RECEIVED
12-09-2019
CLERK OF WISCONSIN
COURT OF APPEALS

STATE OF WISCONSIN
COURT OF APPEALS
DISTRICT III
Case No. 2019AP1404-CR

STATE OF WISCONSIN,
Plaintiff-Respondent,
v.
GEORGE STEVEN BURCH,
Defendant-Appellant.

On Notice of Appeal to Review the Judgment of Conviction entered in the Circuit Court for Brown County, the Honorable John Zakowski Presiding.

CORRECTED BRIEF AND APPENDIX OF DEFENDANT-APPELLANT

ANA L. BABCOCK
State Bar No. 1063719
Attorney for Defendant-Appellant

BABCOCK LAW, LLC
130 E. Walnut Street, St. 602
P.O. Box 22441
Green Bay, WI 54305
(920) 884-6565
ababcock@babcocklaw.org

TABLE OF CONTENTS

TABLE OF AUTHORITIES

STATUTES

CASES

OTHER SOURCES

STATEMENT OF ISSUES

I. WHETHER POLICE VIOLATED BURCH'S FOURTH AMENDMENT RIGHTS BY CONDUCTING A SECOND WARRANTLESS SEARCH OF HIS CELL PHONE EXTRACTION?

The circuit court answered no.

II. WHETHER CRITICAL EVIDENCE FROM FITBIT, INC.'S BUSINESS RECORDS WAS ADMISSIBLE WITHOUT EXPERT TESTIMONY AND WITHOUT A WITNESS FROM FITBIT TO ESTABLISH THAT THE EVIDENCE WAS ACCURATE AND RELIABLE? ALSO, WHETHER THIS ISSUE IMPLICATED BURCH'S RIGHT TO CONFRONTATION?

The circuit court allowed the Fitbit evidence without an expert and without a witness from Fitbit. The court concluded that there was no Confrontation violation.

POSITION ON ORAL ARGUMENT AND PUBLICATION

This case will change the landscape of the law in Wisconsin and the entire country. With advances in technology, police can now gain perpetual access to the privacies of one's life with the click of a button. While the dimensions of physical evidence used to impose natural limitations on searches, these limitations are largely absent when dealing with digital evidence. In this case, the Court is tasked with defining the limitations of searching, retaining, sharing, and continuing to search digital evidence.

The technologies available to us today involve concepts that the Framers would have never contemplated. Cars can drive themselves, we have devices in our homes constantly listening for us to give the "Alexa" or "hey

Google" command, our precise location is tracked across multiple mediums, facial recognition software is used to unlock our cell phones and to tag us in images on social media, to name a few. These advancements will only continue to perpetuate and likely at a rapid pace. Historic Fourth Amendment law simply does not answer the problems that new technology presents, and this case will set the benchmark for how to address these issues.

In addition, this case will establish the standard for admission of this technology, and it explores the Confrontation implications now that machines can be witnesses against us. For these reasons, this Court should publish this decision and oral argument is appropriate.

SUMMARY OF THE CASE

This case involves the tragic brutal murder of a young woman. After exhaustive searches, police arrested her boyfriend, and he was held in custody for eighteen days. Police subsequently reviewed information on the boyfriend's phone, purportedly derived from his Fitbit device, showing that at the time of the murder, he took only about a dozen steps. Police assumed that this information was accurate and reliable, the boyfriend was released, and the investigation continued.

After a few months, DNA suitable for comparison was found on the victim's sock, and a database hit provided an investigative lead that Burch was the source of that DNA. Police then searched their records looking for any information on Burch, and they discovered that an extraction from Burch's cell phone was being held in evidence by another agency. Police obtained and scoured the extraction, and they discovered critical information leading to a trail of inculpatory digital evidence.

STATEMENT OF THE FACTS

On May 20, 2016, the victim, Nicole Vanderheyden, and her boyfriend, Douglass Detrie, went to a concert with a group of friends at a bar called the Watering Hole. R. 242:122-24. At some point, Vanderheyden and Detrie got separated, and Vanderheyden left with some friends to head to another bar, the Sardine Can. *Id.* at 17-20.

While at the Sardine Can, Vanderheyden repeatedly called Detrie, but he was not answering her calls. *Id.* at 22. Another woman in the group then called Detrie, and he answered. *Id.* Vanderheyden became visibly upset that Detrie answered the woman's call but not her own calls, and she took off running out of the bar down the street. *Id.* at 23-24. By that time, Detrie was on his way to the Sardine Can with his friend Greg Mathu. *Id.* at 58. Vanderheyden eventually spoke to Detrie on the phone; she was angry, and the call abruptly ended. *Id.* at 58-59. Over the course of the evening, Vanderheyden sent Detrie a slew of angry text messages, including one that said, "Fuck u, abusive ass hole." *Id.* at 164; R. 126, Exh. 41.

Detrie and Mathu drove up and down a few different roads looking for Vanderheyden but could not locate her. R. 242:60. They ended up going to the Sardine Can and taking shots. *Id.* at 60. Around 2:15 a.m., Detrie and Mathu left the Sardine Can and got back to Detrie's house around 2:45 a.m. *Id.* at 64. Dallas Kennedy, the babysitter for Vanderheyden's and Detrie's infant son, was at the home when they arrived. *Id.* at 64, 122. Detrie told Kennedy that he and Vanderheyden had been in an argument, and Detrie asked Kennedy for some marijuana. R. 240:187, 234. Detrie smoked the marijuana, and Kennedy, feeling scared, then raced out of the house. *Id.* at 235; R. 251:154.

The following afternoon, some farmers were grooming a field off Hoffman Road, and they discovered a body down an embankment. R. 239:58, 62. The field is approximately three miles from Detrie's residence. R. 240:259. At 1:54 p.m., the Brown County Sheriff's Office ("BCSO") arrived on scene. R. 239:96-97. The body was unclothed except for socks on the feet and a pink wristband on the arm. R. 240:14-15. There was obvious trauma to the victim's face, and police were unable to identify the victim. *Id.* at 15, 17. Dental records later confirmed that the victim was Vanderheyden. *Id.* at 26. A subsequent autopsy revealed ligature strangulation and blunt-force injuries to the head as the cause of death. R. 240:117.

By 3:45 p.m. on May 21, a large police presence permeated the area of Hoffman Road. *Id.* at 30-31. While on scene, police received a missing person report from Detrie, and police responded to his residence to take the report. *Id.* at 32-33, 259-61. Around 2:30 a.m. on May 22, a search warrant was executed at Detrie's residence. *Id.* at 169-71. Later that day, the babysitter, Dallas Kennedy, confronted Detrie on what happened to Vanderheyden, and he said "I don't know. She hit her head and then she just wanted to walk home." R. 251:151. At that time, investigators had not disclosed to Detrie that the victim suffered injuries to the head. R. 245:39.

Around 5:45 a.m. on May 22, police discovered a pile of blood-stained clothing on a freeway on-ramp. R. 240:165, 170. A lanyard bearing Vanderheyden's name was also found. *Id.* at 173. On May 23, police got a report of a large amount of blood outside a home on Berkley Road. R. 245:145. The homeowner was Matthew Petersen, Douglass Detrie's neighbor. *Id.* at 100. Petersen testified that around 10:00 a.m. on May 21, he went out to mow his lawn and noted a significant amount of blood in his front yard.

