COURT OF APPEALS
DECISION
DATED AND FILED

April 6, 2021

Sheila T. Reiff
Clerk of Court of Appeals

Appeal No. 2019AP826-CR **Cir. Ct. No. 2016CF906**

STATE OF WISCONSIN **IN COURT OF APPEALS**
DISTRICT III

STATE OF WISCONSIN,

PLAINTIFF-RESPONDENT,

V.

KEVIN M. JERECZEK,

DEFENDANT-APPELLANT.

APPEAL from a judgment of the circuit court for Brown County: JOHN ZAKOWSKI, Judge. *Reversed and cause remanded with directions.*

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

¶1 HRUZ, J. Kevin Jereczek appeals a judgment convicting him of a single count of possession of child pornography as a party to the crime. Jereczek argues the circuit court erroneously denied his suppression motion, in which he alleged that law enforcement had exceeded the scope of consent he had given to

search their family computer. Specifically, Jereczek and the State stipulated that he had told officers they could search only his son's user account on the computer.

¶2 We conclude law enforcement exceeded the scope of that consent when they began their forensic examination of the computer's hard drive by examining the drive's recycle bin container, which aggregated the deleted files of all of the computer's users, including Jereczek. When a person limits his or her consent to search to a particular user account on an electronic device, a reasonable person would interpret that consent as being limited to only those files accessible from that account's user interface. In other words, and contrary to the State's argument, Jereczek's consent did not authorize a search of all files in any shared areas in the computer where data associated with the son's user profile might be found. It authorized a search of only those areas and files visible when one operates within a particular user's account—here, the son's.

¶3 The law enforcement analyst in this case testified that a particular user, while operating within his or her own account, cannot view the deleted files of another user. The analyst also testified that he knew he was likely to encounter the files of other users in the computer's recycle bin while using his forensic software to search the computer. The search of the entire recycle bin was therefore unlawful, and the evidence derived from that search should have been suppressed. We reverse and remand for the circuit court to grant Jereczek's suppression motion and for further proceedings consistent with this opinion.

BACKGROUND

¶4 A criminal complaint and an Information charged Jereczek with eleven counts of possession of child pornography as a party to the crime. The complaint alleged that Jereczek's son was a suspect in a sexual assault

investigation, and police believed that the family computer the son used may have had pornography on it related to the assault. Police met with Jereczek, who gave a desktop computer to police for forensic analysis with the instruction that police were to limit their analysis to the son's user account.

¶5 As described in more detail below, police discovered images appearing to be child pornography when they began their forensic review of the computer's hard drive—specifically, of its recycle bin. Based on these findings, police obtained a warrant to search the entire hard drive. Jereczek filed a motion to suppress the images discovered during the initial forensic analysis and during the subsequent warrant search, asserting that the scope of the initial search exceeded the consent Jereczek had given insomuch as it included the review of files outside of the son's user account.

¶6 At the hearing on Jereczek's motion, he and the State reached a stipulation regarding the scope of consent he had given to search the computer.[1] Specifically, the parties agreed that Jereczek had given limited consent that allowed police to search only his son's user account. The evidentiary portion of the hearing was held to ascertain whether the initial, pre-warrant forensic analysis of the hard drive occurred within the scope of that consent. The only witness to testify was Tyler Behling, the computer forensic crime analyst who had analyzed the hard drive for the Brown County Sheriff's Department.

¶7 Behling testified he had received the computer from an officer with instructions to locate images of child pornography on the son's user account.

[1] Police had audio recorded the conversation in which Jereczek provided consent to search the computer.

Behling removed the hard drive, which had the Windows 7 operating system installed, and connected it to a "write blocker" to prevent modifying the data on the hard drive disc. He also used software called EnCase to examine the contents of the file system on the drive. Behling testified that the software shows law enforcement the file system and data structure of the hard drive, and it "allows us an overview of the entire contents of the disc."

¶8 Behling explained that he began his search in the computer's recycle bin container, at which time he discovered that it contained child pornography that had been deleted from two user accounts.[2] Based upon this discovery, Behling applied for a search warrant for the entire contents of the hard drive. According to Behling, the recycle bin is "a container to temporar[ily] hold files that a user would delete." The recycle bin is a shared container on the hard drive into which any user on a multi-user operating system is able to place discarded files.

