2021 WI 68

SUPREME COURT OF WISCONSIN

CASE NO.:	2019AP1404-CR
COMPLETE TITLE:	State of Wisconsin, Plaintiff-Respondent, v. George Steven Burch, Defendant-Appellant.

ON CERTIFICATION FROM THE COURT OF APPEALS

OPINION FILED:	June 29, 2021
SUBMITTED ON BRIEFS:	
ORAL ARGUMENT:	April 12, 2021

SOURCE OF APPEAL:

COURT:	Circuit
COUNTY:	Brown
JUDGE:	John Zakowski

JUSTICES:

HAGEDORN, J., delivered the majority opinion of the Court, in which ZIEGLER, C.J, ROGGENSACK, and REBECCA GRASSL BRADLEY, JJ., joined, and in which DALLET and KAROFSKY, JJ., joined with respect to Parts I. and II.B. REBECCA GRASSL BRADLEY, J., filed a concurring opinion. DALLET, J., filed an opinion concurring in part and dissenting in part, in which KAROFSKY, J., joined and in which ANN WALSH BRADLEY, J., joined except for footnote 1. ANN WALSH BRADLEY, J., filed a dissenting opinion.

NOT PARTICIPATING:

ATTORNEYS:

For the defendant-appellant, there were briefs filed by *Ana L. Babcock* and *Babcock Law, LLC*. There was an oral argument by *Ana L. Babcock*.

For the plaintiff-respondent, there was a brief filed by *Aaron R. O'Neil*, assistant attorney general; with whom on the brief was *Joshua L. Kaul*, attorney general. There was an oral argument by *Aaron R. O'Neil*.

An amicus curiae brief was filed on behalf of *Legal Action of Wisconsin, Inc.* by *Rebecca M. Donaldson*, Milwaukee.

An amicus curiae brief was filed on behalf of American Civil Liberties Union Foundation, American Civil Liberties Union of Wisconsin Foundation, Electronic Frontier Foundation, and Electronic Privacy Information Center by *Laurence J. Dupuis* and *American Civil Liberties Union of Wisconsin Foundation*, Milwaukee; with whom on the brief was *Jennifer Granick* and *American Civil Liberties Union Foundation*, San Francisco, California; with whom on the brief was *Jennifer Lynch* and *Electronic Frontier Foundation*, San Francisco, California.

2021 WI 68

NOTICE

This opinion is subject to further editing and modification. The final version will appear in the bound volume of the official reports.

No. 2019AP1404-CR
(L.C. No. 2016CF1309)

STATE OF WISCONSIN : IN SUPREME COURT

State of Wisconsin,

Plaintiff-Respondent,

v.

George Steven Burch,

Defendant-Appellant.

FILED

JUN 29, 2021

Sheila T. Reiff
Clerk of Supreme Court

HAGEDORN, J., delivered the majority opinion of the Court, in which ZIEGLER, C.J, ROGGENSACK, and REBECCA GRASSL BRADLEY, JJ., joined, and in which DALLET and KAROFSKY, JJ., joined with respect to Parts I. and II.B. REBECCA GRASSL BRADLEY, J., filed a concurring opinion. DALLET, J., filed an opinion concurring in part and dissenting in part, in which KAROFSKY, J., joined and in which ANN WALSH BRADLEY, J., joined except for footnote 1. ANN WALSH BRADLEY, J., filed a dissenting opinion.

APPEAL from a judgment of the Circuit Court for Brown County. *Affirmed.*

¶1 BRIAN HAGEDORN, J. George Steven Burch appeals a judgment of conviction for first-degree intentional homicide on the grounds that two pre-trial evidentiary motions were incorrectly denied.

¶2 First, relying on the Fourth Amendment, Burch moved to suppress the admission of incriminating cell phone data. This data was obtained via an unrelated criminal investigation and kept in a police database. A different law enforcement agency investigating the homicide came upon this data and used it to connect Burch to the homicide. Burch argues that the initial download of the data exceeded the scope of his consent, the data was unlawfully retained, and the subsequent accessing of the data violated his reasonable expectation of privacy. We conclude that even if some constitutional defect attended either the initial download or subsequent accessing of the cell phone data, there was no law enforcement misconduct that would warrant exclusion of that data. Therefore, we conclude the circuit court correctly denied Burch's motion to suppress that data.

¶3 Regarding the second pre-trial evidentiary motion, Burch asks us to reverse the circuit court's discretionary decision to admit evidence from a Fitbit device allegedly worn by the victim's boyfriend at the time of the homicide. This evidence, Burch maintains, should have been accompanied by expert testimony and was insufficiently authenticated. We agree with the State that the circuit court's decision to admit this evidence was not an erroneous exercise of discretion. Burch's judgment of conviction is affirmed.

I. BACKGROUND

¶4 On May 20, 2016, Nicole VanderHeyden went to a bar with her boyfriend, Douglass Detrie. The two became separated

and, in the course of a subsequent phone call and text messages, got into an argument. Detrie returned alone to their shared home. The next day, VanderHeyden's body was discovered next to a nearby field. Her blood-stained clothing was later found discarded alongside a freeway on-ramp, and some of her blood and hair were identified outside the house of VanderHeyden's neighbor. The Brown County Sheriff's Office (the "Sheriff's Office") opened a homicide investigation that spanned the next several months. Detrie was initially a suspect, but the focus of the investigation shifted away from Detrie in part because his Fitbit device logged only 12 steps during the hours of VanderHeyden's death.[1]

¶5 While the Sheriff's Office investigated VanderHeyden's homicide, the Green Bay Police Department (the "Police Department") undertook an unrelated investigation into three incidents involving the same vehicle——a stolen vehicle report, a vehicle fire, and a hit-and-run. George Burch was a suspect in this investigation, and Police Department Officer Robert Bourdelais interviewed him on June 8, 2016. Burch denied involvement and offered the alibi that he was at a bar that night and texting a woman who lived nearby. As Officer Bourdelais testified, "I asked [Burch] if I could see the text messages between him and [the woman], if my lieutenant and I could take a look at his text messages." Burch agreed. Officer

[1] Detrie wore a Fitbit Flex, a wrist-worn device that continuously tracks the wearer's steps and interfaces with the wearer's phone or computer.

Bourdelais then explained that he preferred to download information off the phone because "it's a lot easier to do that than try to take a bunch of pictures and then have to scan those in." "So I asked him if he would be willing to let me take his phone to this detective, download the information off the phone and then I'd bring the phone right back to him . . . and he said that would be fine."

¶6 Before Officer Bourdelais took the phone to be downloaded, Burch signed a consent form. The form read: "I George Stephen Burch . . . voluntarily give Det. Danielski, Officer Bourdelais or any assisting personnel permission to search my . . . Samsung cellphone." Officer Bourdelais took the phone and the signed consent form to the certified forensic computer examiner for the Police Department. The forensic expert performed a "physical extraction" of all the data on Burch's phone, brought the data into a readable format, and saved the extraction to the Police Department's long-term storage. At a motion hearing, the forensic expert testified that this was consistent with the Police Department's standard practice.

¶7 Two months later, two Sheriff's Office detectives continuing the investigation of VanderHeyden's homicide matched a DNA sample from VanderHeyden's sock to Burch. The detectives then searched their own department's records and the records of other local departments for prior police contacts with Burch. There they discovered the Police Department's file related to the three vehicle-related incidents. The file included Burch's

signed consent form and a copy of the data the Police Department extracted from Burch's phone during the search. It also contained a narrative written by Officer Bourdelais which indicated Burch said Officer Bourdelais "could take his phone to the department to have the information on it downloaded." Nothing in the consent form, the narrative, or anything else in the file, indicated that Burch limited the scope of the data he consented to have downloaded from his phone.

¶8 The Sheriff's Office detectives reviewed the data downloaded from Burch's phone. They noted that Burch's internet history included 64 viewings of news stories about VanderHeyden's death. And they also discovered Burch had an email address associated with a Google account. In light of this discovery, the Sheriff's Office detectives procured a search warrant to obtain the "Google Dashboard" information from Google corresponding to Burch's email address. The data Google provided contained location information that placed Burch's phone at a bar VanderHeyden visited the night of her death, a location near VanderHeyden's residence, the place where VanderHeyden's body was found, and the on-ramp where VanderHeyden's discarded clothing was discovered.

¶9 Burch was arrested and charged with VanderHeyden's death. He filed two pre-trial evidentiary motions relevant to this appeal.

¶10 In one motion, Burch sought to suppress the data obtained from his cell phone for two reasons: (1) the Police Department's extraction of the data exceeded the scope of

Burch's consent by obtaining all the phone's data, rather than just the text messages; and (2) the Sheriff's Office unlawfully accessed the data in August 2016. The circuit court[2] denied Burch's motion. It concluded that the conversation between Burch and Officer Bourdelais did not limit the scope of Burch's consent, and that "the sharing of such information, without first obtaining a warrant, is a common and long-understood practice between related departments."

¶11 Burch also moved to exclude evidence related to Detrie's Fitbit device. He argued the State must produce an expert to establish the reliability of the science underlying the Fitbit device's technology and that the State failed to sufficiently authenticate the records. The circuit court disagreed and refused to exclude the Fitbit evidence related to step-counting.[3]

¶12 Burch testified in his own defense at trial. He denied killing VanderHeyden, but acknowledged he was with her the night she died. According to Burch, he met VanderHeyden at a bar, and the two left together. After parking near VanderHeyden's house, they became intimate. That, Burch said, was the last thing he remembered before waking up on the ground with Detrie there, and VanderHeyden dead. Burch told the jury that Detrie held him at gunpoint and instructed him to move

[2] The Honorable John P. Zakowski of the Brown County Circuit Court presided.

[3] The circuit court granted Burch's motion in part, agreeing to exclude Fitbit evidence related to sleep-monitoring.

VanderHeyden's body into his vehicle, drive to a field, and carry VanderHeyden's body into the ditch. Only then did Burch escape by pushing Detrie, running back to his vehicle, and driving away. Burch added that on his way home he noticed that articles of VanderHeyden's clothing were still in his vehicle and threw them out the window in a panic. In the months that followed, Burch told no one this version of events, even as authorities sought the public's help in solving VanderHeyden's homicide.

¶13 The jury found Burch guilty of first-degree intentional homicide, and the circuit court sentenced him to life in prison. Burch appealed, challenging the circuit court's denial of his motion to suppress the cell phone data and his motion to exclude the Fitbit evidence. The court of appeals certified the case to us, and we accepted the certification.

II. DISCUSSION

A. Cell Phone Data

¶14 Burch asks us to reverse the circuit court's denial of his motion to suppress the cell phone data as contrary to the Fourth Amendment. The Fourth Amendment protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. On review of a circuit court's denial of a suppression motion, we uphold the circuit court's findings of historical fact unless they are clearly erroneous, and independently apply constitutional principles to those facts.

State v. Robinson, 2010 WI 80, ¶22, 327 Wis. 2d 302, 786 N.W.2d 463.

¶15 Before us, Burch argues the cell phone data was obtained in violation of the Fourth Amendment for three reasons: (1) the Police Department obtained the data without his consent; (2) the Police Department unlawfully retained the data after its investigation into the vehicle-related incidents had ended; and (3) the Sheriff's Office unlawfully accessed the data in the Police Department's records without a warrant.[4] However, for the reasons that follow, regardless of whether the data was unlawfully obtained or accessed, we conclude suppression of the data is not warranted under the exclusionary rule. See Herring v. United States, 555 U.S. 135, 139 (2009) (accepting the "assumption that there was a Fourth Amendment violation" and analyzing whether the exclusionary rule applied); see also State v. Kerr, 2018 WI 87, ¶¶20-24, 383 Wis. 2d 306, 913 N.W.2d 787.

