Appeal No. 2019AP1404-CR **Cir. Ct. No. 2016CF1309**

WISCONSIN COURT OF APPEALS
DISTRICT III

STATE OF WISCONSIN,

PLAINTIFF-RESPONDENT,

V.

GEORGE STEVEN BURCH,

DEFENDANT-APPELLANT.

FILED

Oct. 20, 2020

Sheila T. Reiff
Clerk of Supreme Court

CERTIFICATION BY WISCONSIN COURT OF APPEALS

Before Stark, P.J., Hruz and Seidl, JJ.

Pursuant to WIS. STAT. RULE 809.61 (2017-18), this appeal is certified to the Wisconsin Supreme Court for its review and determination.

ISSUES

This case raises several issues regarding the extent to which law enforcement can download and subsequently use information from an individual's cell phone. In June 2016, the Green Bay Police Department (GBPD) downloaded the contents of George Burch's cell phone while investigating him in connection with several incidents involving a vehicle. About two months later, while investigating the unrelated murder of Nicole VanderHeyden, an officer from the Brown County Sheriff's Office (BCSO) reexamined the data that the GBPD had downloaded from Burch's cell phone. Burch was subsequently charged with first-degree intentional homicide in connection with VanderHeyden's murder, and

the circuit court denied his motion to suppress incriminating information derived from the cell phone download. A jury ultimately convicted Burch of first-degree intentional homicide.

Burch now appeals, arguing the circuit court erred by denying his motion to suppress. He contends the GBPD and the BCSO violated his Fourth Amendment rights in three ways: (1) the GBPD exceeded the scope of his consent to search his cell phone by downloading the phone's entire contents, rather than only the text messages; (2) the GBPD unlawfully retained the entire cell phone download after it completed its June 2016 investigation into the vehicle incidents; and (3) the BCSO had no lawful authority to conduct a second search of the cell phone download in August 2016. Because these issues raise novel questions regarding the application of Fourth Amendment jurisprudence to the vast array of digital information contained in modern cell phones, we certify this appeal to the Wisconsin Supreme Court.[1]

---

[1] Burch's appeal raises several additional issues. First, the State argues that even if law enforcement violated Burch's Fourth Amendment rights with respect to the cell phone download, suppression is not warranted because the BCSO acted in good faith. In the alternative, the State argues that if law enforcement violated the Fourth Amendment and the BCSO did not act in good faith, this case should be remanded to the circuit court to address the applicability of the independent-source doctrine.

Burch, in turn, argues that the circuit court erroneously exercised its discretion by admitting "critical evidence from Fitbit, Inc.'s business records ... without expert testimony and without a witness from Fitbit to establish that the evidence was accurate and reliable[.]" He further argues that the admission of the Fitbit evidence without a witness from Fitbit violated his right to confrontation.

We do not believe that any of these additional issues, in and of themselves, are worthy of certification, and we therefore do not address them further. However, if the supreme court were to accept this certification, it would acquire jurisdiction over the entire appeal, including all issues raised before this court. *See* ***State v. Denk***, 2008 WI 130, ¶29, 315 Wis. 2d 5, 758 N.W.2d 775.

BACKGROUND

In June 2016, Burch was living with Edward and Lynda Jackson in Green Bay and, with their permission, was using their extra vehicle to travel to work. On June 8, 2016, Edward Jackson noticed that the vehicle was missing, notified police, and reported that Burch was the last person to have used the vehicle.

At the hearing on Burch's suppression motion, officer Robert Bourdelais of the GBPD testified that he responded to Edward Jackson's complaint and discovered that the vehicle in question had been involved in both a hit-and-run and a vehicle fire the previous night. Bourdelais then questioned Burch, who admitted he had driven the vehicle the prior evening but denied any involvement in the accident or fire. During the course of his conversation with Burch and Edward Jackson, Bourdelais learned that Jordan Schuyler, a female friend of Burch's, lived in the area of the hit-and-run. Bourdelais then asked Burch whether he had gone to Schuyler's house the night before. Burch responded that he and Schuyler were texting back and forth that night while he was at a bar, but at some point she stopped responding to his texts, so he went home.

Bourdelais suspected that Burch had been involved in the hit-and-run. He therefore asked Burch "if I could see the text messages between him and [Schuyler], if my lieutenant and I could take a look at his text messages." Burch responded in the affirmative. Bourdelais testified:

> I don't recall if we looked at [the text messages] there at the scene but one of the things that I prefer to do, I guess, rather than take photographs or screen shots of text messages for evidence purposes for cases, is if it's during the daytime we have a detective and some staff at work that can hook up cell phones to another computer and download information off of it and then it comes printed out and it just gets scanned into the report or added in the report on a disk or something,

> and 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 [Burch] 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.

Bourdelais testified that when he asked Burch about downloading "the information" from Burch's phone, he did not "specifically limit the information to the text messages." Bourdelais explained:

> 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 [Schuyler] back and forth, but from my experience as a police officer I know people communicate [with] 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 [Schuyler] or communication he had supported his claims that he never went over to her house or made arrangements to go over to her house.

Bourdelais also testified that he was interested in viewing any deleted messages that might be recoverable from Burch's phone.

