**COURT OF APPEALS**
**DECISION**
**DATED AND FILED**

**December 29, 2022**

**Sheila T. Reiff**
**Clerk of Court of Appeals**

**NOTICE**

**This opinion is subject to further editing. If published, the official version will appear in the bound volume of the Official Reports.**

**A party may file with the Supreme Court a petition to review an adverse decision by the Court of Appeals. *See* WIS. STAT. § 808.10 and RULE 809.62.**

**Appeal No. 2021AP1767-CR** **Cir. Ct. No. 2017CF95**

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

---

**STATE OF WISCONSIN,**

**PLAINTIFF-APPELLANT,**

**V.**

**STEVEN W. BOWERS,**

**DEFENDANT-RESPONDENT.**

---

APPEAL from an order of the circuit court for Taylor County: ROBERT R. RUSSELL, Judge. *Affirmed.*

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

¶1 STARK, P.J. The State of Wisconsin appeals from the circuit court's decision suppressing evidence obtained from a search of Taylor County

Detective Sergeant Steven Bowers' Dropbox[1] account (Account).[2] Bowers used his Taylor County e-mail address to create the Account, which he allegedly used to share confidential sheriff's department case files with the producers of a television show.

¶2 Bowers was charged with misconduct in public office, and he filed a motion to suppress evidence on the basis that law enforcement conducted a warrantless search of his Account in violation of the Fourth Amendment. The circuit court ultimately granted Bowers' motion, and the State filed a motion for reconsideration of that decision, which the court denied. On appeal, the State argues that Bowers had no reasonable expectation of privacy in his Account, and, in the alternative, if a search occurred, the warrantless search was justified by probable cause and exigent circumstances.

[1] Dropbox is a digital file hosting service that allows users to upload, store, and share documents and photographs on the "cloud" that can be accessed remotely. *See* Dropbox, *Features*, https://www.dropbox.com/features (last visited Dec. 13, 2022).

[2] The State filed its notice of appeal after the circuit court entered a written order denying the State's motion for reconsideration. When it denied the State's motion for reconsideration, the court upheld its prior oral decision granting Bowers' motion for reconsideration, which granted Bowers' motion to suppress evidence after initially denying his motion. Bowers argues that "[t]he State here has appealed a denied motion to reconsider, not a granted motion to suppress." Despite Bowers' arguments, neither party appears to argue that the court's reasoning for either its February 11, 2020 oral decision denying Bowers' initial motion to suppress evidence or its December 14, 2020 oral decision granting Bowers' motion for reconsideration should be affirmed on appeal. Instead and as we will explain below, Bowers and the State developed a different record through motions to supplement and an additional evidentiary hearing. Thus, the court's oral ruling and subsequent September 14, 2021 written order arguably concluded that suppression was appropriate based on entirely new grounds. Given that the court did not issue a written order from its December 14, 2020 oral ruling granting Bowers' motion to reconsider and given that the court provided new bases for suppression of the evidence based on the State's motion for reconsideration, we conclude that the question before us is appropriately whether the court properly granted suppression of the evidence in this case.

¶3 For the reasons that follow, we conclude that Bowers had a reasonable expectation of privacy in the contents of his Account. Although it was established using Bowers' county e-mail address, Bowers paid to create the private Account, the Account was password protected and accessible through Bowers' private devices, and the Account was not stored on county property. In addition, although Bowers' Account was held by Dropbox, an independent entity, Bowers did not grant a third party access to his password or the Account when sharing the case files. Thus, law enforcement engaged in a search of Bowers' Account within the meaning of the Fourth Amendment. Further, while law enforcement had probable cause to search the Account for evidence of Bowers' alleged misconduct in office, we conclude that no exigent circumstances justified a warrantless search of the Account. Accordingly, we affirm.

## BACKGROUND

¶4 For the purpose of this appeal, the facts in this case are largely undisputed. In February 2017, the Taylor County Sheriff's Department (the department) was working with the television program "Cold Justice" on a homicide cold case (Murder 1).[3] According to the State, the department agreed to provide information to Cold Justice's producers only about the Murder 1 investigation.

¶5 The State claimed that Bowers shared two additional homicide files (Murder 2 and Murder 3) with Cold Justice without the department's permission. Bowers is alleged to have provided Murder 2's paper file—which included "one

[3] The State and Bowers use the names Murder 1, Murder 2, and Murder 3 for the cold-case files. For consistency, we will do so as well.

box of reports and one box of medical records"—to Cold Justice's producers. As to the Murder 3 information, the State alleged that Bowers uploaded the file to his Account and then used the Account to share the file with his girlfriend and two members of Cold Justice's staff. According to the State, the department became aware of this unauthorized release of information when another officer overheard Cold Justice's producers talking about the Murder 2 and Murder 3 cases.

¶6 On February 27, 2017, Taylor County's then-Sheriff Bruce Daniels[4] e-mailed Bowers regarding Bowers' release of the Murder 2 and Murder 3 case files.[5] Bowers replied later that day, admitting that he had shared the files without seeking permission. As a result, the department, with help from the Taylor County Information Technology (IT) Department, sought to gain access to Bowers' Account by first contacting Dropbox on March 1, 2017. According to IT Director Melissa Lind, Dropbox was not "cooperative," stating that it "would have to run through different chains to turn over any documents from anyone's account."

¶7 The department then successfully sought to gain access to Bowers' password-protected Account through his official county e-mail address. Bowers had used his county e-mail address to set up his Account, although he paid for it with his own funds. Lind testified that on March 2, 2017, she performed a password reset on Bowers' Account, which then "e-mailed a link to [Bowers' county] e-mail address." Given that she had access to Bowers' county e-mail account through her role in IT, she then entered his e-mail account and used that

[4] Daniels retired from his position in 2019.