Id. While mowing his lawn, something hit the mower blade, and Petersen found a piece of cord, which he picked up and then set aside. *Id.* at 101. Petersen initially thought the blood was from an animal, but after hearing of the incident on the news, Petersen reported this information to law enforcement. *Id.* at 103-04. In searching the area, police found a large amount of blood and collected clumps of hair, bobby pins, and a piece of wire that appeared to have split in two. *Id.* at 141, 145. Swabs taken from the street and the wire matched the victim's DNA. R. 246:180-81, 185. Police subsequently learned that the blood on the street was there as of about 5:40 a.m. on May 21. *See* R. 245:115-16.

Police then executed a second search warrant on Detrie's home on May 23. R. 246:42. Immediately upon entering the residence, a seasoned detective noticed a strong odor of chemical cleaning agents. R. 245:140, 171-72. The detective found this notable because the house was in an unkempt state. *Id.* at 174. Several key pieces of evidence were seized from Detrie's home. R. 246:42. First, police located a pair of Air Jordan shoes that had a herringbone pattern consistent with an unusual pattern identified on the victim's back. *Id.* at 43. Second, police seized another pair of shoes containing a red substance. *Id.* at 44. Third, police identified blood on the garage floor near the victim's vehicle along with suspected blood inside of the vehicle. *Id.* at 50. Fourth, police found tissues and a sweatshirt containing blood in the lower bathroom. *Id.* at 50. Fifth, police found evidence of blood in the master bathroom shower and bedroom carpet. R. 245:63, 84. Finally, police seized a box of wires from Detrie's garage that they believed may have been used to strangle the victim. R. 251:173-74.

Detrie was arrested later that day, on May 23, 2016, for the first-degree intentional homicide of Vanderheyden. R. 240:283-84. Detrie remained in custody for eighteen days. R. 246:52-53. In June 2016, police looked at Detrie's Fitbit app on his phone, which showed that around the time police believed Vanderheyden was murdered, Detrie took about twelve steps. R. 251:49, 51-52, 57. The Fitbit evidence steered the investigation away from Detrie, and he was released. *See id.*; R. 53:1.

Sergeant Richard Loppnow and Sergeant Brian Slinger, both of the Brown County Sheriff's Office ("BCSO"), were appointed the lead detectives on the case. R. 246:40-41. BCSO continued with the investigation sending various evidence transmittals to the state crime lab. *Id.* at 54. According to the lab, they kept seeing an unknown Y profile in several of the items, which the lab coined "Y Profile 1." *Id.* at 61-62, 184. However, unlike autosomal DNA profiles, which are specific to one individual (apart from identical twins), multiple males can share the same Y profile. *Id.* at 163-64. Thus, Y profiles cannot be searched against known profiles in a database. *Id.* at 189.

On August 17, 2016, after testing a sock found on the victim, the lab identified an autosomal DNA profile suitable for comparison in the database. R. 8:5, ¶ 5(d); R. 246:192-93. The lab entered the profile into the database, which developed a hit: George Burch. R. 246:194. However, the database hit did not provide any definitive conclusions; it simply offered an investigative lead for law enforcement. *Id.*

Armed with the database hit, BCSO searched their records for any information about Burch and discovered reports from a vehicle incident in June 2016. R. 234:54-55.

The reports noted that the Green Bay Police Department ("GBPD") had downloaded Burch's cell phone, and the reports contained a signed consent form. *Id.* The BCSO then obtained a copy of the cell phone extraction from the GBPD without a warrant. *Id.* at 55-56. Tyler Behling, a computer analyst with the BCSO, searched the extraction, "looking for anything in the timeframe of the night of the 20th into the morning hours of the 21st, whether it be calls, texts, internet history, any kind of location data available from that device." R. 251:66. During the search of Burch's phone extraction, Behling discovered a Google email address. R. 234:57. In addition, Behling reviewed Burch's internet history and discovered that he had searched for information relating to the Vanderheyden case sixty-four times. R. 251:66.

The BCSO was aware that individuals with a Google email account have a "Google Dashboard," which tracks the user's location via GPS, Wi-Fi, and cell phone tower data. R. 246:95. The BCSO then drafted a warrant for the location information associated with the Google email account found on Burch's phone extraction. R. 234:57. The Google Dashboard data placed Burch at the murder scene: traveling from a bar near the Sardine Can, to Vanderheyden's residence, to the field where the body was found, and to the location where her property was discarded at times consistent with when police believed the victim was killed. R. 251:77-90.

On September 7, 2016, Burch was arrested. R. 246:98. Following his arrest, the BCSO secured a warrant for Burch's DNA and obtained a buccal swab. *Id.* at 99. Using this sample, the lab confirmed Burch's DNA on Vanderheyden's sock to a high probability. *Id.* at 196-97. The lab also developed a Y profile from Burch's DNA sample, and this profile was deemed consistent with "Y

Profile 1" detected on various swabs of the victim's body and on one of the cables found at the scene. *Id.* at 204-06; R. 152:1, 3. On September 16, 2016, Burch was charged with first-degree intentional homicide. R. 8.

At a status conference on October 20, 2017, the defense requested a *Daubert*[1] hearing for any experts the State intended to call from Fitbit. R. 231:3. The defense had concerns over the reliability of the Fitbit evidence and asked for Fitbit's internal validation studies or other information to support reliability. *Id.* at 7-8. The State responded that some of that information may be protected by trade secrets, but agreed that it needs to have a witness from Fitbit testify to its reliability. *Id.* at 8-9.

On December 7, 2017, Burch filed a motion to exclude all Fitbit evidence after learning that the State would not be calling a witness from Fitbit to present that evidence.[2] R. 47. As grounds, Burch argued that the Fitbit evidence required expert testimony and a witness from the company to authenticate the data. *Id.* at 2. In addition, Burch argued that admission of this evidence without a witness from Fitbit or an expert violated his right to Confrontation. *Id.* Following briefing and argument (R. 53; R. 63-64; R. 65; R. 233), the circuit court ruled that the Fitbit evidence was admissible without expert testimony and without any authenticating witness from Fitbit.[3] R. 70; App. 136-156.

On January 25, 2018, Burch filed a motion to suppress all evidence obtained from the August 2016 search of his cell phone extraction, asserting a Fourth

[1] *Daubert v. Merrell Dow Pharm., Inc.,* 509 U.S. 579 (1993).
[2] This case involved significant pretrial motion practice. Given the space limitations of this brief, Burch's appeal focuses on only the cell phone and Fitbit issues.
[3] The issues in this case are complex, and Burch fully develops the facts and reasoning in the argument section.

Amendment violation. R. 68. The circuit court denied the motion, concluding that the BCSO lawfully searched Burch's cell phone extraction in August and that, in any event, the evidence is admissible under the inevitable discovery doctrine. R. 101; App. 115-129.

On February 16, 2018, the trial commenced. R. 237. At trial, there was no question that the victim was brutally murdered. *See* R. 255:90. This was, as the State put it, a "whodunit" case." *Id.* The State relied primarily on the following evidence to support guilt: Burch's DNA on Vanderheyden's sock and body; the Google Dashboard data placing Burch at the four key locations implicated in the crime; and the web history showing Burch "obsessively searching for news accounts" to figure out if he was going to "get away with it[.]" *Id.* at 91-92.

Burch took the stand at trial. R. 252:51. Burch testified that on the evening of May 20 around 11 p.m., he went to a bar called Richard Craniums. *Id.* at 115. At some point in the evening, he saw an attractive blonde woman, who he now knows to be Vanderheyden, standing in the bar area. *Id.* at 117-18. The two started chatting and flirting. *Id.* at 120. At bar close, Burch and Vanderheyden left together and headed to Burch's home. *Id.* at 121. When they went into Burch's house, the elderly father of his roommate was sitting in the living room in his robe, and the two decided to head toward Vanderheyden's house. *Id.* at 122. Vanderheyden navigated Burch to her home but saw a light on in the house, so she told Burch to pull to the side of the road. *Id.* at 123-25. The two became intimate in the front seat of the vehicle and progressed to the back seat. *Id.* at 126. Ultimately, the two had intercourse with Vanderheyden laying on the back seat and Burch standing outside the vehicle. *Id.* at 130-33.

