Michigan Supreme Court
Lansing, Michigan

Syllabus

This syllabus constitutes no part of the opinion of the Court but has been prepared by the Reporter of Decisions for the convenience of the reader.

PEOPLE v HUGHES

Docket No. 158652. Argued on application for leave to appeal October 7, 2020. Decided December 28, 2020.

Following a jury trial, Kristopher A. Hughes was convicted in the Oakland Circuit Court, Hala Jarbou, J., of armed robbery, MCL 750.529, and was sentenced as a fourth-offense habitual offender, MCL 769.12, to 25 to 60 years in prison. On the evening of August 6, 2016, Ronald Stites was at his home with Lisa Weber, whom he had met earlier that day. Weber had agreed to spend the night with Stites and perform sexual acts in exchange for money. At some point during the evening, Weber called a drug dealer known as "K-1" or "Killer" in order to obtain drugs and asked him to come to Stites's residence. A man arrived at the residence, sold Stites and Weber crack cocaine, and departed. Later that night, the drug seller returned to Stites's home with a gun and stole a safe that was located in Stites's bedroom. Weber later identified defendant as the drug dealer and robber, but Stites was not able to identify the perpetrator. A detective submitted a warrant affidavit to search defendant's property for evidence related to separate allegations of drug trafficking. The affidavit included information from a criminal informant that defendant and another man were dealing drugs, and the detective asserted that drug traffickers commonly use mobile phones and other electronic equipment in the course of their activities. The district court, Cynthia Thomas Walker, J., concluded that there was sufficient probable cause to support a search warrant and authorized a warrant to search three properties and a vehicle connected with defendant. While executing a search at one of the addresses identified in the warrant, the police detained defendant and seized a cell phone found on his person. Another detective performed a forensic examination of the phone and extracted all of the phone's data. The extraction software separated the data into categories, including photographs, call logs, and text messages. According to the detective, the software also enabled police to search the data for search terms or specific phone numbers. About a month after the data was extracted, the prosecutor in the armed-robbery case against defendant asked the detective to conduct a second search of defendant's cell-phone data for contacts with the phone numbers of Stites and Weber; for the names "Lisa," "Kris," or "Kristopher"; and for the word "killer." These searches revealed several calls and text messages between defendant and Weber on the night that Stites was robbed, including text messages from Weber to defendant indicating the location of Stites's home, that the home was unlocked, and that it had a flat-screen TV. After his conviction, defendant appealed, arguing that the phone records should have been excluded from the trial because the warrant that authorized the search of his phone's data permitted officers to search for evidence of drug trafficking, not armed robbery. Defendant also argued that trial counsel was ineffective for failing to object to the admission of

the data on Fourth Amendment grounds. The Court of Appeals, TUKEL, P.J., and BECKERING and SHAPIRO, JJ., rejected these arguments and affirmed defendant's conviction in an unpublished per curiam opinion. Defendant sought leave to appeal in the Supreme Court, which ordered oral argument on the application. 505 Mich 855 (2019).

In a unanimous opinion by Justice MARKMAN, the Supreme Court, in lieu of granting leave to appeal, *held*:

1. The Fourth Amendment of the United States Constitution protects against unreasonable searches and seizures. Although a warrant is not always required before a search or seizure, there is a strong preference for searches conducted pursuant to a warrant, and the general rule is that police officers must obtain a warrant for a search to be reasonable under the Fourth Amendment. Under *Riley v California*, 573 US 373 (2014), general Fourth Amendment principles apply with equal force to searches of cell-phone data. In this case, the issue was whether officers violated the Fourth Amendment when they searched defendant's cell phone for *evidence of armed robbery* without obtaining a new warrant when the phone was seized pursuant to a warrant authorizing the search of the phone's data for *evidence of drug trafficking*. The prosecutor argued that defendant lost the reasonable expectation of privacy in his cell-phone data when the phone was seized and the data was searched pursuant to the drug-trafficking warrant. However, under *Riley*, citizens generally maintain a reasonable expectation of privacy in their cell-phone data that is not extinguished merely because a phone is seized during a lawful arrest. Further, the seizure and search of cell-phone data pursuant to a warrant does not extinguish an otherwise reasonable expectation of privacy in the entirety of the seized data. Rather, a warrant authorizing the police to seize and search cell-phone data allows officers to examine the seized data only to the extent reasonably consistent with the scope of the warrant. In this case, the warrant authorized officers to search defendant's cell-phone data for evidence of drug trafficking as described by the warrant and affidavit. Any further review of the data beyond the scope of the warrant constituted a search that was presumptively invalid under the Fourth Amendment.

2. In considering the Fourth Amendment's requirements for a search of digital data authorized by a warrant, as with any other search conducted pursuant to a warrant, a search of digital data must be reasonably directed at uncovering evidence of the criminal activity alleged in the warrant. Any search that is directed instead toward finding evidence of other, unrelated criminal activity is beyond the scope of the warrant. Under the Fourth Amendment, a warrant must state with particularity not only the items to be searched and seized, but also the alleged criminal activity justifying the warrant. Although the prosecutor argued that the search for evidence of armed robbery fell within the scope of the warrant because the warrant authorized officers to review the entire report that represented the totality of defendant's cell-phone data, the warrant authorized a search of the data for evidence of drug trafficking, not armed robbery. Moreover, the affidavit supporting the warrant did not even mention armed robbery, let alone seek to establish probable cause that defendant committed that offense. While officers are not required, when executing a search of digital data, to review only digital content that a suspect has identified as pertaining to criminal activity, neither is it always reasonable for an officer to review the entirety of the seized digital data on the basis that incriminating information could conceivably be found anywhere on the device. Accordingly, an officer's search of seized digital data must be reasonably directed toward finding evidence of the criminal activity identified in the warrant. In this case, about a month after officers searched defendant's digital data for evidence of drug trafficking, the

prosecutor in the armed-robbery case asked a detective to conduct a focused search of the data for terms pertaining to the armed-robbery case. There was no evidence that a search for these terms would uncover evidence relating to defendant's drug-trafficking activity, nor was there any evidence that defendant hid or manipulated his data to conceal evidence related to drug trafficking. Therefore, the second search of the data was not reasonably directed toward obtaining evidence of drug trafficking and exceeded the scope of the warrant. Accordingly, the second review of the data constituted a warrantless search that violated the Fourth Amendment, and the case had to be remanded to the Court of Appeals for that Court to reconsider defendant's claim of ineffective assistance of counsel and to determine whether defendant was entitled to relief.

Reversed and remanded.

Justice VIVIANO, concurring, agreed with the majority that the second search of defendant's cell-phone data was unlawful under the Fourth Amendment but wrote separately to emphasize his view that a law enforcement officer's subjective intent when searching seized digital data should be included as a potentially dispositive factor when a court considers whether a search was reasonably directed at finding evidence of the criminal activity identified in the warrant. Justice VIVIANO argued that if the search was purposefully conducted to obtain evidence of a crime other than the one identified in the warrant, a court could not conclude that the search was reasonably directed at uncovering evidence of the criminal activity alleged in the warrant. In this case, Justice VIVIANO would find this factor dispositive since it was clear that the second search of defendant's cell-phone data was conducted to obtain evidence of a crime other than drug trafficking, the offense identified in the warrant. Therefore, before conducting the second search of defendant's cell phone, the officer should have obtained a second search warrant directed toward obtaining evidence of the armed-robbery offense. Because he did not, the second search was unlawful.

Michigan Supreme Court
Lansing, Michigan

OPINION

FILED December 28, 2020

STATE OF MICHIGAN

SUPREME COURT

PEOPLE OF THE STATE OF MICHIGAN,

Plaintiff-Appellee,

v No. 158652

KRISTOPHER ALLEN HUGHES,

Defendant-Appellant.

BEFORE THE ENTIRE BENCH

MARKMAN, J.

The issue presented here is whether, when the police obtain a warrant to search digital data from a cell phone for evidence of a crime, they are later permitted to review that same data for evidence of another crime without obtaining a second warrant. We conclude-- in light of the particularity requirement embodied in the Fourth Amendment and given meaning in the United States Supreme Court's decision in *Riley v California*, 573 US 373; 134 S Ct 2473; 189 L Ed 2d 430 (2014) (addressing the "sensitive" nature of cell-phone data)-- that a search of digital cell-phone data pursuant to a warrant must be

reasonably directed at obtaining evidence relevant to the criminal activity alleged in *that* warrant. Any search of digital cell-phone data that is not so directed, but instead is directed at uncovering evidence of criminal activity not identified in the warrant, is effectively a warrantless search that violates the Fourth Amendment absent some exception to the warrant requirement. Here, the officer's review of defendant's cell-phone data for incriminating evidence relating to an armed robbery was not reasonably directed at obtaining evidence regarding drug trafficking-- the criminal activity alleged in the warrant-- and therefore the search for that evidence was outside the purview of the warrant and thus violative of the Fourth Amendment. Accordingly, we reverse the judgment of the Court of Appeals and remand to that Court to determine whether defendant is entitled to relief based upon the ineffective assistance of counsel.[1]

I. FACTS & HISTORY

The circumstances of this case arise from concurrent criminal prosecutions against defendant Kristopher Hughes, one related to drug trafficking and the other related to armed robbery. MCL 750.529. Defendant pleaded no contest to the drug-trafficking charges and

[1] Because we conclude that the Fourth Amendment was breached when officers searched a cell phone for evidence of *armed robbery* without having obtained a second warrant when the phone had been seized based upon a warrant for *drug trafficking*, we need not decide (a) whether the warrant affidavit sufficiently connected defendant's cell phone to his drug trafficking or (b) the broader question as to what evidence set forth in an affidavit sufficiently connects a cell phone to alleged criminal activity to support the issuance of a warrant to search the phone's digital contents. We only address the proper manner of searching digital data when such data has been seized pursuant to a valid warrant.

these pleas are not the subject of this appeal.[2] Defendant went to trial on the armed-robbery charge, and after two mistrials due to hung juries, he was convicted of the armed robbery of Ronald Stites.