1. The Exclusionary Rule

¶16 "When there has been an unlawful search, a common judicial remedy for the constitutional error is exclusion." State v. Dearborn, 2010 WI 84, ¶15, 327 Wis. 2d 252, 786

[4] Burch forfeited his argument related to the Police Department's retention of the cell phone data by not raising that argument before the circuit court. See State v. Huebner, 2000 WI 59, ¶10, 235 Wis. 2d 486, 611 N.W. 2d 727. His arguments regarding the initial download of the data and the subsequent accessing of the data are, however, properly before us.

N.W.2d 97. The exclusionary rule is a judicially-created, prudential doctrine designed to compel respect for the Fourth Amendment's constitutional guaranty. Davis v. United States, 564 U.S. 229, 236 (2011). In recent years, the United States Supreme Court has significantly clarified the purpose and proper application of the exclusionary rule. See id.; Herring, 555 U.S. 135. In Davis, the Supreme Court explained that prior cases suggested that the exclusionary rule "was a self-executing mandate implicit in the Fourth Amendment itself." 564 U.S. at 237. However, more recent cases have acknowledged that the exclusionary rule is not one of "reflexive" application, but is to be applied only after a "rigorous weighing of its costs and deterrence benefits." Id. at 238. Thus, in both Herring and Davis, the Court explained that to "trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." Herring, 555 U.S. at 144; see also Davis, 564 U.S. at 240.

¶17 The "sole purpose" of the exclusionary rule "is to deter future Fourth Amendment violations." Davis, 564 U.S. at 236-37. Therefore, exclusion is warranted only where there is some present police misconduct, and where suppression will appreciably deter that type of misconduct in the future. Id. at 237. The exclusionary rule applies only to police misconduct that can be "most efficaciously" deterred by exclusion. Id. (quoting United States v. Calandra, 414 U.S. 338, 348 (1974)).

Specifically, "the exclusionary rule serves to deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence." Herring, 555 U.S. at 144. "But when the police act with an objectively reasonable good-faith belief that their conduct is lawful, or when their conduct involves only simple, isolated negligence, the deterrence rationale loses much of its force, and exclusion cannot pay its way." Davis, 564 U.S. at 238 (cleaned up).

¶18 "Real deterrent value is a 'necessary condition for exclusion,' but it is not 'a sufficient' one." Id. at 237 (quoting Hudson v. Michigan, 547 U.S. 586, 596 (2006)). In Davis, the Court explained that the "analysis must also account for the 'substantial social costs' generated by the rule." Id. (quoting United States v. Leon, 468 U.S. 897, 907 (1984)). It elaborated:

> Exclusion exacts a heavy toll on both the judicial system and society at large. It almost always requires courts to ignore reliable, trustworthy evidence bearing on guilt or innocence. And its bottom-line effect, in many cases, is to suppress the truth and set the criminal loose in the community without punishment. Our cases hold that society must swallow this bitter pill when necessary, but only as a "last resort." For exclusion to be appropriate, the deterrence benefits of suppression must outweigh its heavy costs.

Id. (citations omitted).

¶19 Applying this rationale, the Supreme Court in Herring held that a county's failure to update a computer database to reflect the recall of an arrest warrant was only negligent, and therefore was "not enough by itself to require 'the extreme

sanction of exclusion.'" 555 U.S. at 140 (quoting Leon, 468 U.S. at 916). Similarly, in Davis, the Supreme Court refused to exclude evidence that was obtained via a search conducted in compliance with binding, but subsequently overruled, precedent. 564 U.S. at 232. Exclusion, it explained, was inappropriate because it "would do nothing to deter police misconduct." Id.

¶20 We have followed suit as well. In Kerr, we explained that no police misconduct occurred when an officer conducted an arrest relying on dispatch's confirmation that the defendant had a warrant out for his arrest. 383 Wis. 2d 306, ¶22. Exclusion was improper because "the officers' conduct [was] at most negligent, and isolated negligence is not 'misconduct' for purposes of the exclusionary rule." Id. (citing Herring, 555 U.S. at 146-47).

¶21 Many more examples could be provided,[5] but the principle is clear: unless evidence was obtained by sufficiently deliberate and sufficiently culpable police misconduct, "[r]esort to the massive remedy of suppressing

[5] See, e.g., United States v. Leon, 468 U.S. 897, 916 (1984) (reasonable reliance on a warrant later held invalid); Illinois v. Krull, 480 U.S. 340, 342 (1987) (reasonable reliance on subsequently invalidated statutes); Arizona v. Evans, 514 U.S. 1, 15-16 (1995) (reasonable reliance on arrest warrant information in a database maintained by judicial employees); State v. Ward, 2000 WI 3, ¶63, 231 Wis. 2d 723, 604 N.W.2d 517 (reasonable reliance on settled law subsequently overruled); State v. Dearborn, 2010 WI 84, ¶44, 327 Wis. 2d 252, 786 N.W.2d 97 (refusing to exclude evidence where doing so "would have absolutely no deterrent effect on officer misconduct").

evidence of guilt is unjustified."[6] Hudson, 547 U.S. at 599. With these principles in mind, we turn to the facts at hand.

2. Application

¶22 In this case, the Sheriff's Office detectives acted by the book. After a DNA sample from VanderHeyden's sock matched Burch, officers checked the interdepartmental records already on file with the police.[7] They discovered the two-month-old Police Department file documenting the investigation for the vehicle-related incidents. In it, they found and reviewed Burch's signed consent form and Officer Bourdelais' narrative further documenting Burch's consent. The Sheriff's Office detectives observed that neither the consent form nor the narrative listed any limitations to the scope of consent. And the officers reviewed the downloaded data, having every reason to think it was lawfully obtained with Burch's unqualified consent.

¶23 Burch argues that the Sheriff's Office should have obtained a warrant before accessing the Police Department's

[6] Failure to apply exclusion is usually described in our cases as the "good faith" exception to the exclusionary rule. See, e.g., Dearborn, 327 Wis. 2d 252, ¶4. However, the United States Supreme Court has called the "good faith" label confusing. Herring v. United States, 555 U.S. 135, 142 (2009). The Supreme Court's most recent cases do not use that phrase as a catchall for cases where exclusion is improper, and do not describe their conclusion that exclusion was inappropriate as applying a "good faith" exception. See id. at 147-48; Davis v. United States, 564 U.S. 229, 249-50 (2011).

[7] Officers from both the Police Department and the Sheriff's Office testified that it is common police practice for agencies to share records with other agencies.

data. But no case from this court or the federal courts has suggested that accessing evidence previously obtained by a sister law enforcement agency is a new search triggering a renewed warrant requirement.[8] Rather, the Sheriff's Office detectives reasonably relied on Burch's signed consent form and Officer Bourdelais' narrative to conclude that Burch consented to the download of the data. They had no reason to think they were engaging in illegal activity by reviewing interdepartmental files and evidence. Far from it. Reliance on well-documented computer records, like the detectives did here, is something the Supreme Court has characterized as objectively reasonable police conduct. Arizona v. Evans, 514 U.S. 1, 15-16 (1995). Thus, there was no misconduct that would "render[] the evidence suppressible under the exclusionary rule." Kerr, 383 Wis. 2d 306, ¶22.

¶24 Moreover, even if the Sheriff's Office's actions could be labeled as some kind of misconduct, nothing they did would rise beyond mere negligence. See id., ¶22 (concluding that "to the extent that looking at a warrant before executing it may be

[8] Justice Dallet's concurrence/dissent argues that courts should treat cell phone data collected by law enforcement differently than other types of evidence. It acknowledges that the sharing of already-collected evidence without a warrant by sister law enforcement agencies is routine and unproblematic, but maintains a different kind of analysis should attend cell phone evidence. We need not decide this question to conclude exclusion is not warranted in this case. Justice Dallet's approach would break new ground in Fourth Amendment jurisprudence, and as such, the violation of her new proposed rule does not implicate the kind of gross or systemic law enforcement misconduct the exclusionary rule is meant to deter.

best practice," failing to do so was "at most negligent"); Herring, 555 U.S. at 140 (holding that a county's failure to update a computer database was negligent and therefore "not enough by itself to require" exclusion). And mere negligence does not warrant suppression. Id. at 144-45.

¶25 In addition, the societal cost of excluding the cell phone data would far outweigh any deterrence benefit that exclusion might provide. See Dearborn, 327 Wis. 2d 252, ¶35. This is in part because there is nothing concerning under current Fourth Amendment doctrine with how the Sheriff's Office detectives conducted themselves. Even if the Police Department's initial download or retention gave cause for concern, it's not clear what behavior by the Sheriff's Office Burch would have this court seek to deter.[9] Based on the arguments presented, Burch has given us no reason to deter law enforcement reliance on the computer records of other law enforcement agencies. In this case, the societal cost of

[9] Many of Burch's arguments focus on the conduct of the Police Department and the initial download of his cell phone data. He argues that because the Police Department unlawfully obtained the data, any subsequent accessing of the data violated the Fourth Amendment because he retained a reasonable expectation of privacy in it. But the conduct of the Police Department has little bearing on whether we should apply the exclusionary rule against the Sheriff's Office in this case. The Police Department's involvement in this case was limited to an investigation of unrelated crimes and was only fortuitously useful to the Sheriff's Office's investigation of VanderHeyden's homicide months later. Exclusion therefore would not serve as a meaningful deterrent for the Police Department and is not warranted on that basis.

exclusion would far outweigh the limited benefit——if any——its application could achieve.

¶26 We conclude that suppression of Burch's cell phone data is not warranted under the exclusionary rule. Regardless of whether a constitutional violation occurred, there was no police misconduct to trigger application of the exclusionary rule.

B. Fitbit Evidence

¶27 Burch also appeals the circuit court's denial of his motion to exclude evidence associated with Detrie's Fitbit device. Burch offers two arguments. First, he argues the Fitbit evidence must be excluded because the State did not produce expert testimony to establish its reliability. Second, he maintains the Fitbit evidence was insufficiently authenticated.[10] We review these evidentiary rulings for an erroneous exercise of discretion. State v. Nelis, 2007 WI 58, ¶26, 300 Wis. 2d 415, 733 N.W.2d 619.

[10] Burch also argues that admission of the Fitbit evidence violates the Confrontation Clause of the Sixth Amendment to the United States Constitution. Burch concedes, however, that his novel argument "does not neatly fit within the test set forth in Crawford v. Washington, 541 U.S. 36 (2004)," and that he raised the issue solely "to preserve for review before higher courts." Accordingly, we reject Burch's Confrontation Clause claim and do not address it further.

1. Expert Testimony

¶28 We have held that that "the requirement of expert testimony is an extraordinary one" and should apply only "when the issues before the jury are 'unusually complex or esoteric.'" State v. Kandutsch, 2011 WI 78, ¶28, 336 Wis. 2d 478, 799 N.W.2d 865 (quoting another source). Before compelling expert testimony, "the circuit court must first find that the underlying issue is 'not within the realm of the ordinary experience of mankind.'" Id. (quoting Cramer v. Theda Clark Mem'l Hosp., 45 Wis. 2d 147, 150, 172 N.W.2d 427 (1969)). What falls within the "ordinary experience of mankind," meanwhile, turns on the circuit court's exercise of its discretion "on a case-by-case basis" to decide whether "the issue is outside the realm of lay comprehension" or within the "common knowledge" of "the average juror." Id., ¶29.