Burch subsequently signed a written consent form giving Bourdelais and any assisting personnel "permission to search my ... Samsung cellphone." Nothing on the written form limited the scope of Burch's consent in any way. Bourdelais also testified that Burch did not orally "express any concern as to limiting the search of [his] phone to only certain items on the phone" during their conversation.

Bourdelais then gave Burch's phone to Kendall Danelski, a forensic computer examiner for the GBPD. Bourdelais told Danelski that he wanted her to extract "all data" from the phone "after June 7th, 9:30 p.m." Danelski performed a

"physical extraction" of the phone—that is, she performed a "full forensic download" of the phone's contents. Danelski then prepared a "report" for Bourdelais that contained only information from "the time frame that he asked for."

Sometime after June 15, 2016, Bourdelais wrote a report about the incidents concerning the Jacksons' vehicle, in which he stated: (1) there was "no information to prove [Burch] was the one driving the [vehicle] during the [hit-and-run] accident"; (2) the cause of the vehicle fire was unknown; and (3) there were no current suspects for the vehicle theft. Burch asserts Bourdelais' report shows that the GBPD "closed out the case" regarding the vehicle incidents. The State does not dispute Burch's assertion in that regard. We note, however, that the report also stated another officer was "still investigating the hit[-]and[-]run accident."

In the meantime, the BCSO was actively investigating the murder of Nicole VanderHeyden, whose body had been found in a Brown County field on May 21, 2016. In August 2016, the BCSO learned that Burch had been identified as a possible contributor of male DNA found on a sock on VanderHeyden's right foot. The BCSO then began investigating Burch in connection with VanderHeyden's murder. During that investigation, the BCSO learned that the GBPD had downloaded the data from Burch's cell phone in June 2016. The BCSO then obtained a copy of that download from the GBPD.

After examining the download, the BCSO learned that Burch's internet history included sixty-four viewings of news stories about VanderHeyden's murder between May 22, 2016, and June 6, 2016. The BCSO also learned from the download that Burch had a Gmail account, and it subpoenaed the Google Dashboard records associated with that account. Google Dashboard records can show a cell phone's location at a given time using data collected from cell phone towers, Wi-Fi,

and the phone's GPS. Burch's Google Dashboard records showed that during the early morning hours of May 21, 2016, his phone was located near VanderHeyden's residence and then traveled to the field where her body was found.

Burch was arrested and charged with first-degree intentional homicide in connection with VanderHeyden's murder. He moved to suppress all evidence derived from the BCSO's August 2016 search of his cell phone download, arguing the BCSO had "violated the Fourth Amendment when they searched the phone data initially seized by the [GBPD]." The circuit court denied Burch's motion. The case proceeded to a jury trial, during which the State introduced evidence regarding both Burch's internet history and his phone's location on the night of VanderHeyden's murder. The jury convicted Burch of the charged offense. He now appeals, arguing—as relevant here—that the circuit court erred by denying his suppression motion.

DISCUSSION

I. The scope of Burch's consent to search his cell phone

Burch first argues that the information derived from his cell phone download should have been suppressed because the GBPD "exceeded Burch's scope of consent by extracting his entire phone," rather than only his text messages. It is undisputed that the GBPD did not obtain a warrant to search Burch's cell phone, and that searches conducted without a warrant are generally deemed unreasonable for Fourth Amendment purposes. *See* ***State v. Randall***, 2019 WI 80, ¶10, 387 Wis. 2d 744, 930 N.W.2d 223. Nonetheless, "[i]t is well established that a search is reasonable when the subject consents ...." ***Id.*** (quoting ***Birchfield v. North Dakota***, 136 S. Ct. 2160, 2185 (2016)).

When a search is properly authorized by the subject's consent, "the scope of the search is limited by the terms of its authorization." ***Walter v. United States***, 447 U.S. 649, 656 (1980). As such, "[o]ne who consents to a search 'may of course delimit as he chooses the scope of the search to which he consents.'" ***State v. Matejka***, 2001 WI 5, ¶37, 241 Wis. 2d 52, 621 N.W.2d 891 (quoting ***Florida v. Jimeno***, 500 U.S. 248, 252 (1991)). "The standard for measuring the scope of a suspect's consent under the Fourth Amendment is that of 'objective' reasonableness—what would the typical reasonable person have understood by the exchange between the officer and the suspect?"[2] ***Jimeno***, 500 U.S. at 251.

---

[2] The parties dispute the standard of review we should apply to this issue. Citing ***State v. Garcia***, 195 Wis. 2d 68, 535 N.W.2d 124 (Ct. App. 1995), the State argues the scope of an individual's consent to search presents a question of fact subject to the clearly erroneous standard of review. Burch, in contrast, argues that the determination of objective reasonableness presents a question of law that is reviewed de novo.