On August 6, 2016, Stites was going for a walk when he met Lisa Weber. The two talked, and Stites invited Weber back to his home. At Stites's residence, Weber offered to stay with Stites all night and to perform sexual acts in exchange for $50. Stites agreed, and Weber followed him into his bedroom, where he opened a safe containing $4,200 in cash and other items and pulled out a $50 bill that he agreed to give her after the night was over. Stites then performed oral sex on Weber. Afterward, Weber went to the store to get something to drink. Approximately 15–20 minutes later, she called a drug dealer, who went by the name of "K-1" or "Killer," and asked that he come over and sell drugs to her and Stites. Sometime thereafter, a man arrived at Stites's home, sold Weber and Stites crack cocaine, and then departed. Weber and Stites consumed some of the drugs and continued their sexual activities. Later in the evening, the man who had sold the drugs returned to the home with a gun and stole Stites's safe at gunpoint. Stites testified that Weber assisted in the robbery and departed the home with the robber, while Weber asserted

---

[2] On February 2, 2017, defendant pleaded no contest to two counts of delivery and manufacture of a controlled substance, second or subsequent offense, MCL 333.7401(2)(b)(ii), possession of marijuana, MCL 333.7403(2)(d), possession of suboxone, MCL 333.7403(2)(b)(ii), possession of alprazolam, MCL 333.7403(2)(b)(ii), and possession of dihydrocodeine pills, MCL 333.7403(2)(b)(ii), as a habitual fourth offender. He was sentenced to concurrent prison terms of 36 months to 30 years, 12 to 24 months, and 24 months to 15 years. Defendant appealed and the Court of Appeals denied his application for lack of merit. *People v Hughes*, unpublished order of the Court of Appeals, entered September 28, 2017 (Docket No. 339858). Defendant did not seek leave to appeal in this Court.

that she did not assist in the robbery and only complied with the robber's demands to avoid being harmed. Weber identified defendant as the perpetrator, while Stites could not identify defendant as the perpetrator.

On August 11, 2016, Detective Matthew Gorman submitted a warrant affidavit to search defendant's property for evidence related to separate criminal allegations of drug trafficking. Detective Gorman's affidavit included information from a confidential informant that defendant and an associate named Patrick Pankey were dealing drugs. The warrant affidavit also asserted that as a product of Detective Gorman's experience and training, "drug traffickers commonly use electronic equipment to aid them in their drug trafficking activities. This equipment includes, but is not limited to, . . . mobile telephones . . . ." The warrant affidavit contained no information indicating that Weber was involved in defendant's drug trafficking and did not refer to the previous week's armed robbery at Stites's residence.

The district court judge concluded that there was probable cause for the warrant based upon the attached affidavit and thereby issued a warrant authorizing the police to search three residences that were connected with defendant and his vehicle for further evidence of drug trafficking. As relevant here, the warrant provided:

> [A]ny cell phones or . . . other devices capable of digital or electronic storage seized by authority of this search warrant shall be permitted to be forensically searched and or manually searched, and any data that is able to be retrieved there from shall be preserved and recorded.

The warrant also contained the following limitation:

> Therein to search for, seize, secure, tabulate and make return according to law, the following property and things:

> Crack Cocaine, and any other illegally possessed controlled substances; any raw material, product, equipment or drug paraphernalia for the compounding, cutting, exporting, importing, manufacturing, packaging, processing, storage, use or weighing of any controlled substance; proofs of residence, such as but not limited to, utility bills, correspondence, rent receipts, and keys to the premises; proofs as to the identity of unknown suspects such as but not limited to, photographs, certificates, and/or diplomas; prerecorded, illegal drug proceeds and *any records pertaining to the receipt, possession and sale or distribution of controlled substances including but not limited to documents, video tapes, computer disks, computer hard drives, and computer peripherals*; other mail receipts, containers or wrappers; currency, property obtained through illegal activity, financial instruments, safety deposit box keys, money order receipts, bank statements and related records; firearms, ammunition, and all occupants found inside. [Emphasis added.]

On August 12, 2016, police were executing a search at one of the addresses set forth in the warrant when they detained defendant and seized a phone that was on his person. On August 17, 2016, defendant was arraigned on the charge of armed robbery.

On August 23, 2016, Detective Edward Wagrowski performed a forensic examination of the phone that was seized from defendant, and all of its data was extracted using Cellebrite, software used for extracting digital data. Upon extraction, Cellebrite separated and sorted the device's data into relevant categories by, for example, placing all of the photographs together in a single location. The extraction process resulted in a 600-page report of defendant's cell-phone data, which included more than 2,000 call logs, more than 2,900 text messages, and more than 1,000 photographs. Detective Wagrowski testified at trial that Cellebrite enabled police to enter search terms to isolate data from specific phone numbers or that contained specific words or phrases. If there were no contacts between a searched number and the device being searched, the searcher would receive no results and the software would show a blank screen. It is unclear from the record

whether and to what extent the data extracted from the cell phone was reviewed for evidence of defendant's drug trafficking.

A month or so after the initial extraction, at the request of the prosecutor in defendant's armed-robbery case, Detective Wagrowski conducted further searches of the cell-phone data for: (a) contacts with the phone numbers of Weber and Stites and (b) the name "Lisa," variations on the word "killer" (defendant's nickname), and the name "Kris/Kristopher" (defendant's actual name). These searches uncovered 19 calls between defendant and Weber on the night of the robbery and 15 text messages between defendant and Weber between August 5, 2016 and August 10, 2016. Weber's texts to defendant leading up to the robbery included communications indicating where Stites's home was located, that the home was unlocked, and that there was a flat screen TV in the home. Defendant sent texts to Weber on the night of the robbery asking her to "[t]ext me or call me" and to "open the doo[r]." None of the text messages with the words "killer" or "Kris" were from Weber's number. The prosecutor acknowledged that the results of these searches served as evidence at defendant's armed-robbery trials. Defense counsel objected to the admission of this evidence, arguing that it was "not relevant" and "stale," but the trial court overruled his objection.

Defendant's first two trials on the armed-robbery charge resulted in mistrials due to hung juries. A juror note from the first trial explained that the jury was divided and could not reach a verdict because "Mr. Stites was not able to positively ID Mr. Hughes" and "Mrs. Weber's testimony was not credible (according to some) and she was the only one to positively identify Mr. Hughes from that night." Similarly, a juror note from the second trial listing the jurors' concerns about the evidence stated that "100% of Lisa W[eber's]

testimony is untrue" and further noted the "d[i]screpancy of [defendant's] description by Ron Stites." At defendant's third trial, the prosecutor-- while acknowledging that the jury might have "concerns" regarding Weber's credibility as a "disputed accomplice" to the armed robbery-- argued during both opening and closing statements that the text messages and phone calls discovered on defendant's cell phone bolstered her testimony and established a link between defendant and the armed robbery. The jury at defendant's third trial convicted him of armed robbery, and he was sentenced to 25 to 60 years in prison.

Defendant appealed his conviction, arguing in relevant part that (a) the phone records should have been excluded from trial because the warrant supporting a search of the data only authorized a search for evidence of drug trafficking and not armed robbery and (b) trial counsel had been ineffective in failing to object to the data's admission under the Fourth Amendment. The Court of Appeals rejected these arguments and affirmed defendant's conviction. *People v Hughes*, unpublished per curiam opinion of the Court of Appeals, issued September 25, 2018 (Docket No. 338030). Defendant then sought leave to appeal in this Court, and we ordered oral argument on the application. *People v Hughes*, 505 Mich 855 (2019).[3]

---

[3] The Court asked the parties to address specifically:

> (1) whether the probable cause underlying the search warrant issued during the prior criminal investigation authorized police to obtain all of the defendant's cell phone data; (2) whether the defendant's reasonable expectation of privacy in his cell phone data was extinguished when the police obtained the cell phone data in a prior criminal investigation; (3) if not, whether the search of the cell phone data in the instant case was within the scope of the probable cause underlying the search warrant issued during the prior criminal investigation; (4) if not, whether the search of the cell phone data in the instant case was lawful; and (5) whether trial counsel was

II. STANDARD OF REVIEW

Questions of constitutional law are reviewed de novo. *People v Hall*, 499 Mich 446, 452; 884 NW2d 561 (2016). Defendant did not object to the admission of the evidence from his cell phone under the Fourth Amendment, so this issue is unpreserved. See *People v Kimble*, 470 Mich 305, 309; 684 NW2d 669 (2004). Unpreserved constitutional claims are reviewed for plain error. *People v Carines*, 460 Mich 750, 764; 597 NW2d 130 (1999).[4] Defendant does not argue that he is entitled to relief under this standard but rather argues that trial counsel was ineffective for failing to object under the Fourth Amendment. The standards for "plain error" review and ineffective assistance of counsel are distinct, and therefore, a defendant can obtain relief for ineffective assistance of counsel even if he or she cannot demonstrate plain error. See generally *People v Randolph*, 502 Mich 1; 917 NW2d 249 (2018).

III. ANALYSIS

A. FOURTH AMENDMENT

The Fourth Amendment of the United States Constitution provides:

> ineffective for failing to challenge the search of the cell phone data in the instant case on Fourth Amendment grounds. [*People v Hughes*, 505 Mich 855 (2019).]

[4] "To avoid forfeiture under the 'plain error' rule, three requirements must be met: 1) error must have occurred, 2) the error was plain, i.e., clear or obvious, 3) and the plain error affected substantial rights." *Carines*, 460 Mich at 763. If these requirements are satisfied, a court must exercise its discretion and should reverse only if the "forfeited error resulted in the conviction of an actually innocent defendant or when an error seriously affected the fairness, integrity or public reputation of judicial proceedings independent of the defendant's innocence." *Id*. (quotation marks and brackets omitted).

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. [US Const, Am IV.][5]

As indicated by the Fourth Amendment's text, "reasonableness is always the touchstone of Fourth Amendment analysis." *Birchfield v North Dakota*, 579 US ___, ___; 136 S Ct 2160, 2186; 195 L Ed 2d 560 (2016). Thus, a search warrant is not always required before searching or seizing a citizen's personal effects. See, e.g., *Brigham City v Stuart*, 547 US 398, 403; 126 S Ct 1943; 164 L Ed 2d 650 (2006). However, there is a "strong preference for searches conducted pursuant to a warrant," *Illinois v Gates*, 462 US 213, 236; 103 S Ct

---

[5] Similarly, the Michigan Constitution has provided:

> The person, houses, papers and possessions of every person shall be secure from unreasonable searches and seizures. No warrant to search any place or to seize any person or things shall issue without describing them, nor without probable cause, supported by oath or affirmation. . . . [Const 1963, art 1, § 11.]