As Burch described, the next thing he recalled was awaking on the ground outside the vehicle to a man pointing a gun at him. *Id.* at 133, 137. Burch then saw Vanderheyden, covered in blood, laying on the ground. *Id.* at 142. The armed man said "Look what the fuck you made me do[.]" *Id.* at 143-44. The man instructed Burch to place the victim in the vehicle. *Id.* at 144. The man got into the vehicle, and Burch was able to see the man's face in the rearview mirror. *Id.* at 148-50. Burch did not recognize the armed man at the time, but he now knows him to be Detrie. *Id.* at 150. Burch testified that Detrie directed him to drive and ultimately navigated him to the field off Hoffman Road. *Id.* at 151-54, 161. Burch explained that Detrie ordered him out of the vehicle and directed him to take the victim to a ravine area in the field. *Id.* at 155-58. Burch then lunged at Detrie, knocking him backward, ran back to the vehicle, and was able to get away. *Id.* at 163-64.

The jury ultimately found Burch guilty (R. 255:158), and the Court sentenced Burch to life in prison without the possibility for parole. R. 256:62. This appeal follows.

ARGUMENT

I. THE BROWN COUNTY SHERIFF'S OFFICE'S SEARCH OF BURCH'S CELL PHONE EXTRACTION IN AUGUST 2016 VIOLATED THE FOURTH AMENDMENT

A. Standard of Review

This Court's review of a decision on a motion to suppress presents a question of constitutional fact, and the Court engages in a two-step inquiry. *State v. Robinson*, 2010 WI 80, ¶ 22, 327 Wis. 2d 302, 786 N.W. 2d 463. The Court reviews the circuit court's finding of historical facts under a clearly erroneous standard. *Id.* When evaluating

the circuit court's factual findings, this Court defers to the circuit court's credibility assessments "because of its superior opportunity to observe the demeanor of witnesses and to gauge the persuasiveness of their testimony." *State v. Carnemolla,* 229 Wis. 2d 648, 661, 600 N.W. 2d 236 (Ct. App. 1999). The Court reviews the application of facts to constitutional principles de novo. *See Robinson*, 327 Wis. 2d 302, ¶ 22.

B. Privacy in Cell Phones

In *Riley v. California*, the Supreme Court held that modern cell phones implicate heightened privacy concerns, greater than those at issue with physical objects. 573 U.S. 373, 393-97 (2014). Today, cell phones hold "'the privacies of life.'" *Id.* at 403 (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)). Cell phones now represent a reconstruction of one's private life: photographs stamped with date and location data, medical conditions, prescription information, political affiliation, personal notes, financial data, and one's precise movements down to the minute. *Id.* at 394-96.

> Indeed, a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form–unless the phone is.

Id. at 396-97 (emphasis in original).

This issue involves a series of constitutionally significant events, each of which violated Burch's Fourth Amendment rights. First, police exceeded Burch's scope of consent by extracting his entire phone. Second, police violated the Fourth Amendment by *retaining* the entire

phone extraction. Finally, police conducted a new search without lawful authority to do so.

C. The GBPD Unlawfully Extracted Burch's Entire Phone

The Fourth Amendment generally requires that police obtain a warrant before conducting a search. *State v. Randall*, 2019 WI 80, ¶ 10, 387 Wis. 2d 744, 930 N.W.2d 223. There are several exceptions to the warrant requirement, including consent. *Id.* The scope of consent, however, is limited by its authorization. *Walter v. United States*, 447 U.S. 649, 656-57 (1980). For example, "[c]onsent to search a garage would not implicitly authorize a search of an adjoining house; a warrant to search for a stolen refrigerator would not authorize the opening of desk drawers." *Id.*

In June 2016, Burch was living with friends Edward and Linda Jackson, and the Jacksons allowed Burch to use their extra vehicle to travel to work. R. 249:48-50. On June 8, 2016, Edward Jackson noticed that the vehicle was missing, and he made a report to police. R. 234:4-5; App. 103-04. According to Jackson, Burch was the last one to have used the vehicle. R. 234:6; App. 105. Officer Bourdelais, of the Green Bay Police Department ("GBPD") responded to the complaint. R. 234:4-5; App. 103-04. When Bourdelais ran the license plate, he discovered that the same vehicle had been involved in a hit and run and a vehicle fire the night before. R. 234:5-6, 8; App. 104-05, 107. Bourdelais questioned Burch about the vehicle, and Burch told Bourdelais that when he returned home with the car, he must have left it unlocked with the keys inside because he could not find the keys. R. 234:7; App. 106. Burch denied being involved in the theft, hit and run, or vehicle fire. R. 234:8; App. 107. Bourdelais then learned

that Burch's friend, Jordan Schuyler, lived in the area of the vehicle incident, and asked Burch if he had gone to her house that night. R. 234:9; App. 108. Burch denied going to her home, explaining that he and Schuyler were texting back and forth that night, but at some point she stopped responding, so he just went home. *Id.*

Bourdelais asked Burch "if I could see the text messages between him and Jordan, if my lieutenant and I could take a look at his messages." R. 234:10; App. 109. Burch consented. *Id.* Bourdelais testified that he prefers to download the information from the phone, rather than take a bunch of screen shots of the text messages, so Bourdelais 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." R. 234:10-11; App. 109-10. When Bourdelais asked about "downloading the information[,]" Burch did not limit the information to the text messages; however, Bourdelais made clear that his request to Burch was limited to "hey, do you mind if we take a look at those text messages . . . ." R:234:11; App. 110.

Although the request and consent of Burch was expressly limited to "text messages," Bourdelais admitted that he actually wanted to look at any information to corroborate Burch's statement that he never went to Schuyler's house or made arrangements to do so (*Id.*), including "phone calls, text messages, app messages, Facebook Messenger, photographs, anything." R. 234:14; App. 113. Bourdelais' unilateral expansion of the search beyond Burch's consent was unconstitutional. *United States v. Dichiarinte*, 445 F.2d 126, 129 (7th Cir. 1971)("Government agents may not obtain consent to search on the representation that they intend to look only

for certain specified items and subsequently use that consent as a license to conduct a general exploratory search.") Burch then signed a consent form giving "Det. Danielski, Officer Bourdelais or any assisting personnel permission to search my . . . Samsung Cellphone." R. 234: 12; App. 111; R. 78; App. 114.