[5] Daniels also testified that the department's data records manager informed him that Bowers had shared both paper and electronic versions of the records.

link to change Bowers' Account password, effectively severing Bowers' access to his Account. Lind then personally accessed Bowers' Account "with the [district attorney] and [Daniels] present."[6] According to Lind, the search of Bowers' Account revealed both that the Murder 3 file was in the Account and that Bowers had shared the case file with individuals outside the department. Lind testified that prior to accessing the Account, she did not know exactly what was in Bowers' Account or with whom Bowers may have shared information.

¶8 The State initially charged Bowers with one count of felony misconduct in public office, contrary to WIS. STAT. § 946.12(2) (2019-20),[7] but the charges were later amended by Information to two counts—one for the disclosure of Murder 2's paper file and one for the disclosure of Murder 3's file via Dropbox. Bowers filed a motion to suppress the evidence derived from the warrantless search of his Account on the ground that he had a reasonable expectation of privacy in that Account and the search therefore violated his Fourth Amendment rights. Bowers also argued that his e-mail confession admitting that he shared the files was obtained in violation of ***Garrity v. New Jersey***, 385 U.S. 493 (1967), and could not be used in subsequent criminal proceedings.

¶9 The circuit court held a hearing on the motion to suppress, where Daniels testified regarding the circumstances behind the department gaining access to Bowers' Account. At that hearing, the State's argument focused on an

[6] Daniels testified that prior to instructing Lind to access Bowers' e-mail and Account, he sought "legal advice" from the district attorney.

[7] All references to the Wisconsin Statutes are to the 2019-20 version unless otherwise noted. We note that there are no changes between the 2017-18 and 2019-20 versions of WIS. STAT. § 946.12.

IT agreement that Bowers had signed in 2007 (the 2007 policy). The 2007 policy stated, "I have no expectation of privacy for any material on Taylor County equipment, even if that material was generated for my personal use." It further provided that "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." During the suppression hearing, the State argued that "[t]he IT policy makes it very clear that when someone starts using their county e-mail, they have no expectation of privacy" and that "[t]here was no reason for the IT Department or [Daniels] to believe they had anything but the right to review those communications."

¶10 In an oral ruling, the circuit court denied Bowers' motion to suppress. In reaching its decision, the court reiterated the terms of the 2007 policy, explaining that it gave the county's IT department permission "to monitor all information technology usage, and to access any electronic communication at any time." Accordingly, the court concluded that the Fourth Amendment issue was "covered under the terms of" the 2007 policy and Bowers had "no expectation of privacy in his private account that was used on Taylor County equipment."[8]

¶11 In response, Bowers filed a motion to supplement the record and for reconsideration. In particular, Bowers emphasized that "Dropbox is *not stored* on [Bowers'] computer but rather is a separate remote storage facility for digital

[8] The circuit court also found that no violation of ***Garrity v. New Jersey***, 385 U.S. 493 (1967), occurred, as Bowers' employment was not threatened and his confession was voluntary. The alleged ***Garrity*** violation is not at issue in this appeal.

information that one pays to use, [and] none of the data discovered was ever discovered on any Taylor County [e]quipment." He also argued that the 2007 policy was not in effect at the time of the search and that there were other policies—a 2011 policy supplement related to use of his county-issued cell phone, signed by Bowers, and a 2012 update of the 2007 policy (the 2012 policy), which Bowers did not sign—in effect at the time.

¶12 The circuit court changed course. By oral ruling, it granted Bowers' motion for reconsideration, reversed its prior decision, and suppressed the Dropbox evidence. In reaching its decision, the court found that the 2012 policy "was the controlling IT policy at the time of the Dropbox search," not the 2007 policy, and that "under the terms of the 2012 IT policy, [Bowers' Account] was not an account held on Taylor County equipment." The court further found that the cell phone policy, signed by Bowers in 2011, was in effect at the time of the search, and that policy allowed Bowers to use his department-issued cell phone for work and personal use as if it were his own device. Therefore, Bowers "did have a reasonable expectation of privacy in [his cell phone]," which he could use to "access his Dropbox account." Finally, the court found that "Bowers' Dropbox account was a personal account." Ultimately, the court granted suppression on the basis 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."

¶13 The State, in response, filed its own motion for reconsideration and a motion to supplement the record. Lind testified at the subsequent motion hearing, explaining how she gained access to Bowers' Account. According to Lind, under the 2012 policy, "[t]he IT Department reserve[d] the right to monitor all information technology usage, and access any electronic communications at any

time." She reiterated that the county owns the e-mail addresses the employees use, but she explained that "Dropbox is a cloud-based storage center" that can be accessed from "any device with an internet connection" if an individual has a username and password. Thus, Dropbox is tied to an e-mail address, not to a physical device controlled by the county. In particular, she clarified that Bowers' county-issued cell phone was not related to the Account. Finally, Lind explained that had Bowers used his personal e-mail address to set up the Account, she would not have been able to gain access in the same manner.

¶14 Lind also testified regarding the reason why the department acted as it did. She explained that "part of the concern driving the timing of … getting into [Bowers'] Dropbox" was Bowers' ability to "sign[] into the Dropbox account and delete[] files before" the department could investigate. Lind also admitted, however, that Dropbox keeps any deleted files for thirty days and that when she contacted Dropbox, she never asked them to preserve the files in Bowers' Account.

¶15 After the hearing, the State filed a second motion in support of its request for reconsideration. There, the State argued that: (1) Bowers "had no reasonable expectation of privacy in the Dropbox account he created with his Taylor County email address" and the circuit court's ruling—relying on Bowers' expectation of privacy in his county-issued cell phone—was in error because there was no testimony connecting Bowers' cell phone to his Account; (2) other jurisdictions have not acknowledged an expectation of privacy in similar Dropbox accounts; and (3) the department "also had probable cause of a crime and exigent circumstances necessitating a warrantless search."

