amend. IV.

68. U.S. CONST. amend. IV (emphasis added); *see also* Stanford v. Texas, 379 U.S. 476, 481 (1965) (noting the widespread opposition to writs of assistance and the intent of the Fourth Amendment to prohibit "intrusion and seizure by officers acting under the unbridled authority of a general warrant").

69. United States v. Beaumont, 972 F.2d 553, 560–61 (5th Cir. 1992) (emphasis in original) (also noting that "[g]eneral warrants have long been abhorred in the jurisprudence of both England and the United States").

70. Williams v. Kunze, 806 F.2d 594, 598 (5th Cir. 1986).

71. 480 U.S. 79 (1987).

72. *Id.* at 84.

73. Martha Applebaum, *"Wrong but Reasonable": The Fourth Amendment Particularity Requirement After* United States v. Leon, 16 FORDHAM URB. L.J. 577, 580, 582 (1987); *see also Stanford*, 379 U.S. at 486 (finding the breadth of a warrant covering all types of literary material—"books, records, pamphlets, cards, receipts, lists, memoranda, pictures, recordings and other written instruments"—to be "constitutionally intolerable," particularly because such things to be seized did not inherently involve any type of contraband).

74. Applebaum, *supra* note 73; *see also Stanford*, 379 U.S. at 486.

75. *See, e.g.*, *Morton I*, 984 F.3d 421, 425 (5th Cir. 2021), *rev'd en banc*, 46 F.4th 331 (5th Cir. 2022); Commonwealth v. Snow, 160 N.E.3d 277, 287–88 (Mass. 2021); Taylor v. State, 260 A.3d 602, 609 (Del. 2021).

76. Applebaum, *supra* note 74, at 580–82; Steele v. United States, 267 U.S. 498, 503 (1925) ("It is enough if the description is such that the officer with a search warrant can with reasonable effort ascertain and identify the place intended.").

77. Williams v. Kunze, 806 F.2d 594, 598 (5th Cir. 1986) (citing United States v. Webster, 734 F.2d 1048, 1055 (5th Cir.1984)).

inclusion of facts by law enforcement that a reasonable investigation is expected to uncover under the circumstances.[78]

B. Plain View Doctrine

Under the plain view doctrine, law enforcement agents executing a lawful search are not required to ignore incriminating evidence that becomes visible during the search but was not the intended object of the search.[79] Provided that the law enforcement officers are legally present, it is immediately apparent that they have incriminating evidence before them, and they have a lawful right of access to the object itself without a further intrusion on the protected interests of the person, such evidence may be seized in the absence of a warrant.[80] This concept becomes more contentious in digital search cases due to the, often automated, seizure of nonresponsive data contained within digital devices.[81]

C. Search Incident to Arrest Exception to the Warrant Requirement

Under common law, officers are permitted to conduct a search of the arrestee's person incident to their lawful arrest without obtaining a search warrant.[82] This common-law exception to the warrant requirement has traditionally been viewed as a mechanism to protect the safety of the arresting officers by removing any weapons that may be used to resist arrest or facilitate an escape, as well as to prevent evidence destruction.[83] Importantly, the Court in *Weeks v. United States*[84] did not address any search of the place in which the person was arrested, instead only speaking to the arrestee's "person."[85] Soon after, however, the scope of the permissible search incident to arrest began to expand.[86] In *Carroll v. United States*,[87] the Court expanded the scope of a search incident to an arrest to allow "whatever is found upon his person or in his control which it is unlawful for him to have and which may be used to prove the offense may be seized and held as evidence in the prosecution."[88] A few months later, the Court in *Agnello v. United States*[89] again expanded the permissible scope of such warrantless searches and seizures incident to an arrest, stating the right to search both the person and "the place where the arrest is made . . . is not to be doubted."[90]

---

78. Applebaum, *supra* note 74, at 580–82.

79. Horton v. California, 496 U.S. 128, 135 (1990).

80. *Id.* at 135–37.

81. *See infra* Part III.E (discussing methods of data extraction from cell phones).

82. Weeks v. United States, 232 U.S. 383, 392 (1914) (discussing "the right on the part of the Government, always recognized under English and American law, to search the person of the accused when legally arrested to discover and seize the fruits or evidences of crime").

83. *See* Chimel v. California, 395 U.S. 752, 763 (1969).

84. 232 U.S. 383 (1914).

85. *Chimel*, 395 U.S. at 755.

86. *Id.* at 755–58.

87. 267 U.S. 132 (1925).

88. *Id.* at 158.

89. 269 U.S. 20 (1925).

90. *Id.* at 30. *Compare* Marron v. United States, 275 U.S. 192, 198–99 (1927) (holding that officers "had a right without a warrant contemporaneously to search the place in order to find and seize the things used to

The Court subsequently narrowed the scope of these allowable searches in *Chimel v. California*.[91] In *Chimel*, while conducting a lawful arrest at the defendant's home, the police searched the entire three-bedroom house, including the attic, the garage, and a small workshop, without a search warrant.[92] In considering whether the warrantless search of the defendant's home was constitutionally justified as incident to the arrest, the Court noted that there were no comparable justifications (i.e., safety and preventing evidence destruction) to support such broad warrantless searches.[93] To ensure the justifications for the search were sufficiently correlated to the scope of the permissible searches incident to arrest, the Court limited such searches to the arrestee's person and the area "within his immediate control."[94]

Regardless of the specific facts of the particular case, the Court clarified in *United States v. Robinson*[95] that, in the case of any lawful custodial arrest, "a full search of the person is not only an exception to the warrant requirement of the Fourth Amendment but is also a 'reasonable' search under that Amendment."[96] However, this 1973 decision could not account for the advent and proliferation of smartphones which most people carry in their pockets and are, therefore, likely present and accessible to law enforcement during a search incident to an arrest. This change in how and where information is stored has dramatically changed the amount of personal information potentially available to law enforcement under this exception to the warrant requirement.[97] In 2015, this issue was addressed, in large part, in *Riley v. California*.[98] In *Riley*, the petitioner was stopped pursuant to a traffic violation, which subsequently resulted in an arrest on weapons charges for handguns discovered under the car's hood.[99] In searching the petitioner incident to the arrest, the officer seized a cell phone from his pocket.[100] Proceeding to access information within the phone, the officer discovered repeated usage of a term associated with a street gang and delivered the phone to a detective specializing in gang

carry on the criminal enterprise," mainly a ledger located in a closet relating to illicit business activities because it was under the arrestee's "immediate possession and control" at the time of his arrest), *with* Go-Bart Importing Co. v. United States, 282 U.S. 344, 358 (1931) (distinguishing the unreasonable search of arrestee's desk, filing cabinets, and safe from the search incident to arrest in *Marron*, at which time the arrestee was discovered actually engaged in pursuance of a conspiracy).

91. 395 U.S. 752, 768 (overruling the continued expansion of the incident to arrest exception to the warrant requirement found in *United States v. Rabinowitz*, 339 U.S. 56 (1950), and *Harris v. United States*, 331 U.S. 145 (1947)).

92. *Id.* at 754.

93. *Id.* at 763 (relying, in part, on *Preston v. United States*, 376 U.S. 364 (1964), which found a lack of sufficient justification for warrantless searches which are remote in time or place from an arrest).

94. *Id.*

95. 414 U.S. 218 (1973).

96. *Id.* at 235 (describing safety as "an adequate basis for treating all custodial arrests alike for purposes of search justification"); *see also* Riley v. California, 573 U.S. 373, 374 (2014) (discussing the Robinson Court's determination that the risks presented in *Chimel* are present in all custodial arrests).

97. *See* Riley v. California, 573 U.S. 373, 395–96 (2014).

98. 573 U.S. 373 (2014).

99. *Id.* at 378, 380–81 (explaining that, in the case consolidated on appeal, *United States v. Wurie*, 728 F.3d 1, 1–2 (1st Cir. 2013), officers traced a repeated caller to Wurie's seized cell phone, labelled as "my house" on the phone's external screen, which, upon obtaining a search warrant for the traced address, led to Wurie's convictions for drug and firearm offenses).

100. *Id.* at 379.

activities.[101] Additional examination of the phone uncovered incriminating photographs and video footage which, at least in part, served as the basis for the State to charge Riley in connection with a recent shooting and to seek an enhanced sentence predicated on Riley's alleged gang membership.[102] Riley's motion to suppress the evidence obtained from his cell phone was denied by the trial court, and Riley was convicted.[103] The California Court of Appeals affirmed this ruling, and the California Supreme Court denied Riley's petition for review.[104]

The United States Supreme Court granted certiorari.[105] In evaluating Riley's motion to suppress, the Court recognized the "well accepted" exception to the warrant requirement for searches conducted incident to an arrest.[106] However, the Court declined to extend *Robinson*'s categorical rule to searches of data located on cell phones.[107] The Court reasoned that the interests enumerated in *Chimel*, mainly the government's interest in officer safety and preventing evidence destruction, were far outweighed by the individual privacy interests at stake in cell phone searches.[108] Cell phones also differ both quantitatively and qualitatively from a physical search of an arrestee's person, implicating much more substantial privacy interests than the searches previously authorized as incident to an arrest.[109] Additionally, addressing the governmental interests discussed in *Chimel*, the Court was unconvinced that cell phones present a significant safety risk to officers.[110] Furthermore, the Court found limited evidence to suggest that potential evidence destruction, via remote wiping or data encryption, was a major concern or should be effectively addressed through carte blanche authority to search the phone at the time of arrest.[111] The Court additionally acknowledged it had not been presented with any practical suggestion as to how to limit the scope of a warrantless search of a cell phone incident to an arrest,[112] and rejected the idea that law enforcement should always have access to a phone's call log.[113] The Court ultimately concluded that

101. *Id.*

102. *Id.*

103. *Id.* at 379–80.

104. *Id.* at 380.

105. *Id.*

106. *Id.* at 382.

107. *Id.* at 386.

108. *Id.* at 393 (disregarding the Government's assertion that a search of the data stored on a cell phone is "materially indistinguishable" from other physical searches by explaining "[t]hat is like saying a ride on horseback is materially indistinguishable from a flight to the moon").

109. The Court highlighted the distinct types of information stored, the devices' immense storage capacity, the extended period of time over which data is stored, and the likelihood that data accessed through a cell phone may actually be stored on a remote server, making the scope of the search much broader than a search of the device itself. *Id.* at 393–94. These capabilities create a "gulf between physical practicability and digital capacity" that the Court recognized is only going to continue to widen.

