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

REPLY BRIEF 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

PAGES

TABLE OF AUTHORITIES

Cases

Statutes

INTRODUCTION

Police sergeant Steven W. Bowers shared confidential case files without permission with several people, including the producers of a national television show. He shared the files via a folder in a Dropbox account that he created using his official county-owned and monitored email address instead of a personal email address. The State argues in its opening brief that Bowers had no reasonable expectation of privacy in files that were stored on a Dropbox account created with a government-owned email address and that Bowers voluntarily shared with several people.

Bowers raises several arguments in response to the State's opening brief. He argues that he had a reasonable expectation of privacy in the Dropbox files under Wisconsin's six-factor test and that the persuasive authorities relied upon by the State were not applicable. He argues that the third-party doctrine did not apply to this case. Finally, he argues that there was no time-based exigency to justify a warrantless search.

Bowers's arguments fail. Bowers had no reasonable expectation of privacy in the information he stored in a Dropbox account linked to his official county-owned email address and proceeded to share with several people, including producers of a national television show. Bowers's actions do not suggest any reasonable expectation of privacy under persuasive out-of-state case law or under Wisconsin's six-factor test. Finally, in the alternative, exigent circumstances justified the search because the State had a pressing need to stop the spread of confidential and potentially dangerous information.

ARGUMENT

I. There was no Fourth Amendment search because Bowers had no reasonable expectation of privacy.

A. This appeal concerns the merits of the circuit court's Fourth Amendment ruling.

As a starting point, Bowers misunderstands the standard of review. Bowers asserts that the only ruling at issue here is the circuit court's denial of the State's motion for reconsideration. (Bowers's Br. 16.) He therefore asks this Court to ignore the substantive issues in this case and decide only whether the circuit court's earlier ruling was a "manifest error of law or fact." (Bowers's Br. 16.)

Bowers is incorrect—this appeal incorporates the initial ruling. The general rule is that "[a]n appeal from a final judgment or final order brings before the court all prior nonfinal judgments, orders and rulings adverse to the appellant and favorable to the respondent made in the action or proceeding not previously appealed and ruled upon." Wis. Stat. § (Rule) 809.10(4); *Bank of New York Mellon v. Klomsten*, 2018 WI App 25, ¶ 11, 381 Wis. 2d 218, 911 N.W.2d 364.

The cases Bowers cites do not suggest that this case presents an exception to the rule. Instead, they appear to address the issue of whether this Court has jurisdiction to hear a case. *Helmrick v. Helmrick*, 95 Wis. 2d 554, 291 N.W.2d 582 (Ct. App. 1980), for example, was about whether this Court had jurisdiction to hear an appeal at all. This Court explained that it did not have jurisdiction because a notice of appeal was filed prior to the entry of any final order. *Id.* at 556–57. For that reason, this Court was required to dismiss the appeal entirely. *Id.* at 557–58.

In *Koepsell's Olde Popcorn Wagons, Inc. v. Koepsell's Festival Popcorn Wagons, Ltd.*, 2004 WI App 129, ¶ 44, 275

Wis. 2d 397, 685 N.W.2d 853, this Court merely reiterated the standard for reviewing a denial of a motion for reconsideration, which says nothing about whether the appeal may also incorporate the initial ruling. And the problem in *Koepsell* was that "Koepsell's motion was a thinly veiled attempt to introduce evidence that should have been introduced at the original summary judgment phase." *Id.* ¶ 44. Bowers makes no similar allegation here. In short, Bowers has not shown that this Court should ignore the substantive suppression issue that this case is about.

B. Bowers had no reasonable expectation of privacy because the county owned the email address he used to create the Dropbox account.

As argued in the State's opening brief, one reason Bowers had no reasonable expectation of privacy is that the email address he used to create the Dropbox account did not even belong to him. (State's Opening Br. 16.) Instead, it belonged to Taylor County. A person with a reasonable expectation of privacy would have used a personal email address to create a private Dropbox account. (State's Opening Br. 19.)

In this regard, this case is indistinguishable from *Clark v. Teamsters Local Union 651*, 349 F. Supp. 3d 605, 621 (E.D. Ky. 2018). Bowers's attempts to distinguish *Clark* fall short. Bowers first argues that *Clark* is distinguishable because it was a state law invasion of privacy case, not a Fourth Amendment case. As the State explained in its opening brief, however, Kentucky law uses a reasonable expectation of privacy analysis based on the Fourth Amendment for invasion of privacy claims. *See Pearce v. Whitenack*, 440 S.W.3d 392, 401–02 (Ky. Ct. App. 2014); (State's Opening Br. 16). In *Pearce*, for example, the court explained that a claimant's invasion of privacy claim failed because the Fourth Amendment does not recognize a reasonable expectation of

privacy in a public Facebook post. *Id.* at 402. Therefore, the mere fact that *Clark* was an invasion of privacy case does not distinguish it from this case.