Bourdelais further unilaterally expanded the scope of consent when he turned the phone over to Detective Danelski, a computer analyst with the GBPD, and asked her to "extract the phone for *all data*, he wanted all data after the time of June 7th after 9:30 p.m." R. 234:42 (emphasis added). Burch recognizes that the law sometimes tolerates the "overseizure" of electronic data as an administrative convenience, given the difficulties in isolating relevant digital data. *See, e.g., People v. Thompson*, 51 Misc.3d 693, 28 N.Y.S.3d 237, 254, 257-58 (Sup. Ct. N.Y. County 2016). However, Danelski did not face those difficulties, as she testified that she had the capability to download just text messages. R. 234:50. In addition, once Danelski extracted the data, she converted it to a readable format, tabbed by categories such as text messages, applications, images, internet history, etc. *Id.* at 47-49. Thus, even if it was administratively necessary to extract the entire phone, police could have limited their review to the category to which Burch consented: his text messages. *See id.*

In denying the motion to suppress, the circuit court concluded that Burch's consent was not limited in any way. R. 101:9; App. 123. At the motion hearing, there was no dispute of fact as to what Bourdelais asked of Burch and to what Burch agreed. *See* R: 234:10-12; App. 109-11. The circuit court took those facts and analyzed whether a reasonable person would view those facts as creating limited consent. R. 101:6-7; App. 120-21. Given that the

court was not tasked with resolving credibility and instead applied a reasonableness analysis, Burch submits that this Court should review the court's conclusion under the de novo standard. *State v. Kolp*, 2002 WI App 17, ¶ 5, 250 Wis. 2d 296, 640 N.W.2d 551 ("Whether the facts satisfy the constitutional requirement of reasonableness is a question of law, which this court reviews *de novo*.") In any event, the court's analysis is incorrect under either a de novo or clearly erroneous standard.

The court concluded that initially, the scope of Burch's consent was limited to only the text messages between Burch and Schuyler, but that Bourdelais broadened the scope when he started "using the blanket term 'information.'" R. 101:5-6; App. 119-120. In so concluding, the court omitted one critical word from the testimony: "the." Bourdelais asked if he could "download *the* information off the phone . . . ." R:234:10; App. 109 (emphasis added). The definite article "the" indicates that the noun following "is definite or has been previously specified by context or by circumstance[.]" Merriam Webster's Collegiate Dictionary 1294 (11th ed. 2003); *see also State v. Arberry*, 2018 WI 7, ¶ 19, 379 Wis. 2d 254, 905 N.W.2d 832 ("the" refers to something specific and unique). Thus, Bourdelais' request to download "the information" referenced the specific information to which Burch consented: the text messages. *See id.*; R. 234:10; App. 109. Nothing in the words Bourdelais used indicated that he expressly broadened his request to include information beyond the text messages.

The court also considered the fact that neither Bourdelais nor Burch specifically limited the information to text messages when they discussed downloading the information from Burch's phone. R. 101:5-6; App. 119-120. However, a failure to limit does not equate to expanding

the scope of consent that has already been limited. *United States v. Cotton*, 722 F.3d 271, 277 (5th Cir. 2013). As the court concluded, Burch's consent was limited to just text messages at the outset. R. 101:5; App. 119.

Finally, the court relied on the written consent form, noting that it did not contain any parameters. R. 101:6-7; App. 120-21. However, a general consent form is of little help in determining scope and can be overridden by more explicit statements. *United States v. Lemmons*, 282 F.3d 920, 924 (7th Cir. 2002). The court's conclusion that a reasonable person would have understood that Burch consented to police searching his entire phone is wrong.

D. The GBPD Unlawfully Retained Burch's Entire Phone Extraction

Even if it was reasonable for police to download Burch's entire phone, it was unreasonable to retain the entire phone extraction. *See Thompson*, 28 N.Y.S.3d at 257-58. While 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. *See id.* Instead, police must expunge or return the non-relevant data. *See id.*

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. Burch recognizes that the value of *Ganias I* is somewhat diminished, given that 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. The court, however, did not withdraw the language from *Ganias I* on the Fourth Amendment question, and this Court should look to the sound reasoning of *Ganias I* as persuasive authority.

In this case, after Danelski extracted the phone, she generated a report with the specific data and timeframe Bourdelais requested. R:234:42-43. Bourdelais reviewed the report with the relevant information and found no evidence connecting Burch to the vehicle incident, so he closed out the case. *Id.* at 27-28, 34. Under general Fourth Amendment principles applicable to tangible items, police would need to return items that contain no evidentiary value. *See*, *e.g.*, *United States v. Tamura*, 694 F.2d 591, 596-97 (9th Cir. 1982). There is no reason that the advancement of technology, allowing law enforcement perpetual access to these items, should except digital information from these principles. Given that the report contained no evidence of a crime, the GBPD arguably was required to return or destroy the report. *See id.*

More importantly, the GBPD's retention of the entire extraction, after it had isolated the responsive information, violated the Fourth Amendment. *Ganias I*, 755 F.3d at 137-38. But even if the GBPD lawfully retained Burch's entire phone extraction, law enforcement's access to the extraction did not give it lawful authority to search.

E. The BCSO's Review of the Phone Extraction in August 2016 Constituted a Search

A search involves the rummaging, prying, and exploratory investigating into one's private effects. *Warden v. Hayden*, 387 U.S. 294, 320 (1967)(internal quotations omitted)("the real evil aimed at by the Fourth Amendment is the search itself, that invasion of a man's privacy which consists in rummaging about among his effects to secure evidence against him."); *Edwards v. State*, 38 Wis. 2d 332, 338, 156 N.W.2d 397 (1968)(internal quotations omitted)("A search implies a prying into hidden places for that which is concealed."); *State v. Dombrowski*,

44 Wis. 2d 486, 495, 171 N.W.2d 349 (1969)(internal quotations omitted)("The term search implies exploratory investigation or quest.") While observing an item in plain sight generally does not constitute a search, moving an item, even by mere inches, is a search. *Arizona v. Hicks,* 480 U.S. 321, 324-25 (1987). For Fourth Amendment purposes, the label "search" turns on whether police violate one's reasonable expectation of privacy. *State v. Brereton*, 2013 WI 17, ¶ 23, 345 Wis. 2d 563, 826 N.W.2d 369.

As a starting point, *Riley* makes clear that Burch has a reasonable expectation of privacy in the contents of his cell phone. 573 U.S. at 393-97. While Burch arguably had a reduced expectation of privacy in the information contained in the report reviewed by Bourdelais, nothing reduced his expectation of privacy in the other areas of his phone not exposed to police eyes. When the BCSO reviewed the phone extraction in August 2016, they rummaged through it "looking for anything in the timeframe of the night of the 20th into the morning hours of the 21st, whether it be calls, texts, internet history, any kind of location data available from that device[]" connecting Burch to the homicide. R. 251:66. This exploratory rummaging and prying into his phone extraction constituted a search. *See Hayden*, 387 U.S. at 320; *Edwards*, 38 Wis. 2d at 338; *Dombrowski*, 44 Wis. 2d at 495.

F. The BCSO had no Lawful Authority to Conduct the Second Search in August 2016

As discussed above, the seizure of Burch's entire phone download was beyond the scope of his consent, and the retention of the entire extract violated the Fourth Amendment. Even if this Court disagrees, the BCSO had no authority to conduct a second search of these files.

Unlike in *Ganias*, in August 2016, the BCSO did not seek or obtain a warrant to search Burch's phone extraction for evidence connecting him to a homicide. 824 F.3d at 207, 225-26; R: 234:56. In addition, the authority to conduct a consent search in June 2016 had been exhausted by August 2016. The lawful authority to search is generally limited to a single search. *See State v. Avery*, 2011 WI App 124, ¶ 18, 337 Wis. 2d 351, 804 N.W.2d 216 (overruled on other grounds); *State v. Douglas*, 123 Wis. 2d 13, 21-22, 365 N.W. 2d 580 (1985). In the warrant context, the general quip "one warrant, one search" applies, unless the subsequent intrusion is a continuation of the initial intrusion. *Avery*, 337 Wis. 2d 351, ¶ 18.