¶16 The circuit court denied the State's motion for reconsideration. The court found that Bowers' Account was not owned by the county, was not subject to the 2012 policy, and Bowers had an expectation of privacy in the Account. The court observed that the department would have been justified in searching Bowers' county-issued e-mail account, but the department searched his Dropbox, not his e-mail account. On the issue of exigent circumstances, the court reiterated Lind's testimony at the hearing that Dropbox archives files for a period of time; therefore, the court concluded "that exigent circumstances did not exist to justify Taylor County accessing this account without a warrant."[9] The State appeals. *See* WIS. STAT. § 974.05(1)(d)2.

## DISCUSSION

¶17 On appeal, the State argues that the circuit court erred by granting Bowers' motion to suppress evidence for two reasons. First, the State claims that Bowers had no reasonable expectation of privacy in his Account; therefore, there was no "search" within the meaning of the Fourth Amendment.[10] In the alternative, the State argues that even if a search occurred, it was justified by probable cause and exigent circumstances. We review a circuit court's decision on a motion to suppress under a two-part standard. ***State v. Lonkoski***, 2013 WI 30, ¶21, 346 Wis. 2d 523, 828 N.W.2d 552. We will uphold the court's findings

[9] The circuit court did not specifically address the State's argument that it needed to quickly ascertain who may have had access to the information to potentially stop the information from spreading further.

[10] We note that while the State argued in the circuit court that the IT policy—either the 2007 or the 2012 version of the policy—allowed the department to search Bowers' Account, it has abandoned that argument on appeal. Therefore, we will not address that argument. *See* ***A.O. Smith Corp. v. Allstate Ins. Cos.***, 222 Wis. 2d 475, 491, 588 N.W.2d 285 (Ct. App. 1998) ("[A]n issue raised in the [circuit] court, but not raised on appeal, is deemed abandoned.").

of fact unless they are clearly erroneous, but we review the application of the facts to the constitutional principles independently. ***Id.***

## I. Reasonable Expectation of Privacy

¶18 The Fourth Amendment to the United States Constitution provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV.[11] The fundamental purpose of the Fourth Amendment "is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials." ***Camara v. Municipal Ct. of City & Cnty. of San Francisco***, 387 U.S. 523, 528 (1967). An individual's rights under the Fourth Amendment apply where he or she has "a reasonable expectation of privacy in the property or location." ***State v. Guard***, 2012 WI App 8, ¶16, 338 Wis. 2d 385, 808 N.W.2d 718 (2011); ***State v. Tentoni***, 2015 WI App 77, ¶7, 365 Wis. 2d 211, 871 N.W.2d 285 ("In order to have standing to challenge a search on Fourth Amendment grounds, a defendant must have 'a legitimate expectation of privacy' in the area or items subjected to a search." (citation omitted)). It is the defendant's burden to establish, by a preponderance of the evidence: "(1) that he or she had an actual, subjective expectation of privacy in the area searched and item seized and

[11] The Fourth Amendment is made applicable to the states by the Fourteenth Amendment. *E.g.*, ***State v. Kramer***, 2009 WI 14, ¶18 & n.6, 315 Wis. 2d 414, 759 N.W.2d 598. "The Wisconsin Constitution contains a substantively identical provision, art. I, sec. 11, that this court interprets consistently with the Fourth Amendment." ***State v. Richter***, 2000 WI 58, ¶27, 235 Wis. 2d 524, 612 N.W.2d 29.

(2) that society is willing to recognize the defendant's expectation of privacy as reasonable." ***Tentoni***, 365 Wis. 2d 211, ¶7.

¶19 On the second question—whether the defendant's expectation of privacy was objectively reasonable—we consider the factors outlined in ***State v. Dumstrey***, 2016 WI 3, 366 Wis. 2d 64, 873 N.W.2d 502. *See* ***State v. Baric***, 2018 WI App 63, ¶18, 384 Wis. 2d 359, 919 N.W.2d 221. Those factors include:

> (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.*** (alterations in original; citation omitted). "Although these factors guide our analysis, they are not controlling," and "[w]e consider the totality of the circumstances in determining whether an individual has a reasonable expectation of privacy." ***Id.***; *see also* ***Guard***, 338 Wis. 2d 385, ¶17. As relevant to the issue in this case, "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." *See* ***Baric***, 384 Wis. 2d 359, ¶19.

¶20 The State does not appear to challenge Bowers' assertion that he had a subjective expectation of privacy in his Account, *see* ***Tentoni***, 365 Wis. 2d 211, ¶7, arguing only that if Bowers had a subjective expectation of privacy, that expectation was not objectively reasonable. We therefore address only whether

Bowers' expectation of privacy in his Account was objectively reasonable.[12] We begin with an analysis of the ***Dumstrey*** factors. The State admits that the first two factors "cut in Bowers' favor," those factors being that Bowers had a property interest in his Account, as he independently set up and paid for it, and that he maintained the Account lawfully. *See* ***Dumstrey***, 366 Wis. 2d 64, ¶47.