¶9 Behling provided further details about how a recycle bin functions. If a user logged into a particular account deletes a file (thereby placing the file in the recycle bin), that user would be able to view the deleted file from his or her account, but other users logged into different accounts would not be able to see it. Because Behling's forensic software read data directly from the hard drive disc and did not use the operating system's user interface, Behling could view the aggregate files placed in the recycle bin by all of the computer's users. In other words, under the approach Behling used, the files appearing in the recycle bin were not separated by user account. Behling was aware when he accessed the recycle bin that he would likely find files deleted by other user accounts.

[2] One user profile belonged to Jereczek, and one belonged to his son.

¶10 When Behling initially discovered that there were files containing child pornography in the recycle bin, he did not know the user account or accounts from which they had come. He used other software to examine registry data—which is external to any user account—to identify "artifacts about the user account," including the groups to which the user belongs, the user's security identifier, and the user's last log-in date. Using a globally unique identifier associated with each of the deleted files, Behling was able to connect the deleted images to particular user accounts, at which point he applied for the warrant. Behling stated that prior to obtaining the warrant, he did not believe he had accessed any particular user account.

¶11 Behling also provided additional testimony about the scope of consent provided in relation to his forensic examination. Behling was aware that Windows by default includes multiple user accounts, that there were in fact multiple user accounts on the operating system, and that he was supposed to limit his analysis to the son's user account. Behling testified there are "difficulties" with targeting a specific user profile when conducting a forensic search of a multi-user device, and for this reason he would typically "just start with a warrant" for such devices. Nonetheless, Behling stated that he did not explain to the referring detective any of his concerns regarding his technical ability to adhere to the scope of consent.

¶12 Moreover, Behling conceded that he could have limited his search of the hard drive in a way that was consistent with the scope of consent. Although he initially testified it was impractical to restrict a search to a particular user's profile, he subsequently clarified that it was "not impossible" to do so, "but your exam would not be complete." Instead, using the EnCase software, Behling could select to view all the user data under a single user profile. This type of analysis would be

confined to the user's "home profile path," which is the file structure for each profile and includes "downloads, your documents, music, pictures, that type of material." But Behling testified that such an analysis would exclude the recycle bin, something he "would never exclude" when looking for evidence of child pornography.

¶13 The circuit court denied the suppression motion. It began its decision by emphasizing some of Behling's testimony—in particular, that Behling usually started his analysis with the recycle bin because, in his experience, people would often delete illegal files after viewing them. The court also emphasized Behling's testimony that he would never exclude the recycle bin from a search for child pornography and that he would eventually look at the files located there. After highlighting Behling's testimony regarding the difficulties with limiting a forensic search to a particular user account, the court determined Behling did not exceed the scope of consent.[3]

¶14 Specifically, the circuit court concluded that even if Behling had started with the user data on the son's account, Behling "would have followed the information into the recycle bin where he would have seen the multiple child porn images from the multiple user accounts."[4] The court applied the "inevitable discovery" doctrine as articulated in ***Nix v. Williams***, 467 U.S. 431 (1984), and ***State v. Weber***, 163 Wis. 2d 116, 471 N.W.2d 187 (1991), to conclude that

[3] The circuit court wrote that law enforcement "did not exceed the scope of the warrant." We presume this was an inadvertent misstatement, as law enforcement's compliance with the scope of Jereczek's consent—not the scope of the warrant—was the only issue presented for resolution.

[4] The circuit court did not explain what information derived from the son's user account would have led law enforcement to the recycle bin.

Behling "would have eventually discovered the evidence of the crime in the recycle bin and then asked for a search warrant."