We believe Burch is correct. True, ***Garcia*** states that "[w]hether consent was given and the scope of the consent are questions of fact that we will not overturn unless clearly erroneous." ***Garcia***, 195 Wis. 2d at 75. In ***Garcia***, however, the underlying factual circumstances pertaining to the defendant's consent were disputed. Two detectives had testified that Garcia gave them consent to search his luggage and motel room, but Garcia denied that he consented to the search. ***Id.*** The circuit court "found the detectives' testimony more credible," and we determined the record supported that credibility finding. ***Id.*** As such, we concluded the court's "finding that consent was given to search the entire motel room [was] not clearly erroneous." ***Id.***

As Burch correctly notes, in this case, the underlying facts surrounding Burch's consent to search his cell phone are not disputed. The issue is whether, given those facts, a reasonable person would have understood that Burch was consenting to allow law enforcement to search his entire cell phone, or merely his text messages. When reviewing a circuit court's decision on a motion to suppress, "we uphold the circuit court's findings of evidentiary or historical fact unless they are clearly erroneous," but we then "independently evaluate those facts against a constitutional standard to determine whether the search was lawful." ***State v. Matejka***, 2001 WI 5, ¶16, 241 Wis. 2d 52, 621 N.W.2d 891. We therefore agree with Burch that while any findings regarding the underlying factual circumstances surrounding his consent would be reviewed using the clearly erroneous standard of review, the ultimate issue of what a reasonable person would have understood the scope of his consent to be presents a question of law for our independent review.

It is undisputed that Bourdelais initially asked Burch whether he could look at the "text messages" on Burch's cell phone, and Burch responded in the affirmative. The State argues, however, that Bourdelais "expanded" the scope of their discussion when he asked whether he could take Burch's phone to a detective to download "the information" from the phone.[3] Bourdelais testified that when he asked Burch about "downloading the information off of his phone," he did not "specifically limit the information to the text messages." Burch orally consented to Bourdelais' request to download "the information" from his phone, and he then signed a written consent form giving Bourdelais "permission to search my ... Samsung cellphone." The form did not reflect any limitations regarding the scope of Burch's consent, nor did Burch himself orally limit the scope of the search during his conversation with Bourdelais. The State argues that on these facts, a reasonable person would have understood that Burch had consented to an unlimited search of his cell phone.

Burch, in turn, argues that the scope of his consent must be interpreted in light of Bourdelais' initial request to view only the text messages on his cell phone. He contends that, based on that initial request, a reasonable person would have understood Bourdelais' subsequent request to download "the information" from his phone to mean "the information" they had previously discussed—i.e., the text messages. Relying on a dictionary definition, Burch argues the definite article "the" "indicates that the noun following 'is definite or has been previously specified by context or by circumstance[.]'" Burch further argues that "[n]othing in the words

[3] The circuit court similarly concluded that while Bourdelais initially asked for consent to view only Burch's text messages, he subsequently "broadened his request" to search Burch's phone when he "began using the blanket term 'information.'"

Bourdelais used indicated that he expressly broadened his request to include information beyond the text messages."

Burch also argues it is irrelevant that neither he nor Bourdelais "specifically limited the information to text messages when they discussed downloading the information from Burch's phone." Relying on ***United States v. Cotton***, 722 F.3d 271, 277 (5th Cir. 2013), he contends that when a person has initially consented to a limited search, his or her subsequent failure to impose limitations on the scope of the search does not operate as an expansion of the original consent. Burch therefore argues that because his consent was "limited to just text messages at the outset," he was not required thereafter to specify that the GBPD could search only his text messages. The State responds that ***Cotton*** is inapt because although Burch initially consented to a search of only his text messages, he subsequently broadened his consent when he gave Bourdelais permission to download "the information" from his phone.

Burch further asserts the fact that he ultimately signed a consent form giving the GBPD permission to search his phone, without limitation, is immaterial. Citing ***United States v. Lemmons***, 282 F.3d 920, 924 (7th Cir. 2002), Burch argues a consent form is "of little help" in determining the scope of an individual's consent and can be "overridden by more explicit statements." The State responds that the consent form in this case is relevant because it confirmed "what Burch had consented to in person: a full download and search of his phone's data."

Ultimately, no published Wisconsin case to date resolves the proper analysis to be used in addressing what a reasonable person would have understood the scope of Burch's consent to be under the undisputed facts of this case, or even in a materially similar situation. Would a reasonable person consider the scope of

Burch's consent to be limited by his initial discussion with Bourdelais about his text messages, or would a reasonable person properly consider their subsequent discussion about the GBPD extracting "the information" from Burch's cellphone as showing that Burch consented to the GBPD searching his phone in its entirety? May a reasonable person consider the consent form's broad scope despite Bourdelais' initial request to review only Burch's text messages? Or, as in ***Lemmons***, would a reasonable person conclude the broad consent form was unhelpful in determining the scope of Burch's consent?

Additionally, may a reasonable person consider Burch's failure to subsequently limit the scope of his signed consent as an expansion of the original consent? Or, as in ***Cotton***, is Burch's failure to subsequently limit the scope of his consent irrelevant, given his initial assent to Bourdelais searching only his text messages? Alternatively, would a reasonable person have understood that the scope of the search was limited by the search's purpose, as testified to by Bourdelais—i.e., to look for communications between Burch and Schuyler, regardless of where they were located on the phone? Or would a reasonable person have understood that the scope of the search was limited to a review of the text message communications between Burch and Schuyler that Burch specifically discussed with Bourdelais? Given that our case law does not provide clear answers to these questions, and given potential concerns with granting unlimited access to an individual's electronically stored information, we believe it is more appropriate for the supreme court, rather than the court of appeals, to address them in the first instance.