This provision was recently amended to explicitly protect "electronic data." See Graham, Michigan Radio, *Election 2020: Michigan Voters Approve Proposal 2, Protecting Electronic Data* <https://www.michiganradio.org/post/election-2020-michigan-voters-approve-proposal-2-protecting-electronic-data> (posted November 4, 2020) (accessed November 6, 2020) [https://perma.cc/54KC-6XJY]; 2020 Enrolled Senate Joint Resolution G. "In interpreting our Constitution, we are not bound by the United States Supreme Court's interpretation of the United States Constitution, even where the language is identical." *People v Goldston*, 470 Mich 523, 534; 682 NW2d 479 (2004). However, we have recognized that, at least before its recent amendment, the Michigan Constitution generally has afforded the same protections as those secured by the Fourth Amendment. *People v Slaughter*, 489 Mich 302, 311; 803 NW2d 171 (2011). This is true even though the Michigan Constitution since 1936 has contained an express limitation on the application of the exclusionary rule to violations of Article 1, Section 11. See *Goldston*, 470 Mich at 535 n 8. Defendant, however, has not argued that the Michigan Constitution affords greater protections than the Fourth Amendment in the present context, and therefore our analysis here does not address the recent amendment.

2317; 76 L Ed 2d 527 (1983), and the general rule is that officers must obtain a warrant for a search to be reasonable under the Fourth Amendment. See, e.g., *Riley*, 573 US at 382.

In *Riley v California*, the Supreme Court of the United States held that officers must generally obtain a warrant before conducting a search of cell-phone data. *Riley*, 573 US at 386. In so holding, the Court rejected, with respect to cell-phone data, application of the "search incident to a lawful arrest" exception to the warrant requirement, which generally allows police to search and seize items (including closed containers) located on a person during a lawful arrest. *Id*. at 382-386; *United States v Robinson*, 414 US 218, 234-236; 94 S Ct 467; 38 L Ed 2d 427 (1973). The Court reasoned that the justifications provided in *Chimel v California*, 395 US 752, 762-763; 89 S Ct 2034; 23 L Ed 2d 685 (1969), for this exception to the warrant requirement-- potential harm to officers and the destruction of evidence-- are less compelling in the context of digital data. *Riley*, 573 US at 386.

The Court also noted that a "search incident to a lawful arrest" is justified, at least in part, by "an arrestee's reduced privacy interests upon being taken into police custody." *Id*. at 391. However, it rejected the proposition that an arrestee loses all expectation of privacy, asserting that "when 'privacy-related concerns are weighty enough' a 'search may require a warrant, notwithstanding the diminished expectations of privacy of the arrestee.' " *Id*. at 392, quoting *Maryland v King*, 569 US 435, 463; 133 S Ct 1958; 186 L Ed 2d 1 (2013). The Court held that a warrant was required to search the contents of a cell phone seized during a lawful arrest notwithstanding this reduced expectation of privacy because "[c]ell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person":

> [I]t is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate. Allowing the police to scrutinize such records on a routine basis is quite different from allowing them to search a personal item or two in the occasional case.
>
> Although the data stored on a cell phone is distinguished from physical records by quantity alone, certain types of data are also qualitatively different. An Internet search and browsing history, for example, can be found on an Internet-enabled phone and could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD. Data on a cell phone can also reveal where a person has been. Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building.
>
> Mobile application software on a cell phone, or "apps," offer a range of tools for managing detailed information about all aspects of a person's life. There are apps for Democratic Party news and Republican Party news; apps for alcohol, drug, and gambling addictions; apps for sharing prayer requests; apps for tracking pregnancy symptoms; apps for planning your budget; apps for every conceivable hobby or pastime; apps for improving your romantic life. There are popular apps for buying or selling just about anything, and the records of such transactions may be accessible on the phone indefinitely. There are over a million apps available in each of the two major app stores; the phrase "there's an app for that" is now part of the popular lexicon. The average smart phone user has installed 33 apps, which together can form a revealing montage of the user's life. [*Riley*, 573 US at 393, 395-396 (quotation marks and citations omitted).]

Riley makes clear that, in light of the extensive privacy interests at stake, general Fourth Amendment principles apply with equal force to the digital contents of a cell phone. See *id*. at 396-397 ("[A] cell phone search would typically expose to the government far more than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.").

With this constitutional background in mind, the issue posed in this case is whether officers violated the Fourth Amendment when they searched defendant's cell-phone data in pursuit of evidence that defendant committed an armed robbery when the phone was seized pursuant to a warrant authorizing the search of this data for evidence of unrelated drug trafficking.[6] The prosecutor makes two principal arguments in support of the officer's search of defendant's cell-phone data for evidence of the armed robbery: (a) the warrant to seize and search defendant's cell-phone data for evidence of drug trafficking extinguished

---

[6] Defendant also argues that the district court judge lacked probable cause to authorize the search and seizure of his cell-phone data for evidence of drug trafficking because the probable cause underlying the warrant failed to establish the required nexus between his alleged criminal activity and his cell phone. See *Warden, Maryland Penitentiary v Hayden*, 387 US 294, 307; 87 S Ct 1642; 18 L Ed 2d 782 (1967). He contends that Detective Gorman's opinion, grounded in his training and expertise, that drug traffickers commonly use cell phones to aid in their criminal enterprise was insufficient to provide probable cause that his cell phone would contain evidence of drug trafficking. Cf. *United States v Brown*, 828 F3d 375, 384 (CA 6, 2016) ("[I]f the affidavit fails to include facts that directly connect the residence with the suspected drug dealing activity, . . . it cannot be inferred that drugs will be found in the defendant's home—even if the defendant is a known drug dealer."). In light of the pervasiveness of modern cell-phone use recognized by *Riley*, defendant thus raises a not-unreasonable concern as to the issuance of a warrant to search and seize cell-phone data based solely on the nature of the crime alleged. See *Riley*, 573 US at 399 ("It would be a particularly inexperienced or unimaginative law enforcement officer who could not come up with several reasons to suppose evidence of just about any crime could be found on a cell phone."). On the other hand, there is caselaw to suggest that allegations of drug trafficking are distinct from other alleged criminal activities because cell phones are well-recognized tools of the trade for drug traffickers. See, e.g., *United States v Hathorn*, 920 F3d 982, 985 (CA 5, 2019) ("Cell phones, computers, and other electronic devices are vital to the modern-day drug trade."). Because we conclude that the officer here violated the Fourth Amendment when he searched defendant's cell-phone data for evidence of armed robbery without having obtained a second warrant, we need not decide whether the warrant affidavit provided a sufficient nexus between defendant's drug trafficking and his cell phone. More specifically, we need not decide whether cell phones constitute tools of the trade for drug traffickers such that an affidavit that establishes probable cause of drug trafficking necessarily establishes the required nexus between a suspect's cell phone and the alleged criminal activity.

defendant's reasonable expectation of privacy in all of his data and therefore no search occurred under the Fourth Amendment and (b) the search for evidence of the armed robbery fell within the scope of the warrant issued to search for evidence of drug trafficking because the warrant authorized officers to review all of defendant's data for evidence of drug trafficking and Weber allegedly bought drugs from defendant before the armed robbery. We respectfully find neither argument persuasive.

1. EXPECTATION OF PRIVACY

The first issue is whether defendant lost the reasonable expectation of privacy in his cell-phone data when the cell phone was seized and the data was searched pursuant to the warrant issued in the drug-trafficking case. As this Court has explained:

> A search for Fourth Amendment purposes occurs only when "an expectation of privacy that society is prepared to consider reasonable is infringed." *United States v Jacobsen*, 466 US 109, 113; 104 S Ct 1652; 80 L Ed 2d 85 (1984). "If the inspection by police does not intrude upon a legitimate expectation of privacy, there is no 'search' subject to the Warrant Clause." *Illinois v Andreas*, 463 US 765, 771; 103 S Ct 3319; 77 L Ed 2d 1003 (1983). If a person has no reasonable expectation of privacy in an object, a search of that object for purposes of the Fourth Amendment cannot occur. [*Minnesota v Dickerson*, 508 US 366, 375; 113 S Ct 2130; 124 L Ed 2d 334 (1993)]; *People v Brooks*, 405 Mich 225, 242; 274 NW2d 430 (1979). [*People v Custer*, 465 Mich 319, 333; 630 NW2d 870 (2001).]

It is clear that under *Riley*, citizens maintain a reasonable expectation of privacy in their cell-phone data and this reasonable expectation of privacy does not altogether dissipate merely because a phone is seized during a lawful arrest. The question here is whether the seizure and search of cell-phone data pursuant to a warrant extinguishes that otherwise reasonable expectation of privacy in the entirety of that seized data. We conclude that it does not. Rather, a warrant authorizing the police to seize and search cell-phone data

allows officers to examine the seized data only to the extent reasonably consistent with the scope of the warrant.

The prosecutor argues the seizure of defendant's cell-phone data pursuant to the search warrant eliminated his reasonable expectation of privacy in that data, permitting officers to review all such data without implicating the Fourth Amendment. This argument "overlooks the important difference between searches and seizures." *Horton v California*, 496 US 128, 133; 110 S Ct 2301, 2306; 110 L Ed 2d 112 (1990). "A search compromises the individual interest in privacy; a seizure deprives the individual of dominion over his or her person or property." *Id*. The authority to seize an item does not necessarily eliminate one's expectation of privacy in that item and therefore allow the police to search that item without limitation. See *Jacobsen*, 466 US at 114 ("Even when government agents may lawfully seize . . . a package to prevent loss or destruction of suspected contraband, the Fourth Amendment requires that they obtain a warrant before examining the contents of such a package."); *United States v Chadwick*, 433 US 1, 13 n 8; 97 S Ct 2476; 53 L Ed 2d 538 (1977) ("[T]he [lawful] seizure [of respondents' footlocker] did not diminish respondents' legitimate expectation that the footlocker's contents would remain private."); *Custer*, 465 Mich at 342 ("[W]e do not conclude that, once the police lawfully seize an object from an individual, that individual's reasonable expectation of privacy in that object is altogether lost.") (emphasis omitted). This distinction was also implicitly recognized in *Riley* when the Court held that officers could *seize* a cell phone on a person incident to a lawful arrest but they could not *search* the contents of that phone without a warrant. *Riley*, 573 US at 388, 401. While it may have been reasonable for officers to seize all of defendant's cell-phone data pursuant to the warrant to prevent the destruction of evidence

and to isolate incriminating material from nonincriminating material, it was not necessarily reasonable for police to review that data without limitation.