¶29 Burch argues that the Fitbit evidence was improperly admitted because the circuit court should have required expert testimony to establish the reliability of the science underlying Fitbit's technology. He notes that the Fitbit device features "a three-axis accelerometer sensor that generates data representing the user's movements," but explains that his "greater concern is with how the device processes the data into a meaningful output, how that output is exchanged with a phone or computer, and how that evidence ultimately ended up in Fitbit's business records."

¶30 In its written order rejecting Burch's argument that expert testimony was required, the circuit court explained that

Fitbit's step counters have been in the marketplace since 2009, and the "principle idea behind pedometers . . . for a significantly longer period than that." Many smartphones, the court added, "come equipped with a pedometer by default." Analogizing to a watch and a speedometer, the court noted that even though the average juror may not know "the exact mechanics" of a technology's "internal workings," the public may nevertheless "generally understand[] the principle of how it functions and accept[] its reliability." Similarly, the court reasoned, a Fitbit's use of sophisticated hardware and software does not render it an "unusually complex or esoteric" technology because the average juror is nevertheless familiar with what a Fitbit does and how it is operated.

¶31 This conclusion was reasonable and within the circuit court's discretionary authority. The circuit court correctly interpreted the standard for requiring expert testimony and reasonably applied that standard to the Fitbit evidence before it. Given the widespread availability of Fitbits and other similar wireless step-counting devices in today's consumer marketplace, the circuit court reasonably concluded Detrie's Fitbit was not so "unusually complex or esoteric" that the jury needed an expert to understand it.[11] The circuit court's

[11] To the extent Burch now argues that the Fitbit is outside the realm of lay comprehension because it is an "internet of things" device, we are unpersuaded. Wireless technology is nothing new. It is entirely within the "ordinary experience of mankind" to use a Bluetooth or Wi-Fi connection to transfer data from one device to another.

conclusion that expert testimony was not required under these circumstances was within the circuit court's discretion.[12]

2. Authentication

¶32 Wisconsin Stat. § 909.01 (2019-20)[13] sets out the evidentiary standard for authentication: "The requirements of authentication or identification as a condition precedent to admissibility are satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims." Simply put, authentication requires that a circuit court conclude, within its discretion, that the finder of fact could reasonably determine that the evidence sought to be admitted is what its proponent says it is. Id.; State v. Smith, 2005 WI 104, ¶¶31-33, 283 Wis. 2d 57, 699 N.W.2d 508. In this case, that means the State's authentication obligation is to present sufficient evidence to support a finding that the records produced by the State are in fact Fitbit's records associated with Detrie's Fitbit device.

¶33 Notably, Burch does not actually disagree that the State's records are accurate copies of Fitbit's records associated with Detrie's Fitbit device. Instead, he focuses his challenge on whether the State properly authenticated "the

[12] Of course, opposing counsel may attack the reliability of admitted evidence. T.A.T. v. R.E.B., 144 Wis. 2d 638, 652-53, 425 N.W.2d 404 (1988).

[13] All subsequent references to the Wisconsin Statutes are to the 2019-20 version unless otherwise indicated.

information within those records." Specifically, he argues that "the State failed to show that the Fitbit device reliably and accurately registered Detrie's steps that evening, and that that data was reliably and accurately transmitted to Fitbit's business records without manipulation."

¶34 Burch's argument reaches beyond the threshold question authentication presents. The circuit court's authentication obligation is simply to determine whether a fact-finder could reasonably conclude evidence is what its proponent claims it to be. Wis. Stat. § 909.01. The circuit court did so here by reviewing the Fitbit records and the affidavit of "a duly authorized custodian of Fitbit's records" averring that the records "are true and correct copies of Fitbit's customer data records," and then concluding the data was self-authenticating under Wis. Stat. § 909.02(12).[14] The circuit court's obligation is not to scrutinize every line of data within a given record and decide whether each line is an accurate representation of the facts. Rather, once the circuit court concludes the fact-finder could find that the records are what their proponent claims them to be, the credibility and weight ascribed to those

[14] More precisely, the circuit court held that the records were self-authenticating as certified records of regularly conducted activity. See Wis. Stat. § 909.02(12). Burch has not, either before the circuit court or this court, challenged the statements in the affidavit from Fitbit certifying that the records it provided are accurate copies of its records associated with Detrie's Fitbit device.

records are questions left to the finder of fact.[15] State v. Roberson, 2019 WI 102, ¶25, 389 Wis. 2d 190, 935 N.W.2d 813. The circuit court's conclusion that the Fitbit records were sufficiently authenticated therefore was within its discretion.

III. CONCLUSION

¶35 Burch's appeal of his conviction for first-degree intentional homicide challenged the denial of two pre-trial evidentiary orders. We uphold both orders, and therefore affirm the judgment of conviction. Burch's cell phone data was properly admitted because, even if there was some constitutional defect in how it was obtained or retained, exclusion would be an improper remedy. The circuit court also permissibly exercised its discretion in admitting the Fitbit evidence; no expert was required and the State sufficiently authenticated the records from Fitbit.

By the Court.——The judgment of the circuit court is affirmed.

[15] Here, too, opposing counsel can attack the reliability of admitted evidence. See T.A.T., 144 Wis. 2d at 652-53.

¶36 REBECCA GRASSL BRADLEY, J. *(concurring).* I join the majority opinion in full. Because there are no controlling cases interpreting the Fourth Amendment to prohibit the second search of Burch's cellphone by the Brown County Sheriff's Office (Sheriff's Office), the exclusionary rule does not apply and suppression of the evidence obtained from that search would be improper.[1] I write separately to discuss the application of the Fourth Amendment to warrantless second searches of smartphones without consent.

¶37 Under the original meaning of the Fourth Amendment, law enforcement generally will need a warrant to search the contents of a smartphone, absent an exception to the warrant requirement. The consent-to-search exception, which the State argues authorized law enforcement to conduct a second search of Burch's smartphone data, does not extend to a second search of a smartphone by a different law enforcement agency investigating an entirely separate crime. "Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life.'" Riley v. California, 573 U.S. 373, 403 (2014) (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)). The Fourth Amendment secures "'the privacies of life' against 'arbitrary power,'" and embodies the "central aim of the Framers . . . 'to place obstacles in the way of a too permeating

[1] I also agree with the majority that the circuit court did not erroneously exercise its discretion by admitting evidence from Douglass Detrie's Fitbit device.

police surveillance.'" Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) (quoted sources omitted).

¶38 The contents of smartphones constitute "papers" and "effects" secured by the Fourth Amendment, giving each of those categories their historical meanings and bearing in mind that "a cell phone search would typically expose to the government far more than the most exhaustive search of a house." Riley, 573 U.S. at 396. Accordingly, law enforcement generally must get a warrant before searching a cell phone. Id. at 403. Because Burch's consent to search covered only the Green Bay Police Department's initial search of his smartphone for evidence related to a hit-and-run investigation, a warrant should have been procured before the Sheriff's Office searched Burch's smartphone data as part of an unrelated murder investigation. Because neither this court nor the United States Supreme Court has decided this novel issue, the Sheriff's Office committed no misconduct in searching Burch's cell phone and the circuit court properly admitted the evidence obtained from the search. Accordingly, I respectfully concur.

I

¶39 In June 2016, a few weeks after Nicole VanderHeyden's murder and the ensuing investigation by the Sheriff's Office, the Green Bay Police Department (Police Department) began investigating an entirely unrelated crime: an auto theft that resulted in a hit-and-run incident.[2] The stolen car belonged to Burch's roommate, and law enforcement identified Burch as a

[2] The vehicle was also lit on fire.

person of interest because he had last driven the car. Officer Robert Bourdelais of the Police Department interviewed Burch about the hit and run. Burch denied any involvement, but informed Officer Bourdelais that, on the night of the hit and run, he was texting a woman who lived one block away from the location of the accident. Burch stated that he did not go to the woman's house on the night of the incident, and never made arrangements to go to her house. According to Officer Bourdelais' testimony, he and Burch had the following exchange:

> I asked him if I could see the text messages between him and [the woman], if my lieutenant and I could take a look at his text messages. He said that we could . . . . I [then] asked him if he would be willing to let me take his phone to this detective, download the information off the phone and then I'd bring the phone right back to him, probably take a half an hour and he said that would be fine.

¶40 The attorney eliciting Officer Bourdelais' testimony inquired: "When you asked [Burch] about downloading the information off of his phone, did you specifically limit the information to the text messages when you were talking to him?" Officer Bourdelais responded:

> No, I didn't. Initially, when I had asked him, hey, do you mind if we take a look at those text messages, I refer to them as text messages because he said he was texting [the woman] back and forth, but from my experience as a police officer I know people communicate [by] phone calls, text messages, texting apps like WhatsApp, MINE, Facebook Messenger, things like that. So that's the information, I wanted information to corroborate that whatever conversation he had with [the woman] or communication he had supported his claims that he never went over to her house or made arrangements to go over to her house.

¶41 Following the exchange between Burch and Officer Bourdelais, Burch signed a consent form which read as follows: "I, George Stephen Burch, . . . voluntarily give Det. Danielski, Officer Bourdelais, or any assisting personnel permission to search my . . . Samsung cellphone." Subsequently, at the instruction of Officer Bourdelais, a Police Department forensic examiner downloaded all of the data from Burch's cellphone into the Police Department records database. The forensic examiner then converted the data into a readable format, and tabbed the data into categories such as text messages, images, and internet history. At the homicide trial, the forensic examiner testified that the Police Department retains smartphone data for an indefinite amount of time, noting that "[e]ver since [she] [has] been employed with [the Police Department], [they] have saved all extractions for long-term storage for as far back as [she] [has] been employed," which was roughly two years at the time of trial.

¶42 In August 2016 (two months after Burch consented to the search of his phone for the hit-and-run investigation), the Sheriff's Office identified Burch as a person of interest in the investigation into the murder of VanderHeyden based upon a DNA match on VanderHeyden's socks. Relying on databases shared between the Sheriff's Office and other local entities, detectives from the Sheriff's Office discovered that the Police Department had prior contact with Burch while investigating the unrelated hit-and-run incident. After the detectives learned that the Police Department had extracted all of Burch's

smartphone data in June 2016, they procured a copy of the data from the Police Department and searched its contents "for anything in the timeframe of the night of [the murder] into the [following] morning, whether it be calls, texts, internet history, any kind of location data available from that device." The detectives did not obtain a warrant for this search. In reviewing the data, the detectives discovered that, shortly after the murder, Burch repeatedly searched for news articles about the murder using his internet browser.

¶43 Additionally, during their warrantless search of the smartphone's contents, the detectives learned that Burch had a Google email account (Gmail). The detectives were aware that Gmail addresses are associated with a Google Dashboard, which tracks an individual's location based upon GPS, Wi-Fi, and cellphone tower data. The detectives procured a search warrant to obtain Google Dashboard information from Google. The location data placed Burch's smartphone at various critical places on the night of the murder, including the location of VanderHeyden's body and the on-ramp where her discarded clothing was discovered.

