

RECEIVED**11-15-2019**

STATE OF WISCONSIN
COURT OF APPEALS
DISTRICT III
CLERK OF COURT OF APPEALS
OF WISCONSIN

Case No. 2019AP826-CR

STATE OF WISCONSIN,

Plaintiff-Respondent,

v.

KEVIN M. JERECZEK,

Defendant-Appellant.

ON APPEAL FROM A JUDGMENT OF CONVICTION
ENTERED IN BROWN COUNTY CIRCUIT COURT, THE
HONORABLE JOHN P. ZAKOWSKI, PRESIDING

RESPONSE BRIEF OF PLAINTIFF-RESPONDENT

JOSHUA L. KAUL
Attorney General of Wisconsin

SARAH L. BURGUNDY
Assistant Attorney General
State Bar #1071646

Attorneys for Plaintiff-Respondent

Wisconsin Department of Justice
Post Office Box 7857
Madison, Wisconsin 53707-7857
(608) 261-8118
(608) 266-9594 (Fax)
burgundysl@doj.state.wi.us

TABLE OF CONTENTS

	Page
ISSUE PRESENTED.....	1
STATEMENT ON ORAL ARGUMENT AND PUBLICATION	1
INTRODUCTION	1
STATEMENT OF THE CASE	2
STANDARD OF REVIEW	5
ARGUMENT	5
The circuit court soundly denied Jereczek’s motion to suppress.....	5
A. Whether a search exceeds the scope of the consent given depends on its objective reasonableness.....	6
B. The circuit court’s findings were not clearly erroneous.....	7
C. Behling’s search was objectively reasonable and the items in the recycle bin were discoverable under the plain- view doctrine.	9
D. Jereczek’s other arguments lack support in the law and the record.....	13
CONCLUSION.....	16

TABLE OF AUTHORITIES

Cases

<i>Birchfield v. North Dakota</i> , 136 S. Ct. 2160 (2016)	6
<i>Florida v. Jimeno</i> , 500 U.S. 248 (1991)	6, 14

Page

<i>Schneckloth v. Bustamonte</i> , 412 U.S. 218 (1973)	6
<i>State v. Anker</i> , 2014 WI App 107, 357 Wis. 2d 565, 855 N.W.2d 483	13
<i>State v. Guy</i> , 172 Wis. 2d 862, 492 N.W.2d 311 (1992)	11
<i>State v. Jackson</i> , 2016 WI 56, 369 Wis. 2d 673, 882 N.W.2d 422	12, 13
<i>State v. Lonkoski</i> , 2013 WI 30, 346 Wis. 2d 523, 828 N.W.2d 552	5, 7
<i>State v. Lopez</i> , 207 Wis. 2d 413, 559 N.W.2d 264 (Ct. App. 1996)	13
<i>State v. Matejka</i> , 2001 WI 5, 241 Wis. 2d 52, 621 N.W.2d 891	6
<i>State v. Schroeder</i> , 2000 WI App 128, 237 Wis. 2d 575, 613 N.W.2d 911	7, <i>passim</i>
<i>United States v. Carey</i> , 172 F.3d 1268 (10th Cir. 1999)	12, 13
<i>United States v. Dichiarinte</i> , 445 F. 2d 126 (7th Cir. 1971)	7
<i>United States v. Gray</i> , 78 F. Supp. 2d 524 (E.D. Va. 1999)	11
<i>Vernonia Sch. Dist. 47J v. Acton</i> , 515 U.S. 646 (1995)	14
Other Authorities	
2 LaFave, Wayne R., <i>Search & Seizure</i> § 4.10(d) (5th ed. 2012)	14
4 LaFave, Wayne R., <i>Search & Seizure</i> § 8.1(c) (5th ed. 2012)	7

ISSUE PRESENTED

Did law enforcement exceed the scope of Kevin M. Jereczek's consent to search his son's user account on Jereczek's computer when it searched the recycle bin?

The circuit court said no.

This Court should affirm.