The prosecutor's reliance on cases holding that a suspect loses all expectation of privacy in items seized from his person during a lawful arrest is inapt. The prosecutor cites *United States v Edwards*, 415 US 800, 801-802, 806; 94 S Ct 1234; 39 L Ed 2d 771 (1974), in which the Supreme Court held that the search and seizure of a suspect's clothes the morning after his arrest was reasonable. The Court recognized that officers could have searched and seized the clothes the defendant wore at the time of his arrest immediately after the arrest and held that a reasonable delay in doing so did not render the search and seizure unreasonable. *Id*. at 805. The Court further commented, "[I]t is difficult to perceive what is unreasonable about the police's examining and holding as evidence those personal effects of the accused that they already have in their lawful custody as the result of a lawful arrest." *Id*. at 806. Relying on *Edwards*, some courts have held that an arrestee lacks any reasonable expectation of privacy in items seized during a lawful arrest and therefore a later examination of those items, even for evidence of a crime other than the crime of arrest, is not a search under the Fourth Amendment. See, e.g., *Wallace v State*, 373 Md 69, 90-94; 816 A2d 883 (2003).

These cases are inapplicable here, as *Riley* distinguished cell-phone data from other items subject to a search incident to a lawful arrest in terms of the privacy interests at stake. See *Riley*, 573 US at 393. *Riley* thus stands for the proposition that seizure of a phone and its digital contents-- unlike a seizure of other items on a person-- does not entirely extinguish one's right to privacy in that data. Moreover, *Edwards* itself did not hold that the mere fact an item was lawfully seized eliminated a suspect's reasonable expectation of

privacy; rather, it recognized that a lawful search of an item on an arrestee's person immediately after arrest was *already* reasonable under the exception to the warrant requirement for searches incident to a lawful arrest and that a reasonable delay in conducting that permissible search did not render the search unreasonable. *Edwards*, 415 US at 805. In other words, the police "did no more [at the police station] than they were entitled to do incident to the usual custodial arrest and incarceration." *Id*. Thus, assuming that this caselaw is pertinent in the instant context, it reinforces our conclusion that the later review of defendant's cell-phone data for evidence of an armed robbery was only lawful if this review was permissible in the first instance, i.e., if it was within the scope of the warrant issued to search for evidence of drug trafficking. See *State v Betterley*, 191 Wis 2d 406, 418; 529 NW2d 216 (1995) (holding that, based on *Edwards*, "the permissible extent of the second look [at items seized by police incident to a lawful arrest] is defined by what the police could have lawfully done without violating the defendant's reasonable expectations of privacy during the first search, even if they did not do it at that time").

The prosecutor also argues that because the search warrant authorized officers to search defendant's cell-phone data for evidence of drug trafficking, defendant no longer had a reasonable expectation of privacy in all of his data. Both the prosecutor and the Court of Appeals relied on *United States v Jacobsen* for the proposition that defendant lost all expectation of privacy in his cell-phone data when the search warrant authorized a search of that data for drug trafficking. In *Jacobsen*, the employees of a private freight carrier opened a damaged package and discovered a long tube. *Jacobsen*, 466 US at 111. The employees cut open the tube and discovered plastic bags filled with a white powdery substance. *Id*. The employees summoned a federal agent who, without obtaining a

warrant, removed the bags from the tube, took a small amount of the powder out of the bags, and tested the powder to determine whether it was cocaine. *Id*. at 111-112. The Court noted that a private party's search of an item does not implicate the Fourth Amendment and held that "[t]he agent's viewing of what a private party had freely made available for his inspection did not violate the Fourth Amendment." *Id*. at 119-120. The Court explained:

> Once frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now nonprivate information. . . . The Fourth Amendment is implicated only if the authorities use information with respect to which the expectation of privacy has not already been frustrated. [*Id*. at 117.]

Accordingly, the Court held that "[t]he additional invasions of respondents' privacy by the Government agent must be tested by the degree to which they exceeded the scope of the private search." *Id*. at 115. The Court concluded that the agent's removal of the plastic bags from the tube and his visual inspection of the contents of the bags "infringed no legitimate expectation of privacy and hence was not a 'search' within the meaning of the Fourth Amendment" because this action did not enable the officer to learn anything that had not previously been uncovered during the private search. *Id*. at 120.[7]

---

[7] *Jacobsen* proceeded to consider aspects of the officer's actions that exceeded the scope of the private search: the seizure of the plastic bags containing white powder and the testing of the white powder to determine whether it was cocaine. The Court held that the removal of the plastic bags from the box constituted a seizure because the officer had asserted "dominion and control over the package and its contents," *id*. at 120, but that the seizure nonetheless was reasonable under the Fourth Amendment because "it was apparent that the tube and plastic bags contained contraband and little else." *Id*. at 121-122. It further held that testing the powder did not constitute a search because the test "merely disclose[d] whether or not [the] particular substance [was] cocaine." *Id*. at 123. However, the Court noted that the test of the powder involved destruction of some of that powder and that this

Jacobsen, in our judgment, does not advance the prosecutor's argument. *Jacobsen* addressed the degree to which a private party's search of otherwise private items permits the state to review those items. But there was no private search here. While *Jacobsen* is consistent with the general proposition that one lacks a legitimate expectation of privacy in items that are exposed publicly, see, e.g., *Katz v United States*, 389 US 347, 351; 88 S Ct 507; 19 L Ed 2d 576 (1967), it says little about the extent to which the search of an item pursuant to a search warrant eliminates a citizen's legitimate expectation of privacy.[8] The prosecutor cites no caselaw indicating that the issuance of a warrant eliminates entirely one's reasonable expectation of privacy in the place or property to be searched.[9] To the contrary, it is well established that a search warrant allows the state to examine property only to the extent authorized by the warrant. See, e.g., *Bivens v Six Unknown Named Agents of Fed Bureau of Narcotics*, 403 US 388, 394 n 7; 91 S Ct 1999; 29 L Ed 2d 619

---

deprivation of the defendant's possessory interest constituted a seizure under the Fourth Amendment. *Id*. at 124-125. The Court concluded that this seizure was reasonable because it had a *de minimis* impact on defendant's property interest and that "the suspicious nature of the material made it virtually certain that the substance tested was in fact contraband." *Id*. at 125.

[8] Moreover, the other searches and seizures in *Jacobsen*-- specifically, the officer's reexamination of the contents of the package and seizure of the plastic bags, as well as the field test to determine whether the seized substance was cocaine-- have no analogue in the instant case. The search here did not merely duplicate the previous search, and there was no simple test performed to determine whether the data confirmed illegal activity.

[9] Indeed, the prosecutor cites no caselaw indicating that the issuance of a search warrant eliminates *at all* one's reasonable expectation of privacy in the items to be searched rather than merely permitting officers *temporarily* to compromise that reasonable expectation of privacy. We need not resolve this semantic difference here because, regardless of how it is framed, the result would be the same-- a warrant only permits police to review an item or area to the extent that such review lies within the scope of the warrant.

(1971) ("[T]he Fourth Amendment confines an officer executing a search warrant strictly within the bounds set by the warrant."). "If the scope of the search exceeds that permitted by the terms of a validly issued warrant . . . , the subsequent seizure is unconstitutional without more." *Horton*, 496 US at 140. Thus, a search conducted pursuant to a search warrant-- unlike a private search-- is necessarily limited to the scope of the warrant.

To the extent that *Jacobsen* is relevant in the present context, its reasoning further reinforces our conclusion that the issuance of a search warrant does not eliminate entirely one's reasonable expectation of privacy but only allows a search consistent with the scope of the warrant. As the United States Court of Appeals for the Sixth Circuit explained in applying *Jacobsen* to the search of a laptop, "[f]or the review of [the defendant's] laptop to be permissible, *Jacobsen* instructs us that [the officer's] search had to stay within the scope of [the] initial private search." *United States v Lichtenberger*, 786 F3d 478, 488 (CA 6, 2015). The court therefore concluded that the officer's search exceeded the scope of the warrant because there was "no virtual certainty that [the officer's] review [of the defendant's digital data] was limited to the photographs from" the earlier private search. *Id.*; see also *United States v Sparks*, 806 F3d 1323, 1336 (CA 11, 2015) ("While [the] private search of the cell phone might have removed certain information from the Fourth Amendment's protections, it did not expose every part of the information contained in the cell phone."), overruled on other grounds by *United States v Ross*, 963 F3d 1056 (CA 11, 2020); *State v Terrell*, 372 NC 657, 669, 670; 831 SE2d 17 (2019) ("We cannot agree that the mere opening of a thumb drive and the viewing of as little as one file automatically renders the entirety of the device's contents 'now nonprivate information' no longer [to be] afforded any protection by the Fourth Amendment. . . . [T]he extent to which an

individual's expectation of privacy in the contents of an electronic storage device is frustrated depends upon the extent of the private search and the nature of the device and its contents.").[10] As applied to the instant situation, under *Jacobsen*, the scope of the officer's search of defendant's data for evidence of armed robbery was limited to the scope of the initial lawful intrusion, i.e., the breadth of the warrant in the drug-trafficking case. Accordingly, *Jacobsen* does not support the proposition that defendant lost entirely his expectation of privacy in all of his cell-phone data once the cell phone was seized and the data searched pursuant to a warrant.[11]

---

[10] At least two federal courts of appeals have held that under *Jacobsen*, once there is a private search of any part of a suspect's digital data, police officers are permitted to review all the data on that device without a warrant, comparing digital data to a closed container that when opened loses all expectation of privacy. *United States v Runyan*, 275 F3d 449, 464 (CA 5, 2001); *Rann v Atchison*, 689 F3d 832, 836-837 (CA 7, 2012). For the reasons stated below, we find unpersuasive, in light of the United States Supreme Court's subsequent decision in *Riley*, the analogy of a digital device to a closed container and thus find these cases unpersuasive.