¶44 Burch was arrested and charged with first-degree intentional homicide. In a pre-trial motion, Burch moved to suppress the evidence obtained by the Sheriff's Office from the warrantless search of his smartphone data.[3] Burch argued that the Sheriff's Office "violated the Fourth Amendment when [it]

[3] Burch also filed a motion to exclude evidence related to Detrie's Fitbit device, which the circuit court denied.

searched the phone data initially seized by [the Police Department]." Specifically, Burch contended that the Sheriff's Office "blew past Mr. Burch's scope of consent, and likewise, obliterated any Fourth Amendment warrant exceptions." The circuit court denied Burch's suppression motion, and the State introduced at trial the evidence obtained from the smartphone. The jury convicted Burch of first-degree intentional homicide. Burch appealed the circuit court's decision to admit the evidence procured by the Sheriff's Office from its search of his smartphone data. The court of appeals certified Burch's Fourth Amendment challenge to this court, and we accepted certification.

II

¶45 The Fourth Amendment provides:

> 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.

U.S. Const. amend. IV. "The first clause outlaws promiscuous search and seizure, even as the second clarifies precisely what will be required for a particularized warrant to be valid." Laura K. Donohue, The Original Fourth Amendment, 83 U. Chi. L. Rev. 1181, 1193 (2016); State v. Pinder, 2018 WI 106, ¶¶48-51, 384 Wis. 2d 416, 919 N.W.2d 568. As understood at the time the Fourth Amendment was ratified, "[t]he government could not violate the right against search and seizure of one's person, house, papers, or effects absent either a felony arrest or a

warrant meeting the requirements detailed in the second clause." Donohue, supra, at 1193.

¶46 As the United States Supreme Court has repeatedly held, "the ultimate touchstone of the Fourth Amendment is 'reasonableness.'" Brigham City v. Stuart, 547 U.S. 398, 403 (2006). "[W]hether an individual has a reasonable expectation of privacy in avoiding the method of search and a reasonable expectation of privacy in the place searched are the questions that drive a court's examination of the reasonableness of the search." State v. Brereton, 2013 WI 17, ¶32, 345 Wis. 2d 563, 826 N.W.2d 369. "The general rule is that searches and seizures conducted without a warrant are not reasonable." State v. Randall, 2019 WI 80, ¶10, 387 Wis. 2d 744, 930 N.W.2d 223. However, there are a number of exceptions to the warrant requirement. See Riley, 573 U.S. at 382 ("In the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement."). "One of the exceptions to the warrant rule is that an individual's consent to search satisfies the constitutional 'reasonableness' requirement." Randall, 387 Wis. 2d 744, ¶10; see also Birchfield v. North Dakota, 136 S. Ct. 2160, 2185 (2016) ("It is well established that a search is reasonable when the subject consents[.]"). "If a search is premised on an individual's consent, it must cease immediately upon revocation of that consent," and an individual "may of course delimit as she chooses the scope of the search to which

she consents." Randall, 387 Wis. 2d 744, ¶10 (internal alterations and citations omitted).

¶47 Just a few years ago, the United States Supreme Court addressed the Fourth Amendment's application to a modern phenomenon: the proliferation of smartphones and their ever-increasing capacity to store mass amounts of data. The Court held that law enforcement generally must obtain a warrant before conducting a search of smartphone data. Specifically, the Riley Court clarified that "[its] holding . . . is not that the information on a cell phone is immune from search," but "instead that a warrant is generally required before such a search, even when a cell phone is seized incident to arrest."[4] Riley, 573 U.S. at 401. In reaching this holding, the Court recognized the "pervasiveness that characterizes cell phones" and how "[c]ell phones differ in both a quantitative and a qualitative sense from other objects." Id. at 393, 395. "The possible intrusion on privacy is not physically limited in the same way [as other objects] when it comes to cell phones." Id. at 394. "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," and "historic location

[4] Although Riley involved the search-incident-to-arrest exception to the Fourth Amendment warrant requirement, the principles it espouses apply more broadly. See Riley v. California, 573 U.S. 373, 386 (2014) ("[O]fficers must generally secure a warrant before conducting such a search [of a cell phone]."); see also People v. Hughes, 958 N.W.2d 98, 108 (Mich. 2020) ("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.").

information" could allow law enforcement to "reconstruct someone's specific movements down to the minute." Id. at 395-96.

¶48 The United States Supreme Court fully understood that its decision "[would] have an impact on the ability of law enforcement to combat crime." Id. at 401. After all, "[c]ell phones have become important tools in facilitating coordination and communication" for individuals committing crimes and "can provide valuable incriminating information about dangerous criminals." Id. But "[p]rivacy comes at a cost." Id. And the Fourth Amendment is designed to safeguard the people's security against unreasonable government intrusion. Riley recognizes that the Fourth Amendment safeguards this right by generally requiring law enforcement to procure a warrant before searching a smartphone.

¶49 A warrant requirement for searches of smartphone data comports with the original meaning of the Fourth Amendment. The Framers, "after consulting the lessons of history, designed our Constitution to place obstacles in the way of a too permeating police surveillance, which they seemed to think was a greater danger to a free people than the escape of some criminals from punishment." United States v. Di Re, 332 U.S. 581, 595 (1948). In particular, "the Fourth Amendment was the founding generation's response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity. Opposition to such searches was

in fact one of the driving forces behind the Revolution itself." Riley, 573 U.S. at 403. "Indeed, the character of that threat implicates the central concern underlying the Fourth Amendment—— the concern about giving police officers unbridled discretion to rummage at will among a person's private effects." Arizona v. Gant, 556 U.S. 332, 345 (2009). For the Framers, it was absolutely necessary to ensure "the government not be allowed free rein to search for potential evidence of criminal wrongdoing." Donohue, supra, at 1194.

¶50 The Framers designed the Fourth Amendment to protect the people from government overreach. Described as the "very essence of constitutional liberty and security," the Fourth Amendment applies to "all invasions on the part of the government and its employes of the sanctity of a man's home and the privacies of life." Boyd, 116 U.S. at 630. "It is not the breaking of [one's] doors, and the rummaging of his drawers, that constitutes the . . . offense; but it is the invasion of his infeasible right of personal security, personal liberty, and private property[.]" Id. With this understanding in mind, "[t]he Supreme Court has . . . confirmed that the basic purpose of the Fourth Amendment 'is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials'"——that is, "to secure 'the privacies of life' against 'arbitrary power.'" Matthew DeVoy Jones, Cell Phones are Orwell's Telescreen: The Need for Fourth Amendment Protection in Real-Time Cell Phone Location Information, 67

Clev. St. L. Rev. 523, 533 (2019) (quoting Carpenter, 138 S. Ct. at 2213-14).

¶51 The Fourth Amendment specifically recognizes the right of people to be secure in their "persons, houses, papers, and effects." U.S. Const. amend. IV; see United States v. Jones, 565 U.S. 400, 406 (2012) ("[F]or most of our history the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas ('persons, house, papers, and effects') it enumerates."). Much modern analysis of the Fourth Amendment has centered upon the primacy of protecting "houses." See Payton v. New York, 445 U.S. 573, 589 (1980) ("The Fourth Amendment protects the individual's privacy in a variety of settings. In none is the zone of privacy more clearly defined than when bounded by the unambiguous physical dimensions of an individual's home[.]"). However, as the Riley Court explained, smartphones implicate privacy interests more compelling than even those associated with the home. "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[.]" Riley, 573 U.S. at 396-97.

¶52 Given the nature of its contents, a smartphone is not just another personal item; it is a device that holds many modern "privacies of life"——an area that receives acute and particularized protection from government interference under the

Fourth Amendment. See Boyd, 116 U.S. at 630. Governmental searches of smartphones invade "the indefeasible right of personal security, personal liberty, and private property," which Americans hold "sacred." Id. Permitting law enforcement to rummage through the data residing in smartphones without a warrant would "allow[] free rein to search for potential evidence of criminal wrongdoing," which the Fourth Amendment prohibits. With respect to smartphone data, as in the home, "all details are intimate details, because the entire area is held safe from prying government eyes." See Kyllo v. United States, 533 U.S. 27, 37 (2001).

¶53 The Fourth Amendment includes both "papers" and "effects" among the four enumerated categories protected from unreasonable searches. The contents of smartphones constitute "papers" within the original understanding of the Fourth Amendment. "Historically, private papers, including documents and pamphlets that challenged governmental power, served as a central point of contestation in the Founding era." Andrew Guthrie Ferguson, The "Smart" Fourth Amendment, 102 Cornell L. Rev. 547, 595-96 (2017). The Fourth Amendment's protection of "papers" "reflect[s] the importance of freedom of thought, expression, and communication." Id. According to Lord Camden in his seminal decision in Entick v. Carrington, "papers are often the dearest property a man can have." 19 How. St. Tr. 1029 (C.P. 1765).

¶54 The Framers' inclusion of "papers" within the protections of the Fourth Amendment was motivated in part by the

case of John Wilkes, "who was targeted for writing mocking articles about King George III" and had his papers seized by investigating officers. Ferguson, supra, at 596 (citation omitted). "The Wilkes controversy . . . directly influenced the [F]ramers of the Fourth Amendment. The English search and seizure cases received extensive publicity in England and in America, and the Wilkes case was the subject of as much notoriety and comment in the colonies as it was in Britain." Eric Schnapper, Unreasonable Searches and Seizures of Papers, 71 Va. L. Rev. 869, 912-13 (1985). "Wilkes' cause generated many supporters among American colonists, some of whom became key figures in the framing of the Constitution." Id. at 913. Based upon Wilkes' case, "[p]rotecting private papers . . . became a central rallying cry in the creation of constitutional liberty," receiving explicit protection under the United States Constitution. Ferguson, supra, at 596.

¶55 Today, the people's "papers" largely exist in digital form. "E-mails, texts, and other social media communication have replaced letter writing." Id. at 599. Additionally, calendars, notes, health information, photographs, restaurant and hotel reservations, airline flights, shopping and browsing histories, as well as banking transactions all reside in (or are accessible from) smartphones, forming a digital diary of one's life, accessible from a single source. Given the breadth and detail of this information, "individuals have expectations of privacy in their digital papers." Id. at 600. From the Framers' outrage over the search of Wilkes' papers to the

Court's concern regarding the search of David Riley's smartphone, the overarching aim "has always been the protection of ideas embodied in those papers"——not whether the papers are in physical or digital form. Id. at 613.

¶56 Some portion of the contents of smartphones, as well as the devices themselves, also constitute "effects," which "have historically been understood to mean personal property—— the objects we possess." Id. at 578 (citing Dictionarium Brittanicum (Nathan Baily ed., 1730) (defining "effects" as "the goods of a merchant, tradesman") and Noah Webster, First Edition of an American Dictionary of the English Language (1828) (defining "effects" as "goods; moveables; personal estate")). "The early American understanding distinguished personal property from real property," and "personal property meant physical belongings"——items which were "obviously prized by the Founders" and accordingly received Fourth Amendment protection. Id. Founding-era history "demonstrates that effects were specifically included in the constitutional text [not only] because of the harms to privacy and dignity that could be incurred in their inspection, but also because of the risk of mishandling or damage generally associated with interferences with personal property." Maureen E. Brady, The Lost "Effects" of the Fourth Amendment: Giving Personal Property Due Protection, 125 Yale L.J. 946, 987 (2016). Founding-era sources suggest the Framers understood "[p]ersonal property [to] give[] its owner a right to exclude others from possessing, using, and interfering with the effect"——and most of all to "protect[]

privacy interests with respect to the property." Id. at 993-94 (discussing founding-era sources, including William Blackstone's Commentaries and Lord Camden's judgment in Entick v. Carrington).