II. The GBPD's retention of Burch's cell phone download

Burch next argues that even if the GBPD did not violate his Fourth Amendment rights by searching his entire cell phone in June 2016, it violated his rights by retaining the entire download of his phone's contents. Specifically, Burch argues that after the GBPD isolated the information from the download that it believed was relevant to the vehicle incidents it was investigating, it was required to "expunge or return the non-relevant data." Burch relies on three cases in support of this proposition.

First, Burch relies on ***United States v. Ganias***, 755 F.3d 125 (2d Cir. 2014) (***Ganias I***), *rev'd on reh'g en banc*, 824 F.3d 199 (2d Cir. 2016). In that case, Ganias had provided accounting services to two companies. ***Id.*** at 128. One of those companies was hired to perform work for the United States Army, and in August 2003, the Army received a tip that both companies had been involved in fraudulent conduct. ***Id.*** The tip reported that evidence of the wrongdoing could be found at Ganias's office. ***Id.*** Based on the tip, Army investigators obtained a warrant to search Ganias's office in November 2003, and during the search they created mirror images (i.e., identical copies) of the hard drives from Ganias's computers. ***Id.***

When reviewing the files copied from Ganias's computers, the Army identified potential tax violations by the companies in question, and it therefore gave copies of the files to the Internal Revenue Service (IRS). ***Id.*** at 129. By late 2004, the Army and the IRS had extracted and isolated the files related to the November 2003 warrant; however, they did not purge the non-relevant files because they believed those files were government property. ***Id.***

In 2005, the IRS began to suspect that Ganias, personally, had engaged in tax fraud. ***Id.*** The IRS therefore wanted to review Ganias's personal financial records, which were contained in the digital files that had previously been seized from his office. ***Id.*** The IRS case agent "was aware, however, that Ganias's personal financial records were beyond the scope of the November 2003 warrant, and consequently she did not believe that she could review the non-responsive files, even though they were already in the Government's possession." ***Id.*** The IRS therefore obtained a warrant to search those files. ***Id.*** at 130. Ganias was ultimately convicted of tax evasion, following a jury trial. ***Id.*** at 127.

On appeal, Ganias argued, among other things, that the Government had violated his Fourth Amendment rights when it "copied ... his computer hard drives pursuant to a search warrant and then retained files beyond the scope of the warrant for more than two-and-a-half years." ***Id.*** at 127-28. In addressing that issue, a Second Circuit panel observed that "[i]n light of the significant burdens on-site review would place on both the individual and the Government, the creation of mirror images for offsite review is constitutionally permissible in most instances, even if wholesale removal of tangible papers would not be." ***Id.*** at 135.

Nevertheless, the court concluded the Fourth Amendment does not permit "officials 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." ***Id.*** at 137. The court explained:

> If the 2003 warrant authorized the Government to retain all the data on Ganias's computers on the off-chance the information would become relevant to a subsequent criminal investigation, it would be the equivalent of a general warrant. The Government's retention of copies of Ganias's personal computer records for two-and-a-half years.deprived him of exclusive control over those files for an unreasonable amount of time. This combination of circumstances enabled

> the Government to possess indefinitely personal records of Ganias that were beyond the scope of the warrant while it looked for other evidence to give it probable cause to search the files. This was a meaningful interference with Ganias's possessory rights in those files and constituted a seizure within the meaning of the Fourth Amendment.
>
> We conclude that the unauthorized seizure and retention of these documents was unreasonable. The Government had no warrant authorizing the seizure of Ganias's personal records in 2003. By December 2004, these documents had been separated from those relevant to the investigation of [the companies in question]. Nevertheless, the Government continued to retain them for another year-and-a-half until it finally developed probable cause to search and seize them in 2006. Without some independent basis for its retention of those documents in the interim, the Government clearly violated Ganias's Fourth Amendment rights by retaining the files for a prolonged period of time and then using them in a future criminal investigation.

Id. at 137-38 (citations omitted).

The court rejected the Government's argument that it was entitled to retain the mirror images of Ganias's hard drives because they were "the government's property." ***Id.*** at 138. The court explained that although practical considerations "may well justify a reasonable accommodation in the manner of executing a search warrant, such as making mirror images of hard drives and permitting off-site review ... these considerations do not justify the indefinite retention of non-responsive documents." ***Id.*** The court reasoned that because the November 2003 warrant did not authorize the seizure of Ganias's personal financial records, "the copies of those documents could not become *ipso facto* 'the government's property' without running afoul of the Fourth Amendment." ***Id.***

Ultimately, the court concluded:

> Because the Government has demonstrated no legal basis for retaining the non-responsive documents, its retention and subsequent search of those documents were

> unconstitutional. The Fourth Amendment was intended to prevent the Government from entering individuals' homes and indiscriminately seizing all their papers in the hopes of discovering evidence about previously unknown crimes. Yet this is exactly what the Government claims it may do when it executes a warrant calling for the seizure of particular electronic data relevant to a different crime. Perhaps the "wholesale removal" of intermingled computer records is permissible where off-site sorting is necessary and reasonable, but this accommodation does not somehow authorize the Government to retain all non-responsive documents indefinitely, for possible use in future criminal investigations.