¶21 As to the third factor, the State claims that Bowers did not have "complete dominion and control" over the Account as he shared access with other people, including his girlfriend and employees of Cold Justice. Bowers, however, did not share the password to his Account or otherwise provide others access to his entire Account.[13] Instead, Bowers used his Account to share specific documents

[12] We also note that there was parallel litigation related to this case in federal district court, ***Bowers v. County of Taylor (Bowers I)***, No. 20CV928-JDP, 2022 WL 1121376 (W.D. Wis. Apr. 14, 2022), which the State did not address in its briefing before this court. There, Bowers brought an action, on a slightly different factual record, under 42 U.S.C. § 1983 (2018), against Daniels and Lind for an unlawful search of his Account. As the court explained in that case, there is "uncertainty in the law" on the question of whether a person has an expectation of privacy in cloud-stored data. ***Bowers I***, 2022 WL 1121376, at *9-10. The court nevertheless determined "that Bowers had a reasonable expectation of privacy in his Dropbox account and that defendants should have obtained a warrant before searching his account," but it ultimately concluded that Daniels and Lind were entitled to qualified immunity because Bowers' reasonable expectation of privacy was not clearly established at the time. ***Id.*** at *9. While the federal court's analysis is not dispositive, we find it persuasive and informative under the circumstances. *See* ***City of Weyauwega v. Wisconsin Cent. Ltd.***, 2018 WI App 65, ¶12 n.4, 384 Wis. 2d 382, 919 N.W.2d 609 ("Although federal court decisions, other than United States Supreme Court decisions on questions of federal law, do not bind us, we may follow federal court decisions that we find persuasive.").

[13] While Bowers asserts in his briefing before this court that he "never shared his password with anyone," he fails to provide support for this particular assertion with evidence from the record. The State, however, does not appear to dispute Bowers' claim, noting that he shared the documents, but not specifically alleging that he shared the password to his Account. Further, although Bowers observes that the ***Bowers I*** decision was "[o]n a slightly different factual record, albeit derived from the same facts," that case does state that Bowers did not share his password. *See* ***Bowers I***, 2022 WL 1121376, at *2, *10.

with third parties. As Bowers argues, "[h]e decided who saw what and under what circumstances in his Dropbox."

¶22 The State also claims the fact that Bowers used his county e-mail address to create the Account diminished his dominion and control because "law enforcement was able to gain access using his county-owned e-mail address." We agree with Bowers that this is a slippery slope argument. In essence, the State argues that an individual's expectation of privacy is diminished where a location or an item is accessible or capable of being broken into. *Cf.* ***United States v. Warshak***, 631 F.3d 266, 286 (6th Cir. 2010) ("[T]he mere *ability* of a third-party intermediary to access the contents of a communication cannot be sufficient to extinguish a reasonable expectation of privacy."); ***Kyllo v. United States***, 533 U.S. 27, 35-36 (2001) (discounting an application of the Fourth Amendment that would "leave the homeowner at the mercy of advancing technology"). We agree that under the circumstances of this case, Bowers maintained dominion and control over his Account.

¶23 Next, the State argues that the fourth factor also cuts heavily against Bowers because he took few "precautions customarily taken by those seeking privacy." *See* ***Dumstrey***, 366 Wis. 2d 64, ¶47. The State asserts the same arguments as above, namely that Bowers shared access to his Account and that he used his county-owned e-mail address to create the Account instead of a personal e-mail address. Again, these arguments are unpersuasive. Bowers took privacy precautions to protect his Account by using a password to regulate access to it. *See, e.g.*, ***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); ***United States v. Andrus***, 483 F.3d 711, 719 (10th Cir. 2007) ("Courts addressing the issue of third party consent in the context of computers, therefore,

have examined officers' knowledge about password protection as an indication of whether a computer is 'locked' in the way a footlocker would be."); ***United States v. Thomas***, 818 F.3d 1230, 1241-42 (11th Cir. 2016) (concluding, in a consent--to-search case, that by *not* password protecting his files the defendant "assumed the risk that the other [user] would allow the police to view the computer's contents"). Again, there is nothing in the record to establish that Bowers shared his Dropbox password with anyone; he shared only specific files. Further, Bowers could not have anticipated that using his county-owned e-mail address would destroy his privacy in a password-protected account containing data saved on noncounty property, as he was not given notice of this possibility. *See* ***Bowers v. County of Taylor (Bowers I)***, No. 20CV928-JDP, 2022 WL 1121376, at *8 (W.D. Wis. Apr. 14, 2022) ("[T]he county's IT policy says nothing about monitoring private accounts that are linked to work email. In the absence of a clearer notice from the county, Bowers was entitled to assume that a private account was private.").

¶24 As to the fifth factor, the State claims that "it does not appear that Bowers put the property to some 'private use,'" as he used the Account for sharing county documents with other people. *See* ***Dumstrey***, 366 Wis. 2d 64, ¶47. While it is true that Bowers utilized Dropbox to share the case files, the record is unclear as to whether Bowers used his Account for any other personal purpose. Bowers does not specifically assert that he stored personal documents or files in his Account, but he argues that "everyone including [Lind] assumed that there was private information on the Dropbox" as Lind's testimony "acknowledged that Bowers'[] Dropbox could have contained photographs and personal documents." We agree that given the function of Dropbox as a file-storing and file-sharing service for both personal and business use, a reasonable assumption is that

Bowers' Account contained more than just the county's records and that the Account was put toward some other private use as well. *See* Dropbox, https://www.dropbox.com (last visited Dec. 13, 2022).

¶25 Finally, as to the sixth factor, the State argues that Bowers' claim of privacy is not "consistent with historical notions of privacy." *See* ***Dumstrey***, 366 Wis. 2d 64, ¶47 (citation omitted). According to the State, "[h]istorical notions of privacy do not include spaces that a person shares with others." *See* ***State v. Eskridge***, 2002 WI App 158, ¶19, 256 Wis. 2d 314, 647 N.W.2d 434 (concluding that historical notions of privacy do not include apartment common areas as they are shared areas accessible to and used by other tenants). We disagree with the State's portrayal of a Dropbox account as a shared space. Again, Bowers did not share the password to his Account with other individuals or open the Account to access by others.[14] Instead, he merely shared certain files he had uploaded to that Account with others.