STATEMENT ON ORAL ARGUMENT AND PUBLICATION

Publication may be warranted. While this Court may affirm by applying settled law to the facts, the particular circumstance in this case—the scope of limited consent to search a particular user profile on multiuser computer—has not been addressed in Wisconsin law.

The State expects that oral argument will be unnecessary and that the parties' briefs will be sufficient to allow this Court to decide the issue presented.

INTRODUCTION

Police suspected that evidence of a crime would be found on Jereczek's computer. Specifically, Jereczek's son was accused of a crime that involved his sending explicit messages and pornography from a computer, and the police suspected that Jereczek's son used Jereczek's computer to send some of that material.

Jereczek consented to a search of data on the computer associated with his son's user profile. During that consent search, police identified child pornography in the computer's recycle bin that had been placed there by two different user profiles. Police then obtained a warrant, through which they seized evidence of scores of child pornography files, which Jereczek admitted he had viewed.

Jereczek claims that police exceeded the scope of his consent in the initial search by accessing the recycle bin. Contrary to Jereczek's contentions, police were authorized to search shared areas of the computer, including the recycle bin, where they discovered evidence of a new crime—Jereczek's possession of child pornography—under the plain-view doctrine. This Court should affirm.

STATEMENT OF THE CASE

In January 2015, the Ashwaubenon police were investigating Kevin Jereczek's teenage son for a crime that also allegedly involved the son's sending explicit messages and pornography to the victim. (R. 1:7.) Police suspected that some of the pornography and explicit messages associated with the son's alleged crime would be found on Jereczek's home computer. (R. 1:7.)

At law enforcement's request, Jereczek turned his computer over to police for forensic analysis and consented for it to search his son's user profile for evidence related to his son's alleged crime. (R. 1:7.) According to the criminal complaint, a preview analysis done by the Ashwaubenon police showed that the computer contained child pornography. (R. 1:7.)

The Ashwaubenon police turned the computer over to the Brown County Sheriff's Department, where analyst Tyler Behling—initially searching the computer based on Jereczek's consent and later a warrant—ultimately located images and videos featuring child pornography, 166 files in all. (R. 1:7; 16:2.) Most of those images were attached to Jereczek's user profile. (R. 16:1.)

Based on 11 of the images, the State charged Jereczek with 11 counts of possession of child pornography as a party to a crime. (R. 1:1–6.) Jereczek admitted that the images were his, but he claimed that he believed that the individuals

depicted in them were over 18 years old. (R. 1:7.) The criminal complaint described the pornographic images as featuring children who appeared to range in age from 8 to 14 years old. (R. 1:7–9.)

Jereczek filed a motion to suppress the evidence. He argued that the scope of his consent to search his computer was limited to data attached to his son’s user profile. (R. 10:2.) He asserted that law enforcement exceeded the scope of that consent by accessing files associated with his user profile in the computer’s recycle bin. (R. 10:2.) Because of that, Jereczek argued, all the fruits of that initial consent search and the subsequent warrant search of his computer should have been suppressed. (R. 10:1–2.)

The court held a hearing on the motion, at which the parties agreed that Jereczek consented only to a search of his son’s user profile on his computer. (R. 69:6–7.) As Jereczek’s counsel phrased it, Jereczek “asked authorities when they asked him if they could search the computer, that it be limited to his son’s account. That’s the way we used the term or user account, is how I heard it on the recording.” (R. 69:6.) The State agreed “that the understanding was that [police] would be looking under his son’s account or whatever profile would have been involved with his . . . son.” (R. 69:7.)

Behling offered lengthy testimony at that hearing about his examination of Jereczek’s computer. He testified that he did the forensic search of Jereczek’s computer in January 2015. (R. 69:9.) Behling said that he understood that the search was to focus on the son’s user profile data for images of child pornography. (R. 69:10, 16–17.)

Behling explained that he used software called EnCase, which “allows us an overview of the entire contents of the disc.” (R. 69:15.) Typically, Behling said, when the focus of his search is images or videos, he first looks to “the recycle bin container” given that people who view “this type of material

are known to try to destroy it after they look at it by placing it in a recycle bin.” (R. 69:15, 19.) The recycle bin, as Behling explained, is “just a container to temporary hold files that a user would delete” and is a container to which “any user on a multi-user operating system would have access.” (R. 69:15.)