[11] While not cited by the prosecutor, we recognize that the Minnesota Court of Appeals in *State v Johnson*, 831 NW2d 917, 924 (Minn App, 2013), reached the opposite conclusion to that we reach here, holding that "the execution of the warrant 'frustrated' and terminated appellant's expectation of privacy in the hard drive and the digital contents identified in the warrant." *Johnson* relied on *Illinois v Andreas*, in which the United States Supreme Court held that "the subsequent reopening of [a] container is not a 'search' within the intendment of the Fourth Amendment" and that "absent a substantial likelihood that the contents have been changed, there is no legitimate expectation of privacy in the contents of a container previously opened under lawful authority." *Andreas*, 463 US at 772-773. However, *Andreas*'s holding regarding the opening of a closed container, as with those holdings cited in note 10 of this opinion, is also inapplicable to searches of cell-phone data in light of *Riley*'s subsequent recognition that privacy interests in digital data may greatly exceed those with regard to more mundane physical objects. *Riley*, 573 US at 393, 397 (holding that comparing a search of physical objects to a search of digital data is "like saying a ride on horseback is materially indistinguishable from a flight to the moon," and noting that "[t]reating a cell phone as a container whose contents may be searched incident to an arrest is a bit strained"). See also Kerr, *Searches and Seizures in A Digital World*,

In summary, the search and seizure of defendant's cell-phone data pursuant to a warrant in the drug-trafficking case did not altogether eliminate his reasonable expectation of privacy in that data. Rather, the police were permitted to seize and search that data, but only to the extent authorized by the warrant. Any further review of the data beyond the scope of that warrant constitutes a search that is presumptively invalid under the Fourth Amendment, absent some exception to that amendment's warrant requirement. See *Horton*, 496 US at 140. The remaining question is whether the review of defendant's data for evidence of an armed robbery fell within the scope of the warrant issued in the drug-trafficking case.

2. SCOPE OF THE WARRANT

This Court has yet to specifically address the Fourth Amendment requirements for a search of digital data from a cell phone authorized by a warrant. In considering this issue, we are guided by two fundamental sources of relevant law: (a) the Fourth Amendment's "particularity" requirement, which limits an officer's discretion when conducting a search pursuant to a warrant and (b) *Riley*'s recognition of the extensive privacy interests in cellular data. In light of these legal predicates, we conclude that as with any other search

---

119 Harv L Rev 531, 555 (2005) (arguing that "[a] computer is like a container that stores thousands of individual containers"). Numerous courts since *Riley* have similarly interpreted that decision, as we believe it must be interpreted, as rejecting an analogy between searches of digital data and searches of closed containers. See, e.g., *Lichtenberger*, 786 F3d at 487 ("[S]earches of physical spaces and the items they contain differ in significant ways from searches of complex electronic devices under the Fourth Amendment."); *United States v Jenkins*, 850 F3d 912, 920 n 3 (CA 7, 2017); *Terrell*, 372 NC at 669; *United States v Lara*, 815 F3d 605, 610 (CA 9, 2016). Accordingly, we respectfully find *Johnson* to be unpersuasive and decline to adopt its reasoning in light of *Riley*.

conducted pursuant to a warrant, a search of digital data from a cell phone must be "reasonably directed at uncovering" evidence of the criminal activity alleged in the warrant and that any search that is not so directed but is directed instead toward finding evidence of *other* and *unrelated* criminal activity is beyond the scope of the warrant. *United States v Loera*, 923 F3d 907, 917, 922 (CA 10, 2019); see also *Horton*, 496 US at 140-141.

The Fourth Amendment requires that search warrants "particularly describ[e] the place to be searched, and the persons or things to be seized." US Const, Am IV. A search warrant thus must state with particularity not only the items to be searched and seized, but also the alleged criminal activity justifying the warrant. See *Berger v State of New York*, 388 US 41, 55-56; 87 S Ct 1873; 18 L Ed 2d 1040 (1967); *Andresen v Maryland*, 427 US 463, 479-480; 96 S Ct 2737; 49 L Ed 2d 627 (1976); *United States v Galpin*, 720 F3d 436, 445 (CA 2, 2013) ("[A] warrant must identify the specific offense for which the police have established probable cause."). That is, some context must be supplied by the affidavit and warrant that connects the particularized descriptions of the venue to be searched and the objects to be seized with the criminal behavior that is suspected, for even particularized descriptions will not always speak for themselves in evidencing criminality. See *Hayden*, 387 US at 307 ("There must, of course, be a nexus . . . between the item to be seized and criminal behavior. Thus . . . , probable cause must be examined in terms of cause to believe that the evidence sought will aid in a particular apprehension or conviction. In so doing, consideration of police purposes will be required.").

> The manifest purpose of this particularity requirement was to prevent general searches. By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures 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. [*Maryland v Garrison*, 480 US 79, 84; 107 S Ct 1013; 94 L Ed 2d 72 (1987); see also, e.g., *Horton,* 496 US at 139.]

While "officers do not have to stop executing a search warrant when they run across evidence outside the warrant's scope, they must nevertheless reasonably direct their search toward evidence specified in the warrant." *Loera*, 923 F3d at 920; see also *United States v Ramirez*, 523 US 65, 71; 118 S Ct 992; 140 L Ed 2d 191 (1998) ("The general touchstone of reasonableness . . . governs the method of execution of the warrant."). For example, a warrant authorizing police to search a home for evidence of a stolen television set would not permit officers to search desk drawers for evidence of drug possession. See *Horton*, 496 US at 140-141.[12] This particularity requirement defines the permissible scope of a search pursuant to a warrant, and any deviation from that scope is a warrantless search that is unreasonable absent an exception to the warrant requirement. *Id*. at 140. More specifically, in connection with the present case the state exceeds the scope of a warrant where a search is not reasonably directed at uncovering evidence related to the criminal activity identified in the warrant, but rather is designed to uncover evidence of criminal activity *not* identified in the warrant. See, e.g., *United States v Carey*, 172 F3d 1268, 1272-

---

[12] As noted by *Riley*, a home and a cell phone are similarly situated, at least to the extent that a search of either may result in a significant intrusion into an individual's private affairs. *Riley*, 573 US at 396-397 ("In 1926, [Judge] Hand observed . . . that it is 'a totally different thing to search a man's pockets and use against him what they contain, [than to] ransack[] his house for everything which may incriminate him.' If his pockets contain a cell phone, however, that is no longer true. Indeed, a cell-phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.") (citation omitted).

1273 (CA 10, 1999); *Loera*, 923 F3d at 922; *United States v Nasher-Alneam*, 399 F Supp 3d 579, 593-594 (SD W Va, 2019).

In this regard, we first address the prosecutor's argument that the search for evidence of armed robbery fell within the scope of the warrant because the warrant authorized officers to review the entire 600-page report containing the apparent totality of defendant's cell-phone data, as any segment of this data may have contained evidence of drug trafficking and digital data can be manipulated to hide incriminating content.[13] We are cognizant that a criminal suspect will not always store or organize incriminating information on his or her digital devices in the most obvious way or in a manner that

[13] Implicit in this argument is the assumption that an officer's subjective intention to look for evidence related to a crime not identified in the warrant is immaterial so long as the search is objectively authorized by the scope of the warrant. In other words, the prosecutor's argument seems premised on the proposition that so long as it was objectively reasonable to review *all* of defendant's data for evidence of drug trafficking, it is irrelevant that the genuine purpose of the search was to secure evidence of an armed robbery. The facts that the prosecutor in the armed-robbery case asked Detective Wagrowski-- a month or so after the initial extraction of the data-- to conduct a further search of defendant's cell-phone data using search terms related to the armed robbery and that this evidence was eventually admitted in the armed-robbery trials suggests that this search was not designed to obtain evidence related to drug trafficking, but rather to bolster the prosecutor's case in the armed-robbery trial. Some courts have held that an officer's subjective intention to find evidence of a crime not identified in the warrant constitutes a relevant factor in determining whether a search of digital data falls outside the scope of the warrant, while others have held that this is a purely objective inquiry. Compare *Loera*, 923 F3d at 919 & n 3 (holding that the subjective intention of the officer to discern evidence of a crime not identified in the warrant is a relevant factor in determining whether the search exceeded the scope of the warrant), with *United States v Williams*, 592 F3d 511, 522 (CA 4, 2010) ("[T]he scope of a search conducted pursuant to a warrant is defined objectively by the terms of the warrant and the evidence sought, not by the subjective motivations of an officer.") (emphasis omitted). Because the search here was objectively beyond the scope of the warrant, we need not decide whether an officer's subjective intention is a relevant consideration.

facilitates the location of that information. See, e.g., *United States v Mann*, 592 F 3d 779, 782 (CA 7, 2010) ("Unlike a physical object that can be immediately identified as responsive to the warrant or not, computer files may be manipulated to hide their true contents."). We do not hold or imply here that officers in the execution of a search of digital data must review only digital content that a suspect deigns to identify as pertaining to criminal activity. See *United States v Burgess*, 576 F3d 1078, 1093-1094 (CA 10, 2009). Such an approach would undermine legitimate law enforcement practices and unduly restrict officers well beyond the dictates of the Fourth Amendment.

However, at the same time, we decline to adopt a rule that it is always reasonable for an officer to review the entirety of the digital data seized pursuant to a warrant on the basis of the mere possibility that evidence may conceivably be found anywhere on the device or that evidence might be concealed, mislabeled, or manipulated. Such a per se rule would effectively nullify the particularity requirement of the Fourth Amendment in the context of cell-phone data and rehabilitate an impermissible *general warrant* that "would in effect give 'police officers unbridled discretion to rummage at will among a person's private effects.' " *Riley*, 573 US at 399, quoting *Arizona v Gant*, 556 US 332, 345; 129 S Ct 1710; 173 L Ed 2d 485 (2009); see also *People v Herrera*, 357 P3d 1227, 1228, 1233; 2015 CO 60 (Colo, 2015) (holding that allowing a search of an entire device for evidence of a crime based upon the possibility that evidence of the crime could be found anywhere on the phone and that the incriminating data could be hidden or manipulated would "render the warrant a general warrant in violation of the Fourth Amendment's particularity requirement"). This result would be especially problematic in light of *Riley*'s observations concerning the sheer amount of information contained in cellular data and the highly

personal character of much of that information. *Riley*, 573 US at 394-396; see also *United States v Otero*, 563 F3d 1127, 1132 (CA 10, 2009) ("The modern development of the personal computer and its ability to store and intermingle a huge array of one's personal papers in a single place increases law enforcement's ability to conduct a wide-ranging search into a person's private affairs, and accordingly makes the particularity requirement that much more important."); *Galpin*, 720 F3d at 447 ("There is . . . a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant. This threat demands a heightened sensitivity to the particularity requirement in the context of digital searches.") (quotation marks and citation omitted). Accordingly, an officer's search of seized digital data, as with any other search conducted pursuant to a warrant, must be reasonably directed at finding evidence of the criminal activity identified within the warrant. *Loera*, 923 F3d at 921-922.

