No.

IN THE
Supreme Court of the United States

GEORGE STEVEN BURCH,
Petitioner,

v.

STATE OF WISCONSIN,
Respondent.

On Petition for Writ of Certiorari
to the Supreme Court of Wisconsin

PETITION FOR WRIT OF CERTIORARI

ANA L. BABCOCK
Counsel of Record

BABCOCK LAW, LLC
130 E. Walnut Street, St. 401
P.O. Box 22441
Green Bay, WI 54305
ababcock@babcocklaw.org
(920) 662-3964

QUESTION PRESENTED

After the government obtains consent to search specific information on an individual's smart phone, whether or to what extent the Fourth Amendment tolerates the government (1) duplicating the entire digital contents of the phone, (2) retaining that digital data indefinitely, and (3) warrantlessly searching that data in perpetuity?

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES CITED

CONSTITUTIONAL PROVISION

STATUTE CITED

OTHER SOURCES

PETITION FOR A WRIT OF CERTIORARI

Petitioner George Steven Burch respectfully petitions for a writ of certiorari to review the judgement of the Supreme Court of Wisconsin in case 2019AP1404-CR.

OPINIONS BELOW

The opinion of the Supreme Court of Wisconsin is published at *State of Wisconsin v. Burch,* 2021 WI 68, 961 N.W.2d 314 (2021), attached as Appendix A. The Wisconsin Court of Appeals certification decision, unpublished, is attached as Appendix B, and the decision of the trial court, Brown County case 16 CF 1309, unpublished, is attached as Appendix C.

JURISDICTION

The Supreme Court of Wisconsin issued its decision on June 29, 2021. This Court's jurisdiction is invoked under 28 U.S.C. § 1257(A).

CONSTITUTIONAL PROVISION INVOLVED

The Fourth Amendment states in relevant part "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." U.S. Const. amend IV.

STATEMENT OF THE CASE

This homicide presents a complex factual background with plot twists and serendipitous events. For the issue presented to this Court, the key facts–in chronological order–are as follows:

1. The Murder

In May 2016, the victim in this case was brutally murdered, and evidence of the crime was found at several different locations. All the evidence at the time pointed to the victim's boyfriend, Douglas Detrie, as the culprit, and Detrie was arrested and held in custody for eighteen days. Detrie was later released and not charged. The investigation–led by the Brown County Sheriff's Department ("BCSD")–continued.

2. The Cell Phone Extraction

In June 2016, the Green Bay Police Department ("GBPD") suspected that Petitioner was involved in a wholly unrelated hit and run accident. Petitioner denied involvement. Police asked Petitioner if they could look at his text messages to corroborate his whereabouts. Petitioner gave verbal consent.

The officer told Petitioner it's easier to just download the information off the phone at the station. Petitioner consented. Petitioner then signed a generic consent form allowing the GBPD to "search his cellphone."

The GBPD then performed a full extraction of every bit of data on Petitioner's phone. The examiner then converted the data into a readable format tabbed by categories such as text messages, images, internet history, etc.

The examiner next created a separate report with the specific timeframe and data the investigating officer requested. The officer reviewed this report and found nothing linking Petitioner to the hit and run accident. As a routine procedure, the GBPD shelved the full extraction in evidence.

3. The DNA Database Hit

The BCSD continued investigating the murder. After months of testing various evidence, DNA suitable for comparison was found on the victim's sock, and a database hit provided an investigative lead that Petitioner was the source of that DNA.

The BCSD then began searching a police database for any information related to Petitioner, and investigators learned of the GBPD's contact with Petitioner in relation to the earlier hit and run accident.

4. The Second Search of the Extraction

The GBPD's reports of the hit and run investigation noted that Petitioner's cell phone had been extracted. The BCSD asked the GBPD for a copy of the extraction, and the GBPD gave it to them–no warrant was issued.

The BCSD scoured the extraction and discovered critical information leading to a trail of inculpatory evidence. Petitioner moved to suppress this evidence on grounds that the search violated the Fourth Amendment. Appendix D. The trial court denied Petitioner's motion to suppress, attached as Appendix C, and a jury found Petitioner guilty.