While previewing the contents of the recycle bin, Behling discovered child pornography images. (R. 16:1; 69:16.) By running another program, Behling was able to see that the files were placed there by two different user profiles. (R. 16:1; 69:16, 27.) At that point, Behling stopped his search and sought a warrant. (R. 69:27, 38.)

When asked by Jereczek’s counsel, Behling agreed that he could have started with Jereczek’s son’s user profile and limited his search to only files associated with that profile. (R. 69:34–35.) But Behling explained that such a search would have been incomplete because it would not have reached any data associated with the son’s user profile that had placed in the recycle bin. (R. 69:34–36.)

Behling referenced an October 2016 document from the Scientific Working Group on Digital Evidence, which summarized the difficulties in conducting a search limited to a particular user’s profile. (R. 17:6; 69:34.) According to the document, a specific user’s “profile” is not confined to a discrete area of a hard drive. (R. 17:6.) Rather, user profile data can appear in numerous areas of the system, including areas in which other user profile data and files are located. (R. 17:6–7.)

Along those same lines, Behling explained that limiting a forensic search on a multiuser computer to a single user’s profile presented difficulties, in part because there were shared spaces—like the recycle bin—that all users on a multiuser system could access. (R. 69:28–29, 34, 42.) Behling also explained that had he started by searching the son’s user’s account, he “would have ended up in the [recycle bin]

eventually” and that here, he would have uncovered the items located in the recycle bin regardless whether he started there. (R. 69:18, 40.)

In a written decision and order, the court denied the motion, holding that the police search did not exceed the scope of the consent given by Jereczek. (R. 19:4–5.) It also held that law enforcement would have inevitably discovered the evidence. (R. 19:5.)

Jereczek ultimately pleaded no contest to one count of possession of child pornography. (R. 53:1.) The court sentenced him to three years’ initial confinement and five years’ extended supervision. (R. 53:1.)

Jereczek now appeals, challenging only the circuit court’s decision on the suppression motion.

STANDARD OF REVIEW

This Court reviews the circuit court’s denial of a motion to suppress under a two-step inquiry. *See State v. Lonkoski*, 2013 WI 30, ¶ 21, 346 Wis. 2d 523, 828 N.W.2d 552. First, this Court upholds the circuit court’s factual findings unless they are clearly erroneous. *Id.* Second, this Court independently applies constitutional principles to those facts. *Id.*

ARGUMENT

The circuit court soundly denied Jereczek’s motion to suppress.

Because Behling’s search did not exceed the scope of Jereczek’s consent, this Court should affirm. As discussed, there is no dispute that Jereczek consented to a law enforcement search for materials associated with his son’s user profile on the computer they shared. Moreover, Jereczek does not claim that his consent was involuntary, nor does he directly challenge the scope or execution of the second warrant-based search. Rather, Jereczek argues that Behling’s

accessing the recycle bin exceeded the scope of his consent to search his son's user profile. As a result, he claims, the evidence of child pornography that Behling found during that search, which formed the basis for the later-executed warrant, and the subsequent evidence following the issuance of the warrant must be excluded as fruits of the poisonous tree.

As discussed below, Jereczek is not entitled to relief. Behling was authorized to search for data associated with the son's user profile in the recycle bin, where he found evidence of a crime tied to Jereczek's user account in plain view. This Court should affirm.

A. Whether a search exceeds the scope of the consent given depends on its objective reasonableness.

"It is well-established that a search is reasonable when the subject consents." *Birchfield v. North Dakota*, 136 S. Ct. 2160, 2185 (2016) (citing *Schneckloth v. Bustamonte*, 412 U.S. 218, 219 (1973)). A person consenting to a search "may of course delimit as he chooses the scope of the search to which he consents." *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?" *Id.* at 251. "The scope of a search is generally defined by its expressed object." *Id.*

And based on the expressed object of the search, police are permitted to search any areas where the object sought can be found. *See, e.g., Jimeno*, 500 U.S. at 251 (holding that police reasonably concluded that consent to search a car for drugs "included consent to search containers within that car which might bear drugs"); *State v. Matejka*, 2001 WI 5, ¶ 41, 241 Wis. 2d 52, 621 N.W.2d 891 (consent to search a van for guns,

drugs, and other contraband allows inspection of containers in the van capable of holding those things).