Specifically in the digital context, this requires that courts and officers consider "whether the forensic steps of the search process were reasonably directed at uncovering the evidence specified in the search warrant." *Id*. at 917. Whether a search of seized digital data that uncovers evidence of criminal activity not identified in the warrant was reasonably directed at finding evidence relating to the criminal activity alleged in the warrant turns on a number of considerations, including: (a) the nature of the criminal activity alleged and the type of digital data likely to contain evidence relevant to the alleged activity;[14] (b) the

[14] For example, in the absence of contrary case-specific information, it is unlikely that evidence relating to tax fraud would be discovered by reviewing the images on a digital device. See *Carey*, 172 F3d at 1275 n 8 ("Where a search warrant seeks only financial records, law enforcement officers should not be allowed to search through telephone lists or word processing files absent a showing of some reason to believe that these files contain

evidence provided in the warrant affidavit for establishing probable cause that the alleged criminal acts have occurred;[15] (c) whether nonresponsive files are segregated from

---

the financial records sought.") (quotation marks and citation omitted); Gershowitz, *The Post-Riley Search Warrant: Search Protocols on Particularity in Cell Phone Searches*, 69 Vanderbilt L Rev 585, 630-638 (2016) (arguing that criminals engaged in simpler types of street crimes, such as drug trafficking, are more likely to use cell phones and less likely to "mislabel . . . or bury evidence" than criminals engaged in crimes like child pornography and financial misconduct and therefore searches of cell phones for evidence of these simpler crimes should be more limited in scope than searches of computers for evidence of child pornography or financial misconduct).

[15] "The fact that [a warrant] application adequately described the 'things to be seized' does not save [a] warrant from its facial invalidity. The Fourth Amendment by its terms requires particularity in the warrant, not in the supporting documents." *Groh v Ramirez*, 540 US 551, 557; 124 S Ct 1284; 157 L Ed 2d 1068 (2004) (emphasis omitted). However, the particularity requirement of the Fourth Amendment can be satisfied by an affidavit that the warrant incorporates by reference. See, e.g., *United States v Hamilton*, 591 F3d 1017, 1025 (CA 8, 2010). "[M]ost Courts of Appeals have held that a court may construe a warrant with reference to a supporting application or affidavit if the warrant uses appropriate words of incorporation, and if the supporting document accompanies the warrant." *Groh*, 540 US at 557-558. The prosecutor argues that the warrant here incorporated the warrant affidavit by reference. The warrant stated, "THE ATTACHED AFFIDAVIT, having been sworn to by the affiant, Detective Matthew Gorman, before me this day, based upon facts stated therein, probable cause having been found in the name of the people of the State of Michigan, I command that you enter the following described places and vehicles[.]" The warrant affidavit in this case accompanied the warrant, but it is unclear whether the warrant used "appropriate words of incorporation." We need not resolve this issue here except to say that regardless of whether a warrant incorporates the affidavit by reference, consideration of the evidence provided in the warrant affidavit for establishing probable cause is relevant to whether a search of digital data was reasonably directed at discovering evidence of the crime alleged in the warrant. Cf. *State v Goynes*, 303 Neb 129, 142; 927 NW2d 346 (2019) ("[A] warrant for the search of the contents of a cell phone must be sufficiently limited in scope to allow a search of only that content that is related to the probable cause that justifies the search."); Dennis, *Regulating Search Warrant Execution Procedure for Stored Electronic Communications*, 86 Fordham L Rev 2993, 3012 (2018) (noting that it is relevant to a search's reasonableness "whether the government subjected the materials to subsequent searches based on new information and theories developed about the case. In these instances, courts have expressed concern about continued searches for evidence under new theories of the case or more expansive areas not initially included

responsive files on the device;[16] (d) the timing of the search in relation to the issuance of the warrant and the trial for the alleged criminal acts;[17] (e) the technology available to allow officers to sort data likely to contain evidence related to the criminal activity alleged in the warrant from data not likely to contain such evidence without viewing the contents of the unresponsive data and the limitations of this technology;[18] (f) the nature of the digital

---

in the warrant"), citing *United States v Wey*, 256 F Supp 3d 355, 406 (SDNY, 2017); *People v Thompson*, 28 NYS3d 237, 255 (2016).

[16] See *Loera*, 923 F3d at 919.

[17] See *Nasher-Alneam*, 399 F Supp 3d 579 (holding that a second search of digital data for evidence of fraud 15 months after the records were seized to be searched for evidence of distribution of a controlled substance and after the defendant had already gone to trial once exceeded the scope of the warrant); *United States v Metter*, 860 F Supp 2d 205, 209, 211, 215 (EDNY, 2012) (holding that a fifteen-month delay in the government's review of seized devices violated the Fourth Amendment); *United States v Keszthelyi*, 308 F3d 557, 568-569 (CA 6, 2002) ("[A] single search warrant may authorize more than one entry into the premises identified in the warrant, as long as the second entry is a reasonable continuation of the original search;" "the subsequent entry must indeed be a continuation of the original search, and not a new and separate search."). But see *United States v Johnston*, 789 F 3d 934, 941-943 (CA 9, 2015) (holding that a search of seized data five years after the initial seizure was reasonable where the search was for evidence of the same criminal conduct alleged in the warrant).

[18] "[L]aw enforcement officers can generally employ several methods to avoid searching files of the type not identified in the warrant: observing files types and titles listed on the directory, doing a key word search for relevant terms, or reading portions of each file stored in the memory." *Carey*, 172 F3d at 1276; see also Baron-Evans, *When the Government Seizes and Searches Your Client's Computer*, 18 No. 7 White-Collar Crime Rep 2 (2004); 2004 WL 635186 at 7 ("Various technical means are available to enable the government to confine the search to the scope of probable cause, including searching by filename, directory or subdirectory; the name of the sender or recipient of e-mail; specific key words or phrases; particular types of files as indicated by filename extensions; and/or file date and time."). The availability of such methods does not necessarily foreclose a more general search of the data. See Perldeiner, *Total Recall: Computers and the Warrant Clause*, 49 Conn L Rev 1757, 1777-1779 (2017) (noting four situations in which searching for and isolating data is difficult: (a) when metadata is deleted, (b) when data is encrypted, (c)

device being searched;[19] (g) the type and breadth of the search protocol employed;[20] (h) whether there are any indications that the data has been concealed, mislabeled, or manipulated to hide evidence relevant to the criminal activity alleged in the warrant, such as when metadata is deleted or when data is encrypted;[21] and (i) whether, after reviewing a certain number of a particular type of data, it becomes clear that certain types of files are not likely to contain evidence related to the criminal activity alleged in the warrant.[22]

---

when data is stored off-site, and (d) when searching for images); see also *Rosa v Commonwealth*, 48 Va App 93, 101; 628 SE2d 92 (2006) ("[F]ile extensions may be misleading and may not give accurate descriptions of the material contained in the file."). However, the use and availability of such technology is relevant to whether a more general search of the data is reasonable.

[19] See Note, *What Comes After "Get a Warrant": Balancing Particularity and Practicality in Mobile Device Search Warrants Post-Riley*, 101 Cornell L Rev 187, 204-208 (2015) (arguing that a reasonable search method of cell-phone data will differ from a reasonable search of computer data because "(1) there are different forensic steps involved with mobile device searches compared to computer searches and (2) mobile phones are functionally different from computers").

[20] "To undertake any meaningful assessment of the government's search techniques [of digital data], [a court] would need to understand what protocols the government used, what alternatives might have reasonably existed, and why the latter rather than the former might have been more appropriate." *United States v Christie*, 717 F3d 1156, 1167 (CA 10, 2013). See also *Loera*, 923 F3d at 920.

[21] *Total Recall*, 49 Conn L Rev at 1777-1779; see also *Herrera*, 357 P3d at 1233 (concluding that the "abstract possibility" that files could be hidden or manipulated is insufficient to justify searching the entire phone and noting that the prosecutor "did not present a shred of evidence to suggest, nor did [he] attempt to argue," that the defendant in that case hid or manipulated his files).

[22] See *Carey*, 172 F3d at 1274 ("[E]ach of the files containing pornographic material was labeled 'JPG' and most featured a sexually suggestive title. Certainly after opening the first file and seeing an image of child pornography, the searching officer was aware—in advance of opening the remaining files—what the label meant. When he opened the

To be clear, a court will generally need to engage in such a "totality-of-circumstances" analysis to determine whether a search of digital data was reasonably directed toward finding evidence of the criminal activities alleged in the warrant only if, while searching digital data pursuant to a warrant for one crime, officers discover evidence of a different crime without having obtained a second warrant and a prosecutor seeks to use that evidence at a subsequent criminal prosecution. Courts should also keep in mind that in the process of ferreting out incriminating digital data it is almost inevitable that officers will have to review *some* data that is unrelated to the criminal activity alleged in the authorizing warrant. *United States v Richards*, 659 F3d 527, 539 (CA 6, 2011) ("[O]n occasion in the course of a reasonable search [of digital data], investigating officers may examine, 'at least cursorily,' some 'innocuous documents . . . in order to determine whether they are, in fact, among those papers authorized to be seized.' "), quoting *Andresen*, 427 US at 482 n 11. The fact that some data reviewed turns out to be related to criminal activity not alleged in the authorizing warrant does not render that search per se outside the scope of the warrant. So long as it is reasonable under all of the circumstances for officers to believe that a particular piece of data will contain evidence relating to the criminal activity identified in the warrant, officers may review that data, even if that data ultimately provides evidence of criminal activity not identified in the warrant.

In this case, the warrant authorized officers to search defendant's digital data for evidence of drug trafficking, or more specifically, for evidence of "any records pertaining

---

subsequent files, he knew he was not going to find items related to drug activity as specified in the warrant . . . .").

to the receipt, possession and sale or distribution of controlled substances including but not limited to documents, video tapes, computer disks, computer hard drives, and computer peripherals." The affidavit did not even mention Weber or the armed robbery of Stites, let alone seek to establish probable cause that defendant committed armed robbery. As a result, the warrant did not authorize a search of defendant's data for evidence related to the armed robbery.

A month or so after the initial extraction of the data, the prosecutor in the armed-robbery case asked Detective Wagrowski to use Cellebrite to conduct a focused review of the seized data for (a) contacts with phone numbers of Weber and Stites and (b) data containing the words "Lisa," "killer" (and variations thereof), and "Kristopher." The data obtained from this review was admitted into evidence against defendant at his trials for armed robbery.