¶57 Although "'effects' has captured rather less of the [United States] Supreme Court's attention" than "papers" and "houses," when the Court has addressed the topic, "property considerations loom large." Laura K. Donohue, The Fourth Amendment in a Digital World, 71 N.Y.U. Ann. Surv. Am. L. 553, 679 (2017). For example, in United States v. Jones, the United States Supreme Court held that law enforcement's installation of a GPS device on an individual's vehicle to monitor the vehicle's movements constituted a "search" under the Fourth Amendment, deeming it "beyond dispute" that a vehicle is an "effect" within the meaning of the Fourth Amendment. 565 U.S. 400, 404 (2012). The Court emphasized the government's "physical intrusion" of the "effect" at issue. Id. at 411. The Court did not focus on the physical attachment of the GPS device to the effect but rather the device's capture of sensitive and private information, "relay[ing] more than 2,000 pages of data over [a] 4-week period." Id. at 403; see also Ferguson, supra, at 606 ("[In Jones] the real harm was exposing the revealing personal data about the effect (car)."). That is, in Jones the Fourth Amendment analysis turned on the "capturing of data trails" of the owner and "invad[ing] the informational security of the effect." Ferguson, supra, at 606. The Court's reasoning in Jones applies no less to smartphones and the data they hold,

supporting the characterization of smartphones as "effects" entitled to constitutional protection from unreasonable searches and seizures.

III

¶58 Having established a historical basis for the application of the Fourth Amendment's warrant requirement to smartphones and their data, it is necessary to address the application of the consent exception to the warrant requirement within the context of the facts of Burch's case. It is well-established that "[o]ne of the exceptions to the warrant rule is that an individual's consent to search satisfies the constitutional 'reasonableness' requirement." Randall, 387 Wis. 2d 744, ¶10; see also Birchfield, 136 S. Ct. at 2185. Burch gave consent for the Police Department to download and search his smartphone and its data as part of the investigation of the hit-and-run incident in June 2016. According to his testimony, Officer Bourdelais asked Burch if "[he] could see the text messages between him and [the woman]" on the night of the hit-and-run incident. Officer Bourdelais then asked Burch if he could "take his phone to this detective, download the information off the phone" and then bring it right back to Burch. Burch agreed to all requests in this exchange and signed a consent form saying he "voluntarily give[s] Det. Danielski, Officer Bourdelais, or any assisting personnel permission to search [his] . . . Samsung cellphone." Burch permitted Officer Bourdelais "or any assisting personnel" to download his smartphone's data and search for evidence of the hit-and-run

incident. Burch's consent encompassed the Police Department's investigation of a particular crime. The Constitution permitted this search. Schneckloth v. Bustamonte, 412 U.S. 218, 222 (1973) ("[A] search conducted pursuant to a valid consent is constitutionally permissible.").

¶59 Two months later, a different law enforcement agency—— the Sheriff's Office——searched Burch's smartphone data while investigating an entirely separate crime. This search went beyond the scope of Burch's consent. Officer Bourdelais questioned Burch in June 2016 regarding the hit-and-run incident only, and obtained Burch's consent to download Burch's smartphone data "[to] corroborate that whatever conversation [Burch] had with [the woman] . . . supported his claims that he never went over to her house" the night of the hit and run. The consent form did not include any language authorizing a second search by a separate law enforcement agency for a different crime. The form authorized only Officer Bourdelais, the forensic examiner (Det. Danielski), and their assisting personnel to view the smartphone's contents. Any search beyond the scope of Burch's consent would require a warrant.

¶60 The State argues that this court's decision in State v. Betterley, 191 Wis. 2d 406, 529 N.W.2d 216 (1995), allows law enforcement to take a "second look" at smartphone data that was previously searched. That case does not apply to searches of cell phone data. In Betterley, officers at the St. Croix County Jail seized a ring from the defendant during an inventory search. Id. at 414. Later that day, a New Richmond police

officer asked to see the ring, believing it was evidence that the defendant had committed insurance fraud. Id. at 415. The New Richmond police officer retained the ring as evidence without obtaining a warrant. Id. This court held that "the permissible extent of the second look [at evidence] 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." Id. at 418. Because the defendant had a diminished expectation in privacy in the ring after forfeiting it during the first search, the second look at the ring was permissible, so long as it was "no more intrusive" than the first search. Id.

¶61 Betterley does not apply to cell phone data retrieved pursuant to the owner's consent. Betterley involved an inventory search of an item, not the consent-to-search exception to the warrant requirement. Unlike searches conducted with consent, inventory searches are "administrative by nature, not an investigation motivated by a search for evidence." State v. Weber, 163 Wis. 2d 116, 132, 471 N.W.2d 187 (1991). More importantly, physical items such as rings are qualitatively different than searches of smartphone data. Examination of a ring reveals nothing more than the physically observable item itself, while smartphones contain——and conceal——the "privacies of life," which generally are not viewable by others at a glance. For this reason, smartphones "differ in both a quantitative and a qualitative sense from other objects." Riley, 573 U.S. at 393. "[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." Id. at 395. Certainly, "the possible intrusion on privacy is not physically limited in the same way [as other objects] when it comes to cell phones." Id. at 394. Accordingly, Betterley does not inform the Fourth Amendment analysis governing searches of cell phone data.

¶62 Even if "a Fourth Amendment violation has occurred," however, it "does not mean the exclusionary rule applies," particularly because "exclusion [of evidence] is the last resort." State v. Dearborn, 2010 WI 84, ¶35, 327 Wis. 2d 252, 786 N.W.2d 97. "To trigger the exclusionary rule, police misconduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." Id., ¶36 (quoted source omitted). For the reasons stated in the majority opinion, there was no misconduct by the Sheriff's Office. Neither this court nor the United States Supreme Court has declared that second searches of cell phone data by separate law enforcement agencies require a warrant. Accordingly, suppression of the evidence obtained during the Sheriff's Office's second search would be inappropriate and I respectfully concur.

* * *

¶63 "The great end, for which men entered into society, was to secure their property." Entick v. Carrington, 19 How. St. Tr. 1029 (C.P. 1765) (Lord Camden presiding). "Property must be secured, or liberty cannot exist." Discourses on Davila, in 6 The Works of John Adams 280 (C. Adams ed. 1851). "The Fourth Amendment imposes limits on search-and-seizure powers in order to prevent arbitrary and oppressive interference by enforcement officials with the privacy and personal security of individuals." United States v. Martinez-Fuerte, 428 U.S. 543, 554 (1976). Because smartphones contain the "privacies of life," law enforcement generally needs a warrant to search the data they hold unless an exception to the warrant requirement applies.

¶64 REBECCA FRANK DALLET, J. (*concurring in part, dissenting in part*). Under the Fourth Amendment, when the police want to search a person's private information, they generally need a warrant. The Brown County Sheriff's Office searched George Steven Burch's private cell phone data without obtaining a warrant, assuming that Burch's consent for another agency to download his phone's data for a wholly separate investigation obviated its Fourth Amendment duty to do so. It did not. The Sheriff's Office's warrantless search of Burch's cell phone data violated the Fourth Amendment, and the evidence obtained from that unlawful search should be suppressed. The majority opinion's contrary holding ignores the novel constitutional problems presented by private cell phone information, is inconsistent with the Fourth Amendment's text, and undermines the exclusionary remedy for Fourth Amendment violations. I therefore respectfully dissent from that part of the majority opinion.[1]

I. BACKGROUND

¶65 A Green Bay Police Department (GBPD) officer interviewed Burch while investigating crimes involving the car Burch would borrow for work. Burch denied his involvement but acknowledged that he was text messaging a friend that night who lived near the scene. When the officer asked Burch if he and his lieutenant could see those text messages, Burch verbally consented. After the officer explained that it was easier to

[1] I join Parts I. and II.B. of the majority opinion because I agree that the circuit court permissibly admitted evidence regarding a Fitbit device.

download "the information" from the phone than to take screenshots, Burch verbally consented to allowing the officer to take his phone to a GBPD detective for that purpose.[2] The officer then presented Burch with a standardized written consent form. The form contained the heading "City of Green Bay Police Department" and indicated that Burch "voluntarily" gave a named GBPD officer, a named GBPD detective, as well as any "assisting personnel," "permission to search" his "Samsung Cellphone." Burch signed the form. The officer testified that he requested only "text messages, phone calls, Facebook posts, and photographs taken any time after 11:00 p.m." the night of the accident; yet, to access that information, the GBPD downloaded the entire contents of Burch's phone.

¶66 Two months later, the Sheriff's Office was investigating a homicide that had occurred a few weeks before the crimes being investigated by the GBPD. It matched Burch's DNA to DNA collected from the victim's body, her socks, and a cord believed to be used in her murder. The Sheriff's Office

---

[2] At trial, the officer testified that by "the information," he meant any communications between Burch and his friend that would corroborate Burch's alibi:

> Initially, when I had asked [Burch], hey, do you mind if we take a look at those text messages, I refer to them as text messages because he said he was texting [his friend] back and forth, but from my experience as a police officer I know people communicate phone calls, text messages, texting apps like WhatsApp, MINE, Facebook Messenger, things like that. So that's the information, I wanted information to corroborate that whatever conversation he had with [his friend] or communication he had supported his claims that he never went over to [the victim's] house or made arrangements to go over to her house.

also discovered that the GBPD had retained the full data extraction from Burch's cell phone. After reviewing the GBPD's files and seeing Burch's signed consent form, the Sheriff's Office searched that data without first obtaining a warrant. The search led the Sheriff's Office to Burch's internet search history and his Google email account. The internet history revealed that Burch had viewed online stories about the victim's disappearance 64 times. The email account allowed the Sheriff's Office to issue Google a subpoena for Burch's Google Dashboard records, which included his location data from the night of the murder. The location data placed Burch's cell phone near the victim's residence and the field where her body was discovered around the time of the victim's death.

II. ANALYSIS

¶67 The Fourth Amendment inquiry here is two-fold. The first consideration is whether the Sheriff's Office's warrantless search of the GBPD's download of Burch's data was unreasonable. If so, it violated the Fourth Amendment, and the question becomes whether excluding the unlawfully obtained evidence would sufficiently deter the same police conduct in the future. These questions involve a mixed standard of review, under which we uphold the circuit court's findings of historical fact unless they are clearly erroneous, but we review de novo the application of constitutional principles to those facts. See State v. Blackman, 2017 WI 77, ¶25, 377 Wis. 2d 339, 898 N.W.2d 774.

A. The Sheriff's Office's Warrantless Search Was Unreasonable.

¶68 The Fourth Amendment to the United States Constitution prohibits the government from conducting "unreasonable" searches of a person, a person's home, or her "effects":

> 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 . . . .

The Amendment seeks to secure "the privacies of life" against such unreasonable searches by placing "obstacles in the way of a too permeating police surveillance." See Carpenter v. United States, 585 U.S. ___, 138 S. Ct. 2206, 2214 (2018). Police surveillance amounts to a "search," for purposes of the Fourth Amendment, when it collects information in which the person has a reasonable expectation of privacy. E.g., id. at 2213-14.