Relatedly, a defendant's consent may limit the scope of a warrantless search just as specifications in a warrant will limit a search pursuant to it. 4 LaFave, Wayne R., *Search & Seizure* § 8.1(c), 45–46 (5th ed. 2012) (citing *United States v. Dichiarinte*, 445 F.2d 126 (7th Cir. 1971)). And, as in warrant cases, limiting consent to particular objects to be sought “does not bar the seizure of other incriminating items found in the course of an appropriately limited search.” *Id.*

To that end, evidence discovered by an officer when searching in an area he is authorized to be is discoverable under the plain-view doctrine. *See State v. Schroeder*, 2000 WI App 128, ¶ 14, 237 Wis. 2d 575, 613 N.W.2d 911 (applying plain-view doctrine to computer analyst's discovery of child pornography when searching for evidence of a different crime).

As noted above, this Court reviews a denial of a motion to suppress in two steps, first upholding the court's factual findings unless they are clearly erroneous and second, independently applying constitutional principles to those facts. *Lonkoski*, 346 Wis. 2d 523, ¶ 21. Applying that two-step process here, the circuit court's findings were sound and support the holding that Behling, in his initial search, did not exceed the scope of Jereczek's consent.

B. The circuit court's findings were not clearly erroneous.

The circuit court found that Behling searched the computer in January 2015. (R. 19:1.) “He was told law enforcement was looking for child pornography on the computer. This was the focus of his investigation.” (R. 19:1.)

It found that “Behling testified he followed his normal protocol in conducting such an examination.” (R. 19:1.) “His

understanding was the consent given was the ability to look at the data in the computer.” (R. 19:1.) “The first place Behling looked was the recycle bin container.” (R. 19:2.) It found that, according to Behling, he typically starts such searches in suspected child porn cases with the recycle bin because that “is where evidence of the crime is most likely to be located,” that he would “never exclude the recycle bin from” his analysis, and that if he had started his search with the user account, he “would have ended up in” the recycle bin eventually. (R. 19:2.)

It further found that Behling “chose not to ‘separate out’ the user accounts by limiting his analysis to the son’s file structure and he looked first at the recycle bin because, ‘searching just the data within a user account profile folder is not going to show you the data they had placed in the recycle bin.’” (R. 19:2.)

The court found that Exhibit 2 was a scientific working group document on digital evidence that “explained the complications in trying to limit a search to a single user account on a multi-user account operating system.” (R. 19:2.) It found that Exhibit 2 “was generated years after Behling examined the computer in question.” (R. 19:3.) It found that Behling acknowledged that limiting a search to a single user profile on a multiuser system “may not be impossible, ‘but your exam would not be complete.’” (R. 19:3.)

The court also found that Behling testified that “as he searched the recycle bin he observed child pornography images from multiple user accounts. He then stopped his search and sought a search warrant.” (R. 19:3.) Those actions “followed the standard protocol for which he had been trained through his agency.” (R. 19:3.)

All of those findings have support in Behling’s testimony, as described in the statement of the case, above.

Jereczek challenges several of those findings, first stating that the court found that because Behling “followed his normal protocol” in starting with the recycle bin, it determined that law enforcement did not act in bad faith, whereas Behling’s testimony demonstrated that there was no “standard protocol for exactly how data on a computer is analyzed.” (Jereczek’s Br. 9.)