There was nothing in the warrant or affidavit to suggest that either Weber or Stites was implicated in defendant's drug trafficking or that reviewing data with Weber's name or contacts with her phone number would lead to evidence regarding defendant's drug trafficking. Similarly, there was nothing in the warrant or affidavit to suggest that reviewing defendant's data for the word "killer" or defendant's name would uncover evidence of drug trafficking. Furthermore, there was no evidence that defendant hid or manipulated his files to conceal evidence related to his drug trafficking or that a review of all defendant's data to discover evidence of drug trafficking was reasonable in light of the use and availability of Cellebrite to isolate relevant data. Therefore, this review was not reasonably directed toward obtaining evidence of drug trafficking and exceeded the scope of the warrant.

The prosecutor argues that this review was not beyond the scope of the warrant because defendant allegedly was selling drugs to Weber around the time of the robbery. The prosecutor reasons that defendant's contacts with Weber were rooted in the same illicit activity the warrant had targeted, i.e., drug trafficking. However, any connection between Weber and defendant's drug trafficking was not derived from the warrant or its supportive affidavit. Rather, probable cause that defendant was dealing drugs was based on the tip from a confidential informant that defendant and Pankey were dealing drugs. Therefore, a keyword search of the data for drug references, drug-related items, or contacts with Pankey would certainly have been reasonably directed at finding evidence of drug trafficking and would have fallen well within the scope of the warrant.[23] But there was no indication in the warrant or its affidavit that the review conducted would uncover evidence of defendant's drug trafficking.[24] Rather, the keyword searches were directed toward

---

[23] This list is merely illustrative and is not intended to identify *all* of the potential search terms that would have fallen within the scope of the warrant. Nor is this list intended to imply that officers were only permitted to review defendant's data using search terms rather than employing different search protocols or manually searching the data using other criteria that were reasonably directed in light of the warrant and its affidavit toward finding evidence related to drug trafficking.

[24] We do not mean to hold or imply that police officers are categorically precluded from reviewing cell-phone contacts with a particular person merely because that person has not been explicitly identified in the warrant or supportive affidavit. The evidence set forth for establishing probable cause is but one consideration in determining whether a search of cell-phone data was "reasonably directed" at uncovering evidence related to the crime alleged in the warrant. Therefore, other considerations may well support an officer's review of contacts despite the absence of an express reference to that person in the warrant or affidavit. For example, if, while searching cell-phone data for specific drug-related terms or references used by the defendant, an officer discovers those terms or references within cell-phone contacts, these may of course be reviewed. Further, if an officer were to uncover evidence that digital files containing contacts with a particular person had been

obtaining evidence that defendant committed an armed robbery based on evidence obtained while investigating that armed robbery. Because the warrant did not authorize a search of defendant's data for evidence of armed robbery, these searches fell beyond the scope of the warrant.

To summarize, the officer's review of defendant's cell-phone data for evidence relating to the armed robbery was beyond the scope of the warrant because there was no indication in either the warrant or the affidavit that this review, conducted well after the initial extraction of the data, would uncover evidence of drug trafficking. Additionally, a review of the entirety of defendant's data was unreasonable in light of the lack of evidence that data concerning the drug activity was somehow hidden or manipulated and in light of the officer's ability to conduct a more focused review of the data using Cellebrite to isolate and separate responsive and unresponsive materials. This is not a circumstance in which the officer was reasonably reviewing data for evidence of drug trafficking and happened to view data implicating defendant in other criminal activity. If such were the case and the data's "incriminating character [was] immediately apparent," the plain-view exception would likely apply and permit the state to use the evidence of criminal activity not alleged in the warrant at a subsequent criminal prosecution. *People v Champion*, 452 Mich 92,

---

hidden, manipulated, or encoded in a manner intended to conceal the contacts, the officer might also be justified in suspecting that there was evidence of criminal activity within those contacts regardless of whether that person was referred to in the warrant or affidavit. However, we discern no such considerations in the instant case that would justify the searches of Weber or Stites.

101; 549 NW2d 849 (1996), citing *Horton*, 496 US 128.[25] Rather, this review was directed exclusively toward finding evidence related to the armed-robbery charge, and it was grounded in information obtained during investigation into *that* crime. Accordingly, this review constituted a warrantless search that was unlawful under the Fourth Amendment.[26]

---

[25] The exception is not implicated in this case because "an essential predicate of the plain view doctrine is that the initial intrusion not violate the Fourth Amendment" and the officer's search here *did* violate the Fourth Amendment because it was not reasonably directed at uncovering evidence of the criminal activities alleged in the warrant. *Galpin*, 720 F3d at 451 (quotation marks omitted); see also *United States v Gurczynski*, 76 MJ 381, 388 (2017) ("A prerequisite for the application of the plain view doctrine is that the law enforcement officers must have been conducting a lawful search when they stumbled upon evidence in plain view. As noted, the officers in this case were not [doing so] because the execution of the warrant was constitutionally unreasonable.").

[26] Defendant contends the warrant was overly broad because it allowed officers to search his cell phone for evidence of drug trafficking without limitation. In light of the privacy interests implicated in digital data, some magistrates have been placing more specific limitations upon a warrant to search digital data, such as "by (1) instituting time limits on completion [of the search], (2) mandating return or deletion of non-responsive materials, or (3) enumerating specific search protocol to be utilized during execution." *Regulating Search Warrant Execution*, 86 Fordham L Rev at 3001-3011; see also *In re Search of 3817 W West End, First Floor Chicago, Illinois 60621*, 321 F Supp 2d 953, 961 (ND Ill, 2004) (requiring the government to provide a specific search protocol of digital data to satisfy the particularity requirement of the Fourth Amendment). There is much debate regarding the propriety and constitutionality of ex ante limitations on the manner in which officers may search digital data for evidence. Compare *The Post-Riley Search Warrant*, 69 Vanderbilt L Rev at 638 ("Imposing restrictions on search warrants—in the form of ex ante search protocols and geographic restrictions on the applications police can search—is the best way to ensure that cell phone warrants do not become the reviled general warrants the Fourth Amendment's particularity requirement was designed to prevent."), with Kerr, Abstract, *Ex Ante Regulation of Computer Search and Seizure*, 96 Va L Rev 1241, 1242, 1265, 1267-1268 (2010) ("[E]x ante restrictions on the execution of computer warrants are constitutionally unauthorized and unwise."), citing *United States v Grubbs*, 547 US 90, 98; 126 S Ct 1494; 164 L Ed 2d 195 (2006) ("Nothing in the language of the Constitution or in this Court's decisions . . . suggests that . . . search warrants . . . must include a specification of the precise manner in which they are to be executed.") (quotation marks omitted). But see *In re Search Warrant*, 193 Vt 51, 69; 71 A3d 1158 (2012) (holding that,

B. INEFFECTIVE ASSISTANCE OF COUNSEL

The final issue is whether trial counsel was ineffective when he failed to object under the Fourth Amendment to the admission of the evidence obtained from defendant's cell-phone data. The Court of Appeals rejected out-of-hand defendant's claim of ineffective assistance of counsel based on its conclusion that an objection under the Fourth Amendment would have been futile. *Hughes*, unpub op at 3 n 2. We find it appropriate to remand to the Court of Appeals to reconsider defendant's claim in light of this opinion. When making this determination, the Court of Appeals should consider whether the violation of defendant's Fourth Amendment rights entitled defendant to exclusion of the unlawfully searched data from his armed-robbery trial. See *Kimmelman v Morrison*, 477 US 365, 375; 106 S Ct 2574; 91 L Ed 2d 305 (1986).[27]

---

although ex ante restrictions are not required, such restrictions on searches of digital data "are sometimes acceptable mechanisms for ensuring the particularity of a search"). "[G]iven the unique problem encountered in computer searches, and the practical difficulties inherent in implementing universal search methodologies, the majority of federal courts have eschewed the use of a specific search protocol and, instead, have employed the Fourth Amendment's bedrock principle of reasonableness on a case-by-case basis . . . ." *Richards*, 659 F3d at 538 (citations omitted). We need not decide here whether the warrant was overly broad because "putting aside for the moment the question what limitations the Fourth Amendment's particularity requirement should or should not impose on the government *ex ante*, the Amendment's protection against 'unreasonable' searches surely allows courts to assess the propriety of the government's search methods . . . *ex post* in light of the specific circumstances of each case." *Christie*, 717 F3d at 1166, citing *Ramirez*, 523 US at 71. We conclude that, regardless of whether the warrant itself was overly broad, the search of the data pursuant to that warrant was unreasonable and therefore violated the Fourth Amendment.

[27] The general rule is that evidence obtained in violation of the Fourth Amendment cannot be used against a defendant at a subsequent trial. See, e.g., *United States v Council*, 860 F3d 604, 608-609 (CA 8, 2017); *Mapp v Ohio*, 367 US 643, 655; 81 S Ct 1684; 6 L Ed 2d 1081 (1961) (applying the exclusionary rule to the states). However, the exclusionary rule is a judicially created remedy that does not apply to every Fourth Amendment violation.

IV. CONCLUSION

The ultimate holding of this opinion is simple and straightforward-- a warrant to search a suspect's digital cell-phone data for evidence of one crime does not enable a search of that same data for evidence of another crime without obtaining a second warrant. Nothing herein should be construed to restrict an officer's ability to conduct a reasonably thorough search of digital cell-phone data to uncover evidence of the criminal activity alleged in a warrant, and an officer is not required to discontinue a search when he or she discovers evidence of other criminal activity while reasonably searching for evidence of the criminal activity alleged in the warrant. However, respect for the Fourth Amendment's requirement of particularity and the extensive privacy interests implicated by cell-phone data as delineated by the United States Supreme Court's decision in *Riley v California* requires that officers reasonably limit the scope of their searches to evidence related to the criminal activity alleged in the warrant and not employ that authorization as a basis for seizing and searching digital data in the manner of a *general warrant* in search of evidence of any and all criminal activity. We hold that, as with any other search, an officer must limit a search of digital data from a cell phone in a manner reasonably directed to uncover

---

See, e.g., *Utah v Strieff*, 579 US ___, ___; 136 S Ct 2056, 2061; 195 L Ed 2d 400 (2016). The prosecutor argues in this Court that if the warrant affidavit failed to establish a sufficient nexus between defendant's criminal activity and his cell phone, see note 6 of this opinion, the exclusionary rule does not apply because the officers relied in good faith on the district court judge's finding of probable cause. See *United States v Leon*, 468 US 897; 104 S Ct 3405; 82 L Ed 2d 677 (1984) (holding that the exclusionary rule does not apply if officers rely in good faith on a magistrate's finding of probable cause to issue a warrant). The prosecutor does not specifically argue that if the searches at issue exceeded the scope of the warrant any exception to the exclusionary rule applies. The parties may develop this issue further on remand.

evidence of the criminal activity alleged in the warrant. We hereby reverse the judgment of the Court of Appeals and remand to that Court to address whether defendant is entitled to relief based upon the ineffective assistance of counsel.