110. *See id.* at 387–88 (elaborating that any concerns regarding communications with accomplices that may implicate officer safety should be addressed through case-specific exceptions allowing for warrantless searches).

111. *See id.* at 389–90.

112. *Id.* at 399 (noting only a "particularly inexperienced or unimaginative law enforcement officer" would be unable to compose reasons to believe evidence of a crime may be located on a cell phone).

113. *Id.* at 400 (explaining that a cell phone call log is not analogous to a pen register due to the breadth of information it may contain).

officers must generally obtain a warrant before conducting such a search of a cell phone, even when such cell phone is seized incident to a lawful custodial arrest.[114] The Court did acknowledge the possibility that case-specific exceptions, such as exigent circumstances, may justify warrantless searches of particular phones.[115]

D. The Exclusionary Rule

The exclusionary rule provides for the inadmissibility of evidence obtained in violation of a defendant's Fourth Amendment rights.[116] Though the Court originally only mandated exclusion as a remedy in federal courts,[117] in *Mapp v. Ohio*[118] the Court held that evidence obtained in violation of the search and seizure protections of the Fourth Amendment is inadmissible in both state and federal courts.[119] This holding overruled *Wolf v. Colorado*,[120] where the Court had held that exclusion was not fundamentally ingrained within the rights enumerated in the Fourth Amendment and therefore did not apply to the states.[121] In explaining the application of the exclusionary rule to the states under the Fourteenth Amendment, the *Mapp* Court found exclusion to be the only sufficient remedy to address Fourth Amendment violations, and thus constitutionally required, and that "[t]o hold otherwise is to grant the right but in reality to withhold its privilege and enjoyment."[122]

The suppression of evidence under the exclusionary rule may extend beyond the scope of the initial evidence obtained as a result of the Fourth Amendment violation under "fruit of the poisonous tree" doctrine.[123] When evidence is "derived from the exploitation of an illegal search or seizure," the doctrine requires the suppression of the additional evidence unless the Government can demonstrate a break in the causal chain.[124]

While the Supreme Court has clarified that the exclusionary rule applies equally to violations at the state and federal level, it has not mandated that every violation will automatically result in exclusion.[125] Recognizing that the rule may significantly impede

---

114. *Id.* at 401.

115. *Id.* at 401–02 ("[T]he exigent circumstances exception requires a court to examine whether an emergency justified warrantless search in each particular case.").

116. *See* Wolf v. Colorado, 338 U.S. 25, 28 (1949) (citing Weeks v. United States, 232 U.S. 383 (1914)) (describing the decision as a "matter of judicial implication"), *overruled by* Mapp v. Ohio, 367 U.S. 643 (1961).

117. *Weeks*, 232 U.S. at 398.

118. 367 U.S. 643 (1961).

119. *See id.* at 655.

120. 338 U.S. 25 (1949).

121. *See id.* at 33 (determining that the Fourth Amendment does not forbid the admissibility of evidence obtained in violation of constitutional search and seizure mandates); *Mapp*, 367 U.S. at 655 ("[A]ll evidence obtained by searches and seizures in violation of the Constitution is, by that same authority, inadmissible in a state court.").

122. *Mapp*, 367 U.S. at 655–56.

123. Wong Sun v. United States, 371 U.S. 471, 488 (1963).

124. United States v. Martinez, 486 F.3d 855, 864 (5th Cir. 2007) (citing United States v. Rivas, 157 F.3d 364, 368 (5th Cir. 1998)).

125. United States v. Leon, 468 U.S. 897, 906–07 (1984). The Court previously determined that the suppression is a constitutional requirement, holding in *Mapp* that the "exclusionary rule is an essential part of

the efforts of law enforcement and the integrity of the fact-finding process, the Court has focused on the effectiveness of the exclusion purpose of deterrence when evaluating whether the exclusionary rule should be applied.[126] Utilizing a cost-benefit analysis, the Court has declined to require exclusion for violations that are attenuated from the actions of law enforcement in the execution of the search or seizure, such as for acts of negligence in the keeping of records or certain procedural violations.[127]

1. Good-Faith Exception to the Exclusionary Rule

In *United States v. Leon*,[128] the Court announced the "good-faith exception" to the exclusionary rule.[129] At issue in the case was evidence of criminal drug activity seized pursuant to a facially valid search warrant, substantially supported by unverified information provided by a confidential informant.[130] In response to motions to suppress by the defendants, the district court ordered the suppression of some, but not all, of the evidence, determining that the warrant lacked probable cause but acknowledging standing issues with some of the searches.[131] This was later affirmed by the Ninth Circuit, upon a determination that the information provided by the confidential informant was "fatally stale" and the officer's affidavit "failed to establish the informant's credibility."[132]

In granting the Government's petition for certiorari, the Court sought to evaluate the merits of an exception to the exclusionary rule in cases of reasonable, good-faith reliance on a search warrant that is subsequently held to be defective.[133] In doing so, the Court discussed "the sometimes competing goals of . . . deterring official misconduct and removing inducements to unreasonable invasions of privacy and . . . establishing procedures under which criminal defendants are 'acquitted or convicted on the basis of all the evidence which exposes the truth.'"[134] Reviewing relevant precedent, the Court concluded that the balancing approach to these issues strongly supported the adoption of a modified application of the exclusionary rule.[135]

Particularly important in this calculation was the scrutiny of a detached, neutral magistrate in the issuance of a warrant, which served as a reliable safeguard against potential overreach by law enforcement.[136] Though deference is generally accorded to

---

both the Fourth and Fourteenth Amendments." *Mapp*, 367 U.S. at 657. However, the Court appears to have changed its mind on this point. *Leon*, 468 U.S. at 906.

126. *Leon*, 468 U.S. at 906.

127. *See* Hudson v. Michigan, 547 U.S. 586, 599 (2006) (finding the social costs too great to justify the application of the exclusionary rule to knock-and-announce violations); Herring v. United States, 555 U.S. 135, 137 (2009) (finding exclusion to be an inappropriate remedy for a violation that was the "result of isolated negligence attenuated from the arrest").

128. 468 U.S. 897 (1984).

129. *Id.* at 913.

130. *Id.* at 902.

131. *Id.* at 903.

132. *Id.* at 904.

133. *Id.* at 905.

134. *Id.* at 900–01 (quoting Alderman v. United States, 394 U.S. 165, 175 (1969)).

135. *Id.* at 909.

136. *Id.* at 913–14 (citing United States v. Chadwick, 433 U.S. 1, 9 (1977)).

the magistrate's probable cause finding, courts are not prohibited from reviewing the magistrate's decision.[137] This review may include inquiring into any falsities upon which the determination may have been based, invalidating authorization provided by a magistrate acting as "an adjunct law enforcement officer" rather than a "neutral and detached" magistrate, or reviewing affidavits to ensure the magistrate's probable cause determination reflected a proper analysis of the totality of the circumstances and is otherwise free from defect.[138]

The Court found little deterrence incentive for law enforcement officers in cases of good-faith reliance on a flawed search warrant.[139] The Court suggested that it was inappropriate to expect an officer to question a magistrate's probable cause determination, and penalizing law enforcement for the magistrate's error would not facilitate any additional deterrence.[140] Because the Court determined the primary purpose of the exclusionary rule is deterrence of wrongful police conduct, "evidence obtained from a search should be suppressed only if it can be said that the law enforcement officer had knowledge, or may properly be charged with knowledge, that the search was unconstitutional under the Fourth Amendment."[141] Therefore, exclusion may still be appropriate in cases where "no reasonably well trained officer should rely on the warrant."[142] Under the specific circumstances presented in *Leon*, the Court found the officer's reliance on the magistrate's probable cause determination was objectively reasonable and, therefore, ruled that suppression was an inappropriate remedy.[143]

The Fifth Circuit has held that most searches undertaken pursuant to a warrant will be subject to the good-faith exception, and the evidence will remain admissible unless the warrant is deficient in one of the ways enumerated in *Leon*.[144] When reviewing the constitutionality of a search and seizure conducted pursuant to a warrant, the court applies a two-step analysis.[145] First, in the Fifth Circuit, the court must determine whether

137. *See id.* at 914.

138. *Id.* at 914–15. Many courts, including the Fifth Circuit, have interpreted the examples discussed in *Leon* as establishing four distinct situations in which the good-faith exception would apply. *See, e.g.*, United States v. Massi, 761 F.3d 512, 526 (5th Cir. 2014) ("The Supreme Court in *Leon* identified four situations, or 'exceptions,' that would prevent admission of evidence obtained through a search warrant: the affiant misled the magistrate who issued the warrant; the magistrate 'abandoned his judicial role'; the affidavit is patently inadequate to show probable cause; or the warrant is so deficient on its face that officers could not presume its validity." (quoting *Leon*, 468 U.S. at 921–25)).

139. *Leon*, 468 U.S. at 916–17 (noting also that "there exists no evidence suggesting that judges and magistrates are inclined to ignore or subvert the Fourth Amendment or that lawlessness among these actors requires application of the extreme sanction of exclusion").

140. *Id.* at 921.

141. *Id.* at 919.

142. *Id.* at 923.

143. *Id.* at 926.

144. *Morton I*, 984 F.3d 421, 425 (5th Cir. 2021), *rev'd en banc*, 46 F.4th 331 (5th Cir. 2022); *see also* United States v. Sibley, 448 F.3d 754, 757 (5th Cir. 2006) ("The good-faith exception does not apply when: (1) the magistrate issuing the warrant was misled by information in an affidavit that the affiant knew or should have known was false; (2) the issuing magistrate abandoned the judicial role; (3) the warrant was based on an affidavit so lacking in indicia of probable cause as to render belief in its existence entirely unreasonable; or (4) the warrant was so facially deficient that the executing officers could not have reasonably presumed it to be valid.") (citing United States v. Cherna, 184 F.3d 403, 407–08 (5th Cir. 1999)).

