A19-1886

STATE OF MINNESOTA

IN SUPREME COURT

State of Minnesota,

Respondent,

vs.

Tyler Ray Pauli,

Appellant.

APPELLANT'S BRIEF

KEITH M. ELLISON
Minnesota Attorney General

PETER MAGNUSON
Assistant Attorney General
1800 Bremer Tower
445 Minnesota Street
St. Paul, MN 55101-2134
Telephone: (651) 757-1271

MARK S. RUBIN
St. Louis County Attorney
St. Louis County Courthouse
100 North 5th Avenue West
Duluth, MN 55802
Telephone: (218) 726-2000

ATTORNEYS FOR RESPONDENT

OFFICE OF THE MINNESOTA APPELLATE PUBLIC DEFENDER

LAURA HEINRICH
Assistant State Public Defender
License No. 0390627

540 Fairview Avenue North
Suite 300
St. Paul, MN 55104
Telephone: (651) 219-4444

ATTORNEY FOR APPELLANT

TABLE OF CONTENTS

Page

PROCEDUAL HISTORY 1

ISSUES PRESENTED 4

STATEMENT OF THE CASE 6

STATEMENT OF FACTS 9

ARGUMENT 17

I. The Federal And State Constitutions Prohibit The Government From Searching Without A Warrant Unless An Exception To The Warrant Requirement Is Established. 19

II. Mr. Pauli Had A Reasonable Expectation Of Privacy In His Dropbox Account And Files Therein. 21

A. Mr. Pauli had a subjective expectation of privacy in his Dropbox account and the files therein. 22
B. Society recognizes Mr. Pauli's expectation of privacy in a password protected account as reasonable. 22
C. Terms of service or lease agreements do not determine whether a constitutional expectation of privacy is reasonable. 26
D. The Dropbox terms of service did not make Mr. Pauli's expectation of privacy unreasonable even if terms of service could do so. 28
E. The Dropbox terms of service are similar to leases for physical spaces which include rights of access, and there is no principled distinction between constitutional expectations of privacy in leased physical spaces and digital spaces. 32

III. Mr. Pauli Has A Property Right Against Government Trespass Upon His Papers And Effects 35

IV. The State Failed To Establish Any Constitutional Justification For The Warrantless Searches of Mr. Pauli's Files From His Dropbox Account. 37

A. The State did not present any evidence related to Dropbox's search because the prosecutor's summaries of conversations with Dropbox's counsel are not evidence. 39
B. The State did not prove that Dropbox's search was in pursuit of a private interest. 41
C. The State failed to prove that the government search of Mr. Pauli's files did not exceed the scope of the Dropbox search. 42
D. The private search doctrine does not allow the government to trespass upon Mr. Pauli's property without obtaining a search warrant. 43

CONCLUSION 45

TABLE OF AUTHORITIES

Page

STATE STATUTES

Minn. Stat. § 617.247, subd. 4(a) 1, 6, 9

STATE CASES

Brackens v. State,
312 S.W. 3d 831 (Tex. Crim. App. 2009) 36
Fagin v. State,
933 N.W.2d 774 (Minn. 2019) 21
People v. Gingrich,
862 N.W.2d 432 (Mich. Ct. App. 2014) 36
State v. Bourke,
718 N.W.2d 922 (Minn. 2006) 19
State v. Brooks,
838 N.W.2d 563 (Minn. 2013) 38
State v. Buswell,
460 N.W.2d 614 (Minn. 1990) 41
State v. Carter,
697 N.W.2d 199 (Minn. 2005) 4, 24, 28, 34
State v. Chute,
908 N.W.2d 578 (Minn. 2018) 35, 44
State v. Diede,
795 N.W.2d 836 (Minn. 2011) 20
State v. Dotson,
900 N.W.2d 445 (Minn. Ct. App. 2017) 33
State ex rel. Rasmussen v. Taharsh,
141 N.W.2d 3 (Minn. 1965) 5, 20
State v. ex rel. Sime v. Pennebaker,
9 N.W.2d 257 (Minn. 1943) 40
State v. Hanley,
363 N.W.2d 735 (Minn. 1985) 38
State v. Hatton,
389 N.W. 2d 229 (Minn. Ct. App. 1986) 33
State v. Jorgensen,
660 N.W.2d 127 (Minn. 2003) 41
State v. Leider,
449 N.W.2d 485 (Minn. Ct. App. 1989) 21

State v. Leonard,
943 N.W.2d 149 (Minn. 2020) 4, 20, 25
State v. Licari,
659 N.W.2d 243 (Minn. 2003) 4, 28, 33, 34
State v. Lieberg,
553 N.W.2d 51 (Minn. Ct. App. 1996) 21
State v. Mahkuk,
736 N.W.2d 675 (Minn. 2007) 5, 40, 41
State v. Nissalke,
801 N.W.2d 82 (Minn. 2011) 40
State v. Pauli,
2020 WL 7019328 (Minn. Ct. App. Nov. 30, 2020) (unpublished) 3, 4, 17, 29, 35

FEDERAL CASES

Arizona v. Gant,
556 U.S. 332, 129 S.Ct. 1710 (2009) 20
Berger v. State of N.Y.,
388 U.S. 41, 87 S.Ct. 1873 (1967) 45
Carpenter v. United States,
---U.S.---,138 S. Ct. 2206 (2018) 18, 22, 23, 27
Chapman v. United States,
365 U.S. 610, 81 S. Ct. 776 (1961) 19, 26
City of Ontario v. Quon,
560 U.S. 746, 113 S.Ct. 2619 (2010) 23
Coolidge v. New Hampshire,
403 U.S. 443, 91 S.Ct. 2222 (1971) 20
Corwin v. NYC Bike Share, LLC,
238 F. Supp. 3d 475 (S.D.N.Y. 2017) 31
Grady v. North Carolina,
575 U.S. 306, 135 S.Ct. 1368 (2015) 35, 36
In re Grand Jury Subpoena JK-15-029,
828 F.3d 1023, 1090 (9th Cir. 2016) 18, 22
Johnson v. United States,
333 U.S. 10, 68 S.Ct. 367 (1948) 33
Kyllo v. United States,
533 U.S. 27, 121 S.Ct. 2038 (2001) 27
McDonald v. United States,
335 U.S. 451, 69 S.Ct. 191 (1948) 20, 33
Meyer v. Kalanick,
200 F. Supp. 3d 408 (S.D.N.Y. 2016) 31
Murray v. United States,
487 U.S. 533, 108 S.Ct. 2529 (1988) 21

O'Connor v. Ortega,
480 U.S. 709, 107 S.Ct. 1492 (1987) 33
Olmsted v. United States,
277 U.S. 438, 48 S.Ct. 564 (1928) 45
Packingham v. North Carolina,
---U.S.---., 137 S.Ct. 1730 (2017) 23, 24
Riley v. California,
573 U.S. 373, 134 S.Ct. 2473 (2014) 18, 20, 23
Skinner v. Railway Labor Exec. Ass'n,
489 U.S. 602, 109 S.Ct. 1402 (1989) 41
Specht v. Netscape Communications Corp.,
306 F.3d 17 (2d Cir. 2002) 31
Stoner v. California,
376 U.S. 483, 84 S.Ct. 889 (1964) 26, 33
Taylor v. City of Saginaw,
922 F.3d 328 (6th Cir. 2019) 4, 35, 36
United States v. Ackerman,
831 F.3d 1292 (10th Cir. 2016) 4, 5, 11, 37, 41, 43, 44
United States v. Byrd,
---U.S.--- 138 S.Ct. 1518 (2018) 4, 19, 26, 28
United States v. Carey,
172 F.3d 1268 (10th Cir. 1999) 36
United States v. DiTomasso,
56 F. Supp. 3d 584 (S.D.N.Y. 2014) 22, 25, 26, 27, 34
United States v. Jacobsen,
466 U.S. 109, 104 S.Ct. 1652 (1984) 5, 20, 38, 43
United States, Jones,
565 U.S. 400, 132 S.Ct. 945 (2012) 4, 20, 35, 36
United States v. Katz,
389 U.S. 347, 88 S.Ct. 507 (1967) 21, 45
United States v. Keith,
980 F. Supp. 2d 33 (D. Mass. 2013) 43
United States v. Owens,
782 F.2d 146 (10th Cir. 1986) 27
United States v. Starr,
533 F.3d 985 (8th Cir. 2008) 38
United States v. Thomas,
447 F.3d 1191 (9th Cir. 2006) 28
United States v. Warshak,
631 F.3d 266 (6th Cir. 2010) 24, 27, 33
Walter v. United States,
447 U.S. 649, 100 S.Ct. 2395 (1980) 4, 36

MISCELLANEOUS

18 U.S.C. § 2256 41
18 U.S.C. § 2258A 9, 41, 42

Berreby, David,
Click to agree with what? No one reads terms of service, studies confirm, The Guardian, Mar. 3, 2017, www.theguardian.com/technology/2017/mar/03/terms-of-service-online-contracts-fine-print. 28

Dalmacio, Posadas V.,
The Internet of Things: Abandoning the Third-Party Doctrine and Protecting Data Encryption, 53 Gonz. L. Rev. 89 (2018) 22, 23

Moretti, Marcus and Naughton, Michael,
Why Privacy Policies Are So Inscrutable. The Atlantic, Sept. 5, 2014, www.theatlantic.com/technology/archive/2014/09/why-privacy-policies-are-so-inscrutable/379615. 30

Patar, Dustin,
Most Online 'Terms of Service' Are Incomprehensible to Adults. Study Finds, Vice, Feb. 12, 2019, www.vice.com/en/article/xwgb7j/online-contract-terms-of-service-are-incomprhensible-to-adults-study-finds. 27

Minnesota Constitution, Article I, Section 10 ..... 4, 5, 19

Minn. R. Crim. P. 26.01, subd 4(a) 3, 7, 16

Richards, Neil,
The Third-Party Doctrine and the Future of the Cloud, 94 Wash. U.L. Rev. 1441 (2017) 17, 18, 23

Serafino, Laurie,
I Know My Rights, So You Go'n Need a Warrant For That: The Fourth Amendment, Riley's Impact, and Warrantless Searches of Third-Party Clouds, 19 Berkeley J. Crim. L. 154 (2014) 17, 18, 22

United States Constitution, Fourth Amendment 4, 5, 19

A19-1886

STATE OF MINNESOTA

IN SUPREME COURT

State of Minnesota,

Respondent,

vs.