Id. at 139-40 (citations omitted). Because the court concluded "the Government's retention of the computer records was unreasonable," it vacated Ganias's conviction.[4] ***Id.*** at 128.

Burch also relies on ***People v. Thompson***, 28 N.Y.S.3d 237 (N.Y. Sup. Ct. 2016). Thompson was charged with securities fraud and other related offenses. ***Id.*** at 240. The People of the State of New York obtained search warrants permitting the seizure of communications from two of Thompson's email accounts. ***Id.*** at 240-41. The People then seized 100,000 emails, which included approximately 670,000 electronic records totaling 1.65 million pages. ***Id.*** at 242.

---

[4] As Burch acknowledges, ***Ganias I*** was subsequently reversed in an en banc decision of the Second Circuit. *See* ***United States v. Ganias***, 824 F.3d 199 (2d Cir. 2016) (***Ganias II***). In ***Ganias II***, the en banc court concluded that because the second search of Ganias's files was conducted pursuant to a valid warrant, the good faith exception applied and suppression was not necessary. ***Ganias II***, 824 F.3d at 200. The en banc court therefore declined to address whether the Government's retention of Ganias's files violated the Fourth Amendment. ***Id.***

Burch observes that the en banc court "did not withdraw the language from ***Ganias I*** on the Fourth Amendment question," and he therefore argues we should "look to the sound reasoning of ***Ganias I*** as persuasive authority." The State, however, asserts that ***Ganias I*** is "no longer good law."

Following the seizure, the People retained all of the emails—even those that were not responsive to the warrants and had no apparent relevance to the case against Thompson. ***Id.*** The People conceded that they were not permitted to keep the non-relevant emails indefinitely; however, they asserted there was no bright-line rule defining how long they were entitled to retain the emails. ***Id.*** The People took the position that they should be allowed to keep all of the seized emails until the trial proceedings in Thompson's case had concluded. ***Id.***

The trial court disagreed, concluding the People were not permitted to retain all of Thompson's emails until the conclusion of his trial. ***Id.*** at 254-59. The court reasoned that the emails that were not responsive to the warrant were not seized under the warrant's authority but, rather, as a matter of administrative convenience. ***Id.*** at 257-58. As such, the court concluded the non-responsive emails "must be expunged or returned following the reasonable period allotted for a search." ***Id.*** at 258. The court explained:

> The best analogy here is to a warrant authorizing the search of voluminous paper files and records. When a warrant is issued which authorizes a search of paper records, the government is entitled to search the files and seize responsive material. They are not permitted to search the files, seize responsive material and then retain files they have never identified as relevant for multiple years, because, at some later time, they might want to search the files again. A search warrant which authorizes a search of voluminous digital records is no different. As Defendant's counsel during an argument pointed out, overseizure is "a courtesy that was developed for law enforcement". It is not a license for the government to retain tens of thousands of a defendant's non-relevant personal communications to review and study at their leisure for years on end.

Id. at 258-59 (footnote omitted).

Burch argues ***Thompson*** demonstrates that "[w]hile police can overseize digital data as an administrative convenience, once the relevant data is separated, police cannot conduct a new search of the non-relevant data. Instead, police must expunge or return the non-relevant data." (Citations omitted.) Burch also cites ***United States v. Tamura***, 694 F.2d 591, 596-97 (9th Cir. 1982), for the proposition that "[u]nder general Fourth Amendment principles applicable to tangible items, police would need to return items that contain no evidentiary value." Burch asserts there is "no reason" that this general rule applicable to tangible items should not be equally applicable to digital information.

In response, the State asserts that ***Ganias I***, ***Thompson***, and ***Tamura*** are distinguishable because each of those cases involved warrants that "limited what the [government was] allowed to do with the evidence seized." The State argues the situation in this case is materially different because Burch "consented to the download of all his phone's data." The State contends that by doing so, Burch "lost his privacy interest in what he voluntarily turned over to police, and they were allowed to keep the data."

In support of its assertion that Burch gave up his privacy interest in his cell phone's data, the State cites ***State v. Stout***, 2002 WI App 41, ¶17 n.5, 250 Wis. 2d 768, 641 N.W.2d 474, in which this court stated that when a person consents to a search of either an automobile or a dwelling, that person "is giving up his or her right to privacy by consent." The State also cites ***Randall***, in which a majority of the justices on our supreme court agreed that the defendant lacked a reasonable expectation of privacy in her blood-alcohol content after she consented to the police taking a sample of her blood. *See* ***Randall***, 387 Wis. 2d 744, ¶39 n.14; ***id.***, ¶¶42, 55 (Roggensack, C.J., concurring).

Neither ***Stout*** nor ***Randall***, however, addressed whether a person who consents to a search gives up his or her right to privacy in the searched material in perpetuity. We doubt the State would argue that by consenting to a search of his or her automobile, a person forevermore gives up his or her right to privacy in that automobile. The State does not develop any argument that the result should be different for digital evidence. Moreover, in ***Randall***, the testing of the defendant's blood sample to determine her blood-alcohol content was directly related to the purpose of taking the sample in the first place—i.e., to determine whether the defendant had operated a motor vehicle while intoxicated. Nothing in ***Randall*** suggests that because the defendant consented to law enforcement taking a blood sample under those circumstances, the State could retain that blood sample for an unlimited period of time and then perform different tests on it—for instance, DNA testing—in connection with an unrelated case.