145. *Sibley*, 448 F.3d at 757; United States v. Allen, 625 F.3d 830, 835 (5th Cir. 2010).

the good-faith exception applies.[146] If it does not apply, the court must determine whether the magistrate issuing the warrant had a substantial basis for determining that probable cause existed.[147]

In *United States v. Sibley*,[148] Sibley was charged with several offenses relating to his possession of controlled substances, drug trafficking, and firearm possession.[149] In his initial motion to suppress, the defendant argued that the search warrant affidavits were infirm due to their failure to put forth sufficiently reliable information, including a failure to provide the source of the information provided.[150] The district court denied the motion without an evidentiary hearing because Sibley had failed to demonstrate that the good-faith exception was inapplicable.[151] Sibley ultimately accepted a plea agreement and appealed the denial of his motion to suppress to the Fifth Circuit.[152]

On appeal, the court determined that the affidavits provided did not contain any misleading information.[153] To the contrary, the court found that the warrant was sufficiently supported by affidavits containing a series of connected facts and, thus, not so lacking in indicia of probable cause as to render reliance on the warrant objectively unreasonable.[154] Finding no facts to conclude that the good-faith exception was inapplicable, the court found it unnecessary to proceed with a review of the magistrate's probable cause determination.[155]

A similar situation presented itself before the Fifth Circuit in *United States v. Pope*.[156] Only one month after the decision in *Sibley*, the court found the good-faith exception inapplicable in a case in which a law enforcement officer, in seeking a warrant, attested to a deliberate falsehood and a deliberate omission of material fact.[157] In *Pope*, an undercover police officer purchased several prescription pills from Pope as part of a covert operation for which no charges were pursued.[158] Seventy-eight days later, the officer received a tip that Pope was involved in the manufacture of methamphetamine.[159] Lacking probable cause to obtain a search warrant for Pope's home on suspicion of methamphetamine production, the officer provided an evidentiary search warrant affidavit relating exclusively to the prescription-drug transaction.[160] Upon obtaining the warrant, the officer returned to Pope's home where he discovered the methamphetamine lab in plain view; a subsequent warrant allowed for an additional search of the premises

146. *Sibley*, 448 F.3d at 757.
147. *Id.* at 757–58.
148. 448 F.3d 754 (5th Cir. 2006).
149. *Id.* at 756.
150. *Id.*
151. *Id.*
152. *Id.*
153. *Id.* at 758.
154. *Id.*
155. *Id.*
156. 452 F.3d 338 (5th Cir. 2006), *withdrawn and superseded by* 467 F.3d 912 (5th Cir. 2006).
157. *Id.* at 345.
158. *Id.* at 340.
159. *Id.*
160. *Id.*

for evidence relating to the methamphetamine manufacturing.[161] Importantly, no evidence was ever discovered—and possibly never searched for—relating to the prescription-drug sale.[162] Pope sought to suppress the evidence, arguing the evidence of the prescription-drug sale was stale and, therefore, the warrant lacked probable cause.[163] The district court agreed, but denied suppression under the good-faith exception.[164]

In finding the good-faith exception inapplicable, the Fifth Circuit held that it is "not an instrument that law enforcement may use to manipulate the warrant application process and thereby circumvent the constitutional requirement of probable cause."[165] In evaluating the facts of this case, the court determined the officer had intentionally misled the magistrate regarding the purpose of the search, evidenced through the officer's own testimony at the suppression hearing,[166] the urgency with which the warrant was obtained,[167] and the deliberate misdirection provided to the magistrate regarding the intended purpose of the search.[168] In failing to disclose the target of the search—the methamphetamine production—the officer prevented the magistrate from fulfilling his gatekeeping function because "[t]he facts supporting probable cause and the object of the search are inextricably linked in the probable cause calculus."[169] Thus, any reasonably well-trained officer would have known that, despite the magistrate's authorization, the search was illegal and could not be salvaged by the good-faith exception.[170] The court further emphasized that the magistrate's ability to perform their intended function in the issuance of warrants requires complete and forthright information from the requesting officer, and thus a deceitful officer cannot rely on the good-faith exception to avoid suppression.[171]

However, the panel majority quickly decided, sua sponte, to withdraw and replace this opinion; in a new, unanimous decision, the Fifth Circuit panel affirmed the district court's application of the good-faith exception to avoid the suppression of evidence obtained in the absence of probable cause.[172] The court found that Pope had failed to adequately raise the argument that the officer's "deliberately or recklessly false" affidavit, which omitted details regarding the true purpose of the search and the date of

161. *Id.*

162. *Id.*

163. *Id.* at 340–41.

164. *Id.* at 341.

165. *Id.* at 345.

166. *Id.* at 343. When questioned, the officer stated that he pursued the warrant because of the information received regarding methamphetamine but acknowledged that such information failed to establish sufficient probable cause. *Id.*

167. *Id.* at 344. Despite no action on the narcotics activity for seventy-eight days, the officer worked overtime hours to produce an affidavit overnight and deliver it to the magistrate at seven o'clock in the morning. *Id.*

168. *Id.* at 345.

169. *Id.* (emphasis omitted).

170. *Id.*

171. *Id.*

172. United States v. Pope, 467 F.3d 912, 914 (5th Cir. 2006). The district court had concluded that the information contained in the affidavits was fatally stale. *Id.* at 918.

the initial prescription-drug purchase, precluded good-faith reliance and, thus, was barred from consideration at the appellate level.[173]

In 2013, the Fifth Circuit was asked to consider a categorical expansion regarding circumstances in which the good-faith exception would be deemed inapplicable—when the probable cause determination by a magistrate was founded in evidence uncovered through an illegal search and seizure.[174] In *United States v. Woerner*,[175] officers for the Los Fresnos Police Department (LFPD) executed an expired warrant on Woerner's home and arrested him on child pornography charges.[176] Woerner then waived his *Miranda* rights and proceeded to disclose additional information regarding the possession and dissemination of child pornography, as well as a sexual relationship with a minor.[177] Contemporaneously, the Federal Bureau of Investigation (FBI) began investigating Woerner's online activities and executed a search warrant for Woerner's home.[178]

Information obtained from Woerner following his arrest was shared between the LFPD and FBI officers conducting parallel investigations and was included in support of subsequent warrants for the suspect's house and digital accounts.[179] Woerner filed a motion to suppress the evidence obtained in the interrogation, as well as the initial and subsequent searches, as fruits of the initial illegal search executed by the LFPD based on an expired warrant.[180] The court granted the motion in part but denied the suppression of the evidence obtained in the later searches on the basis of the good-faith exception; in doing so, the court determined that, in this particular instance of parallel investigations, the officers had placed objectively reasonable reliance on evidence they did not know would later be suppressed.[181]

In issuing this denial, the court declined to issue a categorical rule, favoring the opportunity to evaluate the applicability of the exclusionary rule to unusual cases on a case-by-case basis as noted in *Leon*.[182] Because it was not clear that the FBI officers, or the LFPD officer who provided the FBI with the information, could have known the information was obtained illegally, the court found that suppression would do little to deter Fourth Amendment violations in the future.[183] Accordingly, the court held that the information obtained in the subsequent searches should not be suppressed, and Woerner's convictions were affirmed.[184] In the wake of these rulings, the applicability

173. *Id.* at 918–19. The panel also found that the affidavit submitted in support of the warrant was not bare-boned. *Id.* at 919.

174. United States v. Woerner, 709 F.3d 527, 534 (5th Cir. 2013).

175. 709 F.3d 527 (5th Cir. 2013).

176. *Id.* at 531.

177. *Id.* at 532.

178. *Id.* at 531–32.

179. *Id.* at 532–33, 535.

180. *Id.* at 534. The statements made by Woerner following his *Miranda* waiver were excluded as fruit of the expired warrant and, Woerner argued, provided the only evidentiary connection between him and certain online accounts. *Id.*

181. *Id.* (Woerner was convicted on five counts with sentences to be served consecutively for a total of 960 months).

182. *Id.*

183. *Id.* at 534–35.

184. *Id.* at 535, 541.

of the good-faith exception in the Fifth Circuit remains subject to case-by-case analysis, particularly focused on whether the particular wrongdoing of officers would be adequately deterred through exclusion.[185]

2. The Exclusionary Rule in the Wake of *Riley*

Following the introduction of the search warrant requirement for cell phones seized incident to an arrest established in *Riley*, there has been little guidance regarding how to evaluate the sufficiency of such warrants.[186] With little precedent regarding the particularity requirements for search warrants for cell phones or particular limitations regarding the method by which a search is conducted,[187] courts have frequently found that a reasonable officer would not have known that the search warrant was defective.[188] Accordingly, when search warrants for digital devices have been found to be defective—for overbreadth or lack of particularity—the good-faith exception has generally allowed for the admissibility of the evidence obtained.[189] Thus, defective search warrants are frequently successful in allowing for the admissibility of evidence obtained through searches that lack meaningful restraints.[190]

E. General Warrants and Particularity for Cell Phones

The Court has frequently recognized the need to adopt doctrine to account for technological advancements.[191] Orin Kerr similarly described the reasoning in *Riley* as an "equilibrium adjustment"—an acknowledgement that changes in technology and society demand changes to legal doctrines to ensure that protections intended by the Fourth Amendment remain available as technology advances.[192] In support of this goal, *Riley* provided a new, general rule for searches of cell phones that claimed to be "accordingly simple—get a warrant."[193] However, the warrant requirement, in practice,

185. *See id.* at 534.

186. *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, 190 (2015).

187. *See infra* Part III.E.

188. Adam M. Gershowitz, *The Post*-Riley *Search Warrant: Search Protocols and Particularity in Cell Phone Searches*, 69 VAND. L. REV. 585, 590 (2016).

189. *Id.*

190. *See* Tammie Beassie Banko, *"You're Not Gonna Reach My Telephone"— The Resurgence of the Fourth Amendment's Particularity Requirement*, 71 SMU L. REV. 575, 580 (2018); Gershowitz, *supra* note 188, at 590.

191. *See* Kyllo v. United States, 533 U.S. 27, 33–34 (2001) ("It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology."); United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring) (holding that in the absence of legislative action, the Court must "apply existing Fourth Amendment doctrine and . . . ask whether the use of GPS tracking in a particular case involved a degree of intrusion that a reasonable person would not have anticipated"); Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018) ("[T]he progress of science has afforded law enforcement a powerful new tool to carry out its important responsibilities. At the same time, this tool risks Government encroachment of the sort the Framers . . . drafted the Fourth Amendment to prevent.").

192. *See* Orin S. Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 TEXAS TECH L. REV. 1, 10 (2015) (predicting that *Riley* will be the first of a series of decisions intended to address the new technological environment).