Bowers next argues that *Clark* was incorrect because *Clark* held that there was no expectation of privacy in *work* emails, whereas other courts have held that a right to privacy exists in emails more generally. (Bowers's Br. 35 (citing *United States v. Warshak*, 631 F.3d 266, 285–86 (6th Cir. 2010)).) This argument is an equivocation and a red herring. Here, the State never argued that there is no right to privacy in emails in general—only that Bowers did not have a right to privacy in emails sent through his non-private, county-owned work email address. This case has nothing to do with whether there exists a right to privacy in emails more generally. And Bowers does not argue that he had a right to privacy in emails sent to and from his non-private, county-owned email address. If Bowers had used his own private email address, we would not be here. *Clark* cannot be distinguished on this basis either.

For the same reason, Bowers's slippery slope argument fails. Bowers asserts that "[i]f the court accepts the State's arguments, then tens of thousands of Wisconsinites will have their private Dropbox, Google Drive, Microsoft OneDrive, Verizon Cloud, iCloud, and other cloud storage accounts subject to warrantless, government search on the basis that those accounts are not actually private." (Bowers's Br. 14.) This is not true. As the State has pointed out, Bowers did not have a reasonable expectation of privacy in his Dropbox account because he set it up *using an email address that belonged to the county* as opposed to using one that belonged to him. (R. 153:19.) And while Bowers is correct that the use of a password generally heightens an individual's expectation of privacy (Bowers's Br. 32), Bowers overlooks the fact that in this case, he linked a password to an email address that was

not his to keep private.[1] This decision will not impact the tens of thousands of Wisconsinites who use their own email addresses to create cloud-based storage accounts.

Bowers next attempts to distinguish *United States v. Maclin*, 393 F. Supp. 3d 701, 706 (N.D. Ohio 2019), on the basis that in *Maclin*, the defendant shared his entire Dropbox account, whereas here, Bowers shared a specific folder within his Dropbox account. (Bowers's Br. 36–37.) That distinction is immaterial here. The only inculpatory evidence in this case that was recovered from the search of the Dropbox account came from the folder that Bowers shared with his girlfriend and with the television producers. (R. 1:4.) Assuming arguendo that police improperly searched other portions of Bowers's Dropbox account, any error is harmless because that search did not uncover inculpatory evidence.

Finally, contrary to what Bowers argues (Bowers's Br. 28), Bowers did not have a reasonable expectation of privacy under the six *Dumstrey*[2] factors. The first two factors admittedly weigh in Bowers's favor, as he appears to have paid for and, other than using it to share unauthorized case files, maintained the Dropbox account lawfully. (*See* State's Opening Br. 18.) Regarding the third factor, however, Bowers did not maintain control over files that he shared with several other people, including television producers who could have broadcast them to a wide audience. Regarding the fourth factor, the fact that Bowers may have protected the shared case documents with a password (Bowers's Br. 39) is meaningless because he proceeded to share the password-

---

[1] Additionally, courts have found no reasonable expectation of privacy in information that is voluntarily shared with others, even if it is password-protected. *See, e.g.*, *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979)

[2] *State v. Dumstrey*, 2016 WI 3, 366 Wis. 2d 64, 873 N.W.2d 502.

protected documents with several others, including a potential television audience.

Regarding the fifth factor, Bowers may or may not have put his Dropbox to some private use other than sharing unauthorized files. *Dumstrey*, 366 Wis. 2d 64, ¶ 49. The record is not entirely clear as to whether he used the Dropbox account for other purposes. But what is clear is that he used the account—and especially the Murder 3 folder he shared with several other people—for a non-private purpose. And sixth, Bowers's privacy claim is not consistent with historical notions of privacy. Bowers essentially tried to use someone else's lock (his county-owned email address) to hide someone else's property (the unauthorized case files) in his personal storage unit.

C. The third-party doctrine applies here.

Bowers next argues that the third-party doctrine does not apply to this case. (Bowers's Br. 32.) As argued in the State's opening brief, one of the reasons Bowers lacked a reasonable expectation of privacy in the information he stored in his Dropbox folder is that he deliberately shared it with several other people, including the producers of a national television show. (State's Opening Br. 17–18.)

Bowers attempts to create a distinction between content and metadata and asserts that the third-party doctrine applies only to metadata. (Bowers's Br. 32–33.) This distinction does not find support in the case law. In *United States v. Miller*, 425 U.S. 435, 443 (1976), for example, the United States Supreme Court relied on several cases in which content, rather than metadata, was voluntarily turned over to a third party. *See, e.g.*, *Hoffa v. United States*, 385 U.S. 293 (1966) (defendant had no reasonable expectation of privacy in incriminating information about plans to bribe jurors that he voluntarily turned over to a secret informant); *Lopez v. United States*, 373 U.S. 427 (1963) (defendant had no reasonable

expectation of privacy in the content of a phone call, as opposed to merely the numbers dialed).

Additionally, this is not a case involving something like cell phone tracking where a third party such as Verizon simply generates metadata or business records based on a person's cell phone usage. Here, Bowers deliberately chose to share information with several people—including the producers of a national television program who could have broadcast it to a wide audience. This is not the behavior of a person who reasonably expects to keep information private. *See Smith v. Maryland*, 442 U.S. 735, 743–44 (1979).

Bowers next argues that the third-party doctrine does not apply because law enforcement did not happen to obtain the information from one of the third parties. (Bowers's Br. 32.) But the question in Fourth Amendment cases is whether the defendant's expectation of privacy was objectively reasonable. *See, e.g.*, *State v. Tate*, 2014 WI 89, ¶ 25, 357 Wis. 2d 172, 849 N.W.2d 798. And here, law enforcement *knew* that Bowers had disclosed the information to others prior to searching his Dropbox folder. (R. 1:5; 153:18.) Bowers does not explain why the fact that the information was not actually obtained via a third party would affect whether he had a reasonable expectation of privacy.

Similarly, Bowers's argument that *United States v. Caira*, 833 F.3d 803 (7th Cir. 2016), is inapplicable here falls short. (Bowers's Br. 26.) The State cited *Caira* for the general proposition that a person has no reasonable expectation of privacy in information he voluntarily turns over to third parties. (State's Opening Br. 16–17.) As explained above, this is true regardless of whether that information consists of content or metadata. The fact that *Caira* happened to involve metadata is immaterial.

For all these reasons and the reasons explained in the State's opening brief, Bowers had no reasonable expectation

of privacy in the information he stored in a Dropbox folder created with the county's email address and then voluntarily shared with several other people.

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 attempt to limit its spread.

A. There was probable cause for the search.

Bowers does not appear to dispute that there existed probable cause to believe he had committed a crime. Probable cause means there is 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).

Here, Taylor County's data manager had informed law enforcement that Bowers shared confidential case files without permission in both paper and electronic form. (R. 108:6.) Bowers himself admitted in writing that he shared the files. (R. 1:5.) And IT Director Melissa Lind knew at the time of the search that Bowers's Dropbox contained county property that "should not be out there." (R. 153:18.) Therefore, probable cause existed here. *Robinson*, 327 Wis. 2d 302, ¶ 27.

B. Exigent circumstances justified the warrantless search.

As stated in the State's opening brief (State's Opening Br. 22–23), the exigency here was that sensitive and confidential information had been spread and was at risk of being spread further. Bowers misunderstands the State's argument in this regard. According to Bowers, "The State is saying that the department believed that Bowers could have shared the files with more people, thus committing more

crime, and so it should have been allowed to intervene and stop it." (Bowers's Br. 42.) This is not what the State argued. Rather, the State argued that since Bowers shared confidential information with others, *anyone* who Bowers gave access to the information could have disseminated it even further. (State's Opening Br. 22–23.) Any of those people, in turn, would then be able to continue spreading the confidential information. The State needed to quickly identify the people who had access to this information to prevent it from spreading further.

This was indeed an emergency. The State already knew that Bowers had shared confidential medical records with Cold Justice producers, as well as his girlfriend. (R. 1:4.) And the records he disclosed via Dropbox contained juvenile identifying information. (R. 106:2.) As argued in the State's opening brief, the State had a compelling need to keep this sensitive information from being spread any further, whether by Bowers or by others. (State's Opening Br. 23.)

Bowers is correct that it took two days after learning he shared the files to search the Dropbox account. (Bowers's Br. 41.) But this was not without reason. IT Director Lind first contacted Dropbox directly, expecting to remedy the situation without the need for a search. (R. 153:17–18.) However, Dropbox was not cooperative. (R. 153:17–18.) Law enforcement then sought legal advice from the county's district attorney before searching the Dropbox account. (R. 108:12.) The fact that law enforcement first tried unsuccessfully to obtain the information by other means does not make what happened here any less of an emergency.

Bowers also points out that the State did not cite a case with facts similar to this one, in which a court has found an exigency based on release of confidential information. (Bowers's Br. 42.) But as the State argued in its opening brief, the facts of this case fit within the traditional legal framework of an exigency. The State argued that case files can contain

information that could be dangerous to release, such as information about confidential informants, juvenile identifying information, etc. (State's Opening Br. 23.) Protecting an individual's safety is a traditionally accepted circumstance that can justify an exigency. *Robinson*, 327 Wis. 2d 302, ¶ 30.

Finally, Bowers asserts that the State "has never in the litigation of this issue identified a time-based exigency." (Bowers's Br. 43.) On the contrary, the State did raise this argument in the circuit court. (R. 154:6; 157:4 ("Law enforcement needed to know both what had been shared and with whom and needed to cut off access to those persons as quickly as possible to prevent further dissemination.").)

CONCLUSION

This Court should reverse the decision of the circuit court.

Dated this 14th day of July 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

FORM AND LENGTH 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 2,825 words.

Dated this 14th day of July 2022.

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 for all participants who are registered users.

Dated this 14th day of July 2022.

Electronically signed by:

Nicholas S. DeSantis
NICHOLAS S. DESANTIS
Assistant Attorney General