¶26 When an individual uses Dropbox as Bowers did, we are persuaded that a Dropbox account is most reasonably comparable to a modern-day version of a container used to store personal documents and effects. *See* ***Riley v. California***, 573 U.S. 373, 397 (2014) (citing ***New York v. Belton***, 453 U.S. 454, 460 n.4 (1981), for the proposition that a "container" is "any object capable of holding another object"). It is well established that individuals generally have a reasonable

[14] In fact, Dropbox states on its website that "[f]or security reasons, sharing an account with others is not recommended. Sharing your Dropbox password with others also violates the Dropbox Terms of Service." Dropbox, *Help Center: Account Sharing*, https://help.dropbox.com/account-access/share-account (last visited Dec. 13, 2022). Further, Dropbox notes that "[i]t's not necessary to share an account in order to share files with someone. In this case the person you want to share with should create their own account, and then you can send a link to the file." ***Id.***

expectation of privacy in locked or closed containers, *see* ***United States v. Chadwick***, 433 U.S. 1, 13 (1977); ***United States v. Basinski***, 226 F.3d 829, 835 (7th Cir. 2000), which are comparable to password-protected accounts, *see* ***Bowers I***, 2022 WL 1121376, at *7 (noting "the well-established rule that individuals generally have a reasonable expectation of privacy in locked or closed containers, which are comparable to a password-protected account"); ***Andrus***, 483 F.3d at 718-20 (comparing a password-protected computer to locked footlocker or suitcase).

¶27 In particular, Lind testified that "Dropbox is a cloud-based storage center, [that] can be accessed from one device or a thousand devices. As long as you have a username and password, you can get to Dropbox anywhere in the world on any device with an internet connection," and therefore Dropbox is not tied to "a physical device of any kind" and was not stored on county property or controlled by the county. Lind explained that even though she had the e-mail address associated with Bowers' Account, when she contacted Dropbox to obtain access, Dropbox would not provide access to the Account. According to Lind, Dropbox was not "cooperative," telling her that it "would have to run through different chains to turn over any documents from anyone's account," which "could [take] weeks," "because, in their mind, the [A]ccount belonged to" Bowers. In summary, we conclude that an analysis of the ***Dumstrey*** factors under the facts of this case weighs in favor of a finding that Bowers had an objectively reasonable expectation of privacy in the private, password-protected Account that he personally created and maintained on noncounty property.

¶28 The State identifies several cases from other jurisdictions, however, that it argues support its position. First, the State presents ***Clark v. Teamsters Local Union***, 349 F. Supp. 3d 605 (E.D. Ky. 2018), as "helpful in examining

whether an expectation of privacy is objectively reasonable." In ***Clark***, a wrongful termination case alleging a claim for invasion of privacy, an employer accessed Clark's computer after she was terminated and, like in this case, "used a lost password function to recover and review the files in Clark's Dropbox to search for work-related files." ***Id.*** at 621. Clark, like Bowers, had set up the Dropbox account using her work e-mail address. ***Id.*** at 622. 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. ***Id.*** at 621-22. The court's rationale was that if 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.*** at 622.

¶29 We are not persuaded that the ***Clark*** court's decision has any bearing on this case. ***Clark*** is an invasion of privacy case, which involved "intrusion upon seclusion." ***Id.*** It did not address whether an employer's access to an employee's Dropbox account was an objectively reasonable search under the Fourth Amendment. Therefore, in addition to the fact that ***Clark*** hails from a lower federal court in another jurisdiction, the legal analysis in that case was distinct from the legal analysis in this Fourth Amendment case.

¶30 Second, the State invokes the so-called third-party doctrine, arguing that regardless of the ***Dumstrey*** factors, "Bowers lacked a reasonable expectation of privacy in the information he stored in his Dropbox folder [because] he deliberately shared it with several other people, including the producers of a national television show." According to the State, "this sharing alone is fatal to

Bowers' claim that he had any reasonable expectation of privacy in the Dropbox account."

¶31 The third-party doctrine provides that "a person has no legitimate expectation of privacy in information he [or she] voluntarily turns over to third parties." ***United States v. Miller***, 425 U.S. 435, 443 (1976); ***Smith v. Maryland***, 442 U.S. 735, 743-44 (1979). In ***Miller***, for example, the United States Supreme Court held that a bank depositor has no "legitimate 'expectation of privacy'" in financial information that he or she "voluntarily convey[s]" to "banks and expose[s] to [the bank's] employees in the ordinary course of business." ***Miller***, 425 U.S. at 442. According to the Court,

> The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, 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.

***Id.*** at 443 (citation omitted).

¶32 Later, in ***Smith***, the third-party doctrine was applied in the context of information provided to a telephone company. There, the Court held that the government's use of a pen register—a mechanical device used to record numbers dialed on a telephone—was not a search. ***Smith***, 442 U.S. at 736 n.1, 745-46. Considering that the pen register did not record the content of the phone calls, the Court explained that it was doubtful "that people in general entertain any actual expectation of privacy in the numbers they dial." ***Id.*** at 742. According to the Court, when Smith made a call, he "voluntarily conveyed" the numbers he dialed

to the telephone company and, therefore, "assumed the risk" that those records "would be divulged to police." ***Id.*** at 744-55.