Although not cited by either Burch or the State, a recent decision by the Illinois Appellate Court addressed the issue of how long police could retain digital evidence obtained during a lawful search. *See* ***People v. McCavitt***, 2019 IL App (3d) 170830, 145 N.E.3d 638. 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. Officers seized McCavitt's computer and subsequently obtained a warrant allowing them to search the computer for digital images and evidence of sexual assault. ***Id.***, ¶¶3-4. A forensic examiner from the Peoria County Sheriff's Department then made a mirror image of the computer's hard drive. ***Id.***, ¶4.

Based on the images found on his computer, McCavitt was charged with multiple counts of sexual assault. ***Id.***, ¶5. He was acquitted of all counts following a jury trial. ***Id.*** On the day of his acquittal, McCavitt orally requested the

return of his personal property, including his computer, but the trial court denied his request. ***Id.*** McCavitt later filed a written motion for the return of his property, but the court never ruled on that motion. ***Id.***, ¶6.

In March 2014, the Peoria Police Department began investigating McCavitt and requested a copy of the mirror image of his hard drive from the Peoria County Sheriff's Department. ***Id.*** A detective reviewed the mirror image and discovered images that he believed were child pornography. ***Id.*** McCavitt was ultimately charged with seventeen counts of possessing child pornography, and a jury convicted him of fifteen of those charges. ***Id.***, ¶¶7, 9, 11.

On appeal, McCavitt argued the trial court had erred by denying his motion to suppress the evidence obtained from the mirror image of his hard drive. The Illinois Appellate Court agreed that suppression was warranted. ***Id.***, ¶1. In so doing, the court relied upon the following principles:

- Individuals have a reasonable expectation of privacy in their personal computers and computer files. ***Id.***, ¶17.

- However, an owner's expectation of privacy is "significantly reduced" once an item has been lawfully seized and searched by police. ***Id.***

- There is no established upper limit as to when the government must review seized electronic data to determine whether it falls within the scope of a warrant. ***Id.***, ¶19.

- Nevertheless, the Fourth Amendment requires the government to complete its review of electronic data within a reasonable period of time. ***Id.***

- Copying electronic data by creating a mirror image of a computer hard drive for later analysis offsite has become a common practice that does not violate the Fourth Amendment. ***Id.***, ¶20.

- Retention of a mirrored hard drive during the pendency of an investigation and trial does not violate the Fourth Amendment. ***Id.***

- However, the government may not retain seized property indefinitely, and the government's failure to quickly return information from a mirrored hard drive that is not within the scope of a warrant may violate the Fourth Amendment. ***Id.***, ¶21.

- All property seized must be returned to its rightful owner once the criminal proceedings have terminated. ***Id.***, ¶22.

- When no charges are pending against an individual, the government should immediately return to the individual any of his or her property in its possession. ***Id.***

- After criminal proceedings conclude, the government has no right to retain a defendant's property. ***Id.***

Based on these principles, the appellate court concluded McCavitt had an expectation of privacy in his computer files, but that expectation was "significantly diminished" after police took possession of his computer. ***Id.***, ¶24. Nevertheless, the court stated that once McCavitt's trial on the sexual assault charges had concluded, he "could again expect that he had a right to privacy in the contents of his computer." ***Id.*** Accordingly, the police violated McCavitt's right to privacy when they searched the mirror image of his hard drive in March 2014. ***Id.***, ¶25. The court explained:

> While police lawfully created [the mirror image] to forensically examine defendant's hard drive, they were not entitled to retain the entire [mirror image] indefinitely. Rather, police were required to examine the contents of the mirrored hard drive and retain only those files that fit within the scope of the July 17, 2013, warrant. While police could retain the relevant files throughout defendant's trial, once defendant's trial ended, police were not entitled to retain any portion of the [mirror image], much less the entire file.

Id. (citations omitted).

Applying the principles set forth in ***McCavitt*** to this case, an argument could be made that although Burch's expectation of privacy in the data on his cell phone was "significantly diminished" when the GBPD took possession of his cell phone, he could again expect that he had a right to privacy in the contents of his cell phone after the GBPD concluded its investigation of the vehicle incidents. Thus, ***McCavitt*** arguably supports a conclusion that the GBPD violated Burch's rights by retaining the data from his cell phone after that investigation was concluded. Notably, however, the Illinois Supreme Court recently accepted review of ***McCavitt***, and it has not yet released its decision in that case. *See* ***People v. McCavitt***, 147 N.E.3d 692 (2020).

The GBPD's retention of Burch's cell phone download therefore raises numerous questions, none of which have been squarely answered by Wisconsin case law or by binding federal precedent. For instance, after the GBPD performed the download, what portion of Burch's data could it lawfully retain—none of the material, only the material it actually searched during its investigation of the vehicle incidents, or the entire download? If the GBPD was permitted to retain some or all of the downloaded material, how long could it do so? Additionally, did the status of the original investigation that produced the download affect the GBPD's ability to lawfully retain the downloaded material? Stated

differently, if the first investigation was "closed," did that fact affect the validity of the GBPD continuing to retain the downloaded material, or at least continuing to retain the portions of that material that were not deemed relevant to the first investigation? Furthermore, did the GBPD have any obligation to return the downloaded material to Burch, and if so, when? Relatedly, was Burch required to request the return of the downloaded material in order to trigger the GBPD's obligation to return it?