¶69 To protect one's reasonable expectation of privacy, the text of the Fourth Amendment communicates a "strong preference for searches conducted pursuant to a warrant." See Illinois v. Gates, 462 U.S. 213, 236 (1983); U.S. Const. amnd. IV. Indeed, a warrantless search is per se unreasonable, see Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973), and presumptively violates the Fourth Amendment, see State v. Tate, 2014 WI 89, ¶27, 357 Wis. 2d 172, 849 N.W.2d 798. That presumption is overcome only when the warrantless search falls under one of the "few specifically established and well-delineated exceptions." State v. Coffee, 2020 WI 53, ¶24, 391 Wis. 2d 831, 943 N.W.2d 845.

¶70 Consent is one such exception. State v. Hogan, 2015 WI 76, ¶55, 364 Wis. 2d 167, 868 N.W.2d 124. As with any

exception to the warrant requirement, consent is "jealously and carefully drawn," and must be "confined in scope" and "strictly circumscribed." See Jones v. United States, 357 U.S. 493, 499 (1958); Terry v. Ohio, 392 U.S. 1, 25-26, 29 (1968). Consent to a particular search must therefore be "unequivocal and specific." State v. Reed, 2018 WI 109, ¶8, 384 Wis. 2d 469, 920 N.W.2d 56. Even absent express limits, the scope of consent is neither "boundless" nor "perpetual." See State v. Douglas, 123 Wis. 2d 13, 21-22, 365 N.W.2d 580 (1985) (lead opinion). Rather, its scope is determined objectively as "the typical reasonable person [would] have understood" it from "the exchange between the officer and the suspect." Florida v. Jimeno, 500 U.S. 248, 251 (1991). When the police rely on consent as their justification for not getting a warrant, the State carries the burden to demonstrate by clear and convincing evidence that the search remained within the scope of that consent. See Reed, 384 Wis. 2d 469, ¶58; Douglas, 123 Wis. 2d at 22 (explaining that a warrantless search exceeding the scope of consent is unreasonable).

¶71 The lawfulness of the Sheriff's Office's search therefore turns on two sub-questions: (1) although he consented to specific GBPD personnel downloading his cell phone information, did Burch maintain a reasonable expectation of privacy in that information such that the Sheriff's Office review of it was a Fourth Amendment search; and, if so, (2) did the Sheriff's Office act unreasonably by searching the GBPD's download of Burch's cell phone data without a warrant, in light of Burch's consent to the GBPD?

1. Burch Maintained a Reasonable Expectation of Privacy in the GBPD's Download of His Cell Phone Data.

¶72 In the Fourth Amendment context, the United States Supreme Court has clearly expressed that cell phone data is in an evidence class of its own because it "implicate[s] privacy concerns far beyond those implicated by the search of" other physical belongings. Riley v. California, 573 U.S. 373, 393 (2014). Cell phones are unique in that they are almost always with us and they store "vast quantities of personal information." Id. at 386. Thus, by carrying cell phones, people carry with them "a digital record of nearly every aspect of their lives——from the mundane to the intimate." Id. at 395. That digital record may include a person's internet "search and browsing history" and "[h]istoric location information," see id. at 395-96, allowing someone with access to that information to "generate[] a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations," see United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring). Although traditionally most private information was kept in one's home, advances in digital technology have shifted that paradigm such that searching a personal cell phone "would typically expose to the government far more than the most exhaustive search of a house." Riley, 573 U.S. at 396-97. Accordingly, people have a unique and heightened expectation of privacy in their cell phone data that demands commensurate Fourth Amendment protection. See id. at 386, 393; People v. Hughes, 958 N.W.2d 98, 112 (Mich. 2020)

("Riley distinguished cell-phone data from other items . . . in terms of the privacy interests at stake.").

¶73 The unique privacy expectation in cell phone data informs why Burch's consent to the GBPD does not relieve the Sheriff's Office of its obligation to get a warrant for its own review. Burch's consent, as "the typical reasonable person [would] have understood" it, had the "expressed object" of the GBPD reviewing messages to verify his alibi for the GBPD's investigation. See Jimeno, 500 U.S. at 251. The GBPD officer's report explained that Burch "consented to Lt. Allen and I [two GBPD officers] looking at the text messages between him and [Burch's acquaintance] last night and also indicated I could take his phone to the department to have the information on it downloaded." Burch's signed consent form is also specific to the "City of Green Bay Police Department" and indicated that Burch gave certain members of the GBPD permission to search his phone. Critically absent from the report or the consent form is any mention of any other law enforcement agency, the possibility of the GBPD sharing the entirety of the downloaded data, or even that Burch was consenting to the GBPD retaining indefinitely all of his phone's information. Cf. Douglas, 123 Wis. 2d at 21-22.

¶74 Burch's consent was therefore limited to the GBPD for the GBPD's investigation.[3] See Terry, 392 U.S. at 25-26, 29 (requiring courts to interpret warrant exceptions as "confined in scope" and "strictly circumscribed"). With respect to other agencies and their investigations, Burch maintained a reasonable expectation of privacy in the data downloaded by the GBPD but unrelated to its investigation, including his internet search history and Google email account. See Carpenter, 138 S. Ct. at 2217 (holding that, because of cell phone data's "unique nature," a person "maintains a legitimate expectation of privacy" in the data even after consensually giving it to another party for a limited purpose); Hughes, 958 N.W.2d at 111 (concluding that the lawful seizure and search of certain cell phone information does not "extinguish[] that otherwise reasonable expectation of privacy in the entirety" of that information). Consequently, the Sheriff's Office's subsequent review of Burch's data invaded Burch's reasonable expectation of privacy such that it was a search under the Fourth Amendment.

2. The Sheriff's Office Acted Unreasonably in Searching the GBPD's Download of Burch's Cell Phone Data.

¶75 The Sheriff's Office decided that no warrant was required for its search after determining that Burch's consent

[3] The circuit court's determination that Burch placed no parameters on the scope of his consent is suspect given that his conversation with the GBPD about his phone was strictly limited to his text messages. The categorical uniqueness of private cell phone data requires circuit courts to take seriously the admonition that exceptions to the warrant requirement like consent be interpreted as "confined in scope" and "strictly circumscribed." See Riley v. California, 573 U.S. 373, 382, 393 (2014); Terry v. Ohio, 392 U.S. 1, 25-26, 29 (1968).

to the GBPD extended to the Sheriff's Office. But as discussed above, Burch's "unequivocal and specific" consent extended only to certain members of the GBPD, and only so they could review his text messages to confirm his alibi. See Reed, 384 Wis. 2d 469, ¶8. Burch did not consent to all of the information on his phone being available to other law enforcement agencies for some later, unrelated investigation. And the Sheriff's Office did not independently get Burch's consent to search his cell phone information.

¶76 Given those facts, no reasonable person in Burch's position would have understood that his consent to the GBPD was an open invitation for any other law enforcement agency to search his private information whenever it wanted to and without a warrant. Therefore, the consent exception to the Fourth Amendment's warrant requirement does not apply to the Sheriff's Office's subsequent warrantless search of Burch's private cell phone data for an unrelated investigation. That search was unreasonable and violated the Fourth Amendment.

B. Evidence of Burch's Google Location Data and His Internet Search History Should Be Suppressed.

¶77 Having concluded that the Sheriff's Office's search violated the Fourth Amendment, the next question is whether the exclusionary rule applies; that is, whether excluding, or suppressing, the unlawfully obtained evidence would sufficiently deter the same police conduct in the future. Here, Burch's Google location data and his internet search history should be excluded because if they are not, other law enforcement agencies are likely to repeat the Sheriff's Office's unconstitutional

search of downloaded cell phone data, especially given the ubiquity of cell phones and the increasing prevalence of personal digital data in criminal investigations.

¶78 The exclusionary rule——that evidence obtained in violation of the Fourth Amendment be excluded from trial——ensures that the Fourth Amendment's right to be free from unreasonable searches remains one "of substance rather than mere tinsel." Hoyer v. State, 180 Wis. 407, 415, 193 N.W. 89 (1923). By excluding otherwise relevant evidence, "[t]he exclusionary rule generally serves to 'deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence.'" Blackman, 377 Wis. 2d 339, ¶68 (quoting Herring v. United States, 555 U.S. 135, 150-51 (2009)). The rule thus incentivizes "the law enforcement profession as a whole" to conduct itself "in accord with the Fourth Amendment." Gates, 462 U.S. at 261 n.15 (White, J., concurring in the judgment).

¶79 Given that critical function, the United States Supreme Court has permitted deviation from the exclusionary rule only when the deterrent value of excluding the evidence is "marginal" or "nonexistent" and outweighed by the social cost of doing so. See, e.g., United States v. Leon, 468 U.S. 897, 913-17, 922 (1984). Such is the case when there is no police misconduct to deter or when the police misconduct is "isolated," "nonrecurring," and "attenuated." See id. at 922; Herring, 555 U.S. at 137, 144. For example, excluding unlawfully obtained evidence is inappropriate if the police acted in objectively reasonable reliance on either a facially

valid warrant properly issued by a neutral, detached magistrate; an apparently constitutional statute; or a binding appellate precedent. See Leon, 468 U.S. 897 (warrants);[4] Illinois v. Krull, 480 U.S. 340 (1987) (statutes); Davis v. United States, 564 U.S. 229, 239-41 (2011) (appellate precedents). Likewise, exclusion is inappropriate when an arresting officer acts in objectively reasonable reliance on either a judicial or police employees' infrequent clerical mistake. See Arizona v. Evans, 514 U.S. 1, 14-16 (1995) (court clerk made a recordkeeping error regarding outstanding arrest warrants only once "every three or four years"); Herring, 555 U.S. at 144-47 (police employees' clerical error in warrant database had never happened before). The common thread through each of these cases is that the fault lies with someone who is not directly engaged in the "competitive enterprise of ferreting out crime"; who has "no stake in the outcome of particular prosecutions." See Evans, 514 U.S. at 15.

¶80 Conversely, the exclusionary rule applies when evidence is unlawfully obtained due to an error made by law enforcement. See Leon, 468 U.S. at 923. For instance, evidence should be suppressed when law enforcement secures evidence based on a facially deficient warrant, or when a warrant is issued based on an officer knowingly or recklessly stating a falsehood in the warrant affidavit. See id. The same goes for when police exceed a valid warrant's authority when executing it. See id. As for the police relying on statutory authority, the

[4] See also Massachusetts v. Sheppard, 468 U.S. 981, 988-91 (1984).

exclusionary rule still applies when police officers misinterpret and "act outside the scope" of a statute and when a reasonable officer would have known either that the law in question is unconstitutional or that the conduct authorized by the statute violates other clearly established law. Krull, 480 U.S. at 355, 360 n.17. Indeed, the rule applies even to unlawfully negligent police conduct when the conduct is "recurring or systemic." E.g., Herring, 555 U.S. at 144.

¶81 The exclusionary rule applies in this case because it was the Sheriff's Office's conduct that rendered unlawful its search of Burch's cell phone, not some detached third party's. There was no statute or judicial precedent condoning a warrantless search of another agency's download of a person's private cell phone data. Instead, the Sheriff's Office judged for itself, incorrectly, that the Fourth Amendment's warrant requirement did not apply to Burch's cell phone data. The unlawful conduct here——not obtaining a warrant to search Burch's private cell phone data——is solely attributable to the Sheriff's Office's detectives. And because those detectives are directly engaged in the "competitive enterprise of ferreting out crime," the exclusionary rule should apply. See Evans, 514 U.S. at 15.