193. Riley v. California, 573 U.S. 373, 403 (2014).

has proven to be more contentious. As noted by the Court in *Riley*, the information contained in cell phones is dramatically more expansive than other types of physical containers.[194] By removing cell phones from the search incident to arrest exception, the Court recognized the expansive privacy interests implicated by cell phone searches[195] and returned the gatekeeping function to the magistrates charged with reviewing warrant applications.[196]

However, Adam M. Gershowitz argues that the impact of *Riley* has been dampened by the lack of uniformity in the exercise of discretion regarding the permissible scope of warrants issued in the wake of the *Riley* decision.[197] Limited suspicion of criminal activity has proven sufficient for search warrants granting access to a wide range of information—including information found in more traditional telephone capabilities—like text messages and call logs, to more sophisticated functions, like photographs, videos, and other available applications.[198] Drug cases, in particular, have been wrought with this type of authorized broad search authority.[199] Frequently, affidavits supporting the warrants lack any precise nexus to alleged criminal behavior other than officers' assertions that cell phones frequently hold evidence of drug activities.[200]

Sometimes, cell phone searches are conducted through a manual inspection of the phone's features and applications.[201] More frequently, digital searches occur in two stages: first, the device is physically seized by law enforcement, and second, the data on the device is copied and searched in accordance with the warrant.[202] Current practices generally allow law enforcement to overseize in the physical stage—allowing the officers to remove the entire device for later investigation regardless of the scope of the information sought—to ensure that the initial physical intrusions of the officers are relatively brief.[203] This initial overseizure grants law enforcement control over a significant amount of data that is likely to be unresponsive to the particular warrant.[204]

194. *Id.* at 394.

195. Gershowitz, *supra* note 188, at 587.

196. *Id.* at 588.

197. *Id.* at 590 n.20.

198. *Id.* at 589–90.

199. *Id.*

200. *See, e.g.*, United States v. Harris, No. 3:15cr170, 2016 WL 1441382, at *11 (E.D. Va. Apr. 11, 2016) ("Several courts have found that probable cause existed to justify the issuance of a search warrant based solely on law enforcement experience that cell phones found near illegal activity are highly likely to contain incriminating evidence."), *aff'd*, 688 F. App'x 223 (4th Cir. 2017); United States v. Fisher, No. 14-413, 2015 WL 1862329, at *2 (D. Md. Apr. 22, 2015); United States v. Eiland, No. 04-379, 2006 WL 516743, at *12 (D.D.C. Mar. 2, 2006).

201. RICK AYERS, SAM BROTHERS & WAYNE JANSEN, NAT'L INST. STANDARDS & TECH., GUIDELINES ON MOBILE DEVICE FORENSICS 17 (2014), https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-101r1.pdf [https://perma.cc/25D5-KKTL] (defining manual extraction); Gershowitz, *supra* note 188, at 629.

202. Huynh, *supra* note 186, at 197; Kerr, *supra* note 192, at 6.

203. Kerr, *supra* note 192, at 7 (discussing the impracticality of requiring officers to identify and remove only responsive data from a digital device at the time of the seizure given the time-consuming nature of the process).

204. *Id.* at 6.

In the case of cell phones, the entire device may be seized incident to an arrest and held while officers seek a search warrant for data held on the device.[205] Because it is frequently unknown where exactly responsive data will be located on the device, law enforcement agents often view a significant amount of unresponsive data in the course of the second stage of the digital search.[206]

To access the information found on a cell phone, law enforcement typically employs mobile device forensic tools (MDFTs) to extract a full copy of the cell phone's data.[207] Depending on the device, Cellebrite or other similar software may allow investigators to refine the extraction by selecting specific categories or data generated within a specific timeframe to be extracted.[208] In most instances, these types of software can bypass security systems through built-in diagnostic or development tools or flaws within the security features.[209] Though encryption may temporarily impede data access, MDFTs have advanced to include numerous mechanisms to obtain access to such data.[210] MDFTs can access data decryption keys generated from the password, brute-forcing a password until the correct combination is obtained, or utilizing unencrypted features.[211]

Certain MDFTs, including Cellebrite's UFED Cloud, also facilitate the extraction of data not located directly on the device, such as cloud backups and other remote account information.[212] In some instances, account credentials may be accessed by the MDFTs to allow investigators to remain logged in to various accounts utilized by the device owner after extraction has occurred.[213]

Once extracted, MDFTs allow law enforcement to sort the data, search for specific key terms, or view the phone as a typical user of the device.[214] Some software now include machine learning tools to assist with text and image classification, such as the ability to search for images of particular faces or relevant topics.[215] Despite the vast and expanding capabilities of MDFTs, many police departments appear to provide officers with limited constraints or guidance regarding their use.[216] To account for the breadth of nonresponsive data available to law enforcement through these search procedures, a variety of solutions and mitigation strategies have been proposed; these include, but are not limited to, eliminating the plain view doctrine for digital spaces,[217] prohibiting consent searches,[218] requiring greater specificity for purposes of the particularity

205. *Id.* at 6–7.

206. *See id.* at 20; AYERS ET AL., *supra* note 201, at 48 ("Data reduction, separating relevant from irrelevant information, occurs once the data is exposed.").

207. A variety of different terms are used to describe this technology—MDFTs is the umbrella term from the National Institute of Standards and Technology. KOEPKE ET AL., *supra* note 7, at 4, 6 n.2.

208. *Id.* at 11.

209. *Id.*; *see also* AYERS ET AL., *supra* note 201, at 24.

210. KOEPKE ET AL., *supra* note 7, at 28.

211. *Id.*

212. *Id.* at 17.

213. *Id.*

214. *Id.* at 12, 14.

215. *Id.* at 24.

216. *Id.* at 48–49.

217. Kerr, *supra* note 192, at 3–4; KOEPKE ET AL., *supra* note 7, at 5.

218. KOEPKE ET AL., *supra* note 7, at 5.

requirement,[219] reviving inventory requirements,[220] and mandating search protocols.[221] This variety of proposals is indicative of the yet unsolved task of appropriately balancing the competing government and private interests present in digital searches, particularly in cases where a low-level offense facilitates government access to a private cellular device.

F. Recent Cases Challenging Particularity in Cell Phone Warrants

Courts are increasingly encountering legal challenges to the breadth of warrants for searches of digital spaces. Under the Fourth Amendment and similar protections enumerated in state constitutions, complex questions are emerging regarding sufficient probable cause, particularity, and scope in relation to cell phone search warrants, resulting in confusion within the courts.[222] Parts III.F.1 and III.F.2 highlight recent cases grappling with the failures of the current doctrine to provide adequate guidance on the permissible breadth and temporality of cell phone searches.

1. Categorical Limits on the Content of the Search

In 2020, the District of Columbia Court of Appeals invalidated warrants issued to search the cell phones of an individual suspected of murder for being overbroad and lacking probable cause and particularity for all but three narrow categories of data.[223] In *Burns v. United States*,[224] the defendant was arrested for the murder of his friend, Mr. Osuchukwu, following the execution of warrants that uncovered incriminating evidence on his cell phones.[225] Though the warrant affidavits alleged probable cause to search "the phones' subscriber and owner information, call logs, contact lists, voice mail and text messages, videos, photographs, and tweets," the warrants issued were much broader—they allowed for the search of all records for any evidence found on the phone.[226] In evaluating the scope of the warrants, the court determined that the warrant affidavits provided facts sufficient to establish probable cause to search (1) the text messages between Mr. Burns and Mr. Osuchukwu on November 14, 2015; (2) the call log to establish the precise time of a telephone call made to the defendant's cousin; and (3) the GPS tracking features to determine the defendant's whereabouts at specific times over two days.[227] However, the search of the defendant's entire phone violated the Warrant Clause because the warrants authorized law enforcement to extract all information

219. Gershowitz, *supra* note 188, at 634.

220. Laurent Sacharoff, *The Fourth Amendment Inventory as a Check on Digital Searches*, 105 IOWA L. REV. 1643, 1643 (2020).

221. Kerr, *supra* note 192, at 8.

222. *See infra* Parts III.F.1 and III.F.2.

223. Burns v. United States, 235 A.3d 758, 778 (D.C. 2020).

224. 235 A.3d 758 (D.C. 2020).

225. *Id.* at 766.

226. *Id.* at 774 (describing how the warrant enumerated several broad categories of information to be searched, including "schedule and travel information; saved usernames and passwords; documents; and '[r]ecords of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses'" (alteration in original)).

227. *Id.*

contained on the phone based on bare-bones statements regarding the detective's belief that the phones would contain evidence.[228] Alone, the affiant's "training and experience" was insufficient to provide the magistrate with a factual basis that could support a probable cause determination.[229]

Citing *Riley*, the court noted that a defendant's Fourth Amendment interests may be "most compelling when police wish to search the contents of a modern smart phone."[230] Therefore, to comply with the warrant requirement, the warrant must be temporally limited and properly establish probable cause for the particular items to be searched and seized.[231] The court explained, "Vigilance in enforcing the probable cause and particularity requirements is thus essential to the protection of the vital privacy interests inherent in virtually every modern cell phone and to the achievement of the 'meaningful constraints' contemplated in *Riley*."[232] The court, therefore, rejected the scope of the warrants as issued and found probable cause sufficient to support searches for three narrow categories of information.[233]

Questions of appropriate limits on search warrants for digital devices have not been limited to Fourth Amendment challenges. The Pennsylvania Supreme Court recently avoided ruling on a matter of first impression—the permissible scope of search warrants for cell phones under the Pennsylvania Constitution.[234] Law enforcement had seized two cell phones during a search incident to arrest for possession of heroin and stolen firearms.[235] The officers eventually obtained warrants to search the cell phones, and the defendant filed a motion to suppress the evidence obtained on the cell phones for lack of probable cause and overbreadth.[236] He claimed the officers had failed to establish that the defendant was a "drug trafficker" and not merely a guest in the home, and thus had no evidence to support their belief that evidence of the illicit activity may be located on his phones.[237] Additionally, he argued that the scope of the search authorized pursuant to the warrant—"to search, among other things, all his emails, personal calendars, cellular internet usage, wireless internet usage, GPS data, contact information, text messages, voicemails, notes, photos, and IP addresses"—was "ridiculously overbroad."[238]

---

228. *Id.* at 772.

229. *Id.*

230. *Id.* at 773.

231. *Id.*

232. *Id.*

233. *Id.* at 774.

234. Commonwealth v. Johnson, 240 A.3d 575, 578 (Pa. 2020).

> The people shall be secure in their persons, houses, papers and possessions from unreasonable searches and seizures, and no warrant to search any place or to seize any person or things shall issue without describing them as nearly as may be, nor without probable cause, supported by oath or affirmation subscribed to by the affiant.

PA. CONST. art I, § 8.

235. *Johnson*, 240 A.3d at 580.

236. *Id.* at 580, 582.

237. *Id.* at 581–82.

238. *Id.* at 582.