5. The Court of Appeals Certifies the Issue to the Supreme Court

Petitioner appealed. The court of appeals certified[1] the case to the Supreme Court of Wisconsin–noting the heightened privacy interests associated with cell phones, explaining that "[g]iven the importance of the issues raised in this appeal, the lack of clear precedent regarding those issues, and the high likelihood that these issues will recur in future cases, we believe this is a case in which it would be appropriate for the supreme court, rather than the court of appeals, to render a decision." App. B, ¶¶ 27-28. The Supreme Court of Wisconsin granted the certification.

6. The Supreme Court of Wisconsin Affirms the Conviction

The Supreme Court of Wisconsin affirmed the conviction in a four-to-three decision. The four-justice majority declined to address the Fourth Amendment issues; instead, the court concluded that suppression is not

[1] Wis. Stat. § 809.61 allows for an appeal to bypass the court of appeals and be heard directly by the supreme court.

warranted under the exclusionary rule. App. A, ¶ 15. The court explained that the evidence was not "obtained by sufficiently deliberate and sufficiently culpable police misconduct." *Id.*, ¶ 21. Justice Rebecca Grassl Bradley concurred with the majority but wrote separately to explain that a warrant is required when a separate law enforcement agency wants to conduct a second search of cell phone data. *Id.*, ¶¶ 62-63. Because neither this Court nor the state supreme court had spoken on the issue, Justice Bradley concluded that suppression under the exclusionary rule was not required. *Id.*, ¶ 62.

With respect to the issue before this Court, three justices dissented, concluding that a Fourth Amendment violation occurred and that suppression was warranted. *Id.*, ¶¶ 64, 92. The dissent was critical of the majority's conclusion that the exclusionary rule should not applied, explaining that "the common thread through [the cases relied upon by the majority] 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.' *Id.*, ¶ 79 (quoting *Arizona v. Evans*, 514 U.S. 1, 15 (1995)).

REASONS FOR GRANTING THE PETITION

Can the government create a digital portal into nearly every detail of your life and come and go as it pleases for years to come? This case presents the next important step in this Court's continual effort to reconcile bedrock Fourth Amendment principles with the complexities of this new digital world.

People now carry a digital duplication of almost every detail of their life, "from the mundane to the intimate." *Riley v. California*, 573 U.S. 373, 395 (2014). In 2014, this Court noted the "immense storage capacity" of the top-selling smartphone at sixteen gigabytes of data. *Id.* at 393-94. Today, the *minimum* storage capacity of Apple's latest smartphone is 128 gigabytes; the maximum is one terabyte.[2] A single terabyte is the equivalent of approximately 220 million pages of printed text. *McNulty v. Reddy Ice Holdings, Inc.*, 271 F.R.D. 569, 570 n. 1 (E.D. Mich. 2011).

Law enforcement agencies around the country now have at their fingertips powerful tools to obtain–and in this case *retain*–a digital record of every intimate detail of one's private life. Mobile device forensic tools ("MDFTs") enable the government to extract a complete copy of a phone's content. Upturn, *The Widespread Power of U.S. Law Enforcement to Search*

[2] Apple, *Compare iPhone Models*, https://www.apple.com/iphone/compare/?modelList=iphone13promax,iphone13pro,iphone13 (last visited November 3, 2021).

Mobile Phones (Oct. 2020). MSDFs allow the government to sort, organize, search, and view data in ways a phone user cannot. *Id.* at 12. This technology is "cheap in comparison to conventional [search] techniques and, by design . . . it evades the ordinary checks that constrain law enforcement practices . . . ." *United States v. Jones*, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring). This technology gives the government an enduring digital portal into one's privacies of life, allowing the government to "efficiently mine them for information years into the future." *Id.* at 415.

Courts around the country have tackled some issues similar to those presented here, and there has been considerable disagreement among jurists.

In *Morton*, a Fifth circuit panel concluded that in the warrant context, probable cause is required as to each category of data on a cell phone, relying on this Court's discussion in *Riley* that distinct types of information in different components of the phone should be analyzed separately. *United States v. Morton*, 984 F.3d 421, 426-27 (5th Cir. 2021). There the court held that while the affidavit supported probable cause to search the contacts, call logs, and text message sections of the phone, it did not establish probable cause to search the photograph section of the phone. *Id.* The Fifth Circuit vacated the panel opinion and the matter is pending rehearing en Banc. *United States v. Morton*, 996 F.3d 754 (5th Cir. 2021).