For example, in *Avery*, police reentered the defendant's home multiple times over the course of four days following the issuance of the warrant, and this Court concluded that the reentries did not require a separate warrant because they were part of one continuing search. *Id.*, ¶¶ 11, 27. Similarly, in the consent context, "such authorization is not perpetual[,]" and consent does not permit a subsequent investigative intrusion unless it is a continuation of the initial intrusion. *Douglas*, 123 Wis. 2d at 21-24.

Here, there can be no argument that the August search of the extraction for evidence of a homicide was a continuation of the June search for evidence of a hit and run. 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. So too, in this case, Burch's consent in June to look for evidence of a traffic crime did not continue in perpetuity.

In addition, the "second look" doctrine does not apply. In *State v. Betterley*, the court held that police can take a second look at evidence seized pursuant to an inventory search. 191 Wis. 2d 406, 417-18, 529 N.W.2d 216 (1995). There, the defendant was suspected of falsely reporting a ring as stolen to defraud his insurer. *Id.* at 412. The defendant was then taken into custody on a probation hold for an unrelated violation, and police conducted a customary inventory search of the items on his person. *Id.* at 414-15. In doing so, police found a ring in the defendant's pocket, which they removed and placed in a jail property box. *Id.* at 415. Later that day, the insurance fraud investigator learned that a ring was in the jail property, and he took it as evidence. *Id.* at 415. The ring was subsequently identified as the ring reported as stolen. *Id.* The court held that the prior lawful exposure to the ring diminished the defendant's expectation of privacy in the item such that a second look was reasonable. *Id.* at 418.

The rule announced in *Betterley* was limited to "the effects of a person lawfully in custody" seized as part of an inventory search. *Id.* at 417. This distinction is important because of the limited scope of an inventory search. *Florida v. Wells*, 495 U.S. 1, 4 (1990). Given that inventory searches are not predicated on probable cause (*State v. Weber*, 163 Wis. 2d 116, 132, 471 N.W.2d 187 (1991)), in executing such a search, police cannot conduct a general rummaging to discover evidence of a crime; instead, the scope of an inventory search is limited to just that: producing an inventory. *Wells*, 495 U.S. at 4. In other words, examining an item on its face for the purpose of identifying and inventorying. *See id.*[4] In *Betterley*, police

[4] *Wells* did note that the opening of closed containers is permissible, if the contents are not apparent from its exterior. *Id.*

"did no more than look at the ring." *Betterley*, 191 Wis. 2d at 418. When the BCSO conducted the second search, it did much more than look at something already exposed in plain sight; the BCSO rummaged, pried, and explored into places not previously exposed to police eyes. R. 251:66.

Also, there are heightened privacy concerns at issue with a cell phone, containing "the privacies of life[,]" as opposed to a ring, whose contents are facially apparent. *Riley*, 573 U.S. at 403 (quoting *Boyd*, 116 U.S. at 630). Even if Burch had a reduced expectation of privacy in the text messages police already viewed on his phone, there is no indication that the GBPD viewed his web history or Gmail account information in the first search. *See* R. 234:47. Just as a search of one's front hall would not diminish his expectation of privacy in his bedroom, so too, a review of Burch's text messages from June 7 did not reduce his expectation of privacy in the other areas of his phone.

The circuit court concluded that the BCSO's review of the extraction was a "second look." R. 101:10; App. 124. The court relied on the statement in *Betterley* that "the extent of the second look is defined by what 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.* (quoting *Betterley*, 191 Wis. 2d at 418). Because the court concluded that Burch did not place any limitations on the first search, it reasoned that law enforcement's second review of the extraction was likewise limitless. *Id.* But, again *Betterley* was limited to inventory searches; indeed, in making this statement the court relied on language from *Edwards* that a search is "permissible if 'the police did no more . . . than they were entitled to do *incident to the usual custodial arrest and incarceration*.'" *Betterley*, 191 Wis. 2d at 418 (quoting *United States v. Edwards*, 415 U.S. 800, 805

(1974)(emphasis added)). As discussed above, inventory searches are limited in scope, and this Court should not extend the second look doctrine to apply where police rummage through new areas not previously exposed in plain sight, particularly into areas in which one has a heightened privacy interest.

In this case, police downloaded about a dozen cell phones from various individuals, most of whom were just witnesses. *See* R. 251:37. Under the circuit court's reasoning, these entire extractions are now fodder for police. If this decision is upheld, police can create a database of all cell phone extractions ever obtained, readily share them with any government agency, and indefinitely search these extractions for any purpose under the guise of taking a "second look."

G. The Inevitable Discovery Doctrine does not Apply

In *Nix*, the Supreme Court adopted the inevitable discovery doctrine as an exception to the exclusionary rule. *Nix v. Williams,* 467 U.S. 431 (1984). The doctrine applies "[i]f the prosecution can establish by a preponderance of the evidence that the information ultimately or inevitably would have been discovered by lawful means . . . ." *Id.* at 444. This doctrine is a "narrow exception to the exclusionary rule" (*State v. Jackson*, 2016 WI 56, ¶ 72, 369 Wis. 2d 673, 882 N.W.2d 422) that must be applied "with restraint and circumspection[.]" *State v. Kennedy*, 134 Wis. 2d 308, 318, 396 N.W.2d 765 (1986).

In evaluating whether the doctrine applies, important indicia of inevitability includes the following factors: (1) whether there is a reasonable probability that the evidence in question would have been discovered by lawful means absent police misconduct; (2) whether the

leads making discovery inevitable were possessed by the government at the time of the misconduct; and 3) whether the government was actively pursuing some alternate line of investigation prior to the unlawful search. *Jackson*, 369 Wis. 2d 673, ¶¶ 60, 66.

The circuit court concluded that the inevitable discovery applied for two reasons: 1) even without the evidence discovered from the phone, "the BCSO still had more than enough evidence to obtain a warrant for a new DNA sample from Burch, which would have led to his arrest, and the subsequent confiscation of his phone[,]" and 2) "the phone on Burch's person at the time of his arrest was searched incident to arrest and revealed the same email address." R. 101:13-14; App. 127-28.

As to the first point, the court's attenuated analysis is based on conjecture. *Jackson*, 369 Wis. 2d 673, ¶ 72 ("Proof of inevitable discovery turns upon demonstrated historical facts, not conjecture.") The court first assumes that a warrant for Burch's DNA would have been issued, relying on the fact that "the BCSO already had matched multiple DNA samples taken from VanderHeyden's body, clothes, and the murder weapon to Burch's DNA from a database in Virginia." R. 101:13; App. 127. This finding is clearly erroneous.

Around August 17, 2016, the BCSO conducted the second search of the phone extraction, after learning that the lab had a database hit linking Burch to the investigation. R. 8:5, ¶¶ 5(d)-(f); R. 101:12; App. 126. At this time, the only link connecting Burch was the useable DNA profile developed from the sock, which prompted the database hit. R. 151. The link connecting Burch to the victim's body, clothing, and the cord was not developed until September 12, 2016, after the lab compared those

items against the buccal swab obtained from Burch. R. 152. In addition, the database hit provided only an "investigative lead"; it was not a definitive conclusion. R. 246:194. Also, the court assumes that police could have located Burch, served the DNA warrant upon him, and secured the DNA sample. Finally, the court speculates that in the five days it took to analyze the sample, Burch would have been located again for arrest and Burch's cell phone would have been on his person. *See* R. 8:8, ¶¶ 8-9.[5]

As to the court's second reason, that police found the Google email account when they searched Burch's phone incident to his arrest, police searched the phone without lawful authority. R. 101:14; App. 128; *Riley*, 573 U.S. at 401 (a warrant is generally required to search a cell phone, even when seized incident to arrest). To satisfy this exception to the exclusionary rule, the State must show that the evidence "inevitably would have been discovered by *lawful* means[.]" *Nix*, 467 U.S. at 444 (emphasis added).[6] The fact that police discovered the information during a subsequent unlawful search does not legitimize the first unlawful search.