The suppression court denied the defendant's claims, and the case proceeded to a jury trial, which ended in a mistrial.[239] The defendant was found guilty of possession of heroin and possession with intent to deliver in a subsequent bench trial and appealed the suppression decision to the Superior Court of Pennsylvania.[240] In a unanimous decision, the panel affirmed the trial court's ruling, holding that the defendant's proximity to the drugs and guns was sufficient to establish probable cause.[241] Additionally, pointing to the officers' specialized knowledge regarding the use of cell phones in the distribution of narcotics, the panel suggested that "evidence of a narcotics distribution enterprise would not be limited to a distinct period of time, a limited number of people, or a particular form of digital file," and, thus, the breadth of the warrant was also appropriate.[242]

Though the Pennsylvania Supreme Court granted review specifically to address the issue of overbreadth, the court determined that the issues of probable cause and overbreadth could not be "meaningfully untangle[d]" under the facts of the case.[243] Failing to find any demonstrated nexus between the contraband seized and the defendant's presence at the location, the court determined the specialized knowledge of the police in the use of cell phones by drug traffickers was too attenuated from the defendant himself to support probable cause to search his cell phones.[244] Because of the lack of sufficient probable cause to support any search of the phones, the court declined to address any specific issues of particularity in the search of a defendant's cell phone.[245] In finding no specific factual basis for any search of the phones, the court avoided the challenging task of parsing through and evaluating each category of information contained within the device despite the initial question presented to the court.[246] However, this case is indicative of a lack of clear guidance in the appropriate scope of warrants for searches of mobile devices, often resulting in ex post review.[247]

2. Temporal Limits on the Content of the Search

Rather than restricting search authorization to specific types of data, some courts have focused on temporal limitations to restrict the scope of the search. In *Commonwealth v. Snow*,[248] the police arrested the defendant and his two companions for involvement in a recent shooting.[249] When the officers removed the men from the alleged

239. *Id.*

240. *Id.* at 582–83.

241. *Id.* at 583.

242. *Id.* (quoting Commonwealth v. Johnson, No. 1082 WDA 2017, 2018 WL 5077174, at *12 (Pa. Super. Ct. Oct. 18, 2018)).

243. *Id.* at 586.

244. *Id.* at 587–88 (noting the "affidavit does not otherwise allege [the defendant] was personally in possession of (or even aware of) the drugs, guns, or anything else related to criminal activity found in the apartment").

245. *Id.* at 578.

246. *Id.*

247. *See* Gershowitz, *supra* note 188, at 590.

248. 160 N.E.3d 277 (Mass. 2021).

249. *Id.* at 280.

getaway vehicle, the defendant was talking on his cell phone.[250] At that time, the officers discovered a .40 caliber firearm, which they determined had been recently discharged through the use of thermal imaging technology, and seized cell phones belonging to all three men.[251] They also recovered the cell phone of the victim.[252]

The vehicle being utilized at the time of arrest was rented to the defendant's girlfriend.[253] The Commonwealth sought a search warrant for the defendant's cell phone, alleging that the car rental and subsequent behavior of the defendant and his associates were indicative of planning and coordination in relation to the crime, creating a sufficient nexus to the cell phone to authorize a search.[254] The detectives were granted unrestricted authority, including no temporal limitations, to search the phone due to the contention that it was unclear when any conspiracy may have been formed or when the recovered weapon may have been acquired.[255]

Before trial, the defendant was granted a motion to suppress due to a lack of sufficient nexus between the crime and the cell phone evidence.[256] On the State's interlocutory appeal, the appeals court reversed the judge's decision and remanded for a specific determination regarding whether the warrant was properly limited in scope.[257] The Massachusetts Supreme Judicial Court then granted further appellate review.[258]

The Massachusetts Supreme Judicial Court determined that the facts supported a nexus between the crime and the defendant's cell phone sufficient for probable cause.[259] Because the Commonwealth only sought to introduce evidence appropriately within the scope of "communications," the court did not find it necessary to further "opine on the precise parameters of what would have been a reasonable search" of the phone.[260] However, the court held that the particularity requirement presumptively mandates temporal limitations on the scope of such a search due to the magnitude of the privacy invasion implicit in the unrestrained search of a cell phone.[261] The court reasoned that a narrow initial search does not preclude officers from requesting broader search authority

250. *Id.* at 281.

251. *Id.*

252. *Id.*

253. *Id.*

254. *Id.* at 281–82.

255. *Id.* (noting that the warrant allowed for the search of the "[c]ellular telephone number; electronic serial number, international mobile equipment identity, mobile equipment identifier or other similar identification number; address book; contact list; personal calendar, date book entries, and to-do lists; saved, opened, unopened, draft, sent, and deleted electronic mail; incoming, outgoing, draft, and deleted text messages and video messages; history of calls sent, received, and missed; any voicemail messages, including those that are opened, unopened, saved, or deleted; GPS information; mobile instant message chat logs, data and contact information; internet browser history; and any and all of the fruits or instrumentalities of the crime of Murder.").

256. *Id.* at 280.

257. *Id.*

258. *Id.*

259. *Id.* at 284.

260. *Id.* at 286 (considering the probable cause determination under the Fourth Amendment as well as Article 14 of the Massachusetts Declaration of Rights).

261. *Id.* at 288–89.

predicated on results that give rise to additional probable cause for a broader search of the device.[262]

In Delaware, a challenge to a warrant for the search of a smart phone lacking any temporal or scope limitations, reversing convictions for gang-related murder and other violent felonies.[263] In *Taylor v. State*,[264] following a series of violent gang-related incidents, a Wilmington detective relying on her "training, knowledge, and experience" applied for and was granted a search warrant for Taylor's cell phone.[265] Under the authority of the warrant, the police extracted data from January 2005 to June 2016, culminating in a 4,645-page report that included data from twenty-three distinct areas on the phone, with "2,215 contacts, 514 call logs, 4,737 SMS messages . . . , 611 locations, . . . 26,792 web browsing entries . . . [and] 17,672 individual audio, video, image, text, configuration, database and application data files."[266] Finding the warrant not to be a general warrant, as it limited the search to data "pertinent to this investigation," the superior court denied Taylor's motion to suppress the cell phone data.[267]

Reviewing the warrant under the Fourth Amendment of the United States Constitution, Section 6 of Article I of the Delaware Constitution, and other relevant statutory law, the Delaware Supreme Court determined the warrant failed to meet the particularity requirement.[268] The court was not swayed by the superior court's determination that the scope of the warrant was sufficiently narrow because it required that evidence seized be "pertinent to this investigation," thus creating a nexus to the criminal activity and limiting the warrant's scope to a relevant period of time; instead, the warrant authorized a "top-to-bottom" search of the phone's data without any limited timeframe.[269] The Delaware Supreme Court determined that more specificity was possible and required in the immediate case, but the court did not enumerate any specific particularity requirements for search warrants.[270] In the absence of more specific language, the warrant had provided investigators with unconstitutional "unbridled discretion to conduct an exploratory rummaging . . . in search of criminal evidence."[271]

IV. COURT'S ANALYSIS

A. United States v. Morton (Morton I)

In *United States v. Morton* (*Morton I*)—the first Fifth Circuit decision in this case, rendered on January 5, 2021—the court issued a two-part ruling.[272] The court held that

262. *Id.* at 288.
263. Taylor v. State, 260 A.3d 602, 604 (Del. 2021).
264. 260 A.3d 602 (Del. 2021).
265. *Id.* at 609.
266. *Id.* at 609–10.
267. *Id.* at 610.
268. *Id.* at 615.
269. *Id.* at 610, 615.
270. *Id.* at 616.
271. *Id.* at 617.
272. *Morton I*, 984 F.3d 421 (5th Cir. 2021), *rev'd en banc*, 46 F.4th 331 (5th Cir. 2022).

(1) the good-faith exception was inapplicable because a reasonably well-trained officer would have known that the warrants lacked probable cause to search Morton's cell phones for his photographs, and (2) the magistrate did not have a substantial basis for finding probable cause to search the photographs on Morton's cell phone.[273] In reaching this holding, the Fifth Circuit concluded that probable cause must be particularized to each category of information found on the cell phone.[274] Furthermore, the court determined the illicit sexual material obtained as a result of the subsequent set of warrants was tainted by the unreasonable nature of the prior search and was consequently inadmissible as fruit of the poisonous tree.[275]

Utilizing the two-part analysis discussed in *Sibley*, the court began with an evaluation of the good-faith exceptions enumerated in *Leon*.[276] Morton's initial appellate brief argued that the good-faith exception to the suppression of evidence obtained following an illegal search should not "salvage an otherwise infirm search warrant when the affiant-officer . . . misled the magistrate as to the true object of the search."[277] Despite Morton's primary contention that the affidavits were insufficient because they were pretextual,[278] the court instead focused on the bare-bones exception and the specific locations on the cell phones for which the Government sought permission to search.[279]

In light of Morton's claim that the good-faith exception was inapplicable because the warrant "so lack[ed] indicia of probable cause" that any reliance by the officers was unreasonable, the court looked to the circumstances of the warrants' issuance.[280] In the affidavits and subsequently issued warrants, the officers sought evidence of drug crimes located in Morton's "contacts, call logs, text messages, and photographs."[281] Citing *Riley*, the court rejected the notion that searches of cell phones are "materially

273. *Id.* at 431.

274. *Id.* at 427 (concluding, based on the facts of this case, that there was sufficient probable cause to search Morton's contacts, call records, and text messages for evidence relating to illicit use of controlled substances).

275. *Id.* at 431.

276. *Id.* at 425.

277. Appellant's Initial Brief, *supra* note 19, at 1.

278. The affidavits issued in support of the warrants to search Morton's cell phones were limited in scope to evidence of Morton's drug activity, despite evidence of the officers' suspicion regarding Morton's sexual activities demonstrated through their questioning of Morton and the concerns memorialized in an interoffice memo. Appellant's Initial Brief, *supra* note 19, at 10–11. Based on this evidence that the officers' suspicions regarding Morton's possession of child pornography predated their application for a warrant, Morton suggested the omissions were designed to intentionally mislead the magistrate and therefore the good-faith exception was inapplicable. *Id.* at 10–11 (including excerpts from the officer's memo reading "I asked Morton if he cross dressed or if he was a pedophile. . . . Morton was driving down the road with his pants unzipped and I believed he may be in possession of child porn or other illegal sexual acts. I asked Morton for permission to search his cellular phone, searching for downloaded child porn or drug deals."). In response, the Government argued that regardless of officers' suspicions regarding the potential to uncover illicit sexual material, the officers obtained warrants only in regard to the drug offenses; when additional evidence relating to child pornography was discovered, the officers ceased their search and obtained additional warrants. In doing so, the officers demonstrated their good-faith reliance on the warrants. *See* Appellee's Brief, *supra* note 30, at 6–7 (suggesting the issue of probable cause need not be determined and the motion should be denied).