¶82 Applying the rule is also justified because the record demonstrates that warrantless searches of private cell phone information are commonplace, and therefore likely to recur. Officers from both the GBPD and the Sheriff's Office confirmed that it is "very common" for agencies to share "full downloads" of private cell phones with other agencies without first obtaining a warrant, adding that their agencies "regularly" do

so. This widespread neglect of the Fourth Amendment's warrant requirement is just the kind of "systemic negligence" the exclusionary rule is designed to correct. See Herring, 555 U.S. at 144. The exclusionary rule thus squarely applies here.

¶83 The State's counterarguments are unavailing. Its contention that the Sheriff's Office reasonably relied upon its own determination regarding the scope of Burch's consent misses the point. It is not up to the police to determine the contours of an exception to a constitutional requirement restricting their own conduct. See Leon, 468 U.S. at 959 (Brennan, J., dissenting) (presciently lamenting that exceptions to the exclusionary rule would not stay "confined" but instead be wrongfully extended "to situations in which the police have conducted a warrantless search solely on the basis of their own judgment"). Moreover, because the police may encounter circumstances that are on the margins of the law regarding warrant exceptions——as is the case here——police officers are required to "err on the side of constitutional behavior" and get a warrant.[5] See United States v. Johnson, 457 U.S. 537, 561

[5] The State erroneously argues that the Sheriff's Office's search is akin to law enforcement's ability to take a "second look" at physical evidence inventoried during a jail intake or that it already lawfully seized. See State v. Betterley, 191 Wis. 2d 406, 418, 529 N.W.2d 216 (1995); State v. Riedel, 2003 WI App 18, ¶16, 259 Wis. 2d 921, 656 N.W.2d 789. But as the United States Supreme Court explained in Riley, "cell phones, as a category, implicate privacy concerns far beyond those implicated" by physical objects. 573 U.S. at 393. And because a "search of the information on a cell phone bears little resemblance" to other types of searches, the rationales for other searches do not extend to cell phone information. See id. at 386. Therefore, the State's arguments fail. See People v. Hughes, 958 N.W.2d 98, 111-15 (Mich. 2020).

(1982); Blackman, 377 Wis. 2d 339, ¶53 (warrantless searches executed outside any "clearly delineated" warrant exception are "per se unreasonable" and "unlawful"). The Sheriff's Office's erroneous determination that Burch's consent extended to the Sheriff's Office is no justification for failing to get a warrant.

¶84 Nor is the Sheriff's Office relieved of its Fourth Amendment duty to get a warrant simply because law enforcement agencies "regularly" share this type of information. The pervasiveness of this practice is no defense to the exclusionary rule; it is the reason to apply it. See Herring, 555 U.S. at 144 (exclusion applies when unreasonable police conduct is "recurring" or "systemic"). The same goes for the majority's characterization of the Sheriff's Office's conduct as "by the book." Majority op., ¶22. If following "the book" leads to violations of the Fourth Amendment, then the exclusionary rule's deterrent value is at its peak. Excluding evidence obtained by following such an unlawful and widespread policy provides significant societal value by both specifically deterring continued adherence to an unconstitutional practice and more broadly incentivizing police agencies to adopt policies in line with the Fourth Amendment.[6] See Wayne R. LaFave, 1 Search & Seizure § 1.3(i) (6th ed. 2020). This is especially true when

[6] The State counters that because the Sheriff's Office may have had access to Burch's Google email account and internet search history via a lawful, independent source, that evidence should not be excluded. See State v. Carroll, 2010 WI 8, ¶¶44-45, 322 Wis. 2d 299, 778 N.W.2d 1. But the State has forfeited that argument by failing to raise it below. See State v. Counihan, 2020 WI 12, ¶25, 390 Wis. 2d 172, 938 N.W.2d 530.

the Constitution already provides law enforcement with a simple solution for how to lawfully obtain cell phone data: get a warrant. See Riley, 573 U.S. at 403.

C. The Majority Opinion Has No Support in Fourth Amendment Jurisprudence.

¶85 The majority opinion offers a contrary analysis that ignores the novel constitutional problems presented by cell phone data, is inconsistent with the Fourth Amendment's text, and undermines the exclusionary remedy.

¶86 The majority opinion's analysis reveals a lack of appreciation for the fundamental differences between digital cell phone data and more "traditional," non-digital evidence that law enforcement might share with other agencies. The Fourth Amendment treats cell phone data differently because it often contains nearly all the "privacies of [a person's] life," such that "any extension" of Fourth Amendment principles "to digital data has to rest on its own bottom." See Riley, 573 U.S. at 393, 403 (quoting another source); Carpenter, 138 S. Ct. at 2219 (explaining that Fourth Amendment jurisprudence must account for the "seismic shifts in digital technology"). Accordingly, it is a grave analytical error to "mechanically apply[]" to cell phone data Fourth Amendment rationales that were developed without such invasive technologies in mind. Carpenter, 138 S. Ct. at 2219; see also Riley, 573 U.S. at 400-01 (rejecting the argument that the police can search cell phone data under the same rationale that allows them to obtain "the same information from a pre-digital counterpart"). Or, as the United States Supreme Court put it, treating cell

phone data the same as its non-digital analogues "is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together." Riley, 573 U.S. at 393. The majority opinion, however, is content to toss a saddle on a spaceship and call it a horse. Nowhere does the majority opinion account for Burch's special privacy interest in his cell phone data, leaving a tremendous hole in its exclusionary rule analysis.

¶87 More troubling is the majority's disregard for the Fourth Amendment's text. It is bedrock Fourth Amendment law that search warrants are generally required and that a search without a warrant is per se unlawful. See, e.g., City of Ontario v. Quon, 560 U.S. 746, 760 (2010); Blackman, 377 Wis. 2d 339, ¶53. The majority's assertion that "there is nothing concerning under current Fourth Amendment doctrine with how the Sheriff's Office detectives conducted themselves" shockingly discards this well-settled principle. Indeed, the majority opinion fails to even mention the presumption that warrantless searches violate the Fourth Amendment.

¶88 But worse than mere silence, the majority's refusal to apply the exclusionary rule flips this presumption on its head. According to the majority, if "no case from this court or the federal courts" directs the police to get a warrant, then the police act "reasonably" in not getting a warrant. Majority op., ¶23. The majority appears to create a new prerequisite for applying the exclusionary rule, holding that it applies only if a court has previously declared that the police conduct at issue

is unconstitutional. Imposing this hurdle undermines the exclusionary remedy for Fourth Amendment violations and is directly contrary to both our and the United States Supreme Court's Fourth Amendment jurisprudence.

¶89 All of which makes inexcusable the majority opinion's refusal to address the constitutionality of the Sheriff's Office's search. Despite law enforcement's admittedly "very common" practice of sharing with other agencies entire downloads of private cell phone data, that recurring Fourth Amendment violation will continue with impunity unless and until the court engages with the specific Fourth Amendment issue raised by private cell phone information. By skipping straight to whether the exclusionary rule applies, the majority opinion deprives aggrieved defendants——and future courts——of the very prior precedent now necessary to remedy law enforcement's continued unconstitutional conduct:

> Forgoing a knotty constitutional inquiry makes for easier sledding, no doubt. But the inexorable result is "constitutional stagnation"——fewer courts establishing law at all, much less clearly doing so, . . . [creating a] Catch-22. [Defendants] must produce precedent even as fewer courts are producing precedent. Important constitutional questions go unanswered precisely because no one's answered them before. Courts then rely on that judicial silence to conclude there's no equivalent case law on the books. . . . If courts leapfrog the underlying constitutional merits in cases raising novel issues like digital privacy, then constitutional clarity——matter-of-fact guidance about what the Constitution requires——remains exasperatingly elusive. Result: gauzy constitutional guardrails as technological innovation outpaces legal adaptation.

Zadeh v. Robinson, 928 F.3d 457, 479-80 (5th Cir. 2019) (Willet, J., concurring), cert. denied, 141 S. Ct. 110 (2020).

Together with its new prior-precedent requirement, the majority opinion's avoidance of the Fourth Amendment issues here perpetuates a cycle of diminished police accountability and courts' unwillingness to address it.

¶90 Given that the Fourth Amendment law specific to cell phone data is undeveloped, this court should be providing "clear guidance to law enforcement through categorical rules." Riley, 573 U.S. at 398; see also Michigan v. Summers, 452 U.S. 692, 705 n.19 (1981) (explaining that clear "workable" rules are necessary so that difficult Fourth Amendment questions are not resolved in an "ad hoc, case-by-case fashion by individual police officers") (quoting another source)). If a law enforcement agency wishes to search a person's private information, such as cell phone data, and the person did not consent to that agency's search, the agency must get a warrant.

III. CONCLUSION

¶91 The Sheriff's Office should have obtained a warrant to search Burch's private cell phone data. Because it did not, the evidence it found as a result of that search should be suppressed. The majority's refusal to apply the exclusionary rule is incompatible with our Fourth Amendment jurisprudence and perverts the long-standing bedrock requirement that police obtain a warrant to search private information. I therefore respectfully dissent from that part of the majority opinion.

¶92 I am authorized to state that Justice JILL J. KAROFSKY joins this opinion and that Justice ANN WALSH BRADLEY joins this opinion except for footnote 1.

¶93 ANN WALSH BRADLEY, J. *(dissenting).* Ubiquitous use does not mean the average wearer of a Fitbit knows how it works. Nor does ubiquitous use indicate reliability sufficient to be admissible in a court of law.

¶94 An average jury member would likely know what a Fitbit is and what it does. Of course, as relevant here, it counts the wearer's steps. But that isn't the question. In determining whether expert testimony is required, the relevant inquiry is how a Fitbit counts the wearer's steps and then ultimately, whether it does so with sufficient reliability.

¶95 How does it work? A Fitbit device uses a microelectronic triaxial accelerometer to capture a person's body motion in three-dimensional space and record related data. This motion data is then analyzed by utilizing proprietary algorithms to surmise patterns and thus to identify daily steps taken.

¶96 Is it sufficiently reliable to be admitted as evidence in court? I don't know. But, I do know that the answer does not lie in its ubiquitous use.

¶97 I also know that absent expert testimony there is insufficient foundation in this record for the majority to determine, in essence, that a presumption of accuracy and reliability attends the underlying technology of a Fitbit. The error of such a presumption is made manifest by reference to an overarching analysis of 67 studies on Fitbit accuracy disseminated by the National Center for Biotechnology Information (NCBI), under the auspices of the U.S. National

Institutes of Health (NIH). The researchers found that Fitbit devices were "likely to meet acceptable accuracy for step count approximately half the time." Lynne M. Feehan, et al., Accuracy of Fitbit Devices: Systematic Review and Narrative Syntheses of Quantitative Data, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6107736/ (2018).

¶98 In citing this study, I neither endorse nor disclaim its conclusions. It suggests, however, when a compilation of studies indicates acceptable accuracy is met only "half the time," that something may be amiss with the majority's presumption of accuracy and reliability.

¶99 Expert testimony is required when matters are presented that are "unusually complex." White v. Leeder, 149 Wis. 2d 948, 960, 440 N.W.2d 557 (1989). Movement measured by a "microelectronic triaxial accelerometer" and analyzed by proprietary algorithms certainly fits that bill.