In *United States v. Ganias I*, a Second Circuit panel held that the Fourth Amendment does not permit police "executing a warrant for the seizure of particular data on a computer to seize and indefinitely retain every file on that computer for use in future criminal investigations." 755 F.3d 125, 137 (2nd Cir. 2014). There, the government received a tip that certain businesses were engaging in improper conduct and that evidence of the wrongdoing could be found at the office of the accountant for those businesses, Stavros Ganias. *Id.* at 128. The government obtained a search warrant and created mirror images of all the files on Ganias' computer. *Id.* In reviewing the files, the government identified potential tax violations, and it gave the IRS copies of the files to conduct its own investigation. *Id.* By late 2004, the government and the IRS had extracted and isolated the files related to the warrant; however, they did not purge the non-relevant files because they viewed the files as "government property[.]" *Id.* at 129. The following year, the IRS suspected that Ganias was involved in tax fraud, and it wanted to review Ganias' *personal* financial records, which were contained in the files the government seized some twenty months earlier. *Id.* at 129-30. Knowing that reviewing Ganias' personal records was outside the scope of the 2004 warrant, the IRS obtained a new warrant to search those files. *Id.* at 130. Ganias moved to suppress. *Id.*

The court concluded that creating mirror images of all the files for off-site review was reasonable. *Id.* at 135. However, after the relevant files had been isolated, the government's indefinite retention of all the files violated the Fourth Amendment. *Id.* at 137-38.

The Second Circuit, sitting en Banc, reversed the result on different grounds. *United States v. Ganias II*, 824 F.3d 199 (2nd Cir. 2016). The en Banc court concluded that because the second search of the files was conducted pursuant to a valid warrant, the good faith exception applied, and it thus declined to address whether retaining the files violated the Fourth Amendment. *Id.* at 220-21, 225-26.

In *People v. McCavitt*, an Illinois appellate court held that the government cannot retain seized electronic property indefinitely. 2019 IL App (3d) 170830, ¶ 21, 145 N.E.3d 638. There, the court drew the line at the completion of the criminal proceedings or a determination that no charges would be filed. *Id.*, ¶ 22. In July 2013, the Illinois State Police obtained a warrant to search McCavitt's home for any electronic media capable of storing pictures, audio, or video. *Id.*, ¶ 3. Police seized McCavitt's computer and then sought and obtained a second warrant allowing them to search the computer for all digital images and any evidence related to sexual assault, unlawful restraint, and unauthorized video recordings. *Id.*, ¶ 4. The Peoria County

Sheriff's Department then made a mirror image of the computer's hard drive, and the State charged McCavitt with various crimes based on the images found on the computer. *Id.*, ¶¶ 4-5. McCavitt was subsequently acquitted. *Id.*, ¶ 5.

In March 2014, a different agency, the Peoria Police Department, initiated a new investigation and obtained the mirrored hard drive from the sheriff's department. *Id.*, ¶ 6. The police department examined the copy and identified images depicting child pornography. *Id.*, ¶ 6. The police department sought and obtained another warrant to search the mirrored hard drive for images of child pornography. *Id.*, ¶ 7. McCavitt was subsequently indicted on several counts related to the images found. *Id.*

The court concluded that while McCavitt had a diminished expectation of privacy after police took possession of the computer, his expectation of privacy was restored once his trial was complete. *Id.*, ¶ 24. The court held that once the trial ended, police were not entitled to retain any portion of the mirrored hard drive, much less the entire file. *Id.*, ¶ 25. The state supreme court just overturned the appellate court in a decision that, as of this filing, has yet to be released for publication.

Finally, the fractured decision of the Supreme Court of Wisconsin in this case emphasizes the disagreement among jurists.

The time for this Court to decide these manifestly important Fourth Amendment issues is now. This case presents the ideal vehicle to answer these questions, given the comprehensive set of facts. This case will give the Court the opportunity to define 1) how much data the government can seize from one's cell phone; 2) how long the government can retain that data; and 3) if and to what extent the government can continue to search that data in an unrelated investigation.

CONCLUSION

Based on the above reasons, the petition for writ of certiorari should be granted.

Respectfully submitted,

Dated this 10th day of November, 2021

ANA L. BABCOCK
Counsel of Record
SUPREME COURT BAR NO. 310422

BABCOCK LAW, LLC
130 E. Walnut Street, St. 401
P.O. Box 22441
Green Bay, WI 54305
ababcock@babcocklaw.org
(920) 662-3964