279. *Morton I*, 984 F.3d at 426.

280. *Id.* at 425 (alteration in original) (quoting United States v. Leon, 468 U.S. 897, 923 (1984)).

281. *Id.*

indistinguishable" from other types of searches.[282] Intending to follow *Riley*'s precedent, the court determined it was appropriate to view the phones not as a singular container, but as a collection of distinct types of information.[283] Importantly, at oral argument, the Government conceded that separate probable cause was needed "for each individual sort of category of information that could be found [on the cell phones]."[284] In evaluating this distinction in light of the necessary requirements for a reasonable search under the Fourth Amendment, the court concluded that each category of content on a phone must be particularly described and supported by a specific factual basis for the search.[285] Under this analysis, the officer's affidavits only established probable cause for the contacts, call logs, and text messages.[286]

In the majority of cases conducted pursuant to a warrant, the court recognized that the good-faith exception would apply, subject to the exceptions found in *Leon*.[287] However, the court found it necessary to evaluate each category of information individually to determine whether the officer had a good-faith basis to allege facts sufficient to raise a "fair probability" or "substantial chance" that evidence relating to Morton's drug possession would be found in each location on the phones.[288] Having determined there was probable cause as to the search of the contacts, call logs, and text messages, the court decided that the relevant category of information for analysis was the photographs.[289]

In requesting warrants to search Morton's photographs, the court noted that officers may rely on their training and experience when attesting to their belief that probable cause exists.[290] However, the court strongly rejected any suggestion that the facts of the case—Morton's possession of less than two ounces of marijuana, a pipe, and sixteen ecstasy pills—could support an inference that evidence on the phone would implicate Morton in a narcotics trafficking conspiracy.[291] Furthermore, in attesting to their beliefs regarding probable cause, the court observed that officers may not disregard "details that *do not* support probable cause for the particular crime."[292] The syllogism offered by the officer suggested that the photographs on the phone may depict coconspirators, illicit drugs, and proceeds derived from illicit drug sales.[293] Because such potential evidence is

282. *Id.* at 426.

283. The court highlighted *Riley*'s observation that the treatment of "a cell phone as a container . . . is a bit strained," and described the various types of information which may be contained within a cell phone even within each category of content. *Id.* at 425–26 (omission in original) (internal citations omitted) (quoting Riley v. California, 573 U.S. 373, 397 (2014)).

284. *Id.* at 425 n.2 (citing Oral Argument at 27:28, *Morton I*, 984 F.3d 421 (No. 19-10842), http://www.ca5.uscourts.gov/OralArgRecordings/19/19-10842_10-5-2020.mp3 [https://perma.cc/ZJ65-ANSX]). The Government disputes the court's interpretation of this response in its petition for rehearing.

285. *Id.*, 984 F.3d at 426–27.

286. *Id.* at 427.

287. *Id.* at 425.

288. *Id.* at 427.

289. *Id.*

290. *Id.* at 428.

291. *Id.*

292. *Id.* (emphasis in original).

293. *Id.*

indicative of the crime of drug trafficking, and not simple drug possession, probable cause for a search of the photographs did not exist because there was no evidence that Morton was involved in the distribution of drugs.[294] Further, the good-faith exception did not apply because the reasonably well-trained officer should have been aware that evidence of simple drug possession was insufficient to establish probable cause to believe there would be photographs on the cell phone regarding drug sales.[295]

Having determined that the good-faith exception could not salvage the objectively unreasonable search of Morton's photographs, the court then evaluated whether the magistrate had a "substantial basis" for finding probable cause.[296] Though the magistrate may draw reasonable inferences and their determination is given "great deference," the court found an insufficient basis for the determination of probable cause in relation to the photographs.[297] Because the magistrate lacked a substantial basis for its probable cause determination (thereby violating the Fourth Amendment), and because the search was not subject to any exception, the court held that the evidence uncovered should have been suppressed.[298] Furthermore, because the photographs discovered during the first searches served as the basis for the subsequent warrants, the evidence found pursuant to the additional warrants was tainted as "fruit of the poisonous tree," which must also be suppressed.[299] Because both the searches that uncovered the sexually explicit images of minors were unconstitutional, the defendant's conviction was vacated.[300]

B. United States v. Morton (Morton II)

1. Motion for Rehearing En Banc

On March 11, 2021, the United States Attorney's Office for the Northern District of Texas filed a petition for an en banc rehearing of the panel's opinion.[301] The Government asserted that the panel incorrectly adopted a new rule establishing the need for discrete probable cause determinations for each "place" within a cell phone instead of addressing the primary issue briefed by the parties: whether the allegedly pretextual nature of the search precluded the application of the good-faith exception.[302] The Government argued that by misinterpreting its perceived concession regarding the need

294. *Id.*

295. *Id.* at 428, 431 (reasoning that any additional assertions found in the affidavits regarding more expansive criminal behavior related to Morton's drug use were too minimal and generalized).

296. *Id.* at 430.

297. *Id.* at 431 (analogizing the defendant's phone's photographs to one drawer of a filing cabinet, the court held such a drawer could only be searched in relation to probable cause for drug trafficking).

298. *Id.*

299. *Id.*

300. *Id.*

301. Petition of the United States for Rehearing En Banc, *supra* note 43.

302. *Id.* at 6–7.

for probable cause for each category of information,[303] misapplying *Riley*,[304] contradicting existing precedent,[305] and ignoring technological limitations,[306] the panel's determination presented significant legal and logistical difficulties in need of further briefing by the parties.[307] The Government also contested the panel's failure to apply the good-faith exception in light of the creation of the new rule, arguing that such a decision was "infected with legal error [and] requires clairvoyance rather than objective reasonableness."[308]

In response to the motion, Morton argued that the panel decision did not establish an entirely new rule but merely responded to the failure of the particular warrant affidavits to support the inference that he was engaged in drug trafficking and, therefore, lacked indicia of probable cause as to his photographs.[309] Instead, he suggested the Government's critiques of the decision required a reading of the opinion that was unnecessarily hypertechnical,[310] and the case was a poor candidate for en banc review.[311] However, amici briefs submitted in support of the initial panel decision did not downplay the significance of the panel opinion to the same extent.[312]

The Electronic Frontier Foundation, the American Civil Liberties Union, and the Electronic Privacy Information Center submitted a joint brief arguing that cell phone searches must closely adhere to the probable cause showing.[313] The brief further argued that "[t]o safeguard our constitutional rights, courts must apply Fourth Amendment law stringently to address the unique attributes of digital data, ensuring that police direct their searches of electronic data towards evidence for which there is probable cause and away from voluminous, intimate, non-responsive private information."[314] To avoid inadvertently authorizing general searches, the brief asserted that warrants should require "some specific connection to the investigation underway, and not a general assertion that

303. The Government argued that counsel had intended to clarify that probable cause was needed for each authorized target of the search (i.e., evidence of drug possession and evidence of child pornography), but counsel had not intended to concede that each location to be searched within the phone required an independent probable cause determination for Fourth Amendment purposes. *Id.* at 5–6.

304. The Government points to language in *Riley* that describes a cell phone as "one place [with] many distinct types of information." *Id.* at 10 (emphasis omitted) (quoting Riley v. California, 573 U.S. 373, 394 (2014)).

305. *Id.* at 11–12 (first citing United States v. Bishop, 910 F.3d 335, 336 (7th Cir. 2018); then citing United States v. Bass, 785 F.3d 1043, 1049–50 (6th Cir. 2015)).

306. Forensic tools generally extract all cell phone data and do not enable searching by individual location. *Id.* at 14–15.

307. *Id.* at 15–16.

308. *Id.* at 17.

309. Appellant's Response to Petition for Rehearing En Banc at 7, *Morton II*, 46 F.4th 331 (5th Cir. 2022) (No. 19-10842).

310. *Id.* at 11.

311. *Id.* at 7–8.

312. *See* Brief of Amici Curiae Electronic Frontier Foundation, American Civil Liberties Union, and the Electronic Privacy Information Center in Support of Defendant-Appellant, *Morton II*, 46 F.4th 331 (No. 19-10842) [hereinafter Brief of EFF, ACLU, and EPIC]; Brief of Upturn, Inc. as Amicus Curiae Supporting Defendant-Appellant, *Morton II*, 46 F.4th 331 (No. 19-10842) [hereinafter Upturn Brief].

313. Brief of EFF, ACLU, and EPIC, *supra* note 312, at 3.

314. *Id.* at 11.

would apply to any and all such crimes."[315] The brief contested the existence of probable cause not only for the photographs on Morton's cell phones but also for the cell phones entirely in the absence of additional information—beyond officers' generic "training and experience"—tying the cell phones to suspected evidence.[316] Furthermore, pointing to language in *Riley* discussing "'categories,' 'areas,' 'types' of data, and 'apps,'" the brief suggested requiring greater particularity in search of cell phones was entirely consistent with the court's holding and intention to "limit officer's unbridled access to the information stored on the phone."[317] The brief concluded by asking the court to find a lack of probable cause as to any search of Morton's cell phones.[318]

Upturn, Inc., a nonprofit focused on the use of technology in the criminal legal system, provided a brief concentrated primarily on the availability of forensic tools that could effectuate the court's holding in *Morton I*.[319] In seeking to rebut the Government's claims regarding the impracticality of authorizing narrow searches, Upturn detailed the mechanics of the forensic software that have "built-in pre- and post-extraction filtering and categorization features, all of which can be used to narrow the search of cellphone data," including categorizing data in various ways, such as by source application, file type, or date.[320] These features can allow law enforcement to access more discrete categories of data, while preserving Fourth Amendment protections by either preventing the extraction or facilitating the deletion of data that is nonresponsive to the scope of the warrant.[321] Similarly, Upturn argued a more restrictive approach to cell phone searches, like one required by the initial panel decision, was consistent with the court's intentions in *Riley*: "It cannot be the case that to preserve *Riley*, law enforcement must be afforded the same kind of unbridled discretion that the court rejected in *Riley*."[322] Upturn urged the court, on rehearing, to intervene to ensure that forensic software are employed to protect individuals from exhaustive and indiscriminate searches, rather than employed to facilitate "searches of cellphones that fundamentally sit at odds with the protections of the Fourth Amendment."[323]

2. *Morton II* Analysis

The Fifth Circuit vacated the original panel decision and granted the motion for rehearing en banc in May of 2021.[324] More than fifteen months later, the circuit issued a new opinion that reached the opposite conclusion of the original panel and affirmed the district court's decision not to suppress the photographic evidence found on Morton's cell phones as the admissibility of the evidence was protected by the officers' good-faith

315. *Id.* at 13.