¶100 In my view, the technology underlying a Fitbit is not within the ordinary experience of an average jury member. Fitbits and other wearable devices may be ubiquitous, but it does not follow from this premise that the technology underlying their use is not "unusually complex."

¶101 Expert testimony assists the trier of fact to understand the evidence and to determine a fact in issue. The accuracy of the number of steps recorded on Douglass Detrie's Fitbit is certainly a fact in issue. Thus, expert testimony should have been required to assist the jury in understanding the technology and assessing its reliability.

¶102 Invoking a deferential standard, it is not unusual for an appellate court to do only a cursory analysis of an evidentiary issue. But this is not the usual case and a more nuanced analysis is required.

¶103 This case presents a groundbreaking question. To my knowledge, this is the first appellate court decision in the country to conclude that Fitbit step-counting evidence is admissible absent expert testimony explaining how the device works. The parties have not cited, and I have not found, any case making such a proclamation. The majority's analysis provides a slim reed upon which to support such a novel determination.

¶104 Rather than allowing evaluation of the question, the majority cuts off the debate. It essentially rubber stamps the circuit court's erroneous analysis and declares Fitbit's technology to be simple enough to be presented as evidence without the benefit of an expert witness or further consideration of its reliability.

¶105 Although I join Justice Dallet's dissent, concluding that the search of Burch's cell phone at issue violated his Fourth Amendment rights and that the good faith exception to the warrant requirement does not apply, I do not join footnote 1 that concurs with the majority's analysis of the Fitbit evidence. Because I conclude that the circuit court erroneously admitted the Fitbit evidence without an expert witness to establish the reliability of the science underlying the Fitbit technology, I respectfully dissent.

I

¶106 I briefly recount the facts that are relevant to the issue on which I write: the admission of the Fitbit evidence.

¶107 As the majority opinion sets forth, the initial suspect in the crime at issue here was Douglass Detrie, the victim's boyfriend. Majority op., ¶4. However, the investigation shifted after police learned that Detrie's Fitbit device had recorded only 12 steps during the time the homicide was committed. Burch was ultimately arrested and charged.

¶108 The State sought to present evidence regarding Detrie's Fitbit, and Burch moved to exclude it. Id., ¶11. As relevant here, Burch contended that the State must present expert testimony to establish the reliability of the science behind the Fitbit device. Id.[1]

¶109 The circuit court granted Burch's motion in part and denied it in part. Specifically, the circuit court excluded Fitbit evidence related to sleep monitoring, but it allowed the admission of the step-counting data without the testimony of an expert regarding the science underlying the Fitbit technology. Id., ¶11 & n.3.

¶110 In the circuit court's estimation, a Fitbit is more akin to an electronic monitoring device (which does not require expert testimony, see State v. Kandutsch, 2011 WI 78, 336

[1] Burch made several additional arguments, including an assertion that Fitbit's records were not properly authenticated, which he renews on appeal. Because I determine that expert testimony was necessary to admit the evidence in question, I do not reach Burch's arguments regarding authentication.

Wis. 2d 478, 799 N.W.2d 865) than to a preliminary breath test (which requires expert testimony, see State v. Doerr, 229 Wis. 2d 616, 599 N.W.2d 897 (Ct. App. 1999)). Similarly, the circuit court distinguished Fitbit data from DNA, fingerprint analysis, blood alcohol content tests, tool mark evidence and accident reconstruction because "few people encounter those things in their everyday life."

¶111 Comparing a Fitbit to an electronic monitoring device, the circuit court stated that a Fitbit is "passively worn by a person," and the device collects data "based on that person's movements, which is then transmitted and recorded. There is no active manipulation by the wearer to achieve the results; the results are simply a record of the wearer's movements, i.e., their location or the number of steps they took." Thus, in the circuit court's view "the step-counting feature of the Fitbit Flex, like the [electronic monitoring device], is not so unusually complex or esoteric that the jury will require the aid of expert testimony to interpret the information."

¶112 At trial, because it was not required to provide an expert to introduce the data from Detrie's Fitbit, the State relied upon the testimony of Tyler Behling, a computer forensic crime analyst with the Brown County Sheriff's Office. Although Behling claimed to have knowledge of how a Fitbit works "on a high level," he did not know the answer when asked how a Fitbit and a Bluetooth device send information from one to the other, how Fitbit stores its data, whether Fitbit data can be edited,

whether the device would register steps while it is not being worn, or what a Fitbit's error rate is.

¶113 Despite the dearth of technical testimony regarding how a Fitbit actually works, the majority now affirms the circuit court's determination. It concludes that "[g]iven the widespread availability of Fitbits and other similar wireless step-counting devices in today's consumer marketplace, the circuit court reasonably concluded Detrie's Fitbit was not so 'unusually complex or esoteric' that the jury needed an expert to understand it." Majority op., ¶31.

II

¶114 It has long been the law that expert testimony is required when a matter involves "special knowledge or skill or experience on subjects which are not within the realm of the ordinary experience of mankind, and which require special learning, study and experience." Cramer v. Theda Clark Mem'l Hosp., 45 Wis. 2d 147, 150, 172 N.W.2d 427 (1969). "The requirement of expert testimony is an extraordinary one," and should be applied "only when unusually complex or esoteric issues are before the jury." White, 149 Wis. 2d at 960.

¶115 "In considering what constitutes the 'ordinary experience of mankind'——i.e. the average juror——courts have not tailored this standard to the lowest common denominator. Rather, courts attempt to evaluate, on a case-by-case basis, whether expert testimony is required because the issue is outside the realm of lay comprehension." Kandutsch, 336 Wis. 2d 478, ¶29.

¶116 The circuit court here determined that the technology underlying a Fitbit is not outside the realm of lay comprehension. It compared a Fitbit to a watch in that "the public generally understands the principle of how it functions and accepts its reliability without knowing the exact mechanics of its internal workings." Further, it determined that a Fitbit is not subject to "active manipulation by the wearer to achieve the results; the results are simply a record of the wearer's movements, i.e., their location or the number of steps they took."

¶117 But the expert testimony standards do not rest on ubiquity. Instead, they rest on the complexity of the subject matter. Although many members of the jury may have been wearing Fitbits or similar devices, such a fact would not inform the question of whether those jury members understand how a Fitbit works or whether the technology is reliable.

¶118 What does the average person really know about how a Fitbit works, much less its reliability? As one study described it, "Fitbit devices use a microelectronic triaxial accelerometer to capture body motion in 3-dimensional space, with these motion data analyzed using proprietary algorithms to identify patterns of motion to identify daily steps taken, energy expenditure, sleep, distance covered, and time spent in different intensity of activities." Feehan, et al., supra. According to the majority, the average juror would understand, without expert

testimony, not only what a "microelectronic triaxial accelerometer" is, but how it works. Really?[2]

¶119 If the State had presented an expert, that expert would have had to meet the requirements for expert testimony established by the United States Supreme Court in Daubert.[3] Pursuant to the Daubert standard, as codified in Wis. Stat. § 907.02(1),[4] the circuit court must act as a gatekeeper and make a threshold determination that the testimony is reliable in order for it to be presented at trial. State v. Dobbs, 2020 WI 64, ¶43, 392 Wis. 2d 505, 945 N.W.2d 609. By not requiring the State to present an expert, the circuit court and the majority allow the State to skirt this initial reliability determination.

¶120 There are various ways in which threshold reliability can be demonstrated. See 7 Daniel D. Blinka, Wisconsin Practice Series: Wisconsin Evidence § 702.402 (4th ed. 2020). There may

[2] Further, the intricacies of Fitbit's technology are "proprietary," setting up an additional roadblock to the jury's full knowledge and full understanding of how the device works. See State v. Loomis, 2016 WI 68, ¶66, 371 Wis. 2d 235, 881 N.W.2d 749 (explaining that "proprietary nature" has been invoked to prevent disclosure of certain information).

[3] Daubert v. Merrell Dow Pharm., Inc., 509 U.S. 579 (1993).

[4] Wisconsin Stat. § 907.02(1) provides:

> If scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise, if the testimony is based upon sufficient facts or data, the testimony is the product of reliable principles and methods, and the witness has applied the principles and methods reliably to the facts of the case.

be a statute indicating that certain tests or methods are admissible. See, e.g., Wis. Stat. § 885.235 (addressing chemical tests for intoxication). There is no statute addressing Fitbit evidence.

¶121 We can also look to court precedent which has already determined certain principles to be reliable. See, e.g., State v. Hanson, 85 Wis. 2d 233, 244, 270 N.W.2d 212 (1978) (discussing the reliability of the underlying principles of speed radar detection that employs the Doppler effect). The reliability of Fitbit's step counting capability is a novel issue, so there is no precedent on point.

¶122 Stipulations or judicial notice may also be appropriate when a fact is "capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned." Wis. Stat. § 902.01(2)(b). Again, these do not fit the present scenario——the reason we are here is because the parties do not agree and Burch reasonably questions the accuracy of Fitbit's step count.

¶123 Finally, if none of the above proves to be an acceptable avenue to demonstrate the accuracy and reliability of the scientific principles sufficient to be accorded a prima facie presumption, expert testimony is necessary to explain the underlying scientific principles and to demonstrate their reliability. Here, no expert was presented.

¶124 The evidentiary process requires that the scientific principles be presented to the court before the evidence is determined to be reliable. In a court of law, process matters.

Without fulfilling one of these avenues, the threshold reliability determination cannot be made.

¶125 And what of Fitbit's reliability? Such reliability can depend on a number of factors, such as whether the user has self-manipulated the data, if the Fitbit is temporarily removed, where on the body the device is worn, or the type of physical activity in which the wearer is engaged. Feehan, et al., supra; Katherine E. Vinez, The Admissibility of Data Collected from Wearable Devices, 4 Stetson J. Advoc. & L. 1, 16 (2017). In a comprehensive aggregation of 67 different studies, researchers found that "[c]onsistent evidence indicated that Fitbit devices were likely to meet acceptable accuracy for step count approximately half the time." Feehan, et al., supra. Yet in the view of the majority and of the circuit court, an expert is not necessary to establish the reliability of Detrie's step count——the Fitbit evidence can go before the jury with no technical or scientific explanation.

¶126 Indeed, questions arise about the reliability of wearable devices despite their widespread acceptance. See Vinez, supra, at 16. If reliability questions exist, where better than the circuit court to present the case for and against such reliability? Instead of remanding to the circuit court for evaluation of the question, the majority curtly

declares Fitbit's technology to be simple enough to be put before a jury without the benefit of an expert.[5]

¶127 When new and popular devices emerge, courts should be wary of blindly accepting the data they produce without a thorough examination of the underlying technology. "Machines warrant no blind faith, and whatever trust they receive must be earned through the crucible of the rules of evidence." Brian Sites, Machines Ascendant: Robots and the Rules of Evidence, 3 Geo. L. Tech. Rev. 1, 1-2 (2018). In many cases, such an examination will require an expert. In my view, this is such a case.

¶128 Rather than break new ground as does the majority, I would proceed with caution. Basing the necessity of expert testimony on ubiquity rather than complexity sets a dangerous path.

¶129 For the foregoing reasons, I respectfully dissent.

[5] See Nicole Chauriye, Wearable Devices as Admissible Evidence: Technology is Killing our Opportunities to Lie, 24 Cath. U. J. L. & Tech. 495, 517 (2016) (arguing that "the trier of fact would greatly benefit from mandated expert testimony to explain the accuracy and details of the data recorded by the wearable technology").