¶15 Following the suppression ruling, Jereczek entered a no-contest plea to a single count of possession of child pornography as a party to the crime. The remaining counts were dismissed outright. The parties agreed to jointly recommend a sentence consisting of three years' initial confinement and five years' extended supervision. The court accepted that recommendation. Jereczek now appeals, challenging the denial of his suppression motion under WIS. STAT. § 971.31(10) (2019-20).[5]

DISCUSSION

¶16 The Fourth Amendment to the United States Constitution and article I, section 11 of the Wisconsin Constitution prohibit unreasonable searches and seizures.[6] The protections extend to places and things in which a person has a reasonable expectation of privacy. ***State v. Tentoni***, 2015 WI App 77, ¶7, 365 Wis. 2d 211, 871 N.W.2d 285. Jereczek argues—and the State does not dispute—that he had a reasonable expectation of privacy in the computer he and his son used.

¶17 Warrantless searches are presumed to be unreasonable under the Fourth Amendment. ***State v. Matejka***, 2001 WI 5, ¶17, 241 Wis. 2d 52, 621 N.W.2d 891; *see also* ***Birchfield v. North Dakota***, 136 S. Ct. 2160, 2173 (2016).

[5] All references to the Wisconsin Statutes are to the 2019-20 version unless otherwise noted.

[6] The protections under these provisions of the federal and state constitutions are usually interpreted coextensively. ***State v. Artic***, 2010 WI 83, ¶28, 327 Wis. 2d 392, 786 N.W.2d 430.

"Consent is an exception to the warrant requirement." ***State v. Abbott***, 2020 WI App 25, ¶14, 392 Wis. 2d 232, 944 N.W.2d 8. The consent exception is premised on the notion that it is reasonable for police to conduct a search if they have been permitted to do so by the person whose expectation of privacy is implicated. ***Florida v. Jimeno***, 500 U.S. 248, 250-51 (1991) (citing ***Schneckloth v. Bustamonte***, 412 U.S. 218, 219 (1973)). Here, the parties stipulated that Jereczek provided consent to search the computer, but he limited that consent to his son's user account.[7]

¶18 "The scope of consent to search may be limited by the terms of its authorization." ***Matejka***, 241 Wis. 2d 52, ¶37 (citing ***Walter v. United States***, 447 U.S. 649, 656 (1980)). When a person explicitly limits the scope of the consent-based search, courts will give effect to those limitations. *See* ***id.***; *see also* ***Jimeno***, 500 U.S. at 252. The scope of consent is measured by the breadth of the actual consent given, and courts determine whether the search remained within the boundaries of that consent by looking at the totality of the circumstances. ***United States v. Correa***, 908 F.3d 208, 215 (7th Cir. 2018).

¶19 More specifically, "[t]he 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?" ***Jimeno***, 500 U.S. at 251 (citations omitted). Importantly, when a defendant challenges the scope of consent, the State bears the burden of establishing by clear and convincing

[7] The parties do not present any issue related to Jereczek's authority to consent to a search of his son's user account on the computer.

evidence that the warrantless search was reasonable and in compliance with the Fourth Amendment. ***Matejka***, 241 Wis. 2d 52, ¶17.

¶20 When reviewing a suppression motion, we apply a two-step standard of review. ***State v. Lonkoski***, 2013 WI 30, ¶21, 346 Wis. 2d 523, 828 N.W.2d 552. We will uphold a circuit court's factual findings unless they are clearly erroneous. ***Id.*** We review de novo the application of those facts to the relevant constitutional principles. ***Id.***

¶21 We conclude Behling plainly violated the scope of Jereczek's consent, which gave police authority to search only his son's user account. Despite this clear limitation, Behling began his search of the computer in the recycle bin, a location where he knew he was likely to find—and did find—not just files deleted from the son's user account, but the deleted files of the computer's other users as well. Indeed, further investigative efforts were necessary to determine precisely from which account each item of child pornography in the recycle bin had come. A search of the shared recycle bin container was therefore not a search of "the son's account," and it exceeded the scope of the consent that Jereczek had given law enforcement.

¶22 Our conclusion in this regard gives effect to what a reasonable person would have understood the consent limitation to mean. *See* ***Jimeno***, 500 U.S. at 251. Objectively speaking, when a person thinks of a particular user account on a computer, he or she is not likely thinking about where specific items of data are stored on the physical hard drive disc. Rather, the commonly understood meaning of a user account is an interface through which a user can

access his or her own files, folders and personalization options.[8] This is the type of information Behling testified constitutes the user's "home profile path" on the hard drive—i.e., the user's "downloads, … documents, music, pictures, that type of material." A search of a user account, therefore, is functionally a limited search of a particular area of a computer—i.e., everything accessible by that user account. Moreover, even Behling did not regard the aggregate recycle bin as part of a user account, as he testified he did not believe he accessed a user account prior to obtaining a warrant.