¶33 The State also cites ***United States v. Maclin***, 393 F. Supp. 3d 701 (N.D. Ohio 2019), in support of its position that the third-party doctrine applies in this case.[15] ***Maclin*** involved child pornography stored in a Dropbox account and the related warrant-authorized search of that account. ***Id.*** at 706. In that case, although the account was password protected, the defendant shared the password, and therefore access to the account, with multiple individuals. ***Id.*** at 711. The defendant further "trie[d] to distance himself from any association with the account." ***Id.*** As a result, the United States District Court for the Northern District of Ohio held that the defendant had no reasonable expectation of privacy in the Dropbox account, explaining that "[c]ourts have consistently held there is no reasonable expectation of privacy in files contained in peer-to-peer sharing services." ***Id.***

¶34 Apart from the fact that ***Maclin*** falls outside our jurisdiction, we conclude that it is distinguishable based on the facts of the case. Unlike the defendant in ***Maclin***, who shared his password—and thereby access to his entire account—with other people and did not even claim ownership of the account, *see* ***id.*** at 711, Bowers did not share his password or disclaim ownership of his Account. Further, based on the fact that Maclin shared his password, the court analogized his use of Dropbox as more akin to a peer-to-peer network sharing service and recognized a lack of reasonable expectation of privacy in files shared

[15] The State also cites ***United States v. Caira***, 833 F.3d 803 (7th Cir. 2016), but it argues in its reply brief that it did so only "for the general proposition that a person has no reasonable expectation of privacy in information he [or she] voluntarily turns over to third parties."

on those platforms. *See* ***id.***; *see also* ***Baric***, 384 Wis. 2d 359, ¶¶21-22. However, a peer-to-peer service is different from a cloud-based storage account like Dropbox. For example, "[a] crucial aspect of peer-to-peer file-sharing is that the default setting for these networks is that downloaded files are placed in the user's 'shared' folder, which allows others in the network to access the files." Audrey Rogers, *From Peer-to-Peer Networks to Cloud Computing: How Technology is Redefining Child Pornography Laws*, 87 ST. JOHN'S L. REV. 1013, 1031 (2013) (citation omitted). In contrast, "[a] cloud user may permit shared access to his [or her] files by designating users," but "[u]nlike peer-to-peer networks, private cloud services require that a person designate who may have shared access." ***Id.*** at 1032. Here, Bowers did not use his Dropbox like a peer-to-peer network: he did not share his password, and he individually designated who could have access to certain files.

¶35 Bowers argues that the third-party doctrine does not apply under the circumstances given the current case law. Initially, we recognize that the application of the third-party doctrine in the context of a cloud-storage account like Dropbox is both unclear and undeveloped. *See generally* Steven Arango, *Cloudy with a Chance of Government Intrusion: The Third-Party Doctrine in the 21st Century*, 69 CATH. U. L. REV. 723 (2020); Eric Johnson, Note, *Lost in the Cloud: Cloud Storage, Privacy, and Suggestions for Protecting Users' Data*, 69 STAN. L. REV. 867 (2017); David A. Couillard, Note, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 MINN. L. REV. 2205 (2009). Bowers argues, however, that "[t]he extension of Fourth Amendment protection to cloud-stored data and the accounts that hold the data is implied by United States Supreme Court precedent" in ***Carpenter v. United States***, 138 S. Ct. 2206 (2018), and ***Riley***. Specifically,

Bowers claims that the third-party doctrine does not apply to the type of search that occurred here because the department did not gain access to the files from a third party; the Account itself was not a business record, like in ***Miller***; and the information was not "surface-level identifying information or metadata,"[16] like in ***Smith***.

¶36 Bowers argues that these important distinctions between ***Miller*** and ***Smith*** were drawn by the Supreme Court in ***Carpenter***. There, the issue was whether the third-party doctrine applied to cell phone location data obtained from wireless carriers. ***Carpenter***, 138 S. Ct. at 2211-12. Law enforcement used Carpenter's cell-site location information to establish that he was near the locations of several robberies when they occurred and then charged him with those robberies. ***Id.*** at 2212-13. In concluding "that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through [cell-site location information]," the Court "declined to extend ***Smith*** and ***Miller*** to cover these novel circumstances." ***Carpenter***, 138 S. Ct. at 2217. The Court recognized the limits of the ***Miller*** and ***Smith*** decisions, noting that the decisions "did not rely solely on the act of sharing" but involved other considerations. ***Carpenter***, 138 S. Ct. at 2219. Ultimately, the Court reasoned that "[g]iven the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection" because there is "world of difference between the limited types of personal information addressed in ***Smith*** and ***Miller*** and the

[16] Black's Law Dictionary defines "metadata" as "[s]econdary data that organize, manage, and facilitate the use and understanding of primary data." *Metadata*, BLACK'S LAW DICTIONARY 1186 (11th ed. 2019).

exhaustive chronicle of location information casually collected by wireless carriers today." ***Carpenter***, 138 S. Ct. at 2217, 2219.

¶37 Additionally, Bowers points to the Supreme Court's decision in ***Riley***, where the question was "whether the police may, without a warrant, search digital information on a cell phone seized from an individual who has been arrested." ***Riley***, 573 U.S. at 378. The ***Riley*** Court held that "the search incident to arrest exception does not apply to cell phones" and that law enforcement "must generally secure a warrant before conducting such a search," subject to "other case-specific exceptions." ***Id.*** at 386, 401-03.

¶38 In reaching this conclusion, the Court addressed privacy interests in a cell phone by referencing the phone's ability to access cloud-stored data. ***Id.*** at 397. According to the Court, a cell phone differs from a "container whose contents may be searched incident to an arrest" as it may potentially "display data stored on remote servers rather than on the device itself" that would "extend well beyond papers and effects in the physical proximity of an arrestee." ***Id.*** at 397-98. As a result, the government conceded that "the search incident to arrest exception may not be stretched to cover a search of files accessed remotely—that is, a search of files stored in the cloud," and the Court reasoned that "[s]uch 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." ***Id.*** at 397. Thus, Bowers argues that what 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."

¶39 We agree with Bowers that the third-party doctrine does not apply to the type of search performed here. We are persuaded by the ***Bowers I*** court's discussion, which explained that

> ***Smith*** and ***Miller*** are about an expectation of privacy in particular information; the question in both cases was whether the government needed a warrant before seeking information from a third party who also has access.
>
> In this case, Bowers isn't contending that he had a right to keep the case files themselves private. Bowers'[] claim is about restricting access to his account, not protecting the particular files at issue or preventing third parties from sharing the files. One can lose a right to keep information private by disclosing it to the public, but that doesn't mean the government can force entry into someone's home on the ground that the home contains public documents. As another example, if someone sends an email to a friend, the Fourth Amendment won't prevent the friend from sharing the contents of the email with the police, but that doesn't mean the police are entitled to hack an email account because all the emails are being shared with a third party.