Finally, an important indicator of inevitability includes that the leads of inevitability were possessed at the time of the misconduct. *Jackson*, 369 Wis. 2d 673, ¶¶ 60, 66. Here, the court relied on facts that were, or could have been, discovered later in time, that is, after Burch's arrest. R. 101:13-14; App. 127-28.

[5] The DNA warrant was executed on September 7, and the lab report was dated September 12.

[6] Although the State argued this point under the inevitable discovery doctrine, the issue appears to fit more squarely within the independent source doctrine, a closely related but distinct principle, which applies when police *did* discover the evidence. *State v. Quigley*, 2016 WI App 53, ¶ 51, 370 Wis. 2d 702, 883 N.W.2d 139. However, this distinction is of no consequence, as both doctrines require that the evidence was or inevitably would have been discovered by *lawful* means. *Id.*; *Nix*, 467 U.S. at 444.

H. This Court Should not Conduct a Good Faith Analysis

Before the circuit court, neither party raised good faith. R: 101:14-15; App. 128-29. While the court did not specifically find that law enforcement acted in good faith, it noted that "[g]iven the contents of the consent form, it was reasonable for an officer in Detective Loppnow's position to proceed as he did." R: 101:15; App. 129. Because this issue was not raised before the motion hearing, the State did not develop testimony on this point, and Burch did not have an opportunity to cross-examine the officers on any good faith reliance. This Court should therefore invoke the forfeiture rule if the State argues the good faith exception. *See State v. Ndina*, 2009 WI 21, ¶ 30, 315 Wis. 2d 653, 761 N.W.2d 612 (the forfeiture rule gives parties notice and a fair opportunity to address an issue at the trial level).

In any event, the good faith exception to the exclusionary rule generally applies "when a law enforcement officer has reasonably and objectively relied on settled law (whether statute or binding judicial precedent) that was subsequently overruled or a warrant that was subsequently invalidated." *State v. Blackman*, 2017 WI 77, ¶ 70, 377 Wis. 2d 339, 898 N.W.2d 774. The exception does not apply when the court has not spoken on the issue. *State v. Dearborn*, 2010 WI 84, ¶ 46, 327 Wis. 2d 252, 786 N.W.2d 97. Burch is not aware of any case, and the State neither cited nor elicited testimony to any case, that authorizes law enforcement's conduct in this case. Accordingly, good faith has no place here.

Burch's Fourth Amendment rights were violated when police extracted his entire phone, when police retained the entire extraction, and when police conducted a new search of his phone extraction. Burch asks this Court

to reverse the circuit court decision denying his motion to suppress and remand for a new trial.

II. THE CIRCUIT COURT ERRONEOUSLY ADMITTED THE FITBIT EVIDENCE WITHOUT AN EXPERT WITNESS TO ESTABLISH THE RELIABILITY OF THE SCIENCE UNDERLYING THE FITBIT TECHNOLOGY AND WITHOUT A WITNESS FROM FITBIT TO AUTHENTICATE THE EVIDENCE. IN ADDITION, THE COURT'S ERROR IS ONE OF A CONSTITUTIONAL MAGNITUDE.

At trial, the State presented evidence purportedly generated by Detrie's Fitbit that during the time of the murder, Detrie took only about twelve steps and thus could not be the culprit. R. 251:57-58; App. 131-32; R. 53:3. In effect, the Fitbit evidence was Detrie's alibi witness, or as the television program covering the case coined it, the Fitbit was "The Silent Witness."[7] The State presented records obtained from Fitbit Inc., and an accompanying certification, through Sergeant Loppnow under the self-authenticating records statute. R. 251:12-14; R. 70:17; App. 152. The State then called BCSO computer analyst Tyler Behling, who created graphs based on information contained in the records, to establish that Detrie took about twelve steps during the time of the murder. R. 251:52-53, 57-58; App. 131-32. While Behling testified that he understood the "basics" of how a Fitbit works, he was unaware of facts critical to the reliability of this evidence, such as how the device sends information to the "app," how the Fitbit corporation stores its data, the error rate, whether the device can register steps if it is not worn, and whether users can edit or manipulate the data. R. 251:98-100; App. 133-35.

[7] *Dateline: Silent Witness* (NBC television broadcast May 11, 2018)(previously available at https://www.nbc.com/dateline/video/silent-witness/3718679).

This is the first case to address the standard for admitting evidence from a Fitbit against an accused at trial. Based on prior precedent and the limited information we know about the workings of a Fitbit, an expert was required to establish that the science underlying the Fitbit technology is sound. In addition, a witness from the Fitbit corporation was required to authenticate this evidence. Finally, the admission of this evidence without a witness from Fitbit implicated Burch's right to Confrontation.

A. Standard of Review

This Court reviews the circuit court's evidentiary rulings under the erroneous exercise of discretion standard. *State v. Kandutsch*, 2011 WI 78, ¶ 23, 336 Wis. 2d 478, 799 N.W.2d 865. However, when the admission of evidence implicates a defendant's right to Confrontation, this Court conducts a de novo review. *State v. Zamzow*, 2017 WI 29, ¶ 10, 374 Wis. 2d 220, 892 N.W.2d 637.

B. Expert Testimony was Required to Establish the Reliability of the Science Underlying the Fitbit Technology

Expert testimony is necessary "when interpreting the evidence involves special knowledge, skill or experience that is not within an ordinary person's realm of experience or knowledge." *State v. Doerr*, 229 Wis. 2d 616, 623, 599 N.W.2d 987 (Ct. App. 1999); *see also Kandutsch*, 336 Wis. 2d 478, ¶¶ 28-29. For example, in *Doerr*, this Court concluded that the science of a preliminary breath test (PBT) device is outside the knowledge of an ordinary person and thus expert testimony is required. 229 Wis. 2d at 624.

Conversely, in *Kandutsch*, the court concluded that Electronic Monitoring Device ("EMD") technology is within the comprehension of the average juror, given that it involves the well-known and easily understood technology of radio signals and telephone connections. 336 Wis. 2d 478, ¶¶ 37-38. Similarly, in *Hanson*, the court held that expert testimony is not required to establish the initial admissibility of speed radar detection that employs "the Doppler effect" science. *State v. Hanson*, 85 Wis. 2d 233, 244-45, 270 N.W.2d 212 (1978). The court explained that the principles underlying the Doppler effect have been widely accepted as sound science by courts. *Id.* at 237-39. Because the science at issue there had been widely accepted and was considered unassailable, the court held that the proponent need establish only that the particular device was accurate and reliable through an officer trained in its use. *Id.* at 244-25; *Kandutsch*, 336 Wis. 2d 478, ¶ 44.

This is the first case, in any jurisdiction, to address the reliability and accuracy of the science underlying Fitbit devices for admission in court. Thus, unlike *Kandutsch* and *Hanson*, this case does not implicate science that has been widely accepted and deemed unassailable. *Kandutsch*, 336 Wis. 2d 478, ¶¶ 38-40; *Hanson*, 85 Wis. 2d at 238. Although the State presented no testimony explaining the science underlying Fitbit technology, Burch submitted an offer of proof as to the device's complexity. R. 63.