Jereczek misstates the court’s finding. The court found that Behling followed the standard protocol he was trained to follow in doing the search and in stopping it to seek a warrant. That finding had support in the record. Behling testified that it was his normal practice, when searching for child pornography files, to start with the recycle bin. He explained multiple times that that is where such files are typically found. (R. 69:15, 19.) Behling also agreed, when asked about his process in this case—discovering child pornography in the recycle bin, seeing that there were files from two user profiles there, and then stopping and requesting a warrant—was consistent with his training, experience and the protocol he had been trained to follow “in [his] agency.” (R. 69:36–38.) Regardless whether that practice is part of a department- or field-wide protocol or based on his training and experience, the point of the court’s finding was that Behling wasn’t acting on an arbitrary whim: he followed the practice routinely in cases in which he was searching for child pornography.

And applying those findings to constitutional principles, Behling’s search was objectively reasonable.

C. Behling’s search was objectively reasonable and the items in the recycle bin were discoverable under the plain-view doctrine.

Behling’s search was within the scope of Jereczek’s consent to search his computer for data associated with his son’s user profile. Behling testified that the focus of the search was child pornography. Behling knew, from his training and

experience, the place he was most likely to find that evidence was the recycle bin, which was an area within which all users on Jereczek's computer could access and place items. Behling ran software giving him an overview of the items in the recycle bin, where he discovered two things: (1) there were child pornography files in the recycle bin and (2) they were placed there by two different user profiles. With that information, Behling understood that searching more could exceed the scope of what he was authorized to do, so he stopped the search and contacted the investigator, who obtained a warrant.

The crux of Jereczek's argument seems to be that Jereczek's consent limited Behling to searching only areas where Behling could essentially guarantee that he could not view Jereczek's files. (Jereczek's Br. 8–11.) But Jereczek's consent did not limit Behling's search to an exclusive *area* in the computer; it authorized him to access data associated with his son's user profile. That meant that Behling could access and search any area of Jereczek's hard drive where his son's user profile data could be found, including shared common areas of the computer—like the recycle bin. And under those circumstances, the plain-view doctrine meant that Jereczek's child pornography files in the recycle bin were discoverable.

This Court's decision in *Schroeder*, 237 Wis. 2d 575, is instructive. There, police suspected Schroeder of harassment and that his computer contained evidence of harassing messages he had posted. *Id.* ¶ 2. Police obtained a warrant to search for evidence of online harassment on Schroeder's computer. *Id.*

Before police conducted that search, Schroeder told police that the computer might contain child pornography. *Id.* ¶ 3. The lead investigator alerted the crime lab to that fact and, while searching for evidence of online harassment, the analyst found pornographic pictures of children. *Id.* ¶ 4. When the analyst discovered the pornographic material, he stopped

the search and alerted the investigator, who obtained a second warrant giving authority to search for child pornography. *Id.* That subsequent search uncovered more child pornography along with evidence of harassment. *Id.*

Schroeder alleged that the initial search exceeded the scope of the first warrant, arguing that the analyst “was actively looking for child pornography even though there was no warrant for him to do so.” *Id.* ¶ 12. The State responded that at that point, the analyst was looking for evidence of harassment and came across the child pornography, which was discoverable under the plain-view doctrine. *Id.*

This Court agreed with the State. It noted that for the plain-view doctrine to apply, the evidence must be in plain view, the officer must have a prior justification for being in the position for which he or she discovers the evidence in plain view, and the evidence seized must provide probable cause of criminal activity. *Id.* ¶ 13 (citing *State v. Guy*, 172 Wis. 2d 86, 101–02, 492 N.W.2d 311 (1992)). And in Schroeder’s case, all three factors were satisfied, including that the evidence of child pornography was in plain view even though the analyst had to open the file to see its illegal nature. *See id.* ¶ 14.

The court found support for its conclusion in federal case law, specifically *United States v. Gray*, 78 F. Supp. 2d 524 (E.D. Va. 1999), where an agent searching for unauthorized computer intrusions came across child pornography images, which caused the agent to cease and obtain an additional warrant. *Schroeder*, 237 Wis. 2d 575, ¶ 15. There, the federal court held that the child porn files were in plain view, even though the analyst had to open them to be aware of their illegal content, because the analyst “was entitled to examine all of the defendant’s files to determine whether they contained items that fell within the scope of the warrant.” *Id.* (discussing *Gray*, 78 F. Supp. 2d at 529).