***Bowers I***, 2022 WL 1121376, at *8 (citation omitted).

¶40 We agree that Bowers is not arguing that he had a reasonable expectation of privacy in the case files turned over to the Cold Justice employees. The department could have obtained the documents from that third party without ever searching Bowers' Account if it simply desired the documents.[17] To be clear, while Bowers does not have a reasonable expectation of privacy in the contents of the files in his Account that were created by other parties, he does have a reasonable expectation of privacy in the contents of his Account, which is what the department searched. Further, the department did not gain access to Bowers'

[17] In fact, according to the complaint, the department did receive the case file from Murder 2 back from the Cold Justice producer.

Account through the Dropbox company or from any other third-party company that had access to the Account. *See* ***id.*** ("Many cases involving the third-party doctrine involve information that the government actually received from the third-party.").

¶41 Instead, the department seized control of Bowers' private Account located on servers outside the department by using Bowers' county-owned e-mail address to change his Dropbox password.[18] It then accessed and searched the information in his Account. The department did not receive the evidence from a third party, and it did not simply obtain specific files from Bowers' Account. The department seized and searched at least portions of, if not all of, Bowers' Account. Accordingly, the third-party doctrine cases that the State relies upon are inapt under the circumstances of this case. We agree with Bowers that the Court's decisions in ***Miller*** and ***Smith*** do not clearly control the department's actions here, as the department did much more than obtain access to metadata or Dropbox's business records.

¶42 The State focuses on the fact that Bowers created this Account with his county-owned e-mail address. Apart from using that e-mail address, however, Bowers created the Account on his own. Bowers paid for the Account with his own money, and the Account was password protected. The department did not search its own devices to access the information in Bowers' Account; it used the internet as a tool to access the outside server on which the Account was located. Apart from the 2007 or the 2012 policies, which the State no longer argues are

[18] "A seizure deprives an individual of 'dominion over his or her person or property' …." ***State v. Brereton***, 2013 WI 17, ¶23, 345 Wis. 2d 563, 826 N.W.2d 369 (citation omitted).

applicable, the State does not cite any other terms or agreements that would destroy Bowers' reasonable expectation of privacy in his Account and allow the department to access it. In essence, the State does not explain how using a county e-mail address to set up an outside account permits the county to search everything within that private account, absent other factors.

¶43 Use of cloud storage to house an individual's private information is just the latest technological development seeking to test the boundaries of the Fourth Amendment. *See* ***Warshak***, 631 F.3d at 285 ("[T]he Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish."); ***Kyllo***, 533 U.S. at 34 (warning that advancing technology must not be permitted to "erode the privacy guaranteed by the Fourth Amendment"). As Bowers argues, cloud storage has become the equivalent of "a 21st century container used to hold private papers and effects." *See* ***Bowers I***, 2022 WL 1121376, at *7; Johnson, *supra*, at 886 ("Now, as information is increasingly produced and stored in digital form, cloud storage has become the digital equivalent of a traditional storage area."); Couillard, *supra*, at 2223 ("The cloud is now used to store many of the same materials as a briefcase or backpack.").

¶44 We are also to consider societal expectations in determining whether a person has a legitimate expectation of privacy in searched or seized property. *See* ***Minnesota v. Olson***, 495 U.S. 91, 98 (1990). Here, we conclude that society is willing to recognize that a user has a legitimate expectation of privacy in his or her Dropbox account. According to Dropbox, it boasts over 700 million users on its platform, and it specifically tells its users that "[w]ith Dropbox, your files belong to you, not us, so you can be sure we're not reselling your data." Dropbox, https://www.dropbox.com (last visited Dec. 13, 2022). By using a password that

is not shared, these users expect their cloud-storage accounts to remain private unless the user shares the files with others, even if the information is stored by a third party. *See* Johnson, *supra*, at 886 & n.126 ("This is the equivalent of renting a safety deposit box, locking it, and trusting the bank not to break the lock.").

¶45 Thus, under the totality of the circumstances and when considering the ***Dumstrey*** factors, we conclude that Bowers had a reasonable expectation of privacy in his Account. Law enforcement seized Bowers' Account and searched it without a warrant, thereby violating Bowers' Fourth Amendment rights.

## II. Probable Cause and Exigent Circumstances

¶46 The State argues, in the alternative, that even if a Fourth Amendment search occurred in this case, any search was justified by probable cause and exigent circumstances. "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.***

¶47 Under this exception, "a warrantless search does not violate a suspect's Fourth Amendment rights if: (1) the government can show that there is probable cause to believe that 'evidence of a crime will be found'; and (2) there are exigent circumstances." ***State v. Subdiaz-Osorio***, 2014 WI 87, ¶70, 357 Wis. 2d 41, 849 N.W.2d 748 (citing ***State v. Hughes***, 2000 WI 24, ¶¶17, 21, 233 Wis. 2d 280, 607 N.W.2d 621). In order for the government to establish probable cause for a search, it must demonstrate that there "is a 'fair probability' that

contraband or evidence of a crime will be found in a particular place." ***Hughes***, 233 Wis. 2d 280, ¶21 (citation omitted). Courts "evaluate the existence of probable cause objectively, concerned with whether law enforcement acted reasonably," ***State v. Robinson***, 2010 WI 80, ¶26, 327 Wis. 2d 302, 786 N.W.2d 463, eschewing "technicality and legalisms in favor of a 'flexible, common-sense measure of the plausibility of particular conclusions about human behavior,'" ***State v. Kiper***, 193 Wis. 2d 69, 83, 532 N.W.2d 698 (1995) (citation omitted).