Tyler Ray Pauli,

Appellant,

PROCEDURAL HISTORY

August 25, 2017 The State charged Mr. Pauli with four felony counts of possession of pictorial representation of minors, Minn. Stat. § 617.247, subd. 4(a). The charges arose from a search of Mr. Pauli's Dropbox account and the video files therein. (Doc. Id #1).[1]

December 19, 2017 Mr. Pauli filed a motion to suppress the fruits of the searches of his Dropbox account and files. (Doc. Id #14).

December 26, 2017 The State submitted exhibits to the court. (Doc. Id #16).

January 16, 2018 Mr. Pauli filed a memorandum with exhibits. (Doc. Id #17).

February 2, 2018 The State filed a response. (Doc. Id #18).

[1] "Doc. Id" refers to the document ID number provided on the MNCIS printout.

February 26, 2018	The Honorable Eric L. Hylden denied Mr. Pauli's motion to suppress based upon lack of necessary information to decide the legal issue. (Doc. Id #20).
March 6, 2018	Mr. Pauli filed a motion to reconsider or to reopen the record with two attached emails from Dropbox counsel and a summary of a conversation with Dropbox counsel. (Doc. Id #22; Doc. Id #23).
April 12, 2018	The district court reopened the record.
June 4, 2018	The State filed a letter with an attached unsigned document from Dropbox counsel outlining the company's general review process. (Doc. Id #25).
March 6, 2019	The prosecutor filed another letter attaching an email sent to Mr. Pauli's counsel that summarized her communications with attorneys for Dropbox. (Doc. Id #29).
March 14, 2019	Mr. Pauli filed a supplemental memorandum in support of his motion to reconsider, including his objections to the court's reliance on Dropbox attorney representations as evidence. (Doc. Id #31).
April 17, 2019	Judge Hylden denied Mr. Pauli's motion, ruling that Mr. Pauli did not have a reasonable expectation of privacy in his Dropbox account and that the government did not trespass on his property in violation of the constitution. (Doc. Id #33; Add. 1-3).[2]

[2] "Add" refers to the addendum to appellant's brief.

June 18, 2019	Parties submitted a signed stipulation and proceeded to trial to preserve the dispositive pretrial ruling in accordance with Minn. R. Crim. P. 26.01, subd. 4(a). (Doc. Id #38; Doc. Id #39).
November 30, 2020	The Court of Appeals affirmed. *State v. Pauli*, 2020 WL 7019328 at *2-3 (Minn. Ct. App. Nov. 30, 2020).
February 24, 2021	This Court granted review.

ISSUES PRESENTED

I. Does a person have a reasonable expectation of privacy under the Fourth Amendment to the United States Constitution and/or Article I, Section 10 of the Minnesota Constitution in a password protected data storage account when terms of service allow the service provider to access the account only for certain limited purposes?

Ruling below: The Court of Appeals and the district court held that the Dropbox terms of service rendered any expectation of privacy unreasonable. *Pauli*, 2020 WL 7019328 at *2-3; (Doc. Id #33 at 7-8; Add. 7-8).

Apposite authority
United States v. Byrd, ---U.S.---,138 S. Ct. 1518 (2018)
State v. Licari, 659 N.W.2d 243 (Minn. 2003)
State v. Carter, 697 N.W.2d 199 (Minn. 2005)
State v. Leonard, 943 N.W.2d 149 (Minn. 2020)

II. Does the Fourth Amendment to the United States Constitution and/or Article I, Section 10 of the Minnesota Constitution protect a right against government trespass upon a person's digital property?

Ruling below: The Court of Appeals and the district court held that the government did not violate Mr. Pauli's constitutional rights against government trespass when it opened his digital files. *Pauli*, 2020 WL 7019328 at *3 n 4; (Doc. Id #33 at 7-8; Add. 7-8).

Apposite authority
Walter v. United States, 447 U.S. 649, 100 S.Ct. 2395 (1980)
United States v. Jones, 565 U.S. 400, 132 S.Ct. 945 (2012)
United States v. Ackerman, 831 F.3d 1292 (10th Cir. 2016)
Taylor v. City of Saginaw, 922 F.3d 328 (6th Cir. 2019)

III. Did government actors violate the Fourth Amendment to the United States Constitution and/or Article I, Section 10 of the Minnesota Constitution when they searched Mr. Pauli's property without a warrant?

Ruling below: The district court held that Dropbox, a private entity, searched Mr. Pauli's files thereby extinguishing any constitutionally protected privacy interest before a government actor reviewed the files. (Doc. Id #33 at 8-9; Add. 8-9).

Apposite authority

United States v. Jacobsen, 466 U.S. 109, 104 S.Ct. 1652 (1984)
State ex rel. Rasmussen v. Tahash, 141 N.W.2d 3 (Minn. 1965)
State v. Mahkuk, 736 N.W.2d 675 (Minn. 2007)
United States v. Ackerman, 831 F.3d 1292 (10th Cir. 2016)

STATEMENT OF THE CASE

Dropbox provides cloud-based storage for a person's or business's digital files, pictures, video, and other property. A Dropbox account is password protected, and items therein belong to the accountholder. As with the rental of any storage space, Dropbox includes terms of service. The Dropbox terms of service emphasize the private nature of its storage.

Certain files from Mr. Pauli's Dropbox account were searched three times without a search warrant. The information obtained was used to apply for and receive a search warrant for the account. Based on four video files found in his Dropbox account, the State charged Mr. Pauli with four counts of possession of pictorial representation of minors under Minn. Stat. § 617.247, subd. 4(a). Mr. Pauli moved to suppress the files from his Dropbox account as the fruits of violations of his constitutional rights against unreasonable government searches.

Mr. Pauli argued he had a reasonable expectation of privacy in his Dropbox account and the files therein. Mr. Pauli further argued that the Fourth Amendment protected his digital property from the type of government trespass that occurred here—government actors opening his files. Finally, Mr. Pauli argued that the warrantless searches were unreasonable because the State failed to establish any exception to the constitutional warrant requirement.

The State responded that Mr. Pauli did not have a reasonable expectation of privacy in his Dropbox account. The argument relied on exhibits including the Dropbox terms of service. The State also argued that law enforcement's review of Mr. Pauli's files did not

violate any reasonable expectation of privacy because Dropbox, a private entity, had already manually searched the files.

Judge Eric L. Hylden originally denied Mr. Pauli's motions for lack of evidence on the material legal issues. But the district court then reopened the record and provided the State with multiple opportunities to present witnesses. The State, instead, provided only an unsigned letter from an attorney for Dropbox and the trial prosecutor's purported summary of conversations with Dropbox attorneys. Mr. Pauli objected to the district court's consideration of those materials. The district court, without holding an evidentiary hearing, denied the motion to reconsider and Mr. Pauli's original motion to suppress.

The court ruled that no search occurred because 1) trespass protections apply only to physical spaces, and 2) the terms of service made Mr. Pauli's subjective expectation of privacy unreasonable. The court further ruled that even if Mr. Pauli had an expectation of privacy, Dropbox's search made the government's searches lawful under the private search doctrine. The court relied on the unsigned letter from Dropbox's counsel and the prosecutor's summaries of representations of Dropbox's counsel as to the scope of the private search. Parties agreed that the constitutionality of these warrantless searches is the dispositive legal issue in the case and complied with the requirements of Minn. R. Crim. P. 26.01, subd. 4(a) to preserve the pretrial issue for appeal.

The Court of Appeals affirmed. The Court of Appeals held that Mr. Pauli did not have a reasonable expectation of privacy in his Dropbox account. The Court of Appeals also held that Mr. Pauli's right against government trespass was not implicated because government actors did not enter his Dropbox account.

This Court granted review.

STATEMENT OF FACTS

The State charged Mr. Pauli with four counts of possession of pictorial representation of minors pursuant to Minn. Stat. § 617.247, subd. 4(a), based on four video files from his Dropbox account. Mr. Pauli's files were searched four times—the first three times were without a warrant. The statement of facts is organized into three sections: a description of the searches, a chronicle of the litigation in district court, and a summary of the opinion from the Court of Appeals.

Searches of Mr. Pauli's Dropbox Account and Files

Internet service providers must report all "apparent violations" of federal child pornography laws to the CyberTipline maintained by the National Center for Missing and Exploited Children ("NCMEC"). *See* 18 U.S.C. § 2258A(a). NCMEC employees review the reports and forward them to local law enforcement agencies. *See* 18 U.S.C. § 2258(c). Internet service providers face substantial fines and criminal penalties if they fail to report known child pornography. *See* 18 U.S.C. § 2258A (c); 18 U.S.C. § 2258A (a)(1). Dropbox is an Internet service provider required to submit reports of suspected child pornography to the NCMEC CyberTipline. (Doc. Id #17 at Ex. A 1-3). Dropbox provides cloud-based password protected storage for a person's or business's digital files, pictures, video, and other property. (*Id.*; Doc. Id #18 at Ex. A 1-7).

Mr. Pauli had a Dropbox account. (Doc. Id #17 at Ex. D). Dropbox searched Mr. Pauli's account and discovered video files it suspected, for some unknown reason, to be child pornography—when, why, and how the specific search was conducted are unknown. Dropbox submitted a NCMEC CyberTipline report based on its search. (Doc. Id #17 at

Ex. D at 6). A NCMEC employee opened and personally viewed the files, concluded that the videos were child pornography, and forwarded the CyberTipline report to the Minnesota Bureau of Criminal Apprehension ("BCA"). (Doc. Id #17 at Ex. C at 3, 17).

BCA Agent John Nordberg received and opened the 63 files that Dropbox had sent to NCMEC. (Doc Id #17 at Ex. D at 6-7). On January 18, 2017, Agent Nordberg used the information from opening the files and viewing the videos to seek and receive a search warrant for Mr. Pauli's Dropbox account.[3] On May 19, 2017, Agent Nordberg reviewed the 866 files on the USB device he received from Dropbox pursuant to the search warrant for Mr. Pauli's account and identified 156 video files as child pornography. On May 22, 2017, Agent Nordberg submitted the 156 files to NCMEC, and NCMEC concluded that the videos contained previously identified minors. (Doc. Id #17 at Ex. D at 23-28, 31-35).

District Court Pretrial Litigation

Mr. Pauli filed a motion to suppress the fruits of the searches of his Dropbox account and files based on violations of the Fourth Amendment to the United States Constitution and Article I, Section 10 of the Minnesota Constitution. (Doc. Id #14). The parties submitted exhibits as the record for the motion. (MH. 3-5).[4] Mr. Pauli filed a memorandum arguing that the searches of his account were unlawful because he had a reasonable expectation of privacy in his Dropbox account and his files, government actors searched

[3] Agent Nordberg also received a search warrant for Mr. Pauli's cellular phone and computer at his home in Hermantown. Neither device contained contraband. (Doc. Id #17 at Ex. D at 15-20).

[4] "MH" refers to transcripts from the motion hearing on December 22, 2017.

the files without a warrant, and the State failed to establish any exception to the federal or state constitutions' search warrant requirements. (Doc. Id #17).

Specifically, Mr. Pauli asserted that the State failed to establish the applicability of the private search doctrine because the State did not show that the government's visual search was the same in scope as the Dropbox search. (Doc. Id #17 at 6-11). Mr. Pauli explained that Dropbox could have used "hash value matching," a computer-generated method of searching for images of child pornography that is less extensive than viewing files with the human eye, to search his files. (Doc. Id #17 at 2-3, 6-11). Mr. Pauli's argument relied, in part, on an amicus brief Dropbox filed in *United States v. Ackerman*, 831 F.3d 1292 (10th Cir. 2016), in which the company outlined its use of hash value matching to identify child pornography. (Doc. Id #17 at Ex. A at 1-3). As such, NCMEC's search could have exceeded the scope of Dropbox's search. Mr. Pauli further argued that the Fourth Amendment protected the digital files in his Dropbox account from government trespass and the government violated that right when it opened and viewed his files. Mr. Pauli argued this was true even if he did not have a reasonable expectation of privacy in his files following Dropbox's search. (Doc. Id #17 at 11-12).

The State responded that Mr. Pauli did not have a reasonable expectation of privacy in his Dropbox account because the terms of service warned him that his account could be monitored for compliance with the law. (Doc. Id #18 at 3-7). The State did not cite to any evidence that Mr. Pauli had read or accepted the terms of service. *Id.* at 3, 6-7. The State further argued that the private search doctrine rendered any reasonable expectation of privacy moot because Dropbox, a private entity, performed a search first. The State

claimed any subsequent government search did not exceed the scope of that private search. (Doc. Id #18 at 7-12). The State did not cite to anything in the record that explained the method of Dropbox's search or Dropbox's private interest in conducting the search. The State also did not address the constitutional protection against government trespass upon Mr. Pauli's property.

The State provided screenshots of the Dropbox terms of service from November 4, 2015, the Dropbox privacy policy from October 3, 2016, and the Dropbox acceptable use policy. (Doc. Id #18 at Ex. A 1-7). The Dropbox terms of service emphasized the private nature of the information in one's Dropbox account: "When you use our Services, you provide us with things like your files, content, email messages, contacts and so on ('Your Stuff'). Your Stuff is yours. These Terms don't give us any rights to Your Stuff except for the limited rights that enable us to offer the Services." (Doc. Id #18 at Ex. A at 1). The terms of service also stated that Dropbox "may review your conduct and content for compliance with these Terms and our Acceptable Use Policy. With that said, we have no obligation to do so. We aren't responsible for the content people post and share via the Services. Please safeguard your password to the Services, make sure that others don't have access to it, and keep your account information current." (Doc. Id #18 at Ex. A at 1).

The privacy policy stated that "[w]e may disclose your information to third parties if we determine that such disclosure is reasonably necessary to (a) comply with the law; (b) protect any person from death or serious bodily injury; (c) prevent fraud or abuse of Dropbox or our users; or (d) protect Dropbox's property rights." (Doc. Id #18 at Ex. A at 4). The privacy policy also assured users that "[s]tewardship of your data is critical to us

and a responsibility that we embrace. We believe that our users' data should receive the same legal protections regardless of whether it's stored on our services or on their home computer's hard drive." *Id.*

The acceptable use policy stated that "Dropbox is used by millions of people, and we're proud of the trust placed in us. In exchange, we trust you to use our services responsibly." The acceptable use policy then listed examples of what a Dropbox accountholder must not do, including circumvent storage space limits, sell the services unless specifically authorized to do so, publish or share materials that are unlawfully pornographic or indecent, or violate the law. The list was not comprehensive. (Doc. Id #18 at Ex. A at 6).

The district court denied Mr. Pauli's motion. (Doc. Id #20). But, the district court did not decide the merits of the issue, concluding that it was unable to do so because "[t]here is a large factual divide in this case regarding Mr. Pauli's actions in signing up for Dropbox and the procedures of the search done by all involved parties/entities. The analysis that the Court must perform is largely dependent upon the 'hash matching' system and how it applied in this case. The Court does not have enough information at present to determine which side has the better of the argument because the facts are unclear." (Doc. Id #20 at 2).

Mr. Pauli moved to reconsider or reopen the record and submitted a memorandum with attached exhibits of his communications with counsel for Dropbox. (Doc. Id #22; Doc. Id #23). Mr. Pauli argued that the State failed to prove that the government search stayed within the scope of the private search. Specifically, the State failed to prove that a

Dropbox employee opened and personally reviewed the files before sending them to NCMEC. (Doc. Id #23 at 3-4). Mr. Pauli further argued that the State failed to establish that Dropbox had a private interest in reviewing the files other than to assist law enforcement and therefore Dropbox was effectively a state actor for purposes of the private search doctrine. (Doc. Id #23 at 4, Ex. A-C at 6-14). Mr. Pauli also referenced his exhibits in which the attorney from Dropbox stated that he 1) did not know if hash value matching was involved in the review of Mr. Pauli's account, 2) did not know who conducted the review, and 3) reported that Dropbox had no documentation or record of the review of Mr. Pauli's account and files other than the CyberTipline report. (Doc. Id #23 at Ex. A-C).

On April 12, 2018, the district court re-opened the record to allow for testimony or other evidence. The State did not object. (SC. 2).[5] The State suggested that it would be calling witnesses from Dropbox to testify. (SC. 3).

The State, however, did not produce any witnesses. Instead, on June 4, 2018, the prosecutor filed a letter stating that she had spoken with Dropbox counsel and that Dropbox counsel provided her with an unsigned one and half page document which was attached. (Doc. Id. #25). The attorney for Dropbox in the attached document made representations concerning Dropbox's process for reports of potential child sexual abuse content generally and how a Dropbox user can share an account. (Doc. Id. #25 at 2-3). In that document, the attorney did not provide the Dropbox policy, training manuals, business records, or any information specific to the review of Mr. Pauli's Dropbox account.

[5] "SC" refers to the transcript from the settlement conference on April 12, 2018.

On February 11, 2019, the parties reported that there were no identified witnesses from Dropbox to subpoena. Dropbox also did not have records related to the search of Mr. Pauli's account. (CH. 2-3).[6] Judge Hylden granted a continuance and noted that "it will largely, I guess, hedge on the State's ability to prove up that end of the case if they're getting no cooperation from the source of the information." (CH. 4).

On March 5, 2019, the prosecutor filed a letter brief, attaching a copy of the email she sent to Mr. Pauli's attorney summarizing her communications with counsel for Dropbox. The summary stated that Dropbox lawyers told the prosecutor there were no business records of the search Dropbox conducted of Mr. Pauli's account and that it was Dropbox's general policy for employees to manually open files suspected of child pornography. (Doc. Id #26 at 4). The State noted that it was "in agreement with the Defendant that Dropbox's practice of not keeping a record of who is opening each suspected file of child pornography is odd and troubling." (Doc. Id #26 at 2). The State argued, however, that the lawyers' representations provided to the prosecutor as to the general process that Dropbox used when reporting suspected child pornography to NCMEC were sufficient to conclude that an employee looked at the files before sending them to NCMEC. (Doc. Id #26 at 1-2, 4).

On March 7, 2019, Mr. Pauli objected to the State's reliance on the representations of counsel for Dropbox as evidence of the scope of the search Dropbox conducted. (MH. 3).[7] Mr. Pauli later filed a memorandum more thoroughly arguing that representations

[6] "CH" refers to the transcript from the continued hearing on February 11, 2019.
[7] "MH" refers to the transcripts from the motion hearing on March 7, 2019.

from Dropbox's legal counsel and the prosecutor's summaries of those representations were not evidence. (Doc. Id #31 at 2-3). Mr. Pauli also argued that his expectation of privacy in his Dropbox account was as reasonable as that in a storage unit, a hotel room, or any other rented space that included a lease with limited third-party rights of access. (Doc. Id #31 at 3-6).

On April 17, 2019, Judge Hylden denied Mr. Pauli's motion. The court ruled that no constitutionally protected search occurred for three reasons. First, the Fourth Amendment trespass protections apply only to when the government intrudes on a constitutionally protected physical area such as curtilage. Second, the district court acknowledged that Mr. Pauli had a subjective expectation of privacy in his Dropbox account but the Dropbox terms of service made his expectation unreasonable. (Doc. Id #33 at 7-8; Add. 7-8). Finally, the court held that the private search doctrine made the searches lawful. The court found that Dropbox was acting as a private entity when it performed the first search and that Dropbox employees manually reviewed all of the files containing suspected child pornography so the government's visual searches did not exceed the scope of the private search. The district court based the third ruling on summaries of the prosecutor's conversations with Dropbox's counsel and Dropbox counsel's unsigned letter. (Doc. Id #33 at 4-5, 8-9; Add. 4-5, 8-9).

Mr. Pauli and the State appeared on June 18, 2019, for a court trial pursuant to Minn. R. Crim. P. 26.01, subdivision 4(a). (T. 2).[8] The district court found Mr. Pauli guilty of

[8] "T" refers to the transcript from the court trial on June 18, 2019.

all four counts of possession of pictorial representations of minors based on the four files from his Dropbox account. (Doc. Id #36).

Opinion from the Court of Appeals

The Court of Appeals held that Mr. Pauli's expectation of privacy in his Dropbox account and files therein was unreasonable. *State v. Pauli*, 2020 WL 7019328 at *2, *4 (Minn. Ct. App. Nov. 30, 2020). The Court of Appeals also held that the government did not trespass upon Mr. Pauli's property because no government agent entered his Dropbox account without a search warrant. *Id.* at *2 n. 4.

This Court granted further review.

ARGUMENT

Cloud-based storage of information has become the norm in people's personal and business lives at an exponential rate. "[T]he cloud is a network made of hundreds of thousands of servers that store data. A user only needs a computer, tablet or smart phone connected to a cloud provider to network with remote servers and carry out tasks such as working in Google Drive or viewing personal photos." Laurie Serafino, *"I Know My Rights, So You Go'n Need a Warrant For That": The Fourth Amendment, Riley's Impact, and Warrantless Searches of Third-Party Clouds*, 19 Berkeley J. Crim. L. 154, 161-62 (2014). Such a rapid change in where and how we store our private information, from a piece of paper, to a Word document on a hard drive or portable zip drive, to a digital file on the cloud, is unprecedented. *See* Neil Richards, *The Third-Party Doctrine and the*

Future of the Cloud, 94 Wash. U.L. Rev. 1441, 1464-65 (2017); Serafino, 19 Berkeley J. Crim. L. at 161.

"Today we use the Internet to do most everything. . .Countless Internet companies maintain records about us and, increasingly, *for* us. Even our most private documents—those that, in other eras, we would have locked safely in a desk drawer or destroyed—now reside on third party servers." *Carpenter v. United States*,---U.S.---, 138 S.Ct. 2206, 2262 (2018) (Gorsuch, J., dissenting). Every justice in *Carpenter* acknowledged that the Fourth Amendment protects the content of stored digital files and those files are likely on third party servers. 138 S.Ct. at 2222 (majority op., Roberts, C.J., joined by Ginsberg, Breyer, Sotomayor, and Kagan, JJ.); *id* at 2230 (Kennedy, J., dissenting joined by Thomas and Alito, JJ.); *id* at 2262, 2269 (Gorsuch, J., dissenting). The acknowledgements reflect the "ability of digital troves to contain '[t]he sum of an individual's private life,' and the corresponding need of our jurisprudence to reflect the changing technological landscape." *In re Grand Jury Subpoena JK-15-029*, 828 F.3d 1023, 1090 (9th Cir. 2016) (quoting *Riley v. California*, 573 U.S. 373, 394, 134 S.Ct. 2473, 2489 (2014)).

Cloud-based storage accounts like Dropbox include terms of service akin to lease agreements in physical spaces. The Internet and cloud-based storage is all rented space—no one owns the space in which they store their information. The terms of service always include limited rights of access for the company so that it can provide security, stability, and control over the storage network. *See* Serafino, 19 Berkeley J. Crim. L. at 162.

The lower courts concluded that voluntarily placing information into a cloud-based storage account with terms of service that included limited rights of access made Mr.

Pauli's expectation of privacy in that information unreasonable. The lower courts also held that opening a digital file to look for information was not a trespass under the Fourth Amendment or Article I, Section 10. These decisions, if upheld, would eliminate privacy for online accounts. They would remove the critical role of judicial review before the government could access almost all personal data stored on a third party server. Any protection of a person's privacy and property would be left to the company storing that data. In other words, a business contract would dictate the scope of constitutional protections. The United States Supreme Court has consistently rejected this outcome. *See United States v. Byrd*, ---U.S.---, 138 S. Ct. 1518, 1529 (2018); *Chapman v. United States*, 365 U.S. 610, 615-17, 81 S.Ct. 776, 779-80 (1961). This Court should do the same.

The government violated Mr. Pauli's reasonable expectation of privacy in his Dropbox account and files therein and trespassed onto Mr. Pauli's property when it opened his files without a warrant. The State failed to establish any applicable exception to the constitutional requirement for a search warrant. This Court reviews the district court's pretrial legal rulings de novo. *State v. Bourke,* 718 N.W.2d 922, 927 (Minn. 2006). This Court should reverse the Court of Appeals' decision and vacate Mr. Pauli's convictions.

I.

The Federal And State Constitutions Prohibit The Government From Searching Without A Warrant Unless An Exception To The Warrant Requirement Is Established.

All persons are entitled to be "secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. CONST. Am. IV; MINN. CONST. Art. I, § 10. A government search under the Fourth Amendment and Article I, Section 10 may

occur in two ways. First, a search occurs when the government infringes upon an expectation of privacy that society is prepared to consider reasonable. *United States v. Jacobsen*, 466 U.S. 109, 113, 104 S.Ct. 1652, 1656 (1984). Second, a search occurs when the government obtains information by rummaging in a person's papers and effects, historically tied to common law trespass and property rights. *United States v. Jones*, 565 U.S. 400, 404-07, 406 n. 3, 132 S.Ct. 945, 950-51 (2012). The Fourth Amendment protects *both* interests. *Jones*, 565 U.S. at 405-06, 132 S.Ct. at 950.

Warrantless searches are per se unreasonable subject to only a few specifically delineated and well-established exceptions. *Arizona v. Gant*, 556 U.S. 332, 338, 129 S.Ct. 1710, 1716 (2009); *State v. Diede*, 795 N.W.2d 836, 846 (Minn. 2011). The warrant requirement is "not merely 'an inconvenience to be somehow 'weighed' against the claims of police efficiency.'" *Riley*, 573 U.S. at 401, 134 S.Ct. at 2493 (quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 481, 91 S.Ct. 2222, 2046 (1971)). "The right of privacy was deemed too precious to entrust to the discretion of those whose job is the detection of crime and the arrest of criminals." *McDonald v. United States*, 335 U.S. 451, 455-56, 69 S.Ct. 191, 193 (1948).

Mr. Pauli bears the burden to establish that there was a constitutionally protected expectation of privacy or right against government trespass. *State v. Leonard*, 943 N.W.2d 149, 156 (Minn. 2020). Once established, the State bears the burden to prove that the government search was lawful. *State ex rel. Rasmussen v. Tahash*, 141 N.W.2d 3, 13-14 (Minn. 1965). The State is required to produce "evidence" at a "hearing" to show that "the circumstances under which [the evidence against the defendant] was obtained were

consistent with constitutional requirements." *Id.* at 13. Any deficiencies in the record are therefore held against the State. *See Fagin v. State*, 933 N.W.2d 774, 779 (Minn. 2019) (recognizing that "it is black-letter law that the State bears the burden on exceptions [to the warrant requirement].").

The government searched the files from Mr. Pauli's Dropbox account several times without a warrant and used the information it extracted from those warrantless searches to obtain a search warrant. The parties agreed that the later obtained search warrant did not have independent probable cause separate from the fruits of the warrantless searches of Mr. Pauli's files. *See Murray v. United States*, 487 U.S. 533, 536-37, 108 S.Ct. 2529, 2533 (1988). The warrant is therefore invalid if the State did not meet its burden to justify the warrantless searches. *See State v. Lieberg*, 553 N.W.2d 51, 55 (Minn. Ct. App. 1996); *State v. Leider*, 449 N.W.2d 485, 488 (Minn. Ct. App. 1989).

II.

Mr. Pauli Had A Reasonable Expectation Of Privacy In His Dropbox Account And Files Therein.

A government search occurs when law enforcement intrudes upon a person's reasonable expectation of privacy. There are two questions that must be answered affirmatively to demonstrate a reasonable expectation of privacy. First, did the person have a subjective expectation of privacy, and second, does society recognize that expectation of privacy as reasonable. *See United States v. Katz*, 389 U.S. 347, 353, 88 S.Ct. 507, 512 (1967) (Harlan, J., concurring).

A. Mr. Pauli had a subjective expectation of privacy in his Dropbox account and the files therein.

The district court found, and the State and the Court of Appeals did not dispute, that Mr. Pauli had a subjective expectation of privacy in his Dropbox account. Mr. Pauli's subjective expectation of privacy has not been challenged likely because in the digital age, people do not believe storing their private information on a third party server or cloud undermines its private character. *Carpenter*, 138 S.Ct. at 2262 (Gorsuch, J., dissenting). Someone who stores private information in a password protected cloud storage account expects that it will remain private.

B. Society recognizes Mr. Pauli's expectation of privacy in a password protected account as reasonable.

Dropbox is advertised as private cloud-based storage, and even in name, it is the digital equivalent of a secure storage locker or secure file cabinet. *See* Dalmacio V. Posadas, Note, *The Internet of Things: Abandoning the Third-Party Doctrine and Protecting Data Encryption*, 53 Gonz. L. Rev. 89, 91-98 (2018). No reasonable person would think that information stored with a company that advertises the value of its private storage of information is anything other than private. People store a lifetime's worth of private communications, health data, pictures, essays, financial records, etc. in password protected cloud-based storage accounts. Storage of personal digital information in a space that is technically owned by another does nothing to diminish the accountholder's expectation that the information will remain private. *See In re Grand Jury Subpoena JK-15-029*, 828 F.3d at 1090; *United States v. DiTomasso*, 56 F. Supp. 3d, 584, 593 (S.D.N.Y. 2014); Serafino, 19 Berkley J. Crim. L. at 165-182.

The United States Supreme Court has recognized that storing private information on the cloud versus a hard drive does not change the private character of that information. *Riley*, 573 U.S. at 394-97, 134 S.Ct. at 2489-91 ("Cell phone users often may not know whether particular information is stored on the device or in the cloud, and it generally makes little difference."); *see also Carpenter*, 138 S.Ct. at 2217 (2018) (holding that individuals retain a reasonable expectation of privacy in cell site location information stored on a third party server). The Court recognized an expectation of privacy in information stored on the cloud due, in part, to the type of information that is being stored. *See Carpenter*, 138 S.Ct at 2219; *see also* Richards, 94 Wash. U.L. Rev. at 1469-1474. Digital accounts store a person's thoughts, activities, and personal documents—often the core information of the person's identity and private life. *See* Posadas, 53 Gonz. L. Rev. at 93-98.

For years now, the United States Supreme Court has recognized that online accounts have largely replaced private aspects of human life that used to occur in physical spaces. Over ten years ago, the Court noted that email accounts and electronically stored communication are "essential means or necessary instruments for self-expression, even self-identification." *City of Ontario v. Quon*, 560 U.S. 746, 760, 113 S.Ct. 2619, 2630 (2010). More recently, in *Packingham v. North Carolina*, the Court discussed the central role social media accounts play in providing forums for social interaction and political debate: "While we now may be coming to the realization that the Cyber Age is a revolution of historic proportions, we cannot appreciate yet its full dimensions and vast potential to alter how we think, express ourselves, and define who we want to be. The forces and

directions of the Internet are so new, so protean, and so far reaching that courts must be conscious that what they say today might be obsolete tomorrow." ---U.S.---, 137 S. Ct. 1730, 1736 (2017).

The Sixth Circuit similarly discussed the breadth and depth of personal information that people keep in cloud-based accounts: "Lovers exchange sweet nothings, and businessmen swap ambitious plans, all with the click of a mouse button. Commerce has also taken hold in email. Online purchases are often documented in email accounts, and email is frequently used to remind patients and clients of imminent appointments. In short, 'account' is an apt word for the conglomeration of stored messages that comprises an email account, as it provides an account of its owner's life." *United States v. Warshak*, 631 F.3d 266, 284 (6th Cir. 2010).

For similar reasons, two of this Court's cases support that Mr. Pauli's expectation of privacy in his Dropbox account was reasonable. In its immense storage capacity, a Dropbox account is like the storage shed this Court addressed in *State v. Carter*, 697 N.W.2d 199 (Minn. 2005). This Court emphasized that the renter of a storage shed had a reasonable expectation of privacy in part because it was "equivalent in size to a garage and large enough to contain a significant number of personal items and even to conduct some personal activities. Unlike an automobile or luggage, the dominant purpose for such a unit is to store personal effects in a fixed location." 697 N.W.2d 199, 210-11 (Minn. 2005). A Dropbox account is designed to house more private data and property than any physical structure, including the storage shed at issue in *Carter*. The property stored in a Dropbox "shed" is just as private as the property stored in a physical shed.

This Court's recent holding that a person has a reasonable expectation of privacy in information voluntarily provided to hotel staff is also applicable here. *State v. Leonard*, 943 N.W.2d 149 (2020). This expectation was reasonable even though staff is required by statute to provide that information—a guest's name and address—to law enforcement in certain limited situations. *Id.* at 158-59. This Court recognized that "[s]ome third-party institutions are generally considered private (e.g., a doctor's examination room or a lawyer's office.) Thus, sharing private information in these spaces does not destroy someone's reasonable expectation of privacy, but rather contributes to its private character." *Id.* at 159.

This Court reasoned that "most Minnesotans would be surprised and alarmed if the sensitive location information found in the guest registries at hotels, motels, or RV campsites was readily available to law enforcement without any particularized suspicion of criminal activity." *Id.* at 158. Minnesotans would be even more surprised to learn that their password protected online accounts, where they store their most private information, are readily accessible to law enforcement without a warrant or any particularized suspicion of criminal activity. The lower courts held exactly that. Rather, people view their private accounts as private and would think the information they store therein is not available to law enforcement or any other person. *See DiTomasso*, 56 F. Supp. 3d at 593 (noting, in the context of stored emails, that "people expect information to stay shielded from law enforcement even as they knowingly disclose it to other parties.").

C. Terms of service or lease agreements do not determine whether a constitutional expectation of privacy is reasonable.

Recently, the United States Supreme Court held that the terms of a car rental agreement did not determine the driver's reasonable expectation of privacy. *Byrd*, 138 S.Ct. at 1529. *Byrd* builds on a long line of cases warning that private contracts do not dictate the scope of constitutional protections. Fifty years ago, the Supreme Court warned against allowing the nuances of landlord/tenant law to limit the scope of the Fourth Amendment. *Chapman*, 365 U.S. at 615-18, 81 S.Ct. at 779-80. A few years later, the Court again cautioned that the Fourth Amendment protection against unreasonable searches "would disappear if it were left to depend upon the unfettered discretion of an employee of the hotel" and "would leave tenants' homes secure only in the discretion of their landlords." *Stoner v. California*, 376 U.S. 483, 489–90, 84 S.Ct. 889, 893 (1964).

United States v. DiTomasso is particularly on point for a leasing agreement or rental contract in a digital space. DiTomasso was charged with production and transportation of child pornography from information found in his accounts with America Online ("AOL") and an Internet chat service known as Omegle. 56 F.Supp.3d at 586. AOL's privacy policy forbade posting content that included sexual or graphic acts and stated that AOL would disclose such information to law enforcement. *Id.* at 587-88. Omegle's policy stated that it would monitor chats for inappropriate content, including child pornography, and hand the chats over to law enforcement. *Id.* at 588-89.

Notwithstanding these policies, the court found that the defendant had a reasonable expectation of privacy in the information in his AOL and Omegle accounts. This was true,

the court held, because "it would subvert the purpose of the Fourth Amendment to understand its privacy guarantee as 'waivable.'" *Id.* at 592. As to the argument that the policies rendered an expectation of privacy unreasonable, the court recognized that "[i]n today's world, meaningful participation in social and professional life requires using electronic devices—and the use of electronic devises 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." *Id.* at 592; *see also Warshak*, 631 F.3d at 285 (citing *Kyllo v. United States*, 533 U.S. 27, 34, 121 S.Ct. 2038, 2043 (2001)) ("[T]he Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish.").

Moreover, a constitutional expectation of privacy against the government is not made unreasonable based on legal terms buried in lease agreements that no average renter reviews or understands.[9] *Carpenter*, 138 S.Ct. at 2262 (Gorsuch, J., dissenting). In *United States v. Owens*, the Tenth Circuit held that a motel's terms of rental cannot govern the lodger's expectation of privacy in part because lodgers cannot be expected to be familiar with the policies and procedures of the motel. 782 F.2d 146, 149-50 (10th Cir. 1986). In

[9] *See* Dustin Patar, *Most Online 'Terms of Service' Are Incomprehensible to Adults, Study Finds*, Vice, Feb. 12, 2019, *available at*: www.vice.com/en/article/xwbg7j/online-contract-terms-of-service-are-incomprhensible-to-adults-study-finds ("[T]he average readability level of the agreements or [sign-in terms and conditions of 500 popular US websites, including Google and Facebook] reviewed by the researchers was comparable to articles in academic journals.").

United States v. Thomas, the Ninth Circuit similarly held that violation of a leasing contract that was technical and complicated did not vitiate an expectation of privacy in a rental car. 447 F.3d 1191, 1198 (9th Cir. 2006); *see also Byrd*, 138 S.Ct. at 1529. The same is true for the terms of service with an online account, especially given how technical and complicated contractual language can be in online user agreements.[10]

Finally, Mr. Pauli's decision to store contraband in his Dropbox account, when the terms of service included an instruction not to store contraband, did not make his expectation of privacy unreasonable as the district court suggested. Storing contraband does not render a person's expectation of privacy in a leased space unreasonable simply because it is in violation of the terms of the lease. In *State v. Licari*, for example, this Court held that the defendant had a reasonable expectation of privacy in storage unit even though the defendant stored a dead body and evidence of the murder in the unit. 659 N.W.2d 243, 243, 249-50 (Minn. 2003). In *Carter*, this Court found the same for a shed where the defendant stored cocaine. 697 N.W.2d at 203, 210. The analysis here is no different.

D. The Dropbox terms of service did not make Mr. Pauli's expectation of privacy unreasonable even if terms of service could do so.

Lower courts cherry-picked certain lines from the Dropbox terms of service to support the idea that those terms made Mr. Pauli's expectation of privacy unreasonable.

[10] *See* David Berreby, *Click to agree with what? No one reads terms of service, studies confirm*, The Guardian, Mar. 3, 2017, *available at*: www.theguardian.com/technology/2017/mar/03/terms-of-service-online-contracts-fine-print ("[Professors Jonathan Obar and Anne Oeldorf-Hirsch] were confirming, in the lab, what other scholars have found by painstakingly combing data on actual user behavior: nobody reads online contracts, license agreements, terms of service, privacy policies and other agreements.").

(Doc. Id #33 at 7-8; Add. 7-8); *Pauli*, 2020 WL 7019328 at *2. The courts picked one sentence from the Dropbox privacy policy and one sentence from the acceptable use policy that are pages apart. These sentences are not representative of the repeated assurances of privacy that are otherwise the focus. Dropbox's terms of service emphasize that a Dropbox user's data is private and make Mr. Pauli's expectation of privacy reasonable.

The Dropbox terms of service set an expectation of privacy almost immediately: "Your Stuff is yours. These Terms don't give us any rights to your Stuff except for the limited rights that enable us to offer the Services." Dropbox emphasized that the accountholder determines who has access to stored information. (Doc. Id #18 at Ex. A at 1). The Dropbox privacy policy assured that the data belonged to the user and that storing the data with Dropbox was just like storing it on a personal hard drive: "Stewardship of *your* data is critical to us and a responsibility that we embrace. We believe that our *users' data* should receive the same legal protections regardless of whether it's stored on our services or on their home computer's hard drive." (Doc. Id #18 at Ex. A at 4) (emphasis added). Dropbox even promises that it will "[f]ight blanket requests, [p]rotect all users, and [p]rovide trusted services," in response to a government's request for data. *Id.*

In contrast to these specific assurances of privacy, the admonishments were vague and presented in a list of general examples of prohibited conduct. This list was not detailed or inclusive. Some of the examples included sending spam, circumventing storage space limits, violating privacy or infringing on the rights of others, and sending a virus. (Doc. Id #18 at Ex. A at 6). In other words, the examples were largely about conduct that would interfere with Dropbox services themselves. These examples were not immediately

followed by a warning that Dropbox is monitoring and would disclose a user's content to law enforcement, as the lower courts implied.

To be sure, Dropbox stated that it "may review your conduct and content for compliance with these Terms and our Acceptable Use Policy." But it then provided several disclaimers, including that "we have no obligation to do so. We aren't responsible for the content people post and share via the Services." (Doc. Id #18 at Ex. A at 1). A reasonable person would not think the vague, conditional claim of the possibility of some "review" would mean that the contents of his or her account are not private. This is particularly true because, unlike the specific guarantees of privacy discussed above, the terms of service did not explain how, when, or why Dropbox might search a user's property.

These terms and policies are designed to protect Dropbox from civil liability. If a user sues Dropbox for snooping in the user's account, then Dropbox can point to the isolated disclaimers in its terms of service purporting to give it the occasional right of access to an account. If a user sues Dropbox for leaking the user's information, Dropbox can point to the disclaimer directing that the user, not Dropbox, controls the information. If someone sues Dropbox in connection with harmful information stored in an account, then Dropbox can point to the disclaimer absolving itself of responsibility for users' data. These terms are supposed to be a legal shield for Dropbox, not a sword the government can use to defeat a user's expectation of privacy.[11]

[11] *See* Marcus Moretti and Michael Naughton, *Why Privacy Policies Are So Inscrutable*, The Atlantic, Sept. 5, 2014, *available at*: www.theatlantic.com/technology/archive/2014/09/why-privacy-policies-are-so-inscrutable/379615 ("[W]ebsites have adopted a kind of precautionary legalese to

In any event, the bulk of the terms of service and policies are designed to encourage people to store their personal, private information—"Your Stuff"—with Dropbox. Dropbox emphasizes that it will protect the privacy of the user's personal and private information. Dropbox tells the accountholder that a "users' data should receive the same legal protections regardless of whether it's stored on our services or on their home computer's hard drive." (Doc. Id #18 at Ex. A at 4). A reasonable person reading those terms would think the information stored in a Dropbox account is and will remain private.

Moreover, even if Dropbox's terms of service could render a user's expectation of privacy unreasonable, that would only be true if the State proved that the user knew about and agreed to the terms. That was not the case here. The State did not present any evidence about whether or how Mr. Pauli was made aware of the terms of service. Even if it could be assumed that Mr. Pauli clicked a box agreeing to the terms, "a user's clicking of a box is not, without more, sufficient to signal their assent to any contract term. The touchstone in most courts' analysis of the enforceability of clickwrap contracts turns on whether the website provided 'reasonably conspicuous notice that [users] are about to bind themselves to contract terms.'" *Corwin v. NYC Bike Share, LLC*, 238 F. Supp. 3d 475 (S.D.N.Y. 2017) (quoting *Specht v. Netscape Communications Corp.*, 306 F.3d 17, 32 (2d Cir. 2002)); *Meyer v. Kalanick*, 200 F. Supp. 3d 408, 420 (S.D.N.Y. 2016).

Read as a whole, Dropbox's terms of service do not make an accountholder's expectation of privacy unreasonable. Provisions espousing stewardship of the

---

inoculate themselves against lawsuits and fines. The vaguer and more elastic their language, the more risk reduced.").

accountholder's data and comparing Dropbox's privacy protections to those that accountholders have on the hard drives of their personal computers are exactly the kind of assurances that foster a reasonable belief that privately stored data will remain private. Dropbox even assures that it will fight against any government requests for a user's data. The Dropbox terms of service do not make a person's expectation of privacy unreasonable even if contract provisions could hypothetically extinguish Fourth Amendment rights.

E. The Dropbox terms of service are similar to leases for physical spaces which include rights of access, and there is no principled distinction between constitutional expectations of privacy in leased physical spaces and digital spaces.

Dropbox's terms of service laid out a limited right of access to a user's account: "These Terms don't give us any rights to Your Stuff except for the limited rights that enable us to offer the Services." (Doc. Id #18 at Ex. A at 1). The terms stated that Dropbox could access the account in order to perform core functions like "hosting Your Stuff, backing it up, and sharing it when you ask us to. . .These and other features may require our systems to access, store and scan Your Stuff." The right to share access to the account and the information therein, however, belongs to the accountholder, and Dropbox's access is only to maintain the storage of the accountholder's data. (Doc. Id #18 at Ex. A at 1).

These terms of service are remarkably similar to the limited rights of access in leasing or storage agreements for physical spaces where Minnesota courts have upheld a renter's reasonable expectation of privacy. In *Licari,* this Court held that the renter had a reasonable expectation of privacy in a storage unit where the rental agreement allowed

employees to enter the unit "at all reasonable times for the purpose of inspection, cleaning, repairing, altering, or improving." 659 N.W.2d at 248. This Court noted that "a landlord, though she might reserve rights of access, typically does not have rights of use" and that the language in the lease did not extinguish an expectation of privacy. *Id.* at 250-51. The Minnesota Court of Appeals similarly held that registered hotel guests and apartment leasers have reasonable expectations of privacy even with rental agreements that include limited rights of access. *State v. Dotson*, 900 N.W.2d 445, 451 (Minn. Ct. App. 2017); *State v. Hatton*, 389 N.W.2d 229, 232 (Minn. Ct. App. 1986).

These Minnesota cases are in line with United States Supreme Court precedent holding that a person has reasonable expectations of privacy in rented or shared spaces even though others have limited access based on written contracts. The Court recognized constitutional protections in an employee's desk at work, a rented room in a boarding house, a hotel room, and an extended stay hotel. *See O'Connor v. Ortega*, 480 U.S. 709, 717-18, 107 S.Ct. 1492, 1497-98 (1987); *Stoner*, 376 U.S. at 488-89, 84 S.Ct. at 892-93; *McDonald*, 335 U.S. at 455-56, 69 S.Ct. at 193; *Johnson v. United States*, 333 U.S. 10, 13-15, 68 S.Ct. 367, 368-70 (1948). The Sixth Circuit explicitly compared a company's right of access to maintain an email account to the right of access in a leasing or rental agreement for a physical space: "[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. . . .Nor is the *right* of access." *Warshak*, 631 F.3d at 286-87.

Like the lease agreement in *Licari* and the cases cited above, the Dropbox terms of service allow limited access to a user's account to maintain the digital storage space. The

data still belongs to the accountholder, and the accountholder decides who can use the data. Like Licari's landlord, Dropbox cannot use Mr. Pauli's data. (Doc. Id #18 at Ex. A at 1). These analogous provisions in the Dropbox terms of service are indistinguishable from the lease provision in *Licari*.

Dropbox's access to Mr. Pauli's property was limited to maintain the digital storage unit, and Mr. Pauli retained exclusive control over the use and sharing of the data therein. The fact that the Dropbox terms of service allowed limited access to Mr. Pauli's account, just like lease provisions for physical spaces, did not deprive Mr. Pauli of a reasonable expectation of privacy in the contents of his account. Mr. Pauli's expectation of privacy is just as reasonable as the expectation in rented storage units, hotel rooms, or other leased physical spaces. The lower courts' rulings to the contrary create an unsupported and illogical distinction between physical and online rented spaces.

In sum, Mr. Pauli's expectation of privacy in his Dropbox account and files therein is the same as the reasonable expectation of privacy in the information provided to the hotel in *Leonard*, the items in the storage unit in *Licari*, the property in the storage unit in *Carter*, and the stored information in the email account in *DiTomasso*. Dropbox's limited access in the terms of service is akin to leases in physical storage spaces, the terms emphasize that the property is the accountholder's, and Dropbox repeatedly assures the protection and privacy of the accountholder's data. The Dropbox terms of service do not define the scope of Mr. Pauli's constitutional protect against the government, but even if they did, the Dropbox terms of service make that expectation of privacy reasonable, not unreasonable.

Mr. Pauli's expectation of privacy in his online private storage space and property therein was reasonable.

III.
Mr. Pauli Has A Property Right Against Government Trespass Upon His Papers And Effects.

A Fourth Amendment search also occurs when law enforcement trespasses upon a person's property or effects with the purpose of obtaining information. *Jones*, 565 U.S. at 404-05, 408 n. 5, 411, 132 S.Ct. at 949, 951, 953; *see also Grady v. North Carolina*, 575 U.S. 306, 308-10, 135 S.Ct. 1368, 1370-71 (2015); *State v. Chute*, 908 N.W.2d 578, 586-87 (Minn. 2018). The Fourth Amendment limits both law enforcement's incursion onto a person's land and law enforcement's ability to trespass upon a person's effects. *Jones*, 565 U.S. at 404-05, 411, 132 S.Ct. at 949, 953. Nonetheless, the lower courts held that the government had not trespassed upon Mr. Pauli's property because government agents had entered a physical or virtual space—the curtilage of his home or his Dropbox account. (Doc. Id #33 at 7; Add. 7); *Pauli*, 2020 WL 7019328 at *3 n. 4.

The Supreme Court has been clear that the Fourth Amendment protects effects and that the legal analysis for trespass on real property, such as cases addressing curtilage, is inapplicable to the legal analysis for trespass on effects. *Jones*, 565 U.S. at 404-05, 411, 132 S.Ct. at 949, 953. In *Jones*, the Court explained that placing a tracker on a person's car to obtain information about the person's whereabouts violated the Fourth Amendment under a trespass and property analysis. *Id.* at 408, 132 S.Ct. at 951; *see also Grady*, 575 U.S. at 308-09, 135 S.Ct. at 1370-71 (holding that placing a GPS tracker on a person was a constitutional trespass). In *Taylor v. City of Saginaw*, the Sixth Circuit also held that the

government committed a trespassory search under the Fourth Amendment when it placed chalk on the wheel of a parked car to later obtain the information needed to issue a parking citation. 922 F.3d 328, 333 (6th Cir. 2019).

The contents of Mr. Pauli's Dropbox account were his property—that is, his digital "papers" and "effects." *See People v. Gingrich*, 862 N.W.2d 432, 437 (Mich. Ct. App. 2014) (referring to digital data as a person's possessions and effects under the Fourth Amendment). There is no principled constitutional distinction between a physical opening of a file and a digital opening of a file. *See United States v. Carey*, 172 F.3d 1268 (10th Cir. 1999) (discussing the opening of computer files as a search); *Brackens v. State*, 312 S.W.3d 831, 837 (Tex. Crim. App. 2009) (referring to computer files as "similar to the protection afforded to a person's closed containers and closed personal effects."). Law enforcement opened his files without a warrant. That search was as least as invasive as the search in *Jones* and far more invasive than the search in *Taylor*.

Although decided based on a reasonable expectation privacy, the United States Supreme Court's decision in *Walter v. United States* is instructive. 447 U.S. 649, 100 S.Ct. 2395 (1980). There, the Court addressed whether government agents, lawfully in possession of film reels, conducted a search when they played the films. *Id.* at 654-55, 100 S.Ct. at 2400-01. The Court concluded that playing the films was a search. *Id.* at 655, 100 S.Ct. at 2401. The same is true here, especially because nothing about the file names suggested that they were contraband. (Doc. Id #17 at Ex. D at 4-5, 30-31). Law enforcement had to open and play the video files to obtain incriminating information.

In the situation most analogous to the one at issue here, the Tenth Circuit held that the government violates the Fourth Amendment when it trespasses upon stored emails. *United States v. Ackerman*, 831 F.3d 1292, 1307-08 (10th Cir. 2016). Now-Justice Gorsuch wrote that for Fourth Amendment purposes, there is no distinction between physical property and digitally stored email files. *Id.* at 1307-08. To the contrary, opening digitally stored email "seems pretty clearly to qualify as exactly the type of trespass to chattels that the framers sought to prevent when they adopted the Fourth Amendment." *Id.*

Mr. Pauli used his Dropbox account to securely store his property which could have been emails, pictures, medical records, videos, or almost anything else. These are the papers and effects that the Fourth Amendment protects against government trespass. The fact that these papers and effects are now digital and contained in a digital storage space does nothing to change their status as property under the Fourth Amendment. Mr. Pauli's right against government trespass under the Fourth Amendment does not depend on whether police officers double clicked on a file to open it or physically opened a manilla folder with their hands.

IV.

The State Failed To Establish Any Constitutional Justification For The Warrantless Searches Of Mr. Pauli's Files From His Dropbox Account.

The State argued that Dropbox's search of Mr. Pauli's account and the files therein extinguished any expectation of privacy that Mr. Pauli may have had. The "private search doctrine" provides that the Fourth Amendment "is wholly inapplicable to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent

of the Government or with the participation or knowledge of any governmental official." *Jacobsen*, 466 U.S. at 113-14, 104 S.Ct. at 1656-57. But under that doctrine, a subsequent government search is reasonable only if it does "not exceed the scope of the private search. . . ." *Id*. at 116. In other words, the government's examination of the information must go "no further than the private search." *United States v. Starr*, 533 F.3d 985, 995 (8th Cir. 2008).

NCMEC and Agent Nordberg, both government actors, searched files from Mr. Pauli's Dropbox account. For the private search doctrine to apply, the State needed to prove that Dropbox is a private actor that searched Mr. Pauli's account for its own interests and that the search it performed was as extensive as the subsequent government search. The State proved neither.

The private search doctrine is considered a search outside the Fourth Amendment, but it is still the State's justification for why the government searches were valid. The State bears the burden of proving the government search was constitutional regardless of the purported justification. For example, a search based on consent, like the private search exception, is considered a search outside of the Fourth Amendment. *State v. Hanley*, 363 N.W.2d 735, 738 (Minn. 1985). The State still bears the burden of proving the consent was valid. *State v. Brooks*, 838 N.W.2d 563, 568-69 (Minn. 2013).

The State did not meet its burden for three reasons. First, the State did not introduce any evidence at all; instead, it relied on hearsay and double-hearsay representations from Dropbox's legal counsel. Second, the State did not prove that the Dropbox search was for a private interest. Third, the State failed to prove that the government searches of Mr.

Pauli's files did not exceed the scope of the Dropbox search. Finally, even if the State had met its burden, the private search doctrine does not justify or excuse government trespass on Mr. Pauli's property.

A. The State did not present any evidence related to Dropbox's search because the prosecutor's summaries of conversations with Dropbox's counsel are not evidence.

The district court expected the State to present evidence as to the Dropbox search and noted that the legal issues "will largely, I guess, hedge on the State's ability to prove up that end of the case if they're getting no cooperation from the source of the information." (CH. 4). The State did not submit any testimony or business records to support its position that the warrantless searches were lawful. Rather, the State provided the district court with representations from Dropbox's legal counsel.

The prosecutor reported that Dropbox's legal counsel did not know what happened in the review of Mr. Pauli's account. In the summary of her conversations with multiple Dropbox lawyers, the prosecutor claimed the lawyers said that "Dropbox does not keep independent records of which employee views which file and basically said that you can ask for someone to testify, but they still won't have an answer to that." (Doc. Id #29 at 4). The prosecutor also included a summary of Dropbox counsels' explanation of the company's general practices in addressing files that included suspected child pornography.

The district court's order relied on these representations to make findings about Dropbox's search of Mr. Pauli's account. (Doc. Id #33 at 4-5, 9; Add. 4-5, 9). Specifically, the district court found, based on the unsigned letter from a Dropbox lawyer and the prosecutor's summary of her conversations with other Dropbox lawyers, that "Dropbox's

representative offered clarification to the parties, stating that each files [sic] of suspected child pornography is manually reviewed by an employee." (Doc. Id #33 at 9; Add. 9). The order did not reference any other source of information for the scope of the Dropbox search.

Minnesota courts have repeatedly admonished that representations from counsel not based on personal knowledge are not evidence. *State v. ex rel. Sime v. Pennebaker*, 9 N.W.2d 257, 258-59 (Minn. 1943); *see also State v. Nissalke*, 801 N.W.2d 82, 102 (Minn. 2011) (holding that counsel's representations were not evidence to support an alternative perpetrator instruction). In *State v. Mahkuk*, this Court held that the prosecutor had not satisfied her burden to show witness intimidation because "[t]he only thing in the record regarding intimidation and threats made against witnesses consists of the prosecutor's assertions" and "[t]he prosecutor's assertions [ ] are not evidence"—even if they may have been correct. 736 N.W.2d 675, 678 (Minn. 2007). This Court held that "absent evidence in the record and adequate findings by the trial court, we cannot say that the closure decision by the trial court was proper." *Id.*

As in *Mahkuk*, the prosecutor, not a fact witness, is making representations to the court. This prosecutor's representations are similarly not evidence. Like the district court in *Mahkuk*, the district court here should not have relied upon those representations regardless of whether the prosecutor had claimed that Dropbox's attorneys had personal knowledge of the search of Mr. Pauli's account. Here, however, the Dropbox attorneys did not have personal knowledge, and therefore, both the prosecutor's representations and the Dropbox attorneys' representations, even if they had been made at a hearing in district

court, are not evidence. The State therefore did not meet its burden, and the district court's reliance on the prosecutor's representations was error.

B. The State did not prove that Dropbox's search was in pursuit of a private interest.

Although Dropbox is a private company, it is not automatically a private actor for purposes of the private search doctrine. This is because "[t]he Fourth Amendment applies to searches by private individuals acting 'as an instrument or agent of the [g]overnment.'" *State v. Jorgensen*, 660 N.W.2d 127, 131 (Minn. 2003) (quoting *Skinner v. Railway Labor Exec. Ass'n*, 489 U.S. 602, 614, 109 S.Ct. 1402, 1411-12 (1989)). A private party acts as an instrument or agent of the State when (1) the government knows of and acquiesces in the search; and (2) the search is conducted to assist law enforcement efforts rather than the private party's own ends. *State v. Buswell*, 460 N.W.2d 614, 618 (Minn. 1990). "The dispositive question," when distinguishing between public and private entities, "isn't one of form but function, turning on what the entity does, not how it is organized." *Ackerman*, 831 F.3d at 1295.

Dropbox is a state actor if its searches were being done to fulfill perceived statutory obligations to assist with criminal investigations. Dropbox is statutorily required to report any known apparent images of child pornography to the NCMEC CyberTipline. 18 U.S.C. § 2258A. Dropbox faces substantial and criminal penalties if it fails to report known child pornography violations. 18 U.S.C. § 2258A (c); 18 U.S.C. § 2258A (a)(1).

A Dropbox attorney described in its letter to the State that "[w]hen Dropbox discovers apparent child pornography as defined in 18 U.S.C. § 2256, Dropbox provides a

report to NCMEC via the CyberTipline in accordance with its statutory obligation under 18 U.S.C. § 2258A. . . The [content safety] team has been trained on the statutory definition of child pornography and how to recognize it on our services." (Doc. Id #25 at 2-3). This suggests that Dropbox reviews users' files not for some private interest but to comply with federal law. The record is otherwise silent. The State did not meet its burden to establish that Dropbox searched Mr. Pauli's account to advance a private interest.

C. The State failed to prove that the government search of Mr. Pauli's files did not exceed the scope of the Dropbox search.

To be valid under the private search doctrine, the government search cannot exceed the scope of the private search. NCMEC and Agent Nordberg visually searched Mr. Pauli's files. For those searches to have been lawful, the Dropbox search would also need to have been visual. This is not necessarily how Dropbox searches for child pornography. As it explained in its amicus brief, Dropbox uses hash value matching to identify suspected child pornography. (Doc. Id #17 at Ex. A at 1-3).

If Dropbox used the hash value matching method to search Mr. Pauli's files, then the government's visual searches exceeded the scope of the private search, and the private search doctrine does not apply. *Ackerman*, 831 F.3d at 1305-06. This is because of the limited nature of a hash value matching search. "Matching the hash value of a file to a stored hash value [of known child pornography] is not the virtual equivalent of viewing the contents of the file. What the match says is that the two files are identical; it does not itself convey any information about the contents of the file. . . So a match alone indicts a file as

contraband but cannot alone convict it." *United States v. Keith*, 980 F. Supp. 2d 33, 43 (D. Mass. 2013).

The facts surrounding the method and extent of Dropbox's search were paramount to any argument that the private search doctrine applies. The State failed to provide those facts, again putting forth the prosecutor's representation of Dropbox attorneys' representations. Even the information in those representations did not explain why, who, or how Mr. Pauli's Dropbox account was searched.

Instead, the representations were that, generally, Dropbox employees visually reviewed suspected images of child pornography. The Dropbox attorney could not account for the difference in what he believed to be the policy and Dropbox's assertions in its brief in *Ackerman*. This general assertion, without personal knowledge, was insufficient to prove that a Dropbox employee viewed the files in Mr. Pauli's account as opposed to the hash value matching method it previously admitted to using. The State failed to establish the extent of the Dropbox search and therefore did not prove that the government search was no more extensive than the allegedly private search.

D. The private search doctrine does not allow the government to trespass upon Mr. Pauli's property without obtaining a search warrant.

The reasoning behind the private search doctrine is that once a person has revealed information to a private actor, the owner of that information no longer has an expectation of privacy against the government obtaining that same information. *Jacobsen*, 466 U.S. at 118, 104 S.Ct. at 1659. But the private search doctrine does not save the constitutionality of a government search when the government violates the Fourth Amendment's protection

against trespass upon a person's property or effects. *Ackerman*, 831 F.3d at 1307. This is because a trespass is a trespass; a trespass does not become less of a trespass, or any less of a constitutional violation, just because a private party trespassed earlier.

For example, in *Chute*, a police officer violated the Fourth Amendment when he trespassed onto Chute's driveway to photograph a camper suspected to be stolen. 908 N.W.2d at 586-87. The police officer's unconstitutional search of Chute's property would not have been less of a trespass if earlier, a private citizen had trespassed upon Chute's property to look at the camper. A private search may negate a person's reasonable expectation of privacy, but it does not diminish a person's property rights against government trespass that are also protected under the Fourth Amendment.

The same is true here. Mr. Pauli's Fourth Amendment right against government trespass was still violated even if the private search negated his reasonable expectation of privacy. NCMEC and Agent Nordberg trespassed on Mr. Pauli's property when they opened and examined his files. Any previous private search did not diminish Mr. Pauli's Fourth Amendment property right against government trespass.

CONCLUSION

Almost a century ago, Justice Brandies recognized the importance of Fourth Amendment protections beyond simply guarding against the physical intrusion of government agents in a person's home or desk drawer:

> '[I]in the application of a Constitution, our contemplation cannot be only of what has been, but of what may be.'. . . It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offense; but it is the invasion of his indefeasible right of personal security, personal liberty and private property, where that right has never been forfeited by his conviction of some public offense-it is the invasion of this sacred right.

Olmsted v. United States, 277 U.S. 438, 473–75, 48 S.Ct. 564, 570-71 (1928) (Brandeis, J., dissenting), *overruled in part by Berger v. State of N.Y.*, 388 U.S. 41, 87 S.Ct. 1873 (1967), and *overruled in part by Katz*, 389 U.S. 347, 88 S.Ct. 507 (internal citations omitted).

The government would be able to do just that—invade a person's "most intimate occurrences" without physically breaking down doors—if there is no expectation of privacy in password protected cloud-based storage or right against government trespass upon digital property. Law enforcement, with no oversight from the judiciary, would be able to access a person's most private documents, stored in the digital equivalent of a personal file cabinet with storage capacity unlimited by physical constraints.

The government's warrantless searches violated Mr. Pauli's constitutional protections. The State failed to establish any applicable exception to the warrant requirement that applied to the initial searches of Mr. Pauli's account and files. For all of the reasons above, this Court must reverse and vacate Mr. Pauli's convictions.

Dated: April 15, 2021

Respectfully submitted,

OFFICE OF THE MINNESOTA
APPELLATE PUBLIC DEFENDER

/s/ Laura G. Heinrich

LAURA G. HEINRICH
Assistant State Public Defender
License No. 0390627

540 Fairview Ave. N, Suite 300
St. Paul, MN 55104
(651) 219-4444

ATTORNEY FOR APPELLANT