316. *Id.* at 14 ("Drug dealers often keep controlled substances in their homes, purses, or cars, but police are not generally permitted to search these places without investigation-specific reasons to believe evidence will be found in those places.").

317. *Id.* at 19 (quoting Riley v. California, 573 U.S. 373, 395, 396, 399 (2014)).

318. *Id.* at 27–28.

319. Upturn Brief, *supra* note 312, at 1–2; *see also* discussion of MDFTs, *supra* Part III.E.

320. Upturn Brief, *supra* note 312, at 10.

321. *Id.* at 16.

322. *Id.* at 19.

323. *Id.* at 26.

324. United States v. Morton, 996 F.3d 754 (5th Cir. 2021) (mem.).

reliance on search warrants.[325] At the outset, the court clarified that it would not address the degree of privacy secured by citizens under the Fourth Amendment in light of advances in modern technology.[326] Despite recognizing that the development of Fourth Amendment law will be stunted "if courts too often avoid the underlying constitutional question and deny suppression motions based on the good-faith rule," the court found the application of the good-faith exception, rather than a ruling on the validity of the search warrant, to be the most appropriate resolution for the case.[327]

Highlighting suppression as a judicially created remedy rather than a constitutional requirement,[328] the court focused on the exclusionary rule's purpose of deterrence against misconduct by law enforcement, which is generally inapplicable when such officers perform a search under the authority of a warrant.[329] Because the officers relied on warrants issued before the searches of Morton's cell phones, the court next addressed the exceptions to good-faith reliance specifically enumerated in *Leon*.[330]

The court briefly dismissed, in a footnote, the argument that the good-faith exception was inapplicable because the warrants were pretextual, noting that the inquiry regarding probable cause is objective and, therefore, the motive of the officer supplying the affidavit is irrelevant.[331] Focusing instead on the argument that the good-faith exception was inapplicable because the affidavits were bare-boned, the court contrasted the three-page affidavits supplied in support of each warrant—highlighting the specific drugs and drug paraphernalia discovered in Morton's van and the affiant's knowledge that cell phones are utilized in the receipt and delivery of narcotics—with the "wholly conclusory" statements contained in search warrant affidavits in prior Fourth Amendment cases.[332] The court deemed such information sufficient to facilitate an independent probable cause determination by the judge.[333] Thus, the court concluded that Morton's underlying dispute was more appropriately directed at the judge's probable cause determination regarding the sufficiency of user-quantity drug possession evidence to establish probable cause for a cell phone, rather than with the officers' subsequent reliance on the warrants.[334] Regardless, the court noted that "the judge made a judgment call" and "on close calls second guessing the issuing judge is not a basis for excluding evidence."[335]

---

325. *Morton II*, 46 F.4th 331, 339–40 (5th Cir. 2022). One judge from the initial panel, Judge Jolly, chose to stand by the 2021 panel opinion, and the majority opinion also garnered a concurrence and dissent. *Id.* at 333; *id.* at 340 (Higginson, J., concurring); *id.* at 341 (Graves, J., dissenting).

326. *Id.* at 335 (majority opinion) (quoting Kyllo v. United States, 533 U.S. 27, 33–34 (2001)).

327. *Id.* at 335 n.1.

328. *See supra* note 125 and accompanying text.

329. *Morton II*, 46 F.4th at 336.

330. *Id.*

331. *Id.* at 337 n.2. The issue also may not have been adequately preserved for appeal in the district court. *Id.*

332. *Id.* at 337. The concurrence notes, and the majority concedes, that none of the affidavits actually mention the presence of three cell phones in the van, despite the fact that this may be the most compelling justification for a search of any of the cell phones. *Id.* at 338 n.3; *id.* at 340 n.1 (Higginson, J., concurring).

333. *Id.* at 337 (majority opinion).

334. *Id.* at 338.

335. *Id.*

Lastly, the court found that Morton had failed to preserve the claim that good faith should be analyzed separately for each area to be searched, as the argument was not raised in the district court and was absent from his initial appellate brief.[336] The court further noted that, even if the issue had been appropriately raised, it would not change the good-faith analysis, which views the affidavit in its entirety to determine whether it is bare-boned.[337] In making this determination, the court sidestepped nearly all controversial issues raised by Morton and the initial panel decision in favor of simply affirming the status quo allowing for broad cell phone searches when such searches are authorized by warrants.[338]

The concurrence, though generally affirming the application of the good-faith exception, in this case, made two noteworthy contributions.[339] First, it highlighted concern regarding how seemingly low the bar is to establish probable cause for a cell phone, noting that "if the fact that the arrestee was carrying a cell phone at the time of arrest is sufficient to support probable cause for a search, then the warrant requirement is merely a paperwork requirement."[340] The concurrence, critiquing this possibility, commented "[i]t cannot be that *Riley*'s holding is so hollow."[341] The concurring opinion's second contribution was to note the importance of continued innovation regarding mechanisms designed to preserve Fourth Amendment protections, though it did not advocate for any particular development.[342]

The dissent disparaged the trend of allowing the good-faith exception to serve as a safe haven for tenuous probable cause determinations, particularly given the Fifth Circuit practice of first deciding whether the good-faith exception applies before turning to the Fourth Amendment analysis, if at all.[343] The dissent further criticized the insufficient nexus between the authorized search and the evidence sought, asserting that such a lack of nexus should have been dispositive as to the existence of probable cause as well as prohibited good-faith reliance on a warrant under the good-faith exception.[344] To contextualize these issues, the dissent highlighted that a traffic stop "that produced evidence of a marginal offense" was adequate to sanction the search of all of the information stored on Morton's cell phones primarily through sweeping generalizations about the nature of criminal activities and cell phone usage.[345] In failing to rule on the sufficiency of the probable cause determination or demand greater correlation between the alleged offense and the probability of evidence on the cell phone, the dissent argued that the court was condoning "unjust, unfair, and unconstitutional" practices by law enforcement.[346]

336. *Id.* at 339.
337. *Id.*
338. *See id.* at 339–40.
339. *Id.* at 340 (Higginson, J., concurring).
340. *Id.*
341. *Id.*
342. *Id.* at 341
343. *See id.* at 341–42 (Graves, J., dissenting).
344. *Id.* at 342–43.
345. *Id.*
346. *Id.* at 343–44.

IV. PERSONAL ANALYSIS

Many were caught off guard by the Firth Circuit's decision in *Morton I* requiring distinct probable cause determinations for each category or location of information on a cell phone, with some calling the decision "remarkable."[347] In issuing the category-specific probable cause requirement, the court did not actually address the primary question raised by the parties' briefs on appeal—whether the allegedly pretextual nature of the affidavits (purportedly searching for evidence of drug trafficking, rather than child pornography) provided in support of the search warrants was sufficient to prohibit a finding of good-faith reliance under *Leon*.[348] Instead, rather than limiting the decision to the facts of Morton's conviction, the decision could have fundamentally altered procedural requirements relating to all warrants for cell phones issued within the Fifth Circuit.

Not all expressed enthusiasm regarding the *Morton I* court's reasoning—opinions differ drastically regarding if and how particularity with respect to digital devices should be interpreted.[349] Law enforcement is often unable to precisely predict where in a phone evidence may be located, causing some to voice concerns that the rigidity of the court's ruling could handicap law enforcement while incentivizing those engaged in criminal activities to simply hide digital evidence more effectively.[350] In response to the decision, Orin Kerr argued that the court's attempt to require more narrowly tailored warrants for cell phones confused the relevant probable cause determination—mistakenly focusing on limiting the scope of the search rather than upholding Fourth Amendment protections through constraints on the substantive use of the uncovered, nonresponsive evidence made available to law enforcement under the plain view doctrine.[351]

Others were less convinced that issues of administrative and technological convenience sufficiently overshadow the privacy interests implicated in cell phone searches.[352] Applauding the court's *Morton I* ruling, the Electronic Privacy Information Center, along with the American Civil Liberties Union and the Electronic Frontier Foundation, stated that such strict search requirements are necessary to preserve Fourth Amendment protections in the wake of dramatic technological changes.[353] Others suggested that existing technological capabilities can facilitate thorough digital searches for particular information while maintaining the privacy of nonresponsive data.[354] Though establishing the requirement for warrants to apply only to distinct categories of information within a cell phone may have been an imperfect and novel solution, the *Morton I* decision suggested that the court was willing to take an important step towards ensuring Fourth Amendment protections are upheld as technology continues to advance.

---

347. Orin S. Kerr, *Remarkable New Fifth Circuit Decision Limiting Cell Phone Searches*, VOLOKH CONSPIRACY (Jan. 10, 2021, 5:20 PM), https://reason.com/volokh/2021/01/10/remarklable-new-fifth-circuit-decision-limiting-cell-phone-searches/ [https://perma.cc/U4YT-RJS6].

348. Appellant's Initial Brief, *supra* note 19, at 1; Appellee's Brief, *supra* note 30, at 1.

349. Kerr, *supra* note 347; Huynh, *supra* note 186, at 209.

350. *See* Huynh, *supra* note 186, at 198–99.

351. Kerr, *supra* note 347 (advocating instead for use restrictions on nonresponsive data).

352. *See, e.g.*, Brief of EFF, ACLU, and EPIC, *supra* note 312, at 3.

353. *Id.*

354. Upturn Brief, *supra* note 312, at 16.

Cell phones are ubiquitous; ninety-seven percent of Americans own a cell phone, and eighty-five percent own a smartphone.[355] As such, most individuals carry an amount of personal data on their person inconceivable only a couple decades ago.[356] Cell phones often contain information regarding an individual's communications, associations, and physical movements, as well as more discrete personal information such as financial transactions, methods of transportation, and personal notes.[357] It is, therefore, easy to assume that some amount of evidence related to alleged criminal activity may be documented on the device.[358] However, the vast majority of the data available on a cell phone is unlikely to be responsive or incriminating in nature.[359] *Riley* recognized this fundamental shift and attempted to restore balance between the interests of individuals and law enforcement by removing cell phones from effects found during a search incident to arrest that could be presumptively searched without a warrant.[360] *Riley* also required a magistrate to issue a warrant authorizing the search based on probable cause.[361] However, *Riley*'s holding did not address the uncertainty and confusion regarding the amount of specificity required within the warrant itself.[362] The particularity requirement of the Warrant Clause is intended to protect individuals from unreasonable searches, including rendering general warrants insufficient to facilitate a search by limiting the scope of the areas to be searched and the types of evidence sought.[363] Thus far, the particularity requirement has not appeared to provide any strong protections against broad search warrants in the authorization to search cell phones—a result that is plainly evident in the *Morton II* court's refusal to opine on the scope of the authorized warrants.[364]

While some courts have employed significant scrutiny in the issuance and review of search warrants for cell phones and digital devices, others have ignored fatally broad warrants due to a desire to avoid suppression.[365] In the case of warrants that are arguably overly broad or lack particularity, such as the warrants at issue in Morton's case, the admission of evidence under the good-faith exception has allowed ambiguity surrounding cell phone warrants to quietly persist.[366] Such persistent ambiguity is due, at least in part, to the ability of the exception to provide legal justification for the admission of evidence either unsupported by probable cause or unconstitutionally vague in violation of the particularity requirement.[367] Due to the uncertainty and complexity

355. *Mobile Fact Sheet*, *supra* note 1.