¶23 The recycle bin, to be sure, was accessible from the son's user account, but only in a limited manner. Behling testified that when a particular user deletes a file from his or her account, that user would be able to see the deleted file, but other users logged into different accounts would not.[9] On this record, there is no basis to conclude that Jereczek reasonably believed the consent he provided would allow law enforcement to access data from other user accounts, whether located in the recycle bin or elsewhere on the hard drive disk. Moreover, Jereczek authorized police to search within the recycle bin only to the extent the search was of data from the son's user account. Behling's review of the recycle bin's aggregate contents from all users exceeded the explicit limitations Jereczek placed on the search.

[8] *See* Gilberto Perera, *How to Create a New User Account in Windows 7*, LIFEWIRE (updated Mar. 14, 2021), https://www.lifewire.com/create-user-account-in-windows-7-3506832.

[9] Notably, Behling did not attempt to access the son's user account by more traditional means (e.g., by logging into the Windows user interface with the son's account credentials). Doing so would have, according to Behling's testimony, allowed him to view the files the son had placed in the recycle bin without exposing other users' data to Behling's review.

¶24 The State's argument is, essentially, that the limitation Jereczek imposed "authorized [Behling] to access data *associated with* his son's user profile." (Emphasis added.) In the State's view, this consent meant 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." (Emphasis added.) As we have explained, interpreting the scope of consent in this fashion relies on an overly technical understanding of how data is stored on a hard drive disk and how that data is accessed by law enforcement's forensic software. It is not what a typical reasonable person would have understood, nor is it necessarily consistent with the specific limitation Jereczek imposed. The State's assertion that it is entitled to search anywhere that the son's user data could be stored is therefore not objectively reasonable.

¶25 Nonetheless, in terms of authority, the State relies on case law that concerns container searches in vehicles and the plain view doctrine. "The scope of a search is generally defined by its expressed object." ***Jimeno***, 500 U.S. at 251. For example, when an officer asks for permission to search a vehicle for narcotics, it is implied that the officer is requesting permission to access any containers within the vehicle where narcotics might be stored. *See* ***id.*** From this principle, the State reasons that Jereczek was surely authorizing a search "in any areas where that data [i.e., any child pornography his son possessed] might be found." Moreover, the State contends that because Behling was authorized to search the recycle bin container, any child pornography—from any user—he discovered during that search was considered an item in plain view under ***State v. Schroeder***, 2000 WI App 128, ¶¶12-16, 237 Wis. 2d 575, 613 N.W.2d 911.

¶26 As alluded to above, the State's argument proceeds from a faulty premise divorced from the context of electronic devices. By stipulation, the

consent Jereczek provided was limited to his son's user account—not to, in the State's formulation, any "data associated with his son's user profile." We perceive the latter scope of consent to be much broader, and law enforcement certainly could have sought that degree of authorization. Having failed to do so, though, police were not entitled to search other areas of the hard drive merely because it was convenient for them to do so, or because they believed evidence they desired might be located there.[10] Furthermore, police never attempted to clarify the scope of Jereczek's consent with him, which is problematic in this context given that the State carried the burden of establishing by clear and convincing evidence that the warrantless search was reasonable and in compliance with the Fourth Amendment. *See* ***Matejka***, 241 Wis. 2d 52, ¶17.

¶27 The State's arguments appear to be animated, to some extent, by the technical difficulties associated with adhering to the scope of consent Jereczek provided, given the limitations of law enforcement's forensic software. The State emphasizes that Behling could not search the recycle bin for data tied to the son's user profile without previewing all of the files from all users in that container. The State argues that forgoing a search of the recycle bin based on this technical limitation would have rendered the law enforcement search incomplete.