This Court in *Schroeder* also distinguished *United States v. Carey*, 172 F.3d 1268 (10th Cir. 1999). *Schroeder*, 237 Wis. 2d 575, ¶ 16. In *Carey*, the court held that a search was unreasonable when an investigator inadvertently discovered child pornography when searching for evidence of drug sales and, instead of stopping to get a new warrant, abandoned his original search and looked for child pornography. *Carey*, 172 F.3d at 1272–73. There, the first illegal pornographic image was not subject to suppression because it was inadvertently discovered, but the later-discovered evidence did not fall under the plain-view doctrine. *Id.* at 1273 n.4; see *Schroeder*, 237 Wis. 2d 575, ¶ 16.

Here, like in *Schroeder* and *Gray*, Jereczek’s consent authorized a search for particular items (data associated with the son’s user profile), not areas within the system. Behling was authorized to search in any areas where that data might be found, and he was authorized to view files in shared areas to determine whether they fell within the scope of the consent search. Moreover—like the analysts in *Schroeder* and *Gray* and unlike the analyst in *Carey*—when Behling recognized that the child pornography files were associated with two different user profiles, he stopped the search and obtained a warrant before continuing. That search was objectively reasonable and did not exceed the scope of Jereczek’s consent. The circuit court correctly concluded as much.¹

¹ The circuit court here appeared to alternatively hold that the inevitable discovery doctrine under *State v. Jackson*, 2016 WI 56, 369 Wis. 2d 673, 882 N.W.2d 422, applied because, to the extent Jereczek argued that Behling should have started his search with the son’s user profile data outside the recycle bin, Behling would have inevitably ended up in the recycle bin. (R. 19:4–5.) While the State agrees that Behling would have inevitably (and soundly) searched the recycle bin even had he started his search elsewhere in the hard drive, that reasoning supports the constitutionality of

Accordingly, Jereczek cannot enjoy support from *Carey* (see Jereczek's Br. 12) for the same reasons this Court in *Schroeder* distinguished that case: the problem in *Carey* was not the officer's initial plain-view discovery of child pornography while searching for drug evidence. *Carey*, 172 F.3d at 1273 n.4. It was his continuing to search for that evidence after that plain-view initial discovery. *Id.* at 1273. In contrast, here, once Behling discovered child pornography attached to two user profiles, he stopped his search and soundly sought a warrant.

D. Jereczek's other arguments lack support in the law and the record.

Jereczek raises at least three other points, none of which support reversal and several of which mischaracterize Behling's testimony.

First, Jereczek asserts that Behling acknowledged that he could have used his forensic search software to set parameters to search only the son's user profile. (Jereczek's Br. 8.) But Behling actually testified that while he could limit

the scope of the search under *Schroeder* and the plain-view doctrine, as discussed above.

In contrast, inevitable discovery is an exception to the exclusionary rule when there is a constitutional violation that applies when the State can show that evidence that police seize that "is tainted by some illegal act may be admissible" if police would have discovered that tainted evidence by lawful means. *Jackson*, 369 Wis. 2d 673, ¶ 47 (citing *State v. Lopez*, 207 Wis. 2d 413, 427, 559 N.W.2d 264 (Ct. App. 1996)).

If Behling's search violated the constitution, the State possibly could demonstrate inevitable discovery. But the record is undeveloped on that point. Accordingly, remand would be warranted for further factual finding on whether the inevitable discovery doctrine applied. See *State v. Anker*, 2014 WI App 107, ¶ 27, 357 Wis. 2d 565, 855 N.W.2d 483 (remanding for factual development on exception to exclusionary rule).

his search in the main hard drive areas to the son's user profile, he could not do a complete search of data associated with the son's user profile without searching the recycle bin. (R. 69:35–36, 47.) Further, Behling explained, he could not search the recycle bin for data tied to the son's user profile without previewing all of the files from all users. (R. 69:45–47.) Accordingly, it wasn't possible for Behling to search all of Jereczek's son's user profile data without previewing data associated with other users.