The Fitbit Flex is an "Internet of Things" device that extends far beyond one's wrist. R. 63:2. The physical device itself involves a three-axis accelerometer that generates data representing the user's movements. *Id.* at 1. The device then processes that data into a meaningful output: an estimate of one's step count, distance, and

activity. *Id.* The device itself "is just one node resting on top of communications, analytics, policy, and even behavioral infrastructure." *Id.* at 2. The device then exchanges that data with a smartphone or computer using a USB, WIFI, or Bluetooth connection. *Id.* at 3. Fitbit "employs teams of engineers, scientists, and analysts to monitor, interpret, validate, and improve the analytics generated from the sensors in their devices." *Id.* at 4.

Indeed, as the defense established, the reliability and accuracy of Fitbit technology has been questioned in numerous civil lawsuits. R. 64:2-3. Also telling is the fact that the State was unable to secure a witness from Fitbit to verify the unassailability of its science. R. 233:68-69. The defense first raised concern that Fitbit's own internal validation studies might undermine the reliability of its science, and the defense asked to see those studies. R. 231:7-8. The State noted that this information may be protected by trade-secrets, but ultimately acknowledged that it needed to have someone from Fitbit verify reliability. *Id.* at 8-9. The State then changed course, arguing that although it would prefer to have a witness from Fitbit testify at trial, it was not required to do so. R. 233:68-69.

In short, this is the first case to address the admissibility of Fitbit evidence in court, much less using a Fitbit device as an alibi witness in a murder case. The accuracy and reliability of this complex science must be established before this technology is judicially accepted without expert testimony. *See Kandutsch*, 336 Wis. 2d 478, ¶¶ 38-40; *Hanson*, 85 Wis. 2d at 238, 240.

C. The State Failed to Properly Authenticate the Fitbit Evidence

Even when an expert is not required, the proponent must still properly authenticate the evidence by showing that the evidence is what the proponent claims. *Kandutsch*, 336 Wis. 2d 478, ¶ 41 (citing to Wis. Stat. § 909.01). When the evidence involves a process or system that produces a result, this evidence may be authenticated by a "showing that the process or system produces an accurate result." *Id.* (quoting Wis. Stat. § 909.015(9)).

In *Kandutsch*, the State presented considerable evidence to establish the accuracy and reliability of the EMD evidence. 336 Wis. 2d 478, ¶¶ 13-16. First, Kandutsch's probation agent described the electronic monitoring system itself, explaining that it consists of a home monitoring unit and a radio frequency device attached to one's ankle. *Id.*, ¶ 13. The agent explained the range limitations of the device and described that the system connects to the monitoring center by telephone. *Id.* The agent further described how the system is installed and what safeguards are in place to ensure it is working properly. *Id.*, ¶ 14. The agent's supervisor, having used the system for twenty years, testified that he has never heard of a faulty unit and that the same device was reissued to another individual. *Id.*, ¶ 16. In short, the State established how the device works, how the information is transmitted, and why the jury could trust that it was accurate. *Id.*, ¶¶ 13-16.

In this case, the State entered the evidence from Fitbit Inc. and Fitbit's certification of the records through Sergeant Loppnow, who testified that he obtained the records pursuant to a search warrant and provided them to Behling. R. 251:12-14. The court had previously held that

this evidence was admissible as self-authenticating records of regularly conducted activity. R. 70:17; App. 152. Behling created graphs based on the information in the Fitbit records, which showed that Detrie took approximately twelve steps between 3:08 a.m. and 6:09 a.m. R. 251:52-53, 57-58; App. 131-32. While this testimony and the exhibits may have been sufficient to authenticate the Fitbit business records themselves, it did nothing to authenticate the information *within those records*. That is, 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.

The jury heard zero testimony as to the science behind the Fitbit technology, much less any testimony to establish that this science is sound. Indeed, Behling, the witness used to authenticate the data, wholly lacked an understanding of the Fitbit technology, as highlighted by the following testimony:

Q: How familiar are you with fitbit devices?

A: I'm aware of what they are and what they do on a high level.

Q: At a what?

A: A high level.

Q: What does that mean?

A: Meaning I understand the basics of how they work.

Q: Can you tell us more specifically how they work, like the mechanisms within them or how they communicate with the app?

A: They communicate with the app via Bluetooth connection.

Q: And can you tell us how they send that data information from one to the other?

A: I cannot.

Q: Can you tell us the complexities of the data in terms of how it's recovered or how it is stored?

A: I guess I don't understand the question.

…

Q: Do you know are [Fitbit Flex devices] waterproof?

A: I do not know that.

Q: Do you know how fitbit stores their data?

A: Are you asking how it's stored locally on the fitbit device or on the phone?

Q: No. Fitbit themselves.

A: I do not.

Q: Do you know how users can manipulate fitbit data?

A: I do not.

Q: So you don't know if you can edit the fitbit data?

A: I do not know that.

Q: What happens when you are not wearing a fitbit device, is that going to register steps?

A: I do not know.

Q: Can you provide us the error rate of a fitbit?

A: I cannot.

Q: Are you aware of fitbit communities dedicated to troubleshooting and fixing errors within fitbits?

A: I am not.

> Q: Are you aware of how many fitbit app updates there has been?
>
> A: I do not know that.
>
> Q: So if I were to have to update a fitbit or if somebody had to, and it says for a bug fix, can you describe to us what that means?
>
> A: A bug in terms of software?
>
> Q: It would just say b-u-g fix. Can you describe what that is or what that means?
>
> A: It would be hard for me to speculate exactly what they are fixing in their update.

R. 251:98-100; App. 133-35.

In addition, as part of authentication, the State must establish chain of custody. *State v. McCoy*, 2007 WI App 15, ¶ 9, 298 Wis. 2d 523, 728 N.W.2d 54. While a perfect chain is not required, the State must nonetheless establish that it is improbable that the original was exchanged, contaminated, or tampered with. *Id.* Behling did not even know whether one could manipulate the data, much less show that it was not manipulated in this case. R. 251:99; App. 134. Also, we do not know how the data got from the Fitbit device, supposedly affixed to Detrie's wrist, to Fitbit's business records. This case does not involve just gaps in the chain of custody; there is an entire black hole, in which we have no idea if the data was exchanged, contaminated, or tampered with.

After Behling's testimony at trial, Burch renewed his objection that the State failed to properly authenticate the Fitbit evidence, based primarily on Behling's lack of knowledge as to whether the data was edited. R. 251:102. The State responded that had the Fitbit data been edited, the records would have noted such. *Id.* at 103. But how do

we know that? To authenticate and establish a proper chain of custody, the State needed a witness from Fitbit to testify to these facts. *See McCoy*, 298 Wis. 2d 523, ¶ 9.

Finally, the Fitbit evidence left several questions unanswered in this case. For example, the data showed Detrie's device connecting to different Internet Provider addresses in the early hours of May 21. R. 52:10-11. Notably missing is any connection at the critical time period in this case: between 2:57 a.m. and 4:50 a.m. *Id.* Did this mean that the device was turned off? Did someone delete or edit this data? There was no witness to whom to ask these critical testing questions.

D. The Circuit Court Erred in Allowing the Fitbit Evidence without an Expert and without a Witness from Fitbit

The circuit court concluded that the State could present the step-count data from Fitbit without an expert, likening the Fitbit technology to a watch or a speedometer, for which the court explained the general public accepts as reliable without knowing exactly how they work. R. 70:9; App. 144. However, there are two critical distinctions. First, watches have been around for centuries and speedometers for decades. Case law teaches us that with time, technology and the underlying science becomes generally accepted as sound. *See Kandutsch*, 336 Wis. 2d 478, ¶¶ 38-40; *Hanson*, 85 Wis. 2d at 238-40.[8] This case is the first time the admissibility of Fitbit evidence, and the underlying science, has been judicially tested.