In addition, we question whether it makes a difference that the material in question was merely a copy of Burch's cell phone data, while the phone itself was promptly returned to him. The parties' briefs do not address whether Burch had a possessory interest in the copy itself, which the GBPD created. Moreover, the parties have not addressed whether it matters that the GBPD shared the downloaded material with another law enforcement agency—i.e., the BCSO. Given the significant number of unanswered questions regarding the legality of the GBPD's retention of Burch's cell phone download, we believe it is appropriate for the supreme court, rather than the court of appeals, to address whether the GBPD's retention of the download violated Burch's Fourth Amendment rights.

III. The BCSO's August 2016 examination of Burch's cell phone download

Finally, Burch argues that even if the GBPD's initial search of his cell phone did not exceed the scope of his consent, and even if the GBPD properly retained the cell phone download, the BCSO had "no authority" to conduct a second search of the download in August 2016 in connection with its investigation of VanderHeyden's murder. Burch observes that the BCSO did not seek or obtain a warrant before examining the download in August 2016. Burch also asserts that the "lawful authority to search is generally limited to a single search," and as a result,

law enforcement's "authority to conduct a consent search in June 2016 had been exhausted by August 2016." In support of this proposition, Burch notes that in the warrant context, searches are generally subject to the "one warrant, one search" rule, unless a subsequent search is a reasonable continuation of the earlier search. *See* ***State v. Avery***, 2011 WI App 124, ¶18, 337 Wis. 2d 351, 804 N.W.2d 216, *abrogated on other grounds by* ***State v. Jackson***, 2016 WI 56, ¶66, 369 Wis. 2d 673, 882 N.W.2d 422.

Burch also relies on ***State v. Douglas***, 123 Wis. 2d 13, 365 N.W.2d 580 (1985). There, the supreme court concluded that even though the defendant had impliedly consented to a search of his home, police needed a warrant to reenter the home to conduct a second search "approximately forty-five hours after the implied consent was given and twenty-two and one-half hours after other investigative activities in the home had ceased." ***Id.*** at 14-15. The court stated that even though the defendant had impliedly consented to the initial search, "such authorization is not perpetual." ***Id.*** at 21. The court further reasoned that the second search was not merely a "continuation" of the initial, lawful search because of the significant temporal delay between the two. ***Id.*** at 23-24.

Burch argues that, in this case, "there can be no argument that the August search of [his cell phone download] for evidence of a homicide was a continuation of the June search for evidence of a hit and run." He reasons, "By way of analogy, no one would suggest that if one consents to police searching his home for evidence of marijuana possession, that police could use that consent to reenter his home months later searching for evidence of a homicide."

The State, for its part, does not argue that the BCSO's examination of the cell phone download in August 2016 was a continuation of the June 2016 search.

Instead, the State contends that the BCSO's examination of the download did not constitute a "search" under the Fourth Amendment because Burch gave up his expectation of privacy in the phone's contents when he consented to the GBPD performing the extraction. *See* ***Stout***, 250 Wis. 2d 768, ¶17 n.5. The State therefore asserts ***Douglas*** is distinguishable because it involved the repeated search of the defendant's home, in circumstances where the defendant's consent was "limited to the initial entry." In contrast, the State argues that Burch "consented to have law enforcement download and search his entire phone," and as a result, the BCSO's "later examination of the phone's data did not implicate the Fourth Amendment."

The State also argues that our case law gives law enforcement permission to "reexamine evidence that is lawfully in its possession." The State relies on three cases in support of that proposition.

First, the State cites ***State v. Petrone***, 161 Wis. 2d 530, 538, 468 N.W.2d 676 (1991), *abrogated on other grounds by* ***State v. Greve***, 2004 WI 69, ¶31 n.7, 272 Wis. 2d 444, 681 N.W.2d 479, in which police executing a search warrant seized cannisters containing undeveloped film from the defendant's home. On appeal, the defendant argued that "developing the film later at the police station was a second, separate search for which a warrant should have been obtained." ***Id.*** at 544. The supreme court rejected that argument, concluding that developing the film was "simply a method of examining a lawfully seized object," akin to laboratory testing of blood gathered during a lawful search or using a magnifying glass to examine lawfully seized documents. ***Id.*** at 545.

Second, the State cites ***State v. VanLaarhoven***, 2001 WI App 275, 248 Wis. 2d 881, 637 N.W.2d 411. In that case, the court of appeals concluded a warrant was not required to test a blood sample that the defendant had consented to

provide. ***Id.***, ¶¶8, 17. Relying in part on ***Petrone***, we stated that "the examination of evidence seized pursuant to the warrant requirement or an exception to the warrant requirement is an essential part of the seizure and does not require a judicially authorized warrant." ***Id.***, ¶16.

Third, the State relies on ***State v. Reidel***, 2003 WI App 18, 259 Wis. 2d 921, 656 N.W.2d 789 (2002). There, we concluded police were not required to obtain a warrant in order to test a blood sample that they had lawfully obtained under the exigent circumstances exception to the warrant requirement. ***Id.***, ¶¶1, 17.