And even if it was possible for Behling to have started his search by segregating the son's user profile data in the main hard drive as Jereczek proposes, identifying the least-intrusive means of rendering a search does not mean that Behling's actual search was unreasonable. *See Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 663 (1995) (“We have repeatedly refused to declare that only the ‘least intrusive’ search practicable can be reasonable under the Fourth Amendment.”). In addition, if Jereczek is suggesting that his consent limited Behling to implementing a specific search protocol, that is not an objectively reasonable interpretation of the scope of the consent. *See Jimeno*, 500 U.S. at 256. Again, warrant cases are illustrative on that point: in cases involving a challenge to the scope of a forensic computer search warrant, courts “appear disinclined” to require those warrants to contain a search protocol, in part because the forensic process is so contingent and unpredictable. *See 2 LaFave* § 4.10(d), 969–70 & n.163 (and cases cited therein).

Second, Jereczek premises much of his position on claims that Behling accessed the recycle bin and proceeded with “opening,” “examining,” and “rummaging through” files there. (Jereczek's Br. 8–9.) But Behling never testified that he opened, examined, or rummaged through files during his initial search. Rather, Behling testified in this case that all he was doing in his search was “previewing the data” in the computer to look for child pornography. (R. 69:12.) Consistent

with that, when Behling accessed the recycle bin, he previewed the files there. (R. 16:2; 69:24.) Behling further explained that this process was not a search process for particular files or data but more of an overview of the system: “I used the software to view the file system and the data structure of that hard drive.” (R. 69:23.)

To that end, in the written report Behling submitted, he indicated that he “previewed the data with Encase, upon preview I found evidence of child pornography under two different user accounts. I further examined these user accounts with the use of Internet Evidence Finder.” (R. 16:1.) The two user profile names he identified were the first names of Jereczek and his son. (R. 16:1–2.)

Hence, if Jereczek suggests that Behling was arbitrarily opening and accessing files, that inference lacks support. It is not even apparent that Behling opened or viewed the child pornography images he discovered during the first search. That said, even if the preview showed Behling suspected child pornography and he opened the files to confirm that they were, he was entitled to do that under the plain-view doctrine. *See Schroeder*, 237 Wis. 2d 575, ¶ 13 (holding that electronic files are still within plain view even if agent must open them to determine their incriminating nature).

Third, Jereczek analogizes the consent in this case to a scenario where law enforcement was permitted to search only one room of a house but decided to search the entire house instead. (Jereczek’s Br. 11.) That analogy for consent to search a room with search of an entire house is inapt; again, Jereczek did not limit his consent to a particular area on his hard drive, but rather his son’s user profile data. A more appropriate analogy to the consent Jereczek gave here is to a scenario where police obtained consent to search common areas of a shared house for one user’s belongings. As discussed, under that scenario, police are authorized to search all of the shared spaces and accessible containers in that

common area that could contain the user's belongings and—in determining whether items they see belong to the user—to discover any illegal items in plain view in those areas.

In sum, the circuit court's factual findings were sound and Behling's initial search was objectively reasonable. Jereczek is not entitled to relief.

CONCLUSION

This Court should affirm the judgment of conviction.

Dated this 15th day of November 2019.

Respectfully submitted,

JOSHUA L. KAUL
Attorney General of Wisconsin

SARAH L. BURGUNDY
Assistant Attorney General
State Bar #1071646

Attorneys for Plaintiff-Respondent

Wisconsin Department of Justice
Post Office Box 7857
Madison, Wisconsin 53707-7857
(608) 261-8118
(608) 266-9594 (Fax)
burgundysl@doj.state.wi.us

CERTIFICATION

I hereby certify that this brief conforms to the rules contained in Wis. Stat. § 809.19(8)(b) and (c) for a brief produced with a proportional serif font. The length of this brief is 4,535 words.

SARAH L. BURGUNDY
Assistant Attorney General

CERTIFICATE OF COMPLIANCE WITH WIS. STAT. § 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 Wis. Stat. § 809.19(12).

I further certify that:

This electronic brief is identical in content and format to the printed form of the brief filed as of 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 15th day of November 2019.

SARAH L. BURGUNDY
Assistant Attorney General