356. *See* Riley v. California, 573 U.S. 373, 386, 395 (2014).

357. *See id.* at 395–96; Banko, *supra* note 190, at 575.

358. *See* Banko, *supra* note 190, at 575.

359. *See* Kerr, *supra* note 192, at 6–7.

360. *See Riley*, 573 U.S. at 386 (noting the "significantly diminished" privacy interests, safety concerns, and potential evidence destruction used to justify exception in *Robinson* were absent from cell phone searches).

361. *See id.*; Huynh, *supra* note 186, at 194.

362. *See generally Riley*, 573 U.S. 373.

363. Maryland v. Garrison, 480 U.S. 79, 84 (1987).

364. *See Morton II*, 46 F.4th 331, 339–40 (5th Cir. 2022); Gershowitz, *supra* note 188, at 599.

365. Huynh, *supra* note 186, at 209.

366. *See, e.g.*, *Morton II*, 46 F.4th at 339–40; United States v. Sibley, 448 F.3d 754, 758 (5th Cir. 2006); Gershowitz, *supra* note 188, at 585.

367. *See* Gershowitz, *supra* note 188, at 585. This is particularly exacerbated by the order in which courts in the Fifth Circuit evaluate cases for the applicability of the good-faith exception, first seeking to determine

surrounding digital search warrants, courts have forgiven a lack of scrutiny by officers in executing flawed warrants.[368] This has been true even in cases where law enforcement officers were searching for singular, discrete pieces of evidence.[369]

In the absence of practical guidance from courts or law enforcement departments, broad searches of individuals' cellular devices authorized by warrants have become routine.[370] According to documents gathered by the nonprofit Upturn,[371] comprehensive extraction technology is employed as an investigative tool in a wide variety of low-level offenses, including "graffiti, shoplifting, marijuana possession, prostitution, vandalism, car crashes, parole violations, petty theft, public intoxication, and the full gamut of drug-related offenses."[372] Many of these offenses bear no direct relation to an individual's cell phone, other than speculation that there may be documentation or communication regarding the crime on the phone.[373] Furthermore, because of the technological forensic tools utilized and general lack of oversight, these searches frequently resemble the long-unfavored general warrants prohibited by the Fourth Amendment.[374] These concerns about overbreadth are amplified by the acknowledgment that defendants and their attorneys have little, if any, opportunity to audit the conduct of a search to determine whether any meaningful steps to constrain the scope of the search were made during execution.[375]

Therefore, it is clear that simply requiring law enforcement to obtain a warrant to search a cell phone has done little to effectively limit law enforcement access to the data contained in a cell phone in the spirit of the protections discussed in *Riley*. Importantly, the harms of this ambiguity extend beyond the Fourth Amendment violations of those whose data is improperly viewed. In cases where warrants are found to be overbroad or to lack particularity, and the good-faith exception is deemed inapplicable, the societal cost may be high; litigation drains court resources, evidence of criminal activity is suppressed, and potentially dangerous individuals are released.[376] Even when the evidence uncovered is ultimately deemed admissible, significant private and public resources can be expended in making such a determination.[377]

Due to the variety of ways in which criminals may disguise the location of relevant information on their cell phones, many appear hesitant to authorize anything short of

---

whether there was good-faith reliance by law enforcement officers before, potentially, turning to the issue of whether probable cause actually existed. *See Morton II*, 46 F.4th at 341–42 (Graves, J., dissenting).

368. *See* Gershowitz, *supra* note 188, at 590.

369. *See id.* at 589 (citing People v. Watkins, 994 N.Y.S.2d 816, 817 (N.Y. Sup. Ct. 2014)) (describing a case in New York in which a judge upheld a warrant officers received to search for a video a suspect was taking on their iPhone at the time of arrest—despite the fact that the circumstances of the arrest afforded the suspect no time to strategically hide video, the warrant authorized a search of the entire contents of the phone).

370. *See id.* at 599.

371. Upturn is a nonprofit organization with the goal of "advanc[ing] equity and justice in the design, governance, and use of digital technology." KOEPKE ET AL., *supra* note 7, at 2.

372. *Id.* at 42.

373. *Id.*

374. *See id.* at 62.

375. *See id.* at 51.

376. Huynh, *supra* note 186, at 219.

377. Consider the resources expended throughout the lifespan of Morton's case. *See generally Morton II*, 46 F.4th 331 (5th Cir. 2022).

sweeping searches of cell phones.[378] In many cases, however, the types of evidence legitimately sought are of a limited nature.[379] Mandating narrower, more focused initial searches, like the categorical requirement enumerated in *Morton I*, would not necessarily prevent law enforcement from accessing information in more discrete or disguised locations not included in an initial warrant. Should incriminating information be found in the initial search, it may be included in affidavits in support of subsequent warrants for more expansive searches.[380] It also follows from the Massachusetts Supreme Judicial Court's discussion in *Snow*[381] that if the initial search proves unsuccessful, law enforcement can return to the magistrate for additional authorization to search other locations on the phone, provided there is still probable cause to believe evidence is stored within the device.[382] Given the method of data extraction currently employed in cell phone searches, there is little reason such a delay in receiving broader search authorization would be detrimental to the investigation.[383] Such detriment is particularly unlikely when a complete copy of the device's data is downloaded by law enforcement during the execution of the initial search.[384] Additionally, depending on the nature of the crime, it may be plausible that probable cause exists to support a search of the entire phone without restriction.[385] The *Morton I* holding similarly did not discount the possibility that the unique facts of a particular case may create probable cause for unrestricted review of the entire device; evidence of simple drug possession, however, should not be sufficient to support such a search.

To be clear, though the holding in *Morton I* took a step towards preserving Fourth Amendment protections, the decision would not have entirely alleviated the ambiguity surrounding particularity in search warrants for cell phones. Though the court attempted to require greater particularity in search warrants by referring to limitations by "category of content,"[386] "category of information,"[387] or "cell phone feature,"[388] it is unclear how this standard would have been applied in practice. The court failed to clearly define these terms or articulate whether these restrictions are intended to limit the object of the search or the locations on the cell phone where law enforcement may search for the relevant evidence. It is also unclear if this type of restriction would require more explicit search procedures or whether officers would still be permitted to sift through most, if not all, data contained on the device in search of the type of information described by the search

378. *See* Sacharoff, *supra* note 220, at 1643.

379. *See* Gershowitz, *supra* note 188, at 632.

380. Commonwealth v. Snow, 160 N.E.3d 277, 288 (Mass. 2021).

381. *See supra* Part III.F.2.

382. *See Snow*, 160 N.E.3d at 288 (suggesting that officers may utilize any information gathered in the initial search to support more expansive search authority); *see also* Gershowitz, *supra* note 188, at 636 (noting that subsequent warrants are commonly issued in computer search cases).

383. Gershowitz, *supra* note 188, at 636 n.260 (comparing digital device searches to traditional searches of physical locations).

384. *See* Kerr, *supra* note 192, at 6.

385. Gershowitz, *supra* note 188, at 608.

386. *Morton I*, 984 F.3d 421, 426 (5th Cir. 2021), *rev'd en banc*, 46 F.4th 331 (5th Cir. 2022).

387. *Id.*

388. *Id.* at 427.

warrant. Therefore, the viewing of nonresponsive data would have likely remained prevalent and admissible under the plain view doctrine.

Despite these uncertainties, the holding in *Morton I* represented one court's attempt to remedy the ambiguity surrounding the proper application of the warrant requirement to cell phones. As technology advances, there is often a need to review and revise doctrine to ensure such protections remain available.[389] Due to the nature of the privacy interests at stake and the societal costs of evidence suppression and overturned convictions, law enforcement practice should err on the side of caution when requesting and executing search warrants for digital devices. It is not sufficient to hope that fruits of broad searches can be salvaged by the good-faith exception or that ex post deferential review of the magistrate's finding of probable cause declines to sanction questionable searches. In 2016, Adam Gershowitz wrote that "[u]ntil appellate courts signal a more robust particularity guarantee for post-*Riley* cell phone search warrants, . . . confusion and erroneous rulings are likely to continue in numerous other cases."[390] Since then, the technological capabilities of digital devices have expanded, allowing for overly broad searches to inflict even greater harms to privacy interests while threatening to undermine the judicial process.[391] The holding in *Morton I*, therefore, represented a necessary progression in Fourth Amendment jurisprudence to better protect the constitutional rights of individuals while allowing the judicial process to effectively prosecute criminal activities on the basis of lawfully obtained evidence; by contrast, the *Morton II* decision elected to only briefly acknowledge existing problems while perpetuating the analytical processes which facilitate a lack of progress at the expense of constitutional protections. It is unfortunate that the Fifth Circuit retreated so quickly in favor of allowing the good-faith exception to alleviate the consequences of ambiguous jurisprudence.

V. CONCLUSION

Though *Morton I* attracted controversy, the Fifth Circuit's holding represented a valuable attempt to address the uncertainty surrounding Fourth Amendment protections in the digital context. Technological advancements complicate established doctrines. The modern technological landscape demands that courts re-evaluate available mechanisms to balance protections for individual rights with the investigative needs of law enforcement. For cell phones, this means requiring greater specificity and particularity in search warrants delineated by locations or categories of information as outlined in *Morton I*. Doing so will ensure that law enforcement officers are not inadvertently authorized to conduct unconstitutional, overly broad searches and that Fourth Amendment protections are preserved in digital spaces.

389. *See* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 480 (2011).

390. *See* Gershowitz, *supra* note 188, at 608.

391. *See* Kerr, *supra* note 192, at 20.