Burch argues that ***Petrone***; ***VanLaarhoven***, and ***Reidel*** are distinguishable because in each of those cases, law enforcement's examination of the evidence in question could not be "parsed" from its earlier seizure of that evidence. In other words, Burch asserts the "examination of [the] evidence [was] essential to the seizure and constitute[d] a single constitutional event." Conversely, Burch argues the BCSO's search of his cell phone extraction in this case can easily be parsed from the GBPD's earlier search and seizure of his phone, in that the BCSO's search was conducted by a different agency, in an unrelated investigation, approximately two months after the initial search.

The parties also dispute whether the BCSO's examination of Burch's cell phone download was permissible under the "second look" doctrine set forth in ***State v. Betterley***, 191 Wis. 2d 406, 529 N.W.2d 216 (1995). There, Betterley was suspected of having falsely reported a ring as stolen in order to defraud his insurer. ***Id.*** at 411-12, 414. Betterley was taken into custody on a probation hold for an unrelated violation, and jail staff conducted an inventory search of the items on his person. ***Id.*** at 414-15. During the search, a ring was found in Betterley's pocket

and placed in a jail property box. ***Id.*** at 415. Later that day, the officer investigating the insurance fraud matter learned about the ring and took it as evidence in that case. ***Id.*** The ring was subsequently identified as the ring Betterley had reported as stolen. ***Id.***

Following his convictions for felony theft and obstructing an officer, Betterley argued the circuit court should have suppressed evidence regarding the ring because the police violated his Fourth Amendment rights by removing it from the jail property box and examining it in connection with the insurance fraud case. ***Id.*** at 411-12. Relying on ***United States v. Edwards***, 415 U.S. 800 (1974), our supreme court rejected Betterley's argument, concluding police could permissibly take a "second look" at the ring without obtaining a warrant. ***Betterley***, 191 Wis. 2d at 416-18. The court reasoned that a defendant has a diminished expectation of privacy in items legitimately in police possession, by virtue of the fact that those items have already been exposed to law enforcement. ***Id.*** at 417-18. Thus, the court held that it is permissible for law enforcement to take a "second look" at those items, as long as the "second look" does not exceed the extent of the original search. ***Id.*** at 418.

The State argues ***Betterley*** stands for the proposition that "police may subsequently examine an item lawfully in their possession to the same extent they could originally search the item." Burch disagrees, asserting that the "second look" rule announced in ***Betterley*** applies only in the context of inventory searches. Notably, Burch does not cite any authority in support of that proposition. Nevertheless, we have not located any Wisconsin case since ***Betterley*** that has expressly addressed whether the "second look" doctrine announced in that case applies outside the context of inventory searches.

Indeed, after reviewing the authorities cited by the parties and conducting our own research, we are left with significant questions regarding whether the BCSO had authority to search Burch's cell phone download in August 2016. Was the BCSO's examination of the download a search within the meaning of the Fourth Amendment, such that a warrant was required? Or was no warrant required because Burch had previously given up his expectation of privacy in his cell phone data by consenting to the GBPD's June 2016 search? Alternatively, was the BCSO's examination of the download a permissible "second look" under ***Betterley***?

Furthermore, even if the BCSO was not required to obtain a warrant, what was the permissible scope of its examination of Burch's cell phone download, especially if that scope is based upon Burch having given up some expectation of privacy in his phone? Could the BCSO review the entire download, or only the material that was actually reviewed by the GBPD during its June 2016 search? Alternatively, could the BCSO review material in the extraction that was related to the purpose of the first search, regardless of whether the GBPD actually reviewed it? Or, was the BCSO limited to reviewing only data that was actually culled from the first search and used or referred to in reports generated as a result of that search?

CONCLUSION

As the United States Supreme Court has observed, modern cell phones carry vast amounts of data about their owners and therefore implicate heightened privacy concerns that do not necessarily apply to physical objects. *See* ***Riley v. California***, 573 U.S. 373, 393-98 (2014).

> The storage capacity of cell phones has several interrelated consequences for privacy. First, a cell phone collects in one place many distinct types of information—an address, a

> note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier. A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a phone.

Id. at 394-95. Thus, the ***Riley*** Court recognized that a search of a cell phone will typically expose to the government "far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is." ***Id.*** at 396-97.

For these reasons, it is critical that courts, to the best of their ability, clearly delineate the extent to which law enforcement may search, retain, and reexamine the data contained on individuals' cell phones. As set forth above, although some of our prior case law touches on these issues, it does not squarely address them. Furthermore, many of the potentially relevant cases discuss the application of Fourth Amendment principles to traditional, physical evidence, rather than the digital data at issue here.

The Wisconsin Supreme Court "has been designated by the constitution and the legislature as a law-declaring court." ***State v. Grawien***, 123 Wis. 2d 428, 432, 367 N.W.2d 816 (Ct. App. 1985). "While the court of appeals also serves a law-declaring function, such pronouncements should not occur in cases of great moment." ***Id.*** Given 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. A decision by the supreme court "will help develop, clarify or harmonize the law," WIS. STAT. RULE 809.62(1r)(c) (2017-18), thereby providing much needed guidance to Wisconsin residents, attorneys, and lower courts.