[10] Jereczek and the State argue about whether some of the circuit court's findings of fact are consistent with Behling's testimony. We do not regard any of the court's factual findings as clearly erroneous, as the court essentially accepted Behling's testimony about how he performed the search and why he began in the computer's recycle bin. Behling's testimony was undisputed, and we perceive the court to have accepted his testimony as credible. As we explain, however, the court's observations about how complete the search would have been without an examination of the recycle bin, whether Behling would have eventually examined the recycle bin's contents, and whether law enforcement acted in good faith are largely immaterial to the issues on appeal, which concern only the scope of the consent to search and whether the State met its burden of showing that law enforcement adhered to those restrictions.

¶28 Once again, the State misapprehends the scope of consent. Nothing in the consent Jereczek supplied suggested that law enforcement had authority to search anywhere on the hard drive based on whether they regarded their search as "complete"—i.e., until they had satisfied themselves that they had reviewed every piece of data connected to the son's account. As in ***Jimeno***, the terms of the search's authorization in this case were simple—police could search the son's user account, but no more. *See* ***Jimeno***, 500 U.S. at 251. Unlike ***Jimeno***, the terms of the authorization here were insufficient to get police everywhere they wanted to go.[11]

¶29 Nor do technical difficulties in adhering to the scope of consent justify a broader search. Behling was aware it would be difficult, although not impossible, to tailor his search to the contents of only one user profile. Indeed, he testified he would usually seek a warrant initially for single-user searches of computers with multiple user accounts. But Behling did not inform the referring detective that he thought it was necessary to view data from other accounts during his review, nor did he seek to clarify the scope of consent with Jereczek himself. Law enforcement cannot rely on technical limitations of their forensic software to

[11] The parties offer various attempts at analogies to other cases and contexts regarding consent to search or limited-scope warrant-based searches of physical locations in support of their respective arguments regarding Behling's search of the computer hard drive. While we have divined some of our own such analogies, and while we tend to agree more with those advanced by Jereczek, we believe it is more productive to provide the analysis as we have written, without resort to analogies from other cases about searches of physical premises.

We do note, however, that none of the cases to which the State cites regarding searches of computer data involved the type of limited consent at issue here. Instead, they involved consent to generally search an entire computer for particular types of information. *See, e.g.*, ***State v. Schroeder***, 2000 WI App 128, ¶¶12-16, 237 Wis. 2d 575, 613 N.W.2d 911 (applying the plain view doctrine and concluding that police did not violate the Fourth Amendment when they found child pornography on a computer while lawfully searching it, pursuant to a search warrant, for evidence of online harassment).

expand the scope of consent beyond those areas that are reasonably implied by the terms of the consent.

¶30 Because the search of the recycle bin container on the shared computer's hard drive was unlawful, the circuit court should have granted Jereczek's suppression motion and excluded the initial item of child pornography associated with Jereczek's account and all derivative evidence. The State, alternatively, suggests that it could "possibly demonstrate inevitable discovery" of some or all of the relevant items of evidence. It requests that we remand for further factual finding on whether the inevitable discovery exception to the exclusionary rule applies.

¶31 We are disinclined to remand with specific directions that the circuit court hold an evidentiary hearing on the inevitable discovery issue. The State does not appear to have argued inevitable discovery as a basis for admitting the evidence at any point before the court. Rather, that doctrine appears to have been applied on the court's own initiative.[12] We remand generally with directions that the circuit court grant Jereczek's suppression motion. On remand, the court may also conduct further proceedings consistent with this opinion. If the State wishes to file a motion seeking to admit some or all of the evidence at issue based on the notion that it would have been inevitably discovered by lawful means, it may do so on remand.

[12] As the State notes, the inevitable discovery doctrine presumes that the evidence is tainted by an illegal act. *See* ***State v. Jackson***, 2016 WI 56, ¶¶47-48, 369 Wis. 2d 673, 882 N.W.2d 422. The State's primary argument below appears to have been that the search here was consistent with the scope of consent Jereczek provided, and that there was no way for law enforcement to effectuate the search without examining the recycle bin container on the hard drive.

By the Court.—Judgment reversed and cause remanded with directions.

Recommended for publication in the official reports.