[8] Case law has also deemed technology unreliable, as is the case with polygraph devices. *See Lhost v. State*, 85 Wis. 2d 620, 644-45, 271 N.W.2d 121 (1978).

Second, the science here is grounded in the Internet of Things, which is much more complex than someone just looking at the time or speed on a device and testifying to what the reading showed. R. 63:1. Here, the Fitbit was the witness, telling the jury that Detrie took only about twelve steps during the critical time frame, but we do not know how the device calculated that information, how the data got from the device itself to Fitbit's business records, and what happened in between. R. 251:7, 98-100; R. 141, Exh. 166.

As to authentication, the court ruled that the data was self-authenticating under Wis. Stat. § 909.02(12). R. 70:17; App. 152. While Fitbit's business records may have been self-authenticating, the court's decision failed to account for the second and more critical layer: the data contained therein.

As to reliability, the court appeared to take judicial notice that "[t]he step-counting data collected by Fitbit devices has been studied and proved to be accurate and reliable by medical professionals." R. 70:18; App. 153. For support, the court cited to the State's brief, which referenced two medical journal articles. *Id.* (citing to R. 53:4-5). This decision is flawed for several reasons. First, two small studies concluding that Fitbits accurately track activity does not establish the reliability of the technology in a court of law. Second, even if the activity-tracking function of the Fitbit is deemed reliable as a matter of law, this does not address the Internet of Things aspect of the Fitbit and establish that the data from the device was accurately and reliably transmitted to Fitbit Inc. without manipulation.

Further, the court relied on the State's representation that it would establish the device's

reliability by presenting the following video evidence corroborating the Fitbit data: 1) Detrie walking around outside a bar and 2) Detrie being questioned by police. R. 70:19; App. 154. At trial, however, the State chose not to present the video from the bar and showed only the nine-minute segment of Detrie being interviewed, the majority of which Detrie was either seated or out of the room. R. 251:62-63; R. 114, exh. 167. This evidence was a far cry from the twenty-year history testified to in *Kandutsch.* 336 Wis. 2d 478, ¶ 16.

Finally, the court concluded that there were no Confrontation implications with admitting the Fitbit evidence without an expert or a witness from Fitbit, explaining that this evidence is considered a business record and that business records are not testimonial statements for Sixth Amendment purposes. R. 70:20-21; App. 155-56. However, as explained above, this decision failed to account for the second and more critical layer: the data contained within those records. As discussed below, the court not only erred, but that error was one of a constitutional magnitude.

E. The Admission of the Fitbit Evidence without an Expert and without a Witness from Fitbit Implicated Burch's Right to Confrontation

In *Crawford,* the Supreme Court stated, "the [Confrontation] Clause's ultimate goal is to ensure reliability of evidence, but it is a procedural rather than a substantive guarantee. It commands, not that evidence be reliable, but that reliability be assessed in a particular manner. . . ." *Crawford v. Washington*, 541 U.S. 36, 61 (2004). Burch acknowledges that the Clause has traditionally been held to apply to only human witnesses and not to the statements of machines. *See*, *e.g.*, *United*

States v. Lamons, 532 F.3d 1251, 1263 (11th Cir. 2008); *United States v. Washington*, 498 F.3d 225, 230-31 (4th Cir. 2007).

With rapidly evolving technology, the time has come for the Confrontation Clause to evolve. *See* BRIAN SITES, *Rise of the Machines: Machine-Generated Data and the Confrontation Clause*, 16 Colum. Sci. & Tech. L. Rev. 36, 99 (2014). Burch submits that when machines act as witnesses, the Framers would have intended that the Sixth Amendment provide a mechanism to confront the science underlying the machine's operation, given that the ultimate goal of the Clause is to ensure that reliability can be assessed in a particular manner. *See Crawford*, 541 U.S. at 61; *see also* ANDREA ROTH, *Machine Testimony*, 126 Yale L.J. 2042 (2017).[9] In this case, that mechanism would have been the ability to cross-examine an expert on the reliability of the Fitbit technology and to confront a witness from Fitbit on whether the data in Fitbit's business records arrived there in a manner that was accurate, reliable, and free from manipulation.

While it is true that machines cannot lie, forget, or misunderstand (*Kandutsch*, 336 Wis. 2d 478, ¶ 61), machines can utter falsehoods by design. ROTH, 126 Yale L.J. at 1990-96. Take for example the fatal crash involving the self-driving car Tesla, which Tesla believes may have occurred because the car discounted the imminent crash as part of a design flaw to avoid false breaking. *Id.* at 1995. Now that machines can think, act, and speak for us, ensuring that machine testimony is reliable rises to the level of a constitutional issue. Even in *Kandutsch*, the scent of Confrontation concerns was diffused. 336 Wis. 2d

[9] "The State's use of accusatory machine conveyances to prove a defendant's guilt seems to implicate many of the same dignitary and accuracy concerns underlying the framers' preoccupation with in-the-shadows accusations and ex parte affidavits."

478, ¶ 82 n 7 (Abrahamson, J., joined by A.W. Bradley, J., dissenting).

Burch submits that the circuit court not only erred in admitting the Fitbit evidence without an expert to testify to the reliability of the science underlying the technology and without a witness from Fitbit to authenticate the evidence, but also that this error was one of a constitutional magnitude.

CONCLUSION

Burch requests that this Court reverse the decisions of the circuit court and remand for a new trial.

Dated this 2nd day of December, 2019

Signed:

_____

Ana L. Babcock
State Bar. No. 1063719
Attorney for Defendant-Appellant

CERTIFICATION AS TO FORM/LENGTH

I certify that this brief meets the form and length requirements of Rule 809.19(8)(b) and (c) in that it is: proportional serif font, minimum printing resolution of 200 dots per inch, 13 point body text, 11 point for quotes and footnotes, leading of minimum 2 points and maximum of 60 characters per line of body text. The length of the brief is 10,684 words.

Dated this 2nd day of December, 2019

Signed:

_____

Ana L. Babcock
State Bar. No. 1063719
Attorney for Defendant-Appellant

CERTIFICATE OF COMPLIANCE
WITH RULE 809.19(12)

I hereby certify that:

I have submitted an electronic copy of this brief, excluding the appendix, if any, which complies with the requirements of §. 809.19(12). I further certify that:

This electronic brief is identical in content and format to the printed form of the brief filed on or after this date.

A copy of this certificate has been served with the paper copies of this brief filed with the court and served on all opposing parties.

Dated this 2nd day of December, 2019

Signed:

_____

Ana L. Babcock
State Bar. No. 1063719
Attorney for Defendant-Appellant

CERTIFICATE AS TO APPENDICES

I hereby certify that filed with this brief, either as a separate document or as part of this brief, is an appendix that complies with § 809.19(2)(a) and that contains: (1) a table of contents; (2) relevant trial court record entries; (3) the findings or opinion of the trial court; and (4) portions of the record essential to an understanding of the issues raised, including oral or written rulings or decisions showing the trial court's reasoning regarding those issues.

I further certify that if the record is required by law to be confidential, the portions of the record included in the appendix are reproduced using first names and last initials instead of full names of persons specifically including juveniles and parents of juveniles, with a notation that the portions of the record have been so reproduced to preserve confidentiality.

Dated this 2nd day of December, 2019

Signed:

_____

Ana L. Babcock
State Bar. No. 1063719
Attorney for Defendant-Appellant

APPENDIX

TABLE OF CONTENTS OF APPENDIX