Stephen J. Markman
Bridget M. McCormack
Brian K. Zahra
David F. Viviano
Richard H. Bernstein
Elizabeth T. Clement
Megan K. Cavanagh

S T A T E O F M I C H I G A N

SUPREME COURT

PEOPLE OF THE STATE OF MICHIGAN,

Plaintiff-Appellee,

v No. 158652

KRISTOPHER ALLEN HUGHES,

Defendant-Appellant.

VIVIANO, J. (*concurring*).

I concur in the majority's holding but write separately because I take issue with one aspect of its reasoning. The majority identifies several factors that a court must consider to determine whether a police officer's search of seized digital cell-phone data is reasonably directed at finding evidence of the criminal activity identified in the warrant. See *ante* at 26-30. I do not take issue with the factors identified by the majority, at least to the extent that they may apply in the cases to which they might be relevant.[1] But I believe the list is incomplete without the addition of another potentially dispositive factor: the officer's subjective intention in conducting the search. If the search was purposefully conducted to obtain evidence of a crime other than the one identified in the warrant, I do not see how we can conclude that same search was " 'reasonably directed at uncovering' evidence of the criminal activity alleged in the warrant." *Ante* at 22.

---

[1] It is worth pointing out that, with the exception of Factor (h), the majority does not reference the factors or apply them in its analysis.

Citing conflicting caselaw from the federal circuit courts, the majority expressly declines to address whether the officer's subjective intention is relevant to the inquiry. See note 13 of the majority opinion (comparing *United States v Loera*, 923 F3d 907 (CA 10, 2019), and *United States v Williams*, 592 F3d 511 (CA 4, 2010)). In *Loera*, the court persuasively explained why such a restriction is needed in the context of searches of electronic storage devices:

> The general Fourth Amendment rule is that investigators executing a warrant can look anywhere where evidence described in the warrant might conceivably be located.
>
> * * *
>
> This limitation works well in the physical-search context to ensure that searches pursuant to warrants remain narrowly tailored, but it is less effective in the electronic-search context where searches confront what one commentator has called the "needle-in-a-haystack" problem. Given the enormous amount of data that computers can store and the infinite places within a computer that electronic evidence might conceivably be located, the traditional rule risks allowing unlimited electronic searches.
>
> To deal with this problem, rather than focusing our analysis of the reasonableness of an electronic search on "what" a particular warrant permitted the government agents to search (i.e., "a computer" or "a hard drive"), we have focused on "how" the agents carried out the search, that is, the reasonableness of the search method the government employed. Our electronic search precedents demonstrate a shift away from considering what digital location was searched and toward considering whether the forensic steps of the search process were reasonably directed at uncovering the evidence specified in the search warrant. Shifting our focus in this way is necessary in the electronic search context because search warrants typically contain few—if any—restrictions on where within a computer or other electronic storage device the government is permitted to search. Because it is "unrealistic to expect a warrant prospectively [to] restrict the scope of a search by directory, filename or extension or to attempt to structure search methods," our [*ex post*] assessment of the propriety of a government search is essential to ensuring that the Fourth Amendment's protections are realized

> in this context. [*Loera*, 923 F3d at 916-917 (citations and emphasis omitted; first alteration in original).]

Later, in a footnote, the court acknowledged that inadvertence was abandoned as a necessary condition for a legitimate plain-view seizure in *Horton v California*, 496 US 128, 130, 139; 110 S Ct 2301; 110 L Ed 2d 112 (1990), but explained that it persisted in "includ[ing] inadvertence as a factor to consider when deciding whether an electronic search fell within the scope of its authorizing warrant or outside of it [because of] . . . [t]he fundamental differences between electronic searches and physical searches, including the fact that electronic search warrants are less likely prospectively to restrict the scope of the search . . . ." *Loera*, 923 F3d at 920 n 3.

A different approach was taken by the court in *Williams*, which was decided prior to *Riley v California*, 573 US 373; 134 S Ct 2473; 189 L Ed 2d 430 (2014). In that case, in examining the plain-view exception, the court held that a warrant authorizing a search of a computer and digital storage device "impliedly authorized officers to open each file on the computer and view its contents, at least cursorily, to determine whether the file fell within the scope of the warrant's authorization . . . ." *Williams*, 592 F3d at 521. See also *id*. at 522 ("Once it is accepted that a computer search must, by implication, authorize at least a cursory review of each file on the computer, then the criteria for applying the plain-view exception are readily satisfied."). Citing *Horton*, the court concluded that "[i]nadvertence focuses incorrectly on the subjective motivations of the officer in conducting the search and not on the objective determination of whether the search is authorized by the warrant or a valid exception to the warrant requirement." *Id*. at 523. The court made it very clear that it would not adopt new rules to govern the search and seizure

of electronic files: "At bottom, we conclude that the sheer amount of information contained on a computer does not distinguish the authorized search of the computer from an analogous search of a file cabinet containing a large number of documents." *Id*. at 523.

Williams's approach is less persuasive in light of *Riley*. As the majority notes, "*Riley* distinguished cell-phone data from other items subject to a search incident to a lawful arrest in terms of the privacy interests at stake." *Ante* at 15, citing *Riley*, 573 US at 393. In *Riley*, the government argued that a search of all data stored on a cell phone is "materially indistinguishable" from searches of other items found on an arrestee's person. *Riley*, 573 US at 393. Apparently not impressed with this argument, the Court responded tartly: "That is like saying a ride on horseback is materially indistinguishable from a flight to the moon." *Id*. The Court observed that "[o]ne of the most notable distinguishing features of modern cell phones is their immense storage capacity," noting that "[t]he current top-selling smart phone has a standard capacity of 16 gigabytes . . . [which] translates to millions of pages of text, thousands of pictures, or hundreds of videos." *Id*. at 393-394 (citation omitted). The rule adopted in *Loera*, which was decided after *Riley*, accounts for the realities of modern electronic storage devices. These privacy concerns are only heightened when it comes to the types and volume of data contained on modern smart phones, as the majority ably explains. See *ante* at 10-11, quoting *Riley*, 573 US at 393, 395-396.

Following the approach in *Loera*, I would adopt inadvertence as a factor to consider when deciding whether an electronic search fell within the scope of its authorizing warrant. Here, I would find that factor dispositive since it was clear that the second search of defendant's cell phone was conducted to obtain evidence of a crime other than the drug-

trafficking offense identified in the warrant. At the time of the second search, the only crime defendant was charged with arising out of the August 6 incident was armed robbery. The prosecutor assigned to the armed-robbery case requested that the second search be conducted to obtain evidence to support that charge. Therefore, for this separate reason, I agree with the majority that the second search was beyond the scope of the warrant because it was not "reasonably directed at uncovering" evidence of drug trafficking.

Instead of relying on the lack of inadvertence, however, the majority focuses on whether there was any indication in the warrant or affidavit that that the searches performed would uncover evidence of defendant's drug transactions with Weber or Stites. See *ante* at 31 ("There was nothing in the warrant or affidavit to suggest that either Weber or Stites was implicated in defendant's drug trafficking or that reviewing data with Weber's name or contacts with her phone number would lead to evidence regarding defendant's drug trafficking."); *ante* at 32 ("[A]ny connection between Weber and defendant's drug trafficking was not derived from the warrant or its supportive affidavit."). But I do not believe that a search warrant or the affidavit supporting it has to specify the participants of each drug transaction for that evidence to be within the scope of a drug-trafficking warrant.[2]

[2] See *United States v Castro*, 881 F3d 961, 966 (CA 6, 2018) (citation omitted) ("Officers may conduct a more detailed search of an electronic device after it was properly seized so long as the later search does not exceed the probable cause articulated in the original warrant and the device remained secured."). If, for example, defendant had been charged with or was being investigated for a drug crime arising out of the August 6 incident, in my view, nothing would have precluded law enforcement officers from conducting a more detailed search of the properly seized cell-phone data using the new information they obtained concerning this additional instance of drug trafficking. See *id*. ("It is sometimes the case, as it was the case here, that law enforcement officers have good reason to revisit previously seized, and still secured, evidence as new information casts new light on the previously seized evidence."). As the prosecutor points out, defendant's interactions with

Such a requirement would go well beyond prospectively "considering whether the forensic steps of the search process were reasonably directed at uncovering the evidence specified in the search warrant." *Loera*, 923 F3d at 917.[3]

Under the circumstances of this case, before conducting another search of defendant's cell phone, the officer should have obtained a second search warrant directed toward obtaining evidence of the armed-robbery offense. Because he did not, I concur with the majority that the second search was unlawful under the Fourth Amendment.[4]

David F. Viviano

Weber and Stites on August 6 included the purchase and sale of illegal drugs. And once the evidence has been properly obtained, there is nothing that would prevent it from being used to prove a separate crime. See *Williams*, 592 F3d at 520, quoting *United States v Phillips*, 588 F3d 218, 224 (CA 4, 2009) (" 'Courts have never held that a search is overly broad merely because it results in additional criminal charges.' "). But we are not confronted with that situation. Instead, it is clear that the second search was conducted to obtain evidence of the alleged armed robbery.

[3] The majority's reliance on this factor is perplexing for an additional reason: it is not one of the factors identified by the majority for determining whether a search is beyond the scope of the warrant. And I fear that it may lead to confusion about whether the absence of such details will constitute grounds to challenge the search and seizure of any drug-trafficking evidence that is not specifically referred to in the search warrant or affidavit.

[4] It appears that a plausible claim could be made that the government would have inevitably discovered the evidence contained on defendant's cell phone through lawful means given that the cell phone was lawfully in the government's possession. See *Loera*, 923 F3d at 928 ("When evidence is obtained in violation of the Fourth Amendment, that evidence need not be suppressed if agents inevitably would have discovered it through lawful means independent from the unconstitutional search."). But since no such claim has been raised, I decline to consider it further.