Case No.: A19-1886

STATE OF MINNESOTA

IN SUPREME COURT

State of Minnesota,

Respondent,

vs.

Tyler Ray Pauli,

Appellant.

BRIEF AMICI CURIAE OF ELECTRONIC FRONTIER FOUNDATION, AMERICAN CIVIL LIBERTIES UNION, AND AMERICAN CIVIL LIBERTIES UNION OF MINNESOTA

Scott M. Flaherty (MN Bar No. 388354)
TAFT, STETTINIUS & HOLLISTER LLP
2200 IDS Center
80 South 8th Street
Minneapolis, MN 55402-2157
Tel: 612.977.8400
Fax: 612.977.8650
SFlaherty@Taftlaw.com

Jennifer Lynch, *pro hac vice*
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Tel: 415.436.9333
Fax: 415.436.9993
jlynch@eff.org

Counsel for amici curiae

Teresa Nelson (MN Bar No. 269736)
AMERICAN CIVIL LIBERTIES UNION OF MINNESOTA
P.O. Box 14720
Minneapolis, MN 55414
Tel: 651.529.1692
tnelson@aclu-mn.org

Jennifer S. Granick
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
39 Drumm Street
San Francisco, CA 94103
Tel: 415.621.2493
jgranick@aclu.org

TABLE OF CONTENTS

TABLE OF AUTHORITIES ii

STATEMENT OF INTEREST 6

INTRODUCTION 7

ARGUMENT 10

I. Cloud-Based Technology is Part of Day-to-Day Life 10

A. The Global Pandemic Has Increased Reliance on Technology for Everyday Activities 14

B. Cloud-Computing Services Come with Terms of Service Drafted to Protect the Providers' Business Interests, Including by Permitting Some Access to Stored Customer Data. 