¶48 As to exigent circumstances, in Wisconsin, consistent with United States Supreme Court precedent, we recognize

> four circumstances which, when measured against the time required to procure a warrant, constitute exigent circumstances that justify a warrantless entry: (1) an arrest made in "hot pursuit," (2) a threat to the safety of the suspect or others, (3) a risk that evidence will be destroyed, and (4) a likelihood that the suspect will flee.

***Robinson***, 327 Wis. 2d 302, ¶30.

> The objective test for determining whether exigent circumstances exist is whether a police officer, under the facts as they were known at the time, would reasonably believe that delay in procuring a search warrant would gravely endanger life, risk destruction of evidence, or greatly enhance the likelihood of the suspect's escape.

***Hughes***, 233 Wis. 2d 280, ¶24; *see also* ***Mitchell v. Wisconsin***, 139 S. Ct. 2525, 2534 (2019) ("[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.'" (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 question of whether exigent circumstances justified a warrantless search is also a mixed question of constitutional fact, ***id.***,

¶26, as is whether law enforcement had probable cause, ***State v. Popke***, 2009 WI 37, ¶10, 317 Wis. 2d 118, 765 N.W.2d 569.

¶49 On appeal, the State argues that law enforcement had both probable cause and exigent circumstances to justify a search of Bowers' Account. We agree with the State that law enforcement had probable cause to search Bowers' Account. Daniels testified that the county's data manager informed him that Bowers had shared both paper and electronic county records without permission. Further, Bowers himself informed Daniels that he had shared the case file records without authorization prior to the search. Lind testified that she was aware that Bowers' Account contained county property that "should not be out there." Bowers was ultimately charged with the unauthorized sharing of these records. Therefore, there was a "'fair probability' that contraband or evidence of a crime" would be found in Bowers' Account. *See* ***Hughes***, 233 Wis. 2d 280, ¶21 (citation omitted).

¶50 The State further argues that exigent circumstances existed "because the State had an urgent need to figure out what information was shared with whom and to stop it from being disseminated further." According to the State, "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" and no one knew "who, or how many people, had access to the case files information Bowers had shared." The State claimed that the "sensitive" nature of the information typically contained in a case file, such as information related to victims, confidential informants, and medical records, made it "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" by those individuals.

¶51 We disagree that under the facts of this case the search of Bowers' Account was necessitated by exigent circumstances. While we accept the State's argument that it needed to determine what information had been shared and with whom in order to stem the further release of the information, we do not agree that the need for official action was so compelling that there was no time to secure a warrant.

¶52 Daniels was made aware on February 27, 2017, that Bowers had shared the Murder 3 case file, yet the search of Bowers' Account did not take place until March 2, 2017. The State appears to argue that there were "reason[s]" for this delay—including Lind's attempt to contact Dropbox directly and the need to seek legal advice from the county's district attorney—and the delay therefore "does not make what happened here any less of an emergency." We disagree. The fact that law enforcement first attempted other avenues to obtain the evidence it sought actually cuts against its argument that there was any exigency involved. In effect, the delay in seeking a search warrant appears to have created the State's claim of an emergency. Under the circumstances, law enforcement clearly had time to obtain a search warrant prior to accessing Bowers' Account.

¶53 To the extent the State is claiming that Bowers' potential destruction of evidence created the exigency, we are also unpersuaded. In the circuit court, the State argued that there was a risk that Bowers, or someone else with access, would delete the records from his Account, thereby erasing both the evidence and any record of with whom Bowers shared the information. The State claimed at that point "law enforcement would have no idea what had been leaked to whom outside the organization." The court specifically found, however, that "Dropbox does archive files for a period of time after they are deleted," which Lind testified

was thirty days. Therefore, there was no "imminent" risk that the evidence would, in fact, be destroyed. *See* ***Kentucky v. King***, 563 U.S. 452, 460 (2011).

¶54 Finally, the State argues that exigent circumstances existed due to a threat to the safety of others. According to the State, "case files can contain information that could be dangerous to release, such as information about confidential informants [and] juvenile identifying information," and "[p]rotecting an individual's safety is a traditionally accepted circumstance that can justify an exigency." The State, however, cites only to ***Robinson***, 327 Wis. 2d 302, ¶30, for the general proposition that a threat to safety is an exigency. Not only does the State fail to provide any specific details concerning how the release of the confidential information would have in fact threatened anyone's safety in this case, but it also fails to cite any legal authority stating that the release of confidential information itself could create an exigency sufficient to eclipse the protections of the Fourth Amendment.

¶55 Further, while the State argues that "law enforcement already knew Bowers had shared case files containing medical records in paper form," the State notes only that "the files Bowers shared *turned out* to contain juvenile identifying information." (Emphasis added.) The State does not assert that this information was known to law enforcement prior to the search. *See* ***Richter***, 235 Wis. 2d 524, ¶43 ("[W]e do not apply hindsight to the exigency analysis; we consider only the circumstances known to the officer at the time he made the entry and evaluate the reasonableness of the officer's action in light of those circumstances.").

¶56 Under the circumstances of this case, we conclude that the State failed to demonstrate that law enforcement had no time to obtain a warrant and that there was an urgent need to act without one. Accordingly, the State has not

met its burden to establish both probable cause and exigent circumstances necessary to overcome the presumption that the search of Bowers' Account was unreasonable.

¶57 For the foregoing reasons, we conclude that the circuit court properly denied the State's motion for reconsideration of its decision suppressing evidence obtained from a search of Bowers' Account. Bowers had both a subjective and objective reasonable expectation of privacy in his Account. Therefore, law enforcement engaged in an unlawful search of his Account within the meaning of the Fourth Amendment, and no exigent circumstances justified a warrantless search of the Account.

*By the Court.*—Order affirmed.

Recommended for publication in the official reports.