STATE OF WISCONSIN
COURT OF APPEALS
DISTRICT III
CASE NO. 2021AP001767

STATE OF WISCONSIN,

Plaintiff-Appellant,

v.

STEVEN W. BOWERS,

Defendant-Respondent,

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

DEFENDANT-RESPONDENT'S RESPONSE BRIEF

R. Rick Resch
Wisconsin Bar No. 1117722
John H. Bradley
Wisconsin Bar No. 1053124

Strang Bradley, LLC
613 Williamson St., Suite 204
Madison, Wisconsin 53703
[608] 535-1550

Attorneys for Defendant-Respondent

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES AND CONSTITUTIONAL AMENDMENTS

LAW REVIEW ARTICLES AND BOOKS

STATEMENT ON ORAL ARGUMENT AND PUBLICATION

Oral argument is not requested because it is anticipated that the briefs will fully present the legal arguments on appeal. Publication may be warranted because this appeal involves the application of the Fourth Amendment to relatively new technology, which is of substantial and continuing public interest. Wis. Stat. § 809.23(1)(a)2., 5.

STATEMENT OF ISSUES

1. Whether the State established in its motion to reconsider that the circuit court made a manifest error in concluding that Bowers had a reasonable expectation of privacy in his password-protected Dropbox account?

   The circuit court answered: No. The circuit court concluded that:

   > the Defendant's Dropbox account, which was stored on the Dropbox server not owned by Taylor County, was not subject to the 2012 Taylor County IT policy and further finds that the Defendant did have an expectation of privacy in his Dropbox account. This finding is consistent with the Court's prior decision.

   R. 159 at 6–7.

   This court should affirm.

2. Whether the State established in its motion to reconsider that, if Bowers had a reasonable expectation of privacy in his Dropbox account, the circuit court made a manifest error in concluding that there were not exigent circumstances justifying the warrantless search.

   The circuit court answered: No. The circuit court concluded that:

   > Ms. Lind had testified that Dropbox does archive files for a period of time after they are deleted. The Court finds that Ms. Lind did not look into the period of time that the files would be archived.

> Therefore, the Court would find that exigent circumstances did not exist to justify Taylor County accessing this account without a warrant.

R. 159 at 11.

This court should affirm.

STATEMENT OF THE CASE

I. Introduction

This Court should align Fourth Amendment law with the expectations of millions of Americans.

The Taylor County Sheriff's Department searched the private cloud storage of Defendant Steven Bowers, a then-deputy with Taylor County. The department searched Bowers's Dropbox without consent and without a warrant, claiming that it was not a "search," meaning that Bowers did not have a reasonable expectation of privacy in his cloud storage.

But the Fourth Amendment is explicit:

> The right of the people to be secure in their persons, houses, ***papers, and effects***, against unreasonable searches and seizures, shall not be violated, . . .

U.S. Const. Amend IV (emphasis added).

Files stored on the cloud are 21st century papers and effects. And a Dropbox is a 21st century private container for such papers and effects. A Dropbox therefore may not be searched and seized without a warrant, unless an exception to the warrant requirement applies. *See Riley v. California*, 573 U.S. 373, 382 (2014).

Bowers created his Dropbox account. He paid for it. He password protected it. The Dropbox stored files on Dropbox servers, not Taylor County servers. Bowers shared specific *files* from his account with others, but he never shared the *account* with others.

At bottom, the Taylor County Sheriff's Department searched private information on outside servers by accessing a private account. They simply used the internet as a device to access those servers. They didn't search their own devices. They didn't receive documents from a third party. And they didn't just obtain specific files. The department searched and seized Bowers's *entire* Dropbox account.

The extension of Fourth Amendment protection to cloud-stored data and the accounts that hold the data is implied by United States Supreme Court precedent. *See id. and Carpenter v. United States*, 138 S.Ct. 2206, 2219 (2018). *Riley* and *Carpenter* are two landmark opinions that seek to bring the Fourth Amendment into the 21st century by applying the Fourth Amendment protection of privacy to new technologies. And yet, the State's opening brief has zero citations to *Riley* or *Carpenter*.

If 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.

It doesn't matter that cloud storage devices contain non-private information. Consider a government employee who takes her laptop home at night. The government can presumably demand the return of the laptop and may be able to search its contents. That doesn't mean the government can enter her house without a warrant to retrieve the laptop. *O'Connor v. Ortega*, 480 U.S. 709, 715–16 (1987) (government employers may sometimes search "those areas and items that are related to work and are generally within the employer's control.").

Let's also suppose that the government employee uses her work laptop to access her personal Gmail account. Google has access to her emails. The people she sends the emails have access to those specific emails. But no emails are stored locally on the laptop. The government cannot use its own desktop computer to access the employee's emails on her Gmail account and stored on Google servers just because she may have created some of her emails on a government internet connection and sent those emails to other people. *See id., United States v. Maxwell*, 45 M.J. 406, 417–19 (C.A.A.F.

1996), *United States v. DiTomasso*, 56 F. Supp. 584, 592 (S.D.N.Y. 2014), *and United States v. Warshak*, 631 F.3d 266, 285–86 (6th Cir. 2010) ("Given the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection.").

The upshot is clear. Bowers, like many American, had a reasonable expectation of privacy in his personal, password protected Dropbox account. That conclusion is not destroyed by the fact that he used his Taylor County email address to create the account. The account was still his, after all, and the county never gave any indication it would, under any circumstances, recover his password and take over his account. And his expectation of privacy was not destroyed by the fact that third parties had some access to some of the information in his Dropbox account. As we'll see below, that's not how the third-party doctrine works. Under the third-party doctrine, the government can access, without a warrant, the business records created by third parties and turned over by third parties, and the government can access metadata about information but not the contents of the information. *See United States v. Miller*, 425 U.S. 435 (1976) *and Smith v. Maryland*, 442 U.S. 735 (1979).

That's not what happened here, however. The government accessed Bowers's personal Dropbox account by creating a new password and logging on through the internet. And it searched his entire Dropbox, content and all, not just metadata.

Nor does the exigent circumstances exception to the warrant requirement apply here. There simply was no exigency. The sheriff's department waited two days to search Bowers's Dropbox after it concluded that Bowers had shared confidential files with a TV show called *Cold Justice*. The State contends that it couldn't wait for a warrant because it was worried that Bowers would destroy evidence or share the files further. It still, even on appeal, hasn't explained why if the situation was so exigent, the department didn't act like it. The circuit court concluded there was no exigency. It found there was time for the government to obtain a warrant. At bottom, there was no imminent risk of destroyed evidence and no exigency so compelling that there was no time to wait for a warrant. *Brigham City, Utah v. Stuart*, 547 U.S. 398, 403 (2006); *Kentucky v. King*, 563 U.S. 452, 460 (2011).

Finally, there are two important things for this to court to consider when it reviews the below facts and arguments. The State here has appealed a denied motion to reconsider, not a granted motion to suppress. And second, there has been parallel federal litigation on the Fourth Amendment issues in this case.

First, the State is appealing a motion to reconsider, and so it carries a heavy burden. *See* R. 163 and 164. Although the State fashions its brief as an appeal of the order to suppress *and* the motion to reconsider, this Court does not have jurisdiction over the general order to suppress. "An oral ruling must be reduced to writing and entered before an appeal can be taken from it." *Helmrick v. Helmrick*, 95 Wis. 2d 554, 556, 291 N.W.2d 582 (Ct. App. 1980). The State here appeals from a written order entered on 14 September 2022, in which the circuit court denied the State's motion to reconsider. R. 163 and 164. That order specifically said, in total, "For the reasons stated on the record at the July 15, 2021 Oral Ruling, the State's Motion to Reconsider is Denied. This is a final order for purposes of appeal." R. 163 (emphasis and paragraph break removed). Thus, this Court has jurisdiction over only the appeal of the State's motion to reconsider. *See Helmrick*, 95 Wis. 2d at 556.

"To prevail on a motion for reconsideration, the movant must present either newly discovered evidence or establish a manifest error of law or fact." *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 ("*Koepsell's*, 275 Wis. 2d 397"). A "manifest error" is the "'wholesale disregard, misapplication, or failure to recognize controlling precedent.'" *Id.* (quoting *Oto v. Metro. Life Ins. Co.*, 224 F.3d 601, 606 (7th Cir. 2000)).

Second, there is parallel litigation in this case. While Bowers was being prosecuted, he also brought an action in federal court, under 42 U.S.C. § 1983, against the Taylor County Sheriff and Information Technology Director who searched his Dropbox. On a slightly different factual record, albeit derived from the same facts, the district court concluded on summary judgment that Bowers's Fourth Amendment rights were violated, but the Sheriff and IT Director were entitled to qualified immunity because Bowers's rights were not

clearly established. *Bowers v. County of Taylor*, No. 20-CV-928-JDP, 2022 WL 1121376, at *1 (W.D. Wis. Apr. 14, 2022).

The standards are thus flipped here. In the criminal case, Bowers initially bore the burden on his motion to suppress. *State v. Rindfleisch*, 2014 WI App 121, ¶18, 359 Wis. 2d 147, 857 N.W.2d 456. In the civil case, Bowers also bore the burden to establish a Fourth Amendment violation that was clearly established. *Volkman v. Ryker*, 736 F.3d 1084, 1090 (7th Cir. 2013). But in the criminal case, now, the State must show that the circuit court disregarded, misapplied, or failed to recognize—wholesale—controlling precedent. *Koepsell's*, 275 Wis. 2d 397, ¶44.

This Court should affirm the circuit court and find that, like the federal district court did, that Bowers had a reasonable expectation of privacy in his Dropbox. Neither of those findings, by the circuit court or the district court, were wholesale misapplications of controlling precedent.

II. Factual background

The facts presented here and throughout this brief reflect those in the record, and Bowers discusses them as though they are all true for the purpose of appeal only.

A. Bowers shares cold-case files with a TV show brought in by his employer to investigate cold-case files.

In 2017, Steven Bowers was a detective with the Taylor County Sheriff's Department. R. 108 at 04:21–05:03, 15:08.

The State is prosecuting Bowers with two felonies for sharing cold-case homicide files with a TV show that Taylor County brought in to solve, and film itself solving, cold-case homicide files. R. 25 at 1 (Information); R. 1 at 2 (Complaint).

Specifically, Bowers is accused of sharing two sets of files—one by paper and one by Dropbox. This appeal concerns only the warrantless search of the Dropbox file. *Accord* Br. of Appellant at 8, n.1.

In February of 2017, the Taylor County Sheriff's Department and Taylor County agreed to bring in the TV show *Cold Justice* to try and solve a cold-case homicide, "Murder 1."[1]

B. Daniels learns that Bowers had shared a cold-case file on Dropbox but doesn't search the Dropbox until two days later.

On 27 February 2017, Taylor County Sheriff, Bruce Daniels, became aware that two cold-case files, Murder 2 and Murder 3, may have been shared with the staff of *Cold Justice*. R. 97; R. 108 at 14:25–15:16. Bowers responded in less than two hours, just before 7:00pm, saying there he indeed did share two cold-case files. R. 97. He explained that the department and TV show had been working well together, and he thought *Cold Justice* could help with the other two files if they were interested in them. *Id.* By the time Daniels sent his initial email, he had already known that files had been released—physically and digitally by Dropbox. R. 108 at 25:23–26:22.

So on February 27th, Daniels knew that a cold-case file, Murder 3, had been shared on Dropbox. And he knew that Bowers was the one who shared it. And yet Daniels waited until March 2nd to search the Dropbox. R. 153 at 18:24–19:03, 20:03–05.[2]

C. Daniels, the DA, and the IT Director search Bowers's personal, password-protected Dropbox, which had no information stored on Taylor County property.

The Dropbox account was Bowers's personal Dropbox account, set up by Bowers and paid for with his own money. R. 108 at 14:11–23; R. 153 at 26:14–20. It was password protected. R. 153 at 26:21–23. Dropbox offers cloud storage, and all of Bowers's files on his Dropbox were stored on servers outside of Taylor County. R. 153 at 26:07–13, 31:16–23.

---

[1] The Complaint and the Appellant use the names "Murder 1," Murder 2", and "Murder 3" for the cold-case files. R. 1 at 2; Br. of Appellant at 7. Respondent does the same.

[2] *See State v. Subdiaz-Osorio*, 2014 WI 87, ¶73, 357 Wis. 2d 41, 849 N.W.2d 748 ("The State has the burden to prove that exigent circumstances justified the search.").

The IT Director reached out to Dropbox to try and access the account, but Dropbox refused because the account belonged to Bowers. R. 153 at 17:24–18:16, 28:01–15.

But Bowers had used his work email with Taylor County to create his personal account. R. 153 at 19:05–14. So, Daniels ordered the IT Director to lock Bowers out of his work email, reset his Dropbox password, and use the new password to search Bower's Dropbox account. R. 153 at 18:24–20:08, 22:12–22.

III. Procedural Background

In October of 2017, the State charged Bowers with violating Wis. Stat. § 946.12(2), which criminalizes misconduct in public office. R. 1.

A. Bowers moves to suppress the fruits of the warrantless, nonconsensual search of his Dropbox account.

Bowers moved to suppress the information learned in the search of his Dropbox, analogizing to *Carpenter v. United States*, 138 S.Ct. 2206 (2018). R. 44 at 1–2.

The Court held a hearing on the motion, in which Taylor County Sheriff Bruce Daniels testified. R. 108. The State's focus on that hearing was on Exhibit 1, a document titled "Information Technology Agreement for Authorized Users of Taylor County Network." R. 96; *see* R. 108 at 6–9, 39:12–21. That IT Policy is from 2007. R. 96. The last sentence of it says, "I have no expectation of privacy for any material on Taylor County equipment, even if that material was generated for my personal use." *Id.* The State made no mention of the third-party doctrine. *See generally* R. 108.

Its argument was that Bowers has signed away his expectation of privacy, *as to government equipment*. Given the chance to argue, the State argued that Bowers, because of the IT Policy, had no expectation of privacy in his email communication. R. 108 at 39:10–21.

Bowers responded, pointing a large flaw in that argument: "It is one thing to say we have the right to review his e-mails, we have the right to review anything that is created on basically a county-owned

platform, it's another thing completely to say once that we do that, we can then use that password to basically search anything else you possibly own." R. 108 at 40:18–24. Bowers's defense attorney analogized to UW-Madison using the defense attorney's UW email account to recover the passcode for counsel's home front door and then using the code to actually enter his house and poke around. R. 108 at 40:25–09.[3]

B. The Circuit Court's 11 February 2020 Oral Ruling

The circuit court then issued an oral ruling, denying the motion to suppress. R. 107. The circuit court emphasized that last sentence of the IT Policy agreement. R. 107 at 3. It concluded that "Mr. Bowers has no expectation of privacy in his private account that was used on Taylor County equipment." R. 107 at 4.

C. Bowers moves to reconsider.

Bowers then moved to supplement the record and requested that the circuit court reconsider its ruling that denied Bowers's motion to suppress. R. 119. Bowers emphasized to the court in his motion that the place search *was not Taylor County equipment*. R. 119 at 1–2. He also informed that court that the 2007 IT Policy was not in effect at the time of the search, and that there had been superseding polices in the meantime. R. 119 at 7–9.

The circuit court held a hearing, in which it considered the motion to reconsider and other motions. R. 138. The State then conflated Bowers's Taylor County email with Bowers's personal Dropbox, arguing that the "Dropbox was not a personal account as it was set up with a county e-mail. There is no argument that [that] county e-mail is a personal internet account of an employee." R. 138 at 20:07–16. Bowers requested to respond to that argument in writing, which the circuit court agreed to. R. 138 at 23.

---

[3] *See Riley v. California*, 573 U.S. 373, 397 (2014) (searching a cellphone incident to arrest "would be like finding a key in a suspect's pocket and arguing that it allowed law enforcement to unlock and search a house.")

Bowers replied in writing. R. 137. He pointed out that Daniels had testified that the Drobox account was Bowers's personal account, and that Taylor County did not pay for the account. R. 137 at 4.

D. The Circuit Court's 14 December 2020 Oral Ruling

The circuit court then held another hearing, at which it issued an oral ruling on Bowers's motion to reconsider. R. 140. The circuit court acknowledged that there had been updates to the county's technology policy since the 2007 policy it had relied on in its first ruling. R. 140 at 04:15–06:16. The circuit court also recognized Bowers's argument that "the defendant's Dropbox account was not stored on Taylor County property but on a third-party server that the defendant personally obtained and paid for on his own." R. 140 at 06:17–21.

The circuit court made a factual finding that the November 15, 2012 Taylor County IT Policy was controlling when the Dropbox was searched and not the previous 2007 policy it had relied on. R. 140 at 08:25–09:04. It also found that a cellphone policy from 2011 was also in effect at the time of the search. R. 140 at 09:04–08.

The circuit court then granted Bowers's motion on two separate bases. First, it concluded that the updated policies created a reasonable expectation of privacy for Bowers "because the defendant was allowed to use one smartphone for work and personal use." R. 140 at 09:08–21.

The circuit court then made an even more important ruling: It concluded that the Dropbox account was Bowers's personal account. R. 140 at 10:15–11:15.

1. The circuit court concluded that Bowers had an expectation of privacy in his Dropbox, regardless of which device he used to access it.

This is key to this appeal. The State has not argued on appeal that an IT Policy justified the search. *See* Br. of Appellant at 14–20. The circuit court now recognized, and factually found, that Taylor County did not own the Dropbox and therefore it was not located on Taylor County equipment. *Id.* Specifically, the circuit court concluded:

> Therefore, the Court finds that the defendant could access his Dropbox account, which was not housed on Taylor County equipment, by a smartphone that was being used by Mr. Bowers for his personal use and with the consent of Taylor County. The Court finds that the defendant 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 at 11:01–11 (emphasis added). It therefore granted Bowers's motion and suppressed the fruit of the unlawful, warrantless search of Bowers's Dropbox. R. 140 at 11:12–15.

E. The State moves to reconsider.

After the circuit court's decision, the State moved for reconsideration. R. 143. It sought to present testimony from the Taylor County IT Director. *Id.* at 1. It took issue with the circuit court's factual findings regarding which IT policy was active at the time of the search and which device Bowers used to access his Dropbox. *Id.*

The circuit court then held a hearing, at which Taylor County IT Director Melissa Lind testified. R. 153. Lind's testimony did not help the State on the issue of who owned the Dropbox.

Lind explained that Dropbox is a cloud storage company, and a person can access Dropbox from any computer with internet access because Dropbox information is not stored locally. R. 153 at 17:02–13, 27:07–13. She also explained that Bowers's account was password protected. R. 153 at 26:05–06. She told the court that Bowers's Dropbox was not paid for by Taylor County and was set up by Bowers with his own money. R. 153 at 26:14–20.

Lind also testified that she had asked Dropbox to grant her access to the account, but Dropbox refused because the account belonged to Bowers. R. 153 at 28:01–15.

And Lind admitted that the sheriff's department search was *not* of Taylor County property:

> Q. What you actually searched was the Dropbox server; is that correct?
> A. Correct.

> Q. And that Dropbox server was not owned by you?
> A. Correct.

R. 153 at 36:21–25. She conceded that Dropbox servers are located throughout the United States, are not controlled by Taylor County, and do not belong to Taylor County. R. 153 at 31:16–23, 35:17–16. Finally, Lind admitted the county's IT policies did not allow her to search privately owned, non-Taylor County, property, and that she had never before used an email recovery to access another person's private account. R. 154 at 32:11–20, 39:19–24.

The State also added an exigent circumstances argument. Lind testified that she was concerned that Bowers could potentially have deleted the files on his Dropbox before another way was found to access it. R. 153 at 23:01–13. But on direct she also admitted that when a person deletes a file from Dropbox, Dropbox will store those files for another 30 days. R. 153 at 22:12–19. And on cross she admitted that she could have asked Dropbox, when she contacted them, to preserve the files on Bowers's account, but she failed to do so. R. 153 at 30:07–10.

The State filed another document making arguments in support of its motion. R. 154. The State's brief was broken into three parts. First, the State argued that Bowers did not have a reasonable expectation of privacy in his phone or email address. *Id.* at 2–3. Second, it argued that courts in other jurisdictions had held that people don't have an expectation of privacy in their Dropbox accounts. *Id.* at 3–4. And third, it argued that there were exigent circumstances justifying the search because the sheriff's department was worried about destruction of evidence. *Id.* at 5–6.

As to the latter two arguments, the State offered no reasoning for how they met the standard for a motion to reconsider. *See* Wis. Stat. § 806.07(1); *see Koepsell's*, 275 Wis. 2d 397, ¶44. As to the first argument, the State claimed that the circuit court had made its ruling on inaccurate or incomplete information because it did not have the benefit of Lind's testimony when it ruled. R. 154 at 1.

F. The Circuit Court's 15 July 2021 Oral Ruling

The circuit court denied the State's motion. R. 159. The circuit court recognized that "in order to prevail on a motion for reconsideration the burden is on the moving party and the moving party must present either newly discovered evidence or establish a manifest error of law or fact." R. 159 at 03:08–12.

The circuit court again found that Bowers had an expectation of privacy in his Dropbox account "which was stored on the Dropbox server not owned by Taylor County." R. 159 at 06:24–07:04.

The circuit court also concluded that none of Bowers's work devices were ever searched and there was no evidence that his Dropbox was ever synced on Taylor County property. R. 159 at 07:14–08:04. It observed that the sheriff's department would have been justified in searching Bowers's emails on his Taylor County email account, but it did not do that—it searched his Dropbox. R. 159 at 08:11–24.

As to the out of jurisdiction opinions, the circuit court distinguished them as different types of searches for different types of information. R. 159 at 9. Because the State reiterates these arguments on appeal, Bowers will respond to them while discussing the circuit court's analysis below in the argument section of this brief. *See* Br. of Appellant at 16–17.

And as to exigent circumstances, the circuit court made a common-sense finding that Lind's own testimony showed that deleted files on Dropbox would've been archived and that the sheriff's department had ample time to obtain a warrant before then. R. 159 at 11:02–21, 16:08–12. The State also argued that there was an exigency because it was concerned that Bowers might share confidential information again. It never offered a factual basis for inferring that Bowers had any desire or reason to share the files again and it never cited any cases supporting the idea that sharing confidential information could be an exigency. *See* R. 154 at 6 *and* R. 159 at 15:11–16:01 and 17:20–18:04.

ARGUMENT

I. The warrantless search of Bowers's Dropbox was unreasonable because Bowers had a reasonable expectation of privacy in it and there were no exigent circumstances.

Bowers, like millions of Americans, has an expectation of privacy in his personal Dropbox account. He created the account. He paid for it. He protected it with a password. And there were no exigent circumstances justifying a warrantless search. Indeed, the sheriff's department waited two days to search the Dropbox.

The State here cannot meet its burden to show that the circuit court abused its discretion when it found that Bowers had an expectation of privacy in his Dropbox account and that the sheriff's department had time to obtain a warrant but didn't.

Bowers had a reasonable expectation of privacy in his Dropbox. A Dropbox is the digital era equivalent of a storage unit. Both may be operated by a third party. Both allow the lessee to hold items for friends without losing control of the unit. A storage unit is protected by a key. And a Dropbox is protected by a password. Traditional notions of privacy, by way of analogy, show that the Fourth Amendment protects a Dropbox account the way the Fourth Amendment protects a storage unit. *See United States v. Johnson*, 584 F.3d 995, 1001 (10th Cir. 2009) (collecting cases in which courts find that storage units have Fourth Amendment protection).

The remainder of this brief, after discussing the standards of review and legal standards, proceeds as this.

First, millions of Americans use cloud storage, and they expect their files and effects to remain private, especially when their accounts are password protected. *See* Steven Arango, *Cloudy with a Chance of Government Intrusion: the Third-Party Doctrine in the 21st Century*, 69 Cath. U.L. Rev. 723, 725 (2020) *and* Eric Johnson, *Lost in the Cloud: Cloud Storage, Privacy, and Suggestions for Protecting Users' Data*, 69 Stan. L. Rev. 867, 871–72, 885–86 (2017).

Second, the third-party doctrine does not apply here because the sheriff's department did receive documents from a third party, did not obtain business records created by a third party, and did not access mere metadata. *United States v. Miller*, 425 U.S. 435, 440 (1976); *Smith v. Maryland*, 442 U.S. 735, 743 (1979). These nuances were reiterated in *Carpenter*, 138 S.Ct. 2206 (2018). And the Court in *Riley* explicitly sought to protect the privacy of cloud-stored data. 573 U.S. at 397.

Third, the State's non-precedential cases do not support its conclusion. *Koepsell's*, 275 Wis. 2d 397, ¶6. *Clark*, cited by the State, is not a Fourth Amendment case. *Caira* involved the disclosure of metadata by a third party. And the defendant in *Maclin* gave others access to his entire Dropbox account, while refusing to acknowledge that the account even belonged to him.

Fourth, Wisconsin's expectation of privacy factors show that Bowers's Dropbox was protected by the Fourth Amendment. *See State v. Baric*, 2018 WI App 63, ¶18, 384 Wis. 2d 539, 919 N.W.2d 221. Bowers setup up and paid for his Dropbox; he maintained his account lawfully; he kept his account private with a password; he used his Dropbox to store private information; and historical notions of privacy establish that his expectation of privacy was reasonable.

Finally, there were no exigent circumstances here. The sheriff's department had two days to obtain a warrant and it didn't. And the State, still, has identified no cases establishing that a risk of leaked confidential information can create an exigency.

A. Standard of review

1. Motions to reconsider are subject to review under the erroneous discretion standard.

A motion for reconsideration is reviewed under the erroneous exercise of discretion standard. *Koepsell's*, 275 Wis. 2d 397, ¶6. Under that standard, a discretionary decision is affirmed "as long as the court examined the relevant facts, applies a proper standard of law, and used a demonstrated rational process to reach a reasonable conclusion." *Lakeland Area Prop. Owners Ass'n, U.A. v. Oneida Cnty.*,

2021 WI App 19, ¶14, 396 Wis. 2d 622, 957 N.W.2d 605; *State v. Kennedy*, 2008 WI App 186, ¶21, 315 Wis. 2d 507, 762 N.W.2d 412.

The State is appealing a motion to reconsider here. Appeals are taken from orders reduced to writing. *Helmrick v. Helmrick*, 95 Wis. 2d 554, 556, 291 N.W.2d 582 (Ct. App. 1980). The State here appeals from a written order entered on 14 September 2022, in which the circuit court denied the State's motion to reconsider. R. 163 and 164. That order specifically said, in total, "For the reasons stated on the record at the July 15, 2021 Oral Ruling, the State's Motion to Reconsider is Denied. This is a final order for purposes of appeal." R. 163 (emphasis and paragraph break removed). That is the order on appeal in this case. Although the order may have had the "substantive effect" of "suppressing evidence," it is nevertheless an order denying a motion to reconsider. *See* Wis. Stat. § 974.05(1)(d).

B. Applicable legal standards

1. A successful motion to reconsider requires a manifest error of fact or law.

To prevail on its motion to reconsider, the State was required to "present either newly discovered evidence or establish a manifest error of law or fact." *Koepsell's*, 275 Wis. 2d 397, ¶44. A "manifest error" is the "'wholesale disregard, misapplication, or failure to recognize controlling precedent.'" *Id.* (quoting *Oto v. Metro. Life Ins. Co.*, 224 F.3d 601, 606 (7th Cir. 2000)).

The State presented new testimony in support of its motion to reconsider. R. 159. But it never explained how the IT Director's knowledge was newly discovered. Moreover, even if it was newly found information, it didn't show a manifest error of fact. *Koepsell's*, 275 Wis. 2d 397, ¶44. Indeed, the testimony further solidified that Bowers was the owner of his Dropbox account.

Nor did the State establish that the circuit court had made a manifest error of law. *Id.* As the federal district court found in the civil case in which Bowers sued Taylor County and its official for an unlawful search, there is a dearth of caselaw on whether a person has an expectation of privacy in cloud-stored data. *See Bowers v. Cnty. of Taylor*, No. 20-CV-928-JDP, 2022 WL 1121376, at *9 (W.D. Wis. Apr.

14, 2022). The district court concluded that Sheriff Daniels and the IT Director violated Bowers's Fourth Amendment rights, but those rights weren't clearly established. *Id.* at *1. And so the district court granted the Taylor County defendants qualified immunity. *Id.* Thus, caselaw pointed toward Fourth Amendment protection, and no controlling precedent required a conclusion to the contrary.

2. A reasonable expectation of privacy

A person has standing to challenge a search or seizure when he has a reasonable (sometimes termed legitimate) expectation of privacy in the place searched. *Rakas v. Illinois*, 439 U.S. 128, 139 (1978); *Katz v. United States*, 389 U.S. 347, 360 (1967) (Harlan, J., concurring). Fourth Amendment standing is different from other types of "standing" in the law; it is part of the substantive law of the Fourth Amendment. *Rakas*, 439 U.S. at 138–39. Sometimes whether someone has Fourth Amendment standing is analyzed in terms of whether or not something is a "search." *See e.g.*, *Riley*, 573 U.S. at 400 ("There is no dispute that the officers engaged in a search of Wurie's cell phone.").

All of these terms get at the same thing. If a person has a legitimate expectation of privacy in an area, it is protected by the Fourth Amendment. *United States v. Jones*, 565 U.S. 400, 405–06 (2012)

There are, at least, two tests to determine whether someone has Fourth Amendment standing, one under trespass rules and one under *Katz*. *Jones*, 565 U.S. at 409 ("[T]he *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test.") (emphasis in original); *accord State v. Dumstrey*, 2016 WI 3, ¶28, 366 Wis. 2d 64, 873 N.W.2d 502; *see Florida v. Jardines*, 569 U.S. 1, 11 (2014) (Because the Court found Fourth Amendment standing under trespass rules, it did not need to decide whether there was also standing under *Katz*).

The same Fourth Amendment rules apply to digital spaces as other spaces. *Baric*, 384 Wis. 2d 359, ¶19.

To determine whether someone has Fourth Amendment standing, courts look to the totality of the circumstances. *Id.*, 18. Some non-exhaustive factors include (1) whether a person had a property interest, (2) whether he was lawfully on the property, (3) whether he

had control over the property, (4) whether he took precautions to ensure his privacy, (5) whether property was put to private use, and (6) whether the claim of privacy is consistent with historical notions of property. *Id.* Courts also consider more normative factors, including societal expectations. *Minnesota v. Olson*, 495 U.S. 91, 98 (1990) ("To hold that an overnight guest has a legitimate expectation of privacy in his host's home merely recognizes the everyday expectations of privacy that we all share. Staying overnight in another's home is a longstanding social custom that serves functions recognized as valuable by society.").[4]

3. The State carries the burden to prove exigent circumstances.

And if an area is protected by the Fourth Amendment, law enforcement presumably needs a warrant to search it. *Arizona v. Gant*, 556 U.S. 332, 338 (2009). That presumption is "subject only to a few specifically established and well-delineated exceptions." *Id.* The only exception raised here is the exigent circumstances exception. *See* Appellant's Br. at 20–23.[5]

The exigent circumstances exception requires urgency. Here, the State must prove that the sheriff's department had an urgent need to search Bowers's Dropbox, that the department had probable cause to believe the Dropbox contained evidence of a crime, and that there was not enough time for the department to obtain a warrant. *State v. Robinson*, 2010 WI 80, ¶24, 327 Wis. 2d 302, 786 N.W.2d 463.

Law enforcement's fear of destroyed evidence can be an exigency, but the fear must be of "imminent" destruction. *King*, 563 U.S. at 460.

---

[4] The differing Fourth Amendment tests for standing have caused confusion in the legal field. *See* Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 Stan. L. Rev. 503, 505 (2007).

[5] In the federal civil case, the district court concluded that the government employer exception to the warrant requirement didn't apply, but also that that conclusion wasn't clearly established. *Bowers*, 2022 WL 1121376 at *10–*12; *see O'Connor*, 480 U.S. at 724 (discussing the government employer exception). The civil defendants did not argue that exigent circumstances justified the search.

C. Bowers had a reasonable expectation of privacy in his Dropbox account.

It's important to consider the different types of government actions that might have been searches and seizures here. First, the sheriff's department searched Bowers's Taylor County email account. Second, they used a password recovery to seize his Dropbox password. Third, they used the new password to seize his Dropbox account. And fourth, they used the new password to search Bowers's Dropbox account.

Consider also the different searches and seizures the sheriff's department *could have* done but did not. First, they could've obtained information from Bowers's Dropbox directly from Dropbox with a subpoena or warrant. Second, they could've obtained access to the files shared by Bowers directly from the *Cold Justice* crew members who had access to them. And third, they could have searched Bowers's physical devices (his work computers and phone) to determine whether any of the Dropbox files were synced locally and not only on Dropbox servers. They did not choose any of these options.

Also note what the State is not arguing here anymore. It is not arguing that the Taylor County IT Policy allowed the sheriff's department to take over and search Bowers's Dropbox, and it is not arguing that the sheriff's department searched any locally stored information. *See* Br. of Appellant at 14–20. This is wise decision. The circuit court made a factual finding that the Dropbox was not located on Taylor County property and that no Taylor County property was searched. R. 159 at 07:14–08:04. This factual finding was not a manifest error. *Koepsell's*, 275 Wis. 2d 397, ¶44. It was consistent with the IT Director's testimony. R. 153 at 36:21–25.

What Bowers challenged was the search of his entire Dropbox account—not single files held by multiple people. This distinction is important. The third-party doctrine is not a simple rule, as we shall see. Bowers may not have had standing to challenge the sheriff's department search if it had obtained metadata, if it had obtained information created by third party, or if it had obtained information from a third party. But that's not what happened.

Bowers here never shared his password with anyone; the sheriff's department cancelled his password and created a new one. R. 153 at 18:24–20:08, 22:12–22. And the sheriff's department took over and searched Bowers's account; it did not receive records or information consensually (or by subpoena or warrant) from third parties. *See id.*

Bowers had a legitimate expectation of privacy in his Dropbox account. Millions of Americans also expect their cloud-stored documents, files, and photographs to be private. This is especially so when the account is password protected.

1. Society expects privacy in password protected cloud storage accounts.

Whether a person has a legitimate expectation of privacy in searched or seized property, depends upon societal expectations. *Olson*, 495 U.S. at 98. Americans expect their cloud storage accounts to remain private, even if the information is stored on a third-party server and even if they occasionally share files from their accounts with other people. The State argues that the third-party doctrine and sharing files destroys a person's expectation of privacy in cloud storage accounts. Br. of Appellant at 14–19. Not so. The State's analysis fails to fully analyze the third-party doctrine and fails to consider the expectations of millions of cloud-storage using Americans.

"Cloud computing is the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself." *Riley*, 573 U.S. at 397. "The term 'cloud computing' is based on the industry usage of a cloud as a metaphor for the ethereal internet. An external cloud platform is storage or software access that is essentially rented from (or outsourced to) a remote public cloud service provider, such as Amazon or Google." *United States v. Cotterman*, 709 F.3d 952, 965, n.12 (9th Cir. 2013) (alterations removed) (quoting David A. Couillard, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 Minn. L.Rev. 2205, 2216 (2009)).

Upwards of 80% of Americans own a smartphone. Steven Arango, *Cloudy with a Chance of Government Intrusion: the Third-Party Doctrine in the 21st Century*, 69 Cath. U.L. Rev. 723, 725 (2020). Dropbox and

Google Drive, just two of the most prominent cloud storage companies, combined have 1.5 billion users world-wide. *Id.*

A cloud storage account, like Dropbox, is a 21st century container used to hold private papers and effects. *See* U.S. Const. Amend. IV. Many Americans hold deeply private information in cloud storage, ranging from important documents to family photographs, to banking information. And they "often may not know whether particular information is stored on [their] device or in the cloud, and it generally makes little difference." *Riley*, 573 U.S. at 397.

And a person's expectation of privacy is heightened when he hides private information behind a password, as Bowers did here. *See Antonelli v. Sherrow*, 246 Fed. App'x. 381, 384 (7th Cir. 2007); *see United States v. Buckner*, 473 F.3d 551, 554 n.2 (4th Cir. 2007) (recognizing a reasonable expectation of privacy in password-protected computer files); *see Trulock v. Freeh*, 275 F.3d 391, 403 (4th Cir. 2001) (Plaintiff had a reasonable expectation of privacy in his password-protected computer files); *Scherer Design Grp., LLC v. Ahead Eng'g LLC*, 764 F. App'x 147, 156 (3d Cir. 2019) (private tort, but collecting constitutional cases) ("A cursory review of our sister circuits shows that the mere use of a password to protect an account or files generally conveys a clear intent to prevent others' access. This preserves a user's reasonable expectation of privacy as to the bypassing intruder.").

2. The third-party doctrine does not apply here because the sheriff's department did not access files from, or created by, a third party.

The third-party doctrine limits the expectation of privacy of some types of information available to third parties. A person has an expectation of privacy in the contents of his digital information. That expectation of privacy can be destroyed, however, when a third party uses the information and creates its own records with it. The sheriff's department searched Bowers's Dropbox account, which was created by him, and was not a business record. Further, they searched the contents of his Dropbox and not merely metadata.

People have an expectation of privacy in the content of their information, though they may lack an expectation of privacy in surface-level identifying information or metadata. Thus a person has

an expectation of privacy in the contents of a phone call. *Katz*, 389 U.S. 351-52. But not in the privacy of the numbers he dials. *Smith*, 442 U.S. at 743. Likewise, a person has an expectation of privacy in the contents of things he mails, but not in the information on the outside of the letter of package. *United States v. Jacobsen*, 466 U.S. 109, 114 (1984); *see Ex parte Jackson*, 96 U.S. 727, 733 (1877). Let's call this the *Smith* distinction.

The Supreme Court has carved out an apparent exception to this rule. Records generated and held by a business do not carry an expectation of privacy. Thus, in *Miller*, the Court held that bank records were not Miller's private papers. 425 U.S. at 440. "On their face, the documents subpoenaed here are not respondent's 'private papers.' Unlike the claimant in *Boyd*, respondent can assert neither ownership nor possession. Instead, these are the business records of the banks." *Id.* (referring to *Boyd v. United States*, 116 U.S. 616 (1886)). Let's call this the *Miller* exception.

Thus we have a rule. A person has an expectation of privacy in the *content* of his information, but not surface level metadata. *Smith*, 442 U.S. at 741 (upholding *Katz*) ("Yet a pen register differs significantly from the listening device employed in *Katz*, for pen registers do not acquire the *contents* of communications." (emphasis in original).

The constitutionality of warrantless searches of noncontent data came to a head in *Carpenter*. 138 S.Ct. 2206. In *Carpenter*, the Supreme Court concluded that law enforcement needs a warrant to access cellphone location data. *Id.* at 2221. The issue was whether a person has a legitimate expectation of privacy in their cellphone location data. *Id.* at 2219–20. The Court observed that cellphone location data reveals an "encyclopedic" amount of personal information. *Id.* at 2216. But, it also observed, the cellphone data would seem to trigger the *Smith* distinction and the *Miller* exception. *Id.* at 2216 ("At the same time, the fact that the individual continuously reveals his location to his wireless carrier implicates the third-party principle of *Smith* and *Miller*. But while the third-party doctrine applies to telephone numbers and bank records, it is not clear whether its logic extends to the qualitatively different category of cell-site records."). The Court ultimately carved out an exception from *Miller*, holding "that an individual maintains a legitimate expectation of privacy in

the record of his physical movements as captured through [cell-site location information]." *Id.* at 2217.

The Taylor County Sheriff's Department here did not seize metadata and it did not search Dropbox's business records. The third-party doctrine does not apply to the type of search performed here.

Moreover, the Supreme Court has recognized that *Smith's* content-noncontent distinction extends to cloud-stored data. *Riley*, 573 U.S. at 398. In *Riley*, the Court held that law enforcement officers need a warrant to search cellphones. *Id.* at 403. In doing so, the Court discussed the privacy interests in a cellphone by leading with a discussion about cloud data. *Id.* at 397. The Court reasoned that a cellphone differs from a container in that it potentially contains data not stored on the phone. *Id.* Thus the cellphone (much like the password here) can function as a key:

> Such a search would be like finding a key in a suspect's pocket and arguing that it allowed law enforcement to unlock and search a house. But officers searching a phone's data would not typically know whether the information they are viewing was stored locally at the time of the arrest or has been pulled from the cloud.

Id. The Court then compared cloud-stored data to papers and effects. The Court concluded that the privacy interests at stake in a cellphone were great because a search of the cellphone could extend "well beyond papers and effects in the physical proximity of an arrestee." *Id.* In other words, the government needs a warrant before it can access a container that contains cloud-stored papers and effects.

Thus, as was implied in the pre-digital *Smith*, became express in the modern *Riley*: the content data stored in the cloud, on remote servers, are Fourth Amendment papers and effects. *Id.*; *Smith*, 442 U.S. at 741; *compare to Miller*, 425 U.S. at 440 (no legitimate expectation of privacy because bank business records were not private papers); *see O'Connor*, 480 U.S. at 716 (workplace doctrine search case) ("While whatever expectation of privacy the employee has in the existence and the outward appearance of the luggage is affected by its presence in the workplace, the employee's expectation of privacy in the *contents* of the luggage is not affected in the same way.") (emphasis in original).

With this framework in mind, we can see why the cases cited by the State don't apply to the facts here.

As a threshold matter, or a threshold reminder, because this is a review of a motion to reconsider, the State must show that the circuit court committed a manifest legal error. *Koepsell's*, 275 Wis. 2d 397, ¶44. The State cites cases outside of this jurisdiction. Those cases are not controlling precedent and therefore cannot show manifest legal error. *Id.* (concluding that the circuit court properly denied a motion to consider where the moving party "did not demonstrate that there was a disregard, misapplication or failure to recognize *controlling precedent*") (emphasis added).

Regardless, the out-of-jurisdiction cases cited by the State are materially distinguishable.

a. *Clark* does not apply because it did not use a Fourth Amendment analysis.

The first case cited by the State is not a Fourth Amendment case. Br. of Appellant at 16 (citing *Clark v. Teamsters Loc. Union 651*, 349 F. Supp. 3d 605, 621 (E.D. Ky. 2018)).

Clark is a state law invasion of privacy case. 349 F. Supp. At 621. The Fourth Amendment does not appear in the opinion, nor do any Fourth Amendment cases. *See Rakas*, 439 U.S. at 143 (property and tort law distinctions should not guide Fourth Amendment law). There is no discussion of *Smith, Miller, Riley,* or *Carpenter*. The reasoning used by the decision is also questionable. The court concluded that Clark did not have an expectation of privacy in his personal Dropbox account because Clark did not have an expectation of privacy in his work emails. 349 F. Supp. at 622. Had this analysis used the Fourth Amendment law of its own circuit, it would have reached a different conclusion. *Clark* observed that an employee does not have an expectation of privacy in work emails "even in the absence of a company email policy." *Id.* 621. But the Six Circuit does explicitly recognize a Fourth Amendment expectation of privacy in emails. *Warshak*, 631 F.3d at 285–86.

b. *Caira* does not apply because there the government obtained metadata from a third party.

The second case cited by the State illuminates the third-party rules and actually shows why the search here was unlawful. Br. of Appellant at 16–17 (citing *United States v. Caira*, 833 F.3d 803 (7th Cir. 2016)).

In *Caira*, the government used a subpoena to obtain a criminal suspect's internet protocol address (IP address) from Microsoft. *Caira*, 833 F.3d at 805. The Seventh Circuit concluded that Caira did not have a legitimate expectation of privacy in his IP address. *Id* at 806. In doing so, it analogized to *Miller* and *Smith*. *Id.*

The exceptions prove the rule. In *Caira*, like in *Miller*, the government obtained records from a third-party. And in *Caira*, like in *Smith*, the government obtained noncontent information—an IP address. An IP address is surface level metadata, it is not content. *See Smith*, 442 U.S. at 741 (upholding *Katz*) ("Yet a pen register differs significantly from the listening device employed in *Katz*, for pen registers do not acquire the *contents* of communications." (emphasis in original).

That's different from what happened in this case. The sheriff's department searched Bowers's entire Dropbox account. It did not seek specific files or metadata from Dropbox. To make it an even comparison, the government in *Caira* would have had to have searched Caira's entire computer, after defeating his password, so that they could find his IP address. The IP address itself may not have been protected by the Fourth Amendment, but Caira's computer very much would have been. *See State v. Ramage*, 2010 WI App 77, ¶¶7–18, 325 Wis.2d 483, 784 N.W.2d 746 (upholding the search and seizure of a computer only because consent was offered by an individual who was allowed by the defendant to use the computer without a password).

The same applies here. Even if the shared files were not Fourth Amendment protected, that does not mean that Bowers had no reasonable expectation of privacy in his entire Dropbox account.

c. *Maclin* does not apply because there the defendant shared access to his entire Dropbox.

The third case cited by the State contains a major factual distinction. Br. of Appellant at 17 (citing *United States v. Maclin*, 393 F. Supp. 701,

706 (N.D. Ohio 2019)). The defendant in *Maclin* shared his password and the entire account was shared with other people. *Maclin*, 393 F. Supp. At 711. Maclin didn't even claim the account was his. *Id.* In other words, he and his conspirators used the Dropbox like a peer-to-peer service, which is what the court analogized it too. *Id*. (citing *United States v. Conner*, 521 Fed. App'x 493, 498 (6th Cir. 2013) (a LimeWire case)).

Moreover, a peer-to-peer service is fundamentally different than a cloud storage account like Dropbox. A peer-to-peer service, unlike a cloud storage application, allows anyone, including law enforcement, to access and view files held on the peer-to-peer network. *Baric*, 384 Wis. 2d 359, ¶¶21, n.6, 22.

3. Bowers's expectation of privacy was reasonable under Wisconsin factors.

A Dropbox is a digital-age container used to store private papers and effects. *See Riley*, 573 U.S. at 397–98; *see* Eric Johnson, *Lost in the Cloud: Cloud Storage, Privacy, and Suggestions for Protecting Users' Data*, 69 Stan. L. Rev. 867, 871–72, 885–86 (2017).

"[T]he 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." *Baric*, 384 Wis. 2d 359, ¶19. Society expects privacy in cloud storage accounts. This is true whether the issue is analyzed under a normative analysis, a multi-factor property analysis, or both. "Fourth Amendment decision making relies heavily on analogies[.]" Kerr, *Fourth Amendment Models*, 60 Stan. L. Rev. at 526.

And the best analogy here is a storage unit:

> Traditional storage areas—such as lockers, storage units, and safety deposit boxes—have long been used to store an individual's private documents and effects. And courts have afforded Fourth Amendment protection to such storage areas.[] Now, as information is increasingly produced and stored in digital form, cloud storage has become the digital equivalent of a traditional storage area.

Johnson, *Lost in the Cloud: Cloud Storage, Privacy, and Suggestions for Protecting Users' Data*, Stan. L. Rev. at 886 (note omitted).

A person can lease a storage unit. The owner of the storage unit may maintain the right to perform maintenance on the unit. The owner may even have the ability to consent to government agents entering the unit. The person leasing the unit might keep things in his storage unit that are not necessarily private. He may allow friends and family to use his storage unit. He may allow friends and family to accompany him to check his storage unit. But none of that defeats his objective expectation of privacy in a storage unit for which he pays and for which he controls the key. *See Johnson*, 584 F.3d at 1001 (10th (collecting cases finding a legitimate expectation of privacy in a storage unit or similar area).[6]

In addition to the normative values and analogy described above, Bowers's reasonable expectation of privacy is illuminated by the Wisconsin factors. *Baric*, 384 Wis. 2d 359, ¶18. For reference, these are the non-exhaustive factors:

> (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.

Id.

a. Bowers bought and paid for his Dropbox account.

The State concedes that the first two factors support Bowers's claim of privacy. Br. of Appellant at 18. First, Bowers paid for his Dropbox

---

[6] While a Dropbox is like a storage unit, a peer-to-peer network is more like a public bulletin board. If someone knows where the bulletin board is, she can take what she wants from it or post her own information to it. Anyone can, really, if they know where to look. These attributes make peer-to-peer networks especially useful to people who pirate intellectual property. *See Glacier Films (USA), Inc. v. Turchin*, 896 F.3d 1033, 1035–36 (9th Cir. 2018).

account and acquired it himself. Second, Bowers maintained his account lawfully.

b. Bowers excluded others from his Dropbox account by keeping his password to himself and only sharing specific files on his terms.

The remaining factors also support Bowers. For the third factor, the State uses the wrong scope. *Id.* at 18. Bowers had complete control over his Dropbox *account*. He shared specific *files* with other people. If anything, this illustrates his control. He decided who saw what and under what circumstances in his Dropbox. This is similar to a person allowing a friend to store a bike in his storage unit. The friend has access to the bike, so long as the storage unit owner allows him access to it.

The State argues that Bowers's privacy was diminished because the sheriff's department was able to access his account. Br. of Appellant at 18. This is a dangerous argument. The State shouldn't be able to defeat an expectation of privacy by merely having the capability to access something. The Supreme Court has rejected a similar argument and refused to leave Americans "at the mercy of advancing technology." *Kyllo v. United States*, 533 U.S. 27, 35–36 (2001). Moreover, keeping with our analogy, the Sixth Circuit has found a Fourth Amendment violation where an investigator found a key to a storage unit and used the key to open the unit. *Garcia v. Dykstra*, 260 Fed. App'x. 887, 898 (6th Cir. 2008).

c. Bowers made his Dropbox account private by using a password.

For the fourth factor, Bowers took privacy precautions by protecting his Dropbox account with a password. The State again uses the wrong scope. Bowers protected his Dropbox account with a password, showing his intention of privacy. *Buckner*, 473 F.3d at 554, n.2 (recognizing a reasonable expectation of privacy in password-protected computer files). Bowers could not have expected that Taylor County would recover his password and lock him out of his account because no Taylor County agreement put him on notice of that and Taylor County had never done that before. And, again,

Bowers shared only specific *files* in his account—he kept the entire account private.

d. Bowers, like most Dropbox users, stored private information on his account.

For the fifth factor, Bowers did put his Dropbox to private use. When the IT Director testified, everyone including her assumed that there was private information on the Dropbox. The Director acknowledged that Bowers's Dropbox could have contained photographs and personal documents. R. 153 at 27:21–25. And she implicitly recognized that there were personal files on the Dropbox. She was asked if she would have searched the Dropbox had it contained "just Mr. Bowers's personal pictures or documents." R. 153 at 21:13–15. Thus, the assumption was that the Dropbox contained county records *in addition to* Bowers's personal information.

e. A Dropbox account is a 21st century device used to store private information.

For the sixth factor, Bowers's claim of privacy in his Dropbox is consistent with historical notions of privacy because it was a digital-age container used to store digital papers and effects. The Dropbox was like a storage container.

And, as discussed above, the privacy in a cloud-storage account is not destroyed by the third-party doctrine. Indeed, courts have held, similarly, that email accounts remain private even though the information stored on them is held by tech companies and the information in them (an email) is almost always shared with another person. *Warshak*, 631 F.3d at 285–86 ("Given the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection."). As the Southern District of New York has explained:

> In today's world, meaningful participation in social and professional life requires using electronic devices—and the use of electronic devices almost always requires acquiescence to some manner of consent-to-search terms. If this acquiescence were enough to waive one's expectation of privacy, the result would either be (1) the chilling of social

> interaction or (2) the evisceration of the Fourth Amendment. Neither result is acceptable.

DiTomasso, 56 F. Supp. 3d at 592.

Thus, all six factors, along with a normative analysis, show that Bowers had a legitimate expectation of privacy in his Dropbox account. And that makes sense. Millions of American store private information in the cloud. Sometimes they don't know whether their information is stored locally on their device or at a remote server, "and it generally makes little difference." *Riley*, 573 U.S. at 397. The sheriff's department here did not obtain information from a third party. It did not obtain mere metadata. It intruded into a deeply personal space, without consent and without a warrant.

The sheriff's department should've obtained a warrant. This is important. A warrant ensures probable cause is found by a neutral magistrate and not by an investigator "engaged in the often competitive enterprise of ferreting out crime." *Johnson v. United States*, 33 U.S. 10, 13–14 (1948). And the warrant process allows a neutral magistrate to control what types of information are sought form a place, where investigators can look for that information, and what information they can seize from that place. *State v. Andrews*, 201 Wis. 2d 383, 390, 549 N.W.2d 210 (1996) ("Search warrants must be issued by a neutral, disinterested magistrate to whom it has been demonstrated that there is probable cause to believe that the evidence sought will aid in prosecution for a particular offense, and the warrant must describe with particularity the place to be searched and things to be seized.").

D. There were not exigent circumstances because there was no emergency.

The sheriff's department waited two days to search Bowers's Dropbox after it discovered that Bowers had shared files with *Cold Justice*. R. 97; R. 108 at 14:25–15:16, 25:23–26:22; R. 153 at 18:24–19:03, 20:03–05.

The exigent circumstances exception to the warrant requirement requires an emergency, such that there's no time for an investigator to obtain a warrant. *Robinson*, 327 Wis. 2d 302, ¶24. The gravamen of

the exigent circumstances exception is an immediate emergency. Exigent circumstances include: the hot pursuit of a suspect, a threat to someone's safety, an imminent risk that evidence will be destroyed, and a risk that a suspect will flee. *Id.*, ¶30. There was no exigency here. There was no risk of "imminent" destruction of evidence. *King*, 563 U.S. at 460. The circuit court reasonably concluded that if Bowers deleted files from the Dropbox they would've been archived, and that the department had ample time to obtain a warrant. R. 159 at 11:02–21, 16:08–12. These findings were not manifest errors. *Koepsell's*, 275 Wis. 2d 397, ¶44. The State wisely does not challenge these findings in its brief. Br. of Appellant at 22–23.

Instead, the State argues that the sheriff's department was concerned that Bowers could have shared the files with more people. *Id.* The State claims there were very good reasons for the department to worry about further sharing of confidential files. A "very good reason" is not an exigency. *Contra id.* at 23 The State cites no cases in which a court concluded that the release of confidential information could be an exigency. Indeed, such a conclusion would chill speech and discourage whistleblowers. *See* Andrew E. Taslitz, *Reconstructing the Fourth Amendment, A History of Search and Seizure*, 1789–1868, New York University Press, at 47, 25 (2006) (arguing that the state's power to search and seize is linked to First Amendment ideas of free expression and has historically too often been used to suppress dissent and difference.")

What the State is describing is probable cause. 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. There are three problems with this argument. First, it defies the rule by requiring only probable cause and not exigent circumstances. Second, it doesn't explain why the sheriff's department waited two days to search the Dropbox. And third, this not even a reasonable inference. The State points to no facts from which it could infer that Bowers was even considering sharing the files further. It just says it may have been possible. Br. of Appellant at 22. Without some caselaw, without "controlling precedent," the State cannot succeed on this argument. *Koepsell's*, 275 Wis. 2d 397, ¶44. The circuit court's conclusion that there was no exigency and that there was in fact time to obtain a

warrant was not a manifest error. *Id.* The State has never in the litigation of this issue identified a time-based exigency.

CONCLUSION

Defendant-Respondent respectfully requests that the Court of Appeals **AFFIRM** the Circuit Court's Order Denying State's Motion to Reconsider. R. 163.

Dated this 16th day of May, 2022.

John H. Bradley
Wisconsin Bar No. 1053124
R. Rick Resch
Wisconsin Bar No. 1117722

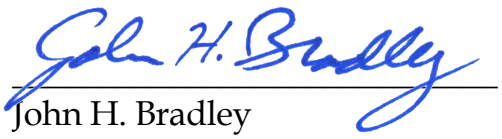
Strang Bradley, LLC
613 Williamson St., Suite 204
Madison, Wisconsin 53703
[608] 535-1550

Attorneys for Defendant-Respondent

CERTIFICATION OF BRIEF COMPLIANCE WITH WIS. STAT. § 809.19(8)(b) and (c)

I certify that this brief conforms with the rules contained in Wis. Stat. §§ 809.19(8)(b) and (c), for a brief produced using proportional serif font. The length of the portions of this brief described in Wis. Stat. §§ 809.19(1)(d), (e) and (f) is 10,829 words. *See* Wis. Stat. § 809.19(8)(c)1.

Dated this 16th day of May, 2022.



John H. Bradley
Wisconsin Bar No. 1053124
R. Rick Resch
Wisconsin Bar No. 1117722

Strang Bradley, LLC
613 Williamson St., Suite 204
Madison, Wisconsin 53703
[608] 535-1550

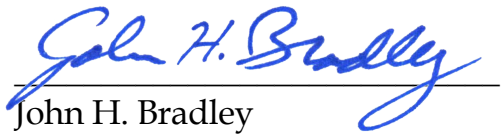
Attorneys for Defendant-Respondent

CERTIFICATE OF EFILE/SERVICE

I hereby certify that:

I have submitted an electronic copy of this brief, which complies with the requirements of Wis. Stat. § 801.18(6).

Dated this 16th day of May, 2022.



John H. Bradley
Wisconsin Bar No. 1053124
R. Rick Resch
Wisconsin Bar No. 1117722

Strang Bradley, LLC
613 Williamson St., Suite 204
Madison, Wisconsin 53703
[608] 535-1550

Attorneys for Defendant-Respondent