FILED
02-03-2022
CLERK OF WISCONSIN
COURT OF APPEALS

STATE OF WISCONSIN

C O U R T O F A P P E A L S

DISTRICT III

Case No. 2021AP1767-CR

STATE OF WISCONSIN,

Plaintiff-Appellant,

v.

STEVEN W. BOWERS,

Defendant-Respondent.

APPEAL FROM AN ORDER SUPPRESSING EVIDENCE AND A DENIAL OF A MOTION FOR RECONSIDERATION, ENTERED IN TAYLOR COUNTY CIRCUIT COURT, THE HONORABLE ROBERT R. RUSSELL, PRESIDING

BRIEF AND SUPPLEMENTAL APPENDIX OF PLAINTIFF-APPELLANT

JOSHUA L. KAUL
Attorney General of Wisconsin

NICHOLAS S. DESANTIS
Assistant Attorney General
State Bar #1101447

Attorneys for Plaintiff-Appellant

Wisconsin Department of Justice
Post Office Box 7857
Madison, Wisconsin 53707-7857
(608) 266-8556
(608) 294-2907 (Fax)
desantisns@doj.state.wi.us

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

ISSUES PRESENTED

Taylor County Police Sergeant Steven Bowers, acting without authorization, shared confidential case files with the producers of a television show through Dropbox, an online filesharing service. He uploaded the case files to a Dropbox account that he set up through his official county-owned email address, then granted the producers and his girlfriend access to the Dropbox account. Law enforcements were able to access the contents of the Dropbox without a warrant by changing Bowers' password, as Bowers created the account with his Taylor County email address. Bowers was charged with misconduct in public office.

1. Did Bowers have a reasonable expectation of privacy in his Dropbox account that he set up through his county-owned email address and shared with several other people?

The circuit court answered: "Yes."

This Court should reverse.

2. If law enforcement's examination of Bowers' Dropbox account constituted a search, was the search justified by probable cause and exigent circumstances due to the county's urgent need to figure out who had access to its confidential case files and stop its spread?

The circuit court declined to address this question.

This Court should answer: "Yes."

STATEMENT ON ORAL ARGUMENT AND PUBLICATION

The State requests neither oral argument nor publication because the briefs should adequately set forth the facts and applicable precedent and because resolution of this appeal requires only the application of well-established precedent to the facts of the case.

INTRODUCTION

The Taylor County Sheriff's Office entered into an agreement with to share the case files from one homicide case—and only that case—with the producers of an investigative television series, "Cold Justice." Police Sergeant Steven Bowers, acting without authorization, shared the files from two other homicide cases. He shared the files from one case through paper copies. He shared the files from the other case by uploading them to a Dropbox account. He used his official Taylor County email address, which was owned by the county, to create the Dropbox account. He then shared access to the account with the producers of Cold Justice, as well as with his girlfriend, who was not a police officer or county employee. County officials accessed the Dropbox account through Bowers' county-owned email address by using the "reset password" function and changing his Dropbox password. Bowers was charged with two counts of misconduct in public office: one for the shared paper filed and one for the shared Dropbox files.

Bowers moved to suppress the information stored on Dropbox, asserting that the county unlawfully searched his Dropbox account. The circuit court initially denied the motion, holding that Bowers had no reasonable expectation of privacy in the Dropbox account. Bowers moved for reconsideration, and this time the circuit court granted his suppression motion

on the grounds that he *could* access the Dropbox account through his cell phone—despite no evidence that the phone had anything to do with the Dropbox account. The State moved for reconsideration and the circuit court affirmed its order suppressing evidence for the same reason. The State also argued exigent circumstances due to the urgent need to figure out who had access to the information and stop its spread, but the circuit court chose not to address this argument.

This Court should reverse the circuit court's order suppressing evidence. First, law enforcement did not need a warrant to examine Bowers' Dropbox account because Bowers had no reasonable expectation of privacy in the account, which he set up using county-owned email address and then deliberately allowed several other people to freely access. The examination of the Dropbox account was therefore not a Fourth Amendment search. Second, even if this Court concludes that a search occurred, any search was nevertheless justified by probable cause and exigent circumstances. Law enforcement had an urgent need to figure out who had access to what information and stop it from being disseminated further.

STATEMENT OF THE CASE

In February 2017, the Taylor County Sheriff's Department worked with the television program "Cold Justice" on a homicide cold case ("Murder 1"). (R. 1:3.) "Murder 1" was the only case for which the department agreed to provide information to "Cold Justice." (R. 1:3.) Steven Bowers, a Detective Sergeant with the Taylor County Sheriff's Department, shared confidential reports on two other homicides, "Murder 2" and "Murder 3," with the producers of Cold Justice. (R. 1:3.) Bowers did not ask anyone for permission to share the reports. (R. 1:3.)

Bowers provided paper files for "Murder 2" to the Cold Justice producers.[1] (R. 1:4.) He uploaded the files for "Murder 3" to a Dropbox account, then shared access to the account with his girlfriend and with Cold Justice employees. (R. 1:4.) Police learned about these actions when they heard Cold Justice producers discussing the two cases Bowers had shared with them. (R. 1:3.) Bowers used his official Taylor County Sheriff's Department email address to set up the Dropbox account. (R. 1:4.) Bowers admitted in an email to Sheriff Bruce Daniels on February 27, 2017 that he shared the confidential files without seeking permission, in violation of department policy. (R. 1:5.)

The police department was able to access Bowers' Dropbox account through his county email address. (R. 108:10.) IT director Melissa Lind contacted Dropbox on March 1, 2017 regarding Bowers' suspected sharing of information, but Dropbox was not cooperative. (R. 153:17–18.) Lind did not know exactly what was in the Dropbox account or with whom Bowers had shared it. (R. 153:18.) So, on March 2, Lind performed a password reset at law enforcement's instruction using Bowers' county-owned email address. (R. 153:19.) She clicked Dropbox's "forgot password" link, which sent a password reset email to Bowers' County email address. (R. 153:19.) She then reset the password through the email address and was able to access the Dropbox account. (R. 153:19–20.)

[1] The shared paper files for "Murder 2" are not at issue on this appeal.

Lind's search of the Dropbox account showed that Bowers had indeed shared the case files with people who did not work for the county. (R. 153:21.) Sheriff Daniels sought legal advice from the county's district attorney before they accessed the account. (R. 108:12.)

Bowers was originally charged in October 2017 with one count of misconduct in public office. (R. 1.) In July 2018, however, the charge was amended to two counts on misconduct in public office; one for sharing the paper files for "Murder 2" and one for sharing the Dropbox files for "Murder 3." (R. 25:1.)

Bowers moved to suppress the fruits of the examination of his Dropbox account on the ground that it violated his Fourth Amendment reasonable expectation of privacy. (R. 44:2.) He also argued that his confession to sharing the files was a *Garrity*[2] violation.[3] (R. 44:3.) At the suppression hearing, Taylor County Sheriff Bruce Daniels testified that Bowers had signed an information technology office policy in 2007 that stated, "I have no expectation of privacy for any material on Taylor County equipment, even if that material was generated for my personal use." (R. 108:8.)

The policy signed by Bowers stated, "Taylor County retains exclusive ownership and control of all hardware, software, and the data that is generated through the use of its facilities. "The Information Technology Department reserves the right to monitor all information technology usage and to access any electronic communications at any time." (R. 96:1.) Sheriff Daniels explained that if he had used his official Taylor County email to set up other accounts, he would not

---

[2] *Garrity v. New Jersey*, 385 U.S. 493 (1967).

[3] The alleged *Garrity* violation is not at issue on this appeal.

have an expectation of privacy in those other accounts. (R. 108:9–10.)

Sheriff Daniels explained that the department was able to access Bowers' Dropbox account through his county email address using Dropbox's "reset password" function. (R. 108:10.) On cross-examination, Sheriff Daniels stated that Bowers appeared to have set up the Dropbox account on his own and paid for it himself. (R. 108:21.) He also acknowledged that Dropbox is a cloud-based storage service and was not located on the county's servers. (R. 108:22.) Finally, he admitted that while the county email address got them the password to the Dropbox account, they still had to enter the password to access the account. (R. 108:33–34.)

The circuit court denied Bowers' motion to suppress in an oral ruling on February 11, 2020. (R. 107:4.) The circuit court was persuaded by the agreement signed by Bowers that gave the Information Technology department the right to monitor all information technology usage, gave them the right to access any electronic communications, and clarified that Bowers had no reasonable expectation of privacy for any material on Taylor County equipment. (R. 107:3–4.) The circuit court also found that no *Garrity* violation occurred because Bowers was not threatened with loss of employment and made his confession voluntarily. (R. 107:4–6.)

On July 16, 2020, Bowers filed a motion for reconsideration of his suppression motion. (R. 119:1.) He attached a 2011 "policy supplement" related to the use of his county-issued phone.[4] (R. 119:6.) The supplement clarified that he was permitted to use his county-issued smartphone

[4] Bowers' smartphone was never searched, and there was no evidence that the Dropbox account was somehow tied to the phone. (R. 153:24–25.)

"as [he] would [his] own." (R. 129:1.) He also pointed out that a new information technology policy took effect in 2012—although he admitted there was "no evidence" he "signed any documents related to this policy." (R. 119:6.) He claimed this policy superseded the 2007 policy he signed. (R. 119:6.)

In an oral ruling on December 14, 2020, the circuit court found that due to the 2011 policy supplement that allowed him to use his county-issued smartphone as he would his own, Bowers had a reasonable expectation of privacy in the contents of his county-issued smartphone. (R. 140:9.) The circuit court acknowledged that Bowers *could* access the Dropbox account through his county-issued smartphone. (R. 140:11.) Based on this finding, the circuit court held that Bowers "had a reasonable expectation of privacy in the smartphone and, further, had a reasonable expectation of privacy in a Dropbox account that was used for his personal use and not housed on Taylor County equipment." (R. 140:11.) The circuit court therefore granted Bowers' motion for reconsideration and suppressed the Dropbox evidence. (R. 140:11.)

The State filed a motion to supplement the record and a motion to reconsider the December 14, 2020 oral ruling. (R. 143; 154:1.) The record was supplemented with the testimony of Melissa Lind, the Information Technology director for Taylor County. (R. 153:6, 9.) Lind explained that under the 2012 policy, which was in effect at the time Bowers disclosed the information to Cold Justice, the IT department retained the right to "monitor all information technology usage and access any electronic communications at any time." (R. 127:7; 153:14.) She reiterated that Taylor County owns the county email addresses the employees use. (R. 153:16.) Lind explained that Dropbox is a cloud-based storage center that is accessible through a username and password to any device

with an internet connection. (R. 153:16.) Dropbox is tied to an email address, not a physical device. (R. 153:17.)

IT Director Melissa Lind explained that with law enforcement's permission, she searched Bowers' Dropbox account after using the "lost password" function to obtain his password. (R. 153:19–21.) She learned that Bowers had indeed shared the case files with people who did not work for the county. (R. 153:21.) Lind stated that to the best of her knowledge, Bowers' county-issued cell phone was never searched and was not needed to access the Dropbox account. (R. 153:24–25.) On cross-examination, Lind reiterated that the email address alone did not give her access to the Dropbox account; she still needed to use the email address to change the password. (R. 153:27–28.) Finally, she explained that if Bowers had used a personal email rather than a county-owned email to set up the Dropbox account, she would not have been able to access the Dropbox account. (R. 153:40.)

The State argued that there was no testimony connecting Bowers' county-issued phone to his Dropbox account, so the ruling—which relied on Bowers' expectation of privacy in the contents of his phone—was in error. (R. 154:2.) The State pointed out that the email address used to set up the Dropbox account is the property of Taylor County, and that other jurisdictions have declined to acknowledge an expectation of privacy in similar situations. (R. 154:3.) Alternatively, the State argued that the search was justified by probable cause and exigent circumstances. (R. 154:5.) The State asserted that law enforcement reasonably feared a delay would risk destruction of evidence. (R. 154:7.) The State also argued that law enforcement had an urgent need to quickly determine what information was shared with whom in order to stop its spread. (R. 157:4.)

The circuit court denied the State's motion for reconsideration. (R. 159:12.) The circuit court found that Bowers had a reasonable expectation of privacy in his Dropbox account because "the Court's prior finding and decision with respect to smartphones will certainly apply to the Defendant's personal iPad and personal computer." (R.159:7–8.) The court reasoned that Bowers could have accessed Dropbox through his personal devices, and "[n]o evidence has been presented that any of this information was synced to the Taylor County owned equipment." (R. 159:8.) The circuit court distinguished *Clark*,[5] a federal district court case with extremely similar facts, on the basis that in the circuit court's view "[n]o evidence has been presented indicating that Mr. Bowers' Dropbox account was in any way connected to his work emails." (R. 159:10.)

Regarding the State's exigent circumstances arguments, the circuit court relied on Lind's testimony that Dropbox archives deleted files for 30 days, (R. 153:22), and found that the fear of destroying evidence therefore did not justify a warrantless search (R. 159:11). The prosecutor then pointed out that the circuit court had only addressed one of the State's two exigency arguments: the other argument was that the State needed to figure out as quickly as possible exactly who had access to sensitive county information and potentially stop the information from spreading further. (R. 159:17–18.) The circuit court refused to address this issue, instead stating, "all I can say, Counsel, is we're out of time." (R. 159:18.)

[5] *Clark v. Teamsters Local Union*, 349 F. Supp. 3d 605, 621 (E.D. Ky. 2018)

STANDARD OF REVIEW

When reviewing a decision on a motion to suppress evidence, this Court upholds the circuit court's factual findings unless they are clearly erroneous, but it independently applies constitutional principles to the facts. *State v. Lonkoski*, 2013 WI 30, ¶ 21, 346 Wis. 2d 523, 828 N.W.2d 552.

ARGUMENT

I. Bowers had no reasonable expectation of privacy in a Dropbox account that he set up using his official county-owned email address and shared with several other people.

A. A Fourth Amendment search occurs only if a reasonable expectation of privacy in infringed; a person has no reasonable expectation of privacy in electronic storage shared with third parties

The Fourth Amendment to the United States Constitution and Art. I, § 11 of the Wisconsin Constitution prohibit unreasonable searches and seizures.[6] *State v. Pinkard*, 2010 WI 81, ¶ 13, 327 Wis. 2d 346, 785 N.W.2d 592. However, a Fourth Amendment "search" occurs only if "an expectation of privacy that society is prepared to consider reasonable is infringed." *State v. Brereton*, 2013 WI 17, ¶ 23, 345 Wis. 2d 563, 826 N.W.2d 369 (quoting *United States v. Jacobsen*, 466 U.S. 109, 113 (1984)).

[6] Wisconsin courts consider state constitutional protections coextensive with the Fourth Amendment. *State v. Houghton*, 2015 WI 79, ¶ 49, 364 Wis. 2d 234, 868 N.W.2d 143.

The reasonable expectation of privacy analysis remains the same whether physical or digital property is searched. "[T]he expectation of privacy in digital files … is governed by the same standards as the expectation of privacy in physical property," and "the reasonableness of an expectation of privacy in digital files shared on electronic platforms is determined by considering the same factors as in any other Fourth Amendment context." *State v. Baric*, 2018 WI App 63, ¶ 19, 384 Wis. 2d 359, 919 N.W.2d 221.

For this reason, this Court uses the same factors articulated in *State v. Dumstrey*, 2016 WI 3, ¶ 47, 366 Wis. 2d 64, 873 N.W.2d 502, to determine whether a defendant's expectation of privacy in electronic files was objectively reasonable. These factors are:

> (1) whether the defendant had a property interest in the premises; (2) whether he [or she] was legitimately (lawfully) on the premises; (3) whether he [or she] had complete dominion and control and the right to exclude others; (4) whether he [or she] took precautions customarily taken by those seeking privacy; (5) whether he [or she] put the property to some private use; and (6) whether the claim of privacy is consistent with historical notions of privacy.

Dumstrey, 366 Wis. 2d 64, ¶ 47 (quoting *State v. Rewolinski*, 159 Wis. 2d 1, 17–18, 464 N.W.2d 401 (1990)). These non-exclusive factors guide this court's analysis, but they are not controlling. *Baric*, 384 Wis. 2d 359, ¶ 18. "Whether an individual has a reasonable expectation of privacy is determined by examining the totality of the circumstances." *State v. Tentoni*, 2015 WI App 77, ¶ 36, 365 Wis. 2d 211, 871 N.W.2d 285.

Out-of-state case law involving searches of Dropbox and similar electronic storage equipment is helpful in examining whether an expectation of privacy is objectively reasonable. *Clark*, 349 F. Supp. 3d at 621, a wrongful termination case, addressed an employer's search of an employee's Dropbox account. Clark set up a Dropbox account using her work email, which was used to store a mix of personal and professional documents. *Id.* at 622. Her former employer used the "lost password" function to access the Dropbox account through her work email. *Id.* at 621. Clark filed an invasion of privacy[7] claim against her former employer. *Id.*

The United States District Court for the Eastern District of Kentucky granted Clark's employer summary judgment on the basis that Clark had no reasonable expectation of privacy in the Dropbox account. *Clark*, 349 F. Supp. 3d at 621. The court reasoned that because employees "do not have a reasonable expectation of privacy in their work e-mails, then it logically follows that individuals do not have a reasonable expectation of privacy in a Dropbox account that is tied to their work e-mail and that they lose access to if they lose access to the e-mail." *Id.* 622.

Additionally, under the third-party doctrine, a defendant has "no legitimate expectation of privacy in information he voluntarily turns over to third parties ... even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *United States v. Caira*, 833 F.3d 803, 806 (7th Cir. 2016) (quoting *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979)). And the fact that a person may have limited the shared information to certain

---

[7] An invasion of privacy claim under Kentucky law requires the court to determine whether the plaintiff had a "reasonable expectation of privacy," which is analyzed using the same standards that are used under the Fourth Amendment. *See, e.g., Pearce v. Whitenack*, 440 S.W.3d 392, 401–02. (Ky. Ct. App. 2014.)

people does not mean he has any legitimate expectation of privacy with the world at large. *Caira*, 833 F.3d at 806. This rule does not change when the defendant has deliberately shared information with others via an electronic service such as Dropbox rather than in person.

In *United States v. Maclin*, 393 F. Supp. 3d 701, 706 (N.D. Ohio 2019), for example, a child pornography defendant stored images on a personal Dropbox account that showed the sexual exploitation of minors. The account was password-protected and was connected to a personal email account. *Id.* at 711. However, the defendant deliberately shared access to the Dropbox account with other people. *Id.*

Because the defendant shared access to the Dropbox account with others, the United States District Court for the Northern District of Ohio held that the defendant had no reasonable expectation of privacy in the Dropbox files. *Maclin*, 393 F. Supp. 3d at 711. "Courts have consistently held there is no reasonable expectation of privacy in files contained in peer-to-peer sharing services," so the court reasoned that "that determination is not changed simply when a defendant 'closes' the network and grants access only to his 'friends.'" *Id.*; *See Baric*, 384 Wis. 2d 359, ¶ 21 (defendant had no reasonable expectation of privacy in child pornography files he publicly shared on a peer-to-peer file sharing network); *Smith*, 442 U.S. at 743–44.

B. Bowers had no reasonable expectation of privacy in a shared Dropbox account that was set up through his county-owned email address.

Here, if Bowers had a subjective expectation of privacy in his Dropbox account, this expectation was not objectively reasonable. As a starting point, Bowers voluntarily and deliberately shared access to his Dropbox account and the files inside it with several other people—including the

producers of a popular television show. Under the third-party doctrine, this sharing alone is fatal to Bowers' claim that he had any reasonable expectation of privacy in the Dropbox account. *Smith*, 442 U.S. at 743–44; *Maclin*, 393 F. Supp. 3d at 711.

An analysis of the six *Dumstrey* factors confirms that Bowers had no reasonable expectation of privacy in his Dropbox account. The first two factors admittedly cut in Bowers' favor. He had a property interest in the Dropbox account, and he appears to have created and maintained the account lawfully. *See Dumstrey*, 366 Wis. 2d 64, ¶ 47. The other four factors, however, show that he had no reasonable expectation of privacy.

Regarding the third factor, Bowers did not have "complete dominion and control" over Dropbox account. *Dumstrey*, 366 Wis. 2d 64, ¶ 47. On the contrary, he shared dominion and control over the account with several other people, including the producers of a television show. (R. 47:10; 153:21–22.) As Lind testified, any of these people would have been able to add, save, delete, download, or view the contents of the Dropbox account from anywhere in the world. (R. 153:16–17.) The fact that Bowers set up the Dropbox account through his county-owned email address, rather than a personal email he himself owned, further diminishes his dominion and control over the account—as is evidenced by the fact that law enforcement was able to gain access using his county-owned e-mail address. (R. 108:10.)

The fourth factor also cuts heavily against Bowers because he took few "precautions customarily taken by those seeking privacy." *Dumstrey*, 366 Wis. 2d 64, ¶ 47. It is true that Bowers took the precaution of protecting the Dropbox account with a password. However, he then shared access to the account with several other people, including the producers of a popular television show. (R. 47:10; 153:21.) A person seeking privacy customarily does not share with several other

people information he intends to keep private, *Maclin*, 393 F. Supp. 3d at 711, especially in conjunction with a television show. The fact that he chose to connect the account to his official county-owned email address, rather than a personal email, is further evidence of the lack of privacy precautions taken by Bowers because his actions allowed anyone with access to his county-email to reset and access the account.

Regarding the fifth factor, it does not appear that Bowers put the property to some "private use." *Dumstrey*, 366 Wis. 2d 64, ¶ 47. On the contrary, he used it for the purpose of sharing county documents with other people. And regarding the sixth factor, his claim of privacy is not "consistent with historical notions of privacy." *Id.* (citation omitted). Historical notions of privacy do not include spaces that a person shares with others. Just as courts have not recognized an expectation of privacy in an apartment building's common spaces, *State v. Eskridge*, 2002 WI App 158, ¶ 19, 256 Wis. 2d 314, 647 N.W.2d 434, courts have not recognized a right to privacy in an online space such as Dropbox that a person has deliberately chosen to share with others, *See, e.g., Maclin*, 393 F. Supp. 3d at 711.

In summary, courts have held that a person who uses her employer-owned email address to create a Dropbox account has no reasonable expectation of privacy in that account. *Clark*, 349 F. Supp. 3d at 621. Separately, courts have also held that a person who shared access to a Dropbox account with others has no reasonable expectation of privacy in that account. *Maclin*, 393 F. Supp. 3d at 711; *See also United States v. Sawyer*, 786 F. Supp. 2d 1352, 1356 (N.D. Ohio 2011) (no reasonable expectation of privacy in filed shared with a group of friends via a filesharing service).

Bowers did both of these things: he used his official county-owned email address to set up a Dropbox account, then shared access to that Dropbox account with several other people. For all these reasons, Bowers had no reasonable expectation of privacy in the account. *Dumstrey*, 366 Wis. 2d 64, ¶ 47. Therefore, there was no Fourth Amendment "search" of his Dropbox account, so his Fourth Amendment right was not violated. *Brereton*, 345 Wis. 2d 563, ¶ 23.

II. Alternatively, if a search occurred, it was justified by probable cause and exigent circumstances because the State had an urgent need to figure out who had access to sensitive county information and to attempt to limit its spread.

As explained above, no Fourth Amendment search occurred in this case because Bowers did not have a reasonable expectation of privacy in a Dropbox account that he created through his county-owned email address and shared with several other people. Even if this Court disagrees, however, any search was nevertheless justified by probable cause and exigent circumstances. Law enforcement needed to determine as quickly as possible what information was shared with whom so they could stop its spread.

"A warrantless search is presumptively unreasonable and is constitutional only if it falls under an exception to the warrant requirement." *State v. Tullberg*, 2014 WI 134, ¶ 30, 359 Wis. 2d 421, 857 N.W.2d 120 (citations omitted). "One exception to the warrant requirement is the exigent circumstances doctrine, which holds that a warrantless search complies with the Fourth Amendment if the need for a search is urgent and insufficient time to obtain a warrant exists." *Id.* "An exception to the warrant requirement arises when the State can demonstrate 'both probable cause and exigent circumstances that overcome the individual's right to be free from government interference.'" *State v. Mielke*, 2002

WI App 251, ¶ 6, 257 Wis. 2d 876, 653 N.W.2d 316 (citation omitted).

"In the search context, probable cause requires a 'fair probability' that contraband or evidence of a crime will be found in a particular place.'" *State v. Robinson*, 2010 WI 80, ¶ 26, 327 Wis. 2d 302, 786 N.W.2d 463 (citation omitted). Courts "evaluate the existence of probable cause objectively, concerned with whether law enforcement acted reasonably." *Id.* "'[P]robable cause' is not a terribly high standard." *State v. Weber*, 2016 WI 96, ¶ 55, 372 Wis. 2d 202, 887 N.W.2d 554 (Kelly, J., concurring) (citing *State v. Blatterman*, 2015 WI 46, ¶ 35, 362 Wis. 2d 138, 864 N.W.2d 26). "[A]lthough probable cause must amount to 'more than a possibility or suspicion that the defendant committed an offense,' the evidence required to establish probable cause 'need not reach the level of proof beyond a reasonable doubt or even that guilt is more likely than not.'" *State v. Lange*, 2009 WI 49, ¶ 38, 317 Wis. 2d 383, 766 N.W.2d 551 (quoting *State v. Secrist*, 224 Wis. 2d 201, 212, 589 N.W.2d 387 (1999)).

"[U]nder the exception for exigent circumstances, a warrantless search is allowed when 'there is compelling need for official action and no time to secure a warrant.'" *Mitchell v. Wisconsin*, 139 S. Ct. 2525, 2534 (2019) (citation omitted). "The State bears the burden of proving the existence of exigent circumstances." *State v. Richter*, 2000 WI 58, ¶ 29, 235 Wis. 2d 524, 612 N.W.2d 29.

"The exigent circumstances inquiry is limited to the objective facts reasonably known to, or discoverable by, the officers at the time of the entry." *State v. Kiekhefer*, 212 Wis. 2d 460, 476, 569 N.W.2d 316 (Ct. App. 1997). "When a police officer is confronted with two reasonable competing inferences, one that would justify the search and another that would not, the officer is entitled to rely on the reasonable inference justifying the search." *Mielke*, 257 Wis. 2d 876, ¶ 8. Finally, this Court "do[es] not apply hindsight to the exigency

analysis; [it] consider[s] only the circumstances known to the officer at the time he made the entry and evaluate[s] the reasonableness of the officer's action in light of those circumstances." *Richter*, 235 Wis. 2d 524, ¶ 43.

Here, law enforcement had both probable cause and exigent circumstances to justify any search of Bowers' Dropbox account. First, law enforcement had probable cause. Taylor County's data manager informed Sheriff Daniels that Bowers had shared both paper and electronic county records without permission. (R. 108:6.) Lind was aware that Bowers' Dropbox account contained county property that "should not be out there." (R. 153:18.) This unauthorized sharing of county property was the action that led to the charges against Bowers. (R. 1.) Finally, Bowers admitted to sharing the records prior to the search. (R. 1:5.) Based on this knowledge, there was a "'fair probability' that that contraband or evidence of a crime" would be found in Bowers' Dropbox account. *Robinson*, 327 Wis. 2d 302, 26. Therefore, law enforcement had probable cause. *Id.*

Second, any search was justified by exigent circumstances because the State had an urgent need to figure out what information was shared with whom and to stop it from being disseminated further. Lind testified that at the time of the alleged search, law enforcement did not know exactly what case files Bowers had stored in the Dropbox account. (R. 153:21.) Law enforcement did not know who, or how many people, had access to the case files information Bowers had shared. (R. 153:20–23.) What they knew was that these documents could be accessed, downloaded, deleted, and possibly edited, by anyone, from anywhere in the world, so long as Bowers gave them access to the password to the Dropbox account. (R. 153:21–22.)

As Sheriff Daniels explained, there are "very good reasons" case files cannot be shared without permission. (R. 1:5.) Case files may contain sensitive victim information. They may contain information regarding confidential informants that could be dangerous to release. They may contain confidential medical records. They may contain sensitive financial information. The list goes on and on.

In this case, for example, law enforcement already knew Bowers had shared case files containing medical records in paper form (R. 1:4), and the files Bowers shared turned out to contain juvenile identifying information, (R. 106:2). It was imperative that law enforcement determine, as quickly as possible, what information was shared with whom in order to promptly prevent it from being disseminated any further. In order to prevent the information from spreading any further, law enforcement needed to immediately figure out who had access to the information. Based on the facts known to law enforcement at the time, there was a "compelling need for official action and no time to secure a warrant." *Mitchell*, 139 S. Ct. at 2534 (citation omitted). Therefore, if this Court determines that the examination of Bowers' Dropbox account was a search, the search was nevertheless justified by probable cause and exigent circumstances. *Tullberg*, 359 Wis. 2d 421, ¶ 30.

CONCLUSION

This Court should reverse the decision of the circuit court.

Dated: February 3, 2022.

Respectfully submitted,

JOSHUA L. KAUL
Attorney General of Wisconsin

Electronically signed by:

Nicholas S. DeSantis
NICHOLAS S. DESANTIS
Assistant Attorney General
State Bar #1101447

Attorneys for Plaintiff-Appellant

Wisconsin Department of Justice
Post Office Box 7857
Madison, Wisconsin 53707-7857
(608) 266-8556
(608) 294-2907 (Fax)
desantisns@doj.state.wi.us

CERTIFICATION

I hereby certify that this brief conforms to the rules contained in Wis. Stat. § (Rule) 809.19(8)(b), (bm) and (c) for a brief produced with a proportional serif font. The length of this brief is 5073 words.

Electronically signed by:

Nicholas S. DeSantis
NICHOLAS S. DESANTIS
Assistant Attorney General

CERTIFICATE OF EFILE/SERVICE

I certify that in compliance with Wis. Stat. § 801.18(6), I electronically filed this document with the clerk of court using the Wisconsin Court of Appeals Electronic Filing System, which will accomplish electronic notice and service

Dated this 3rd day of February 2022.

Electronically signed by:

Nicholas S. DeSantis
NICHOLAS S. DESANTIS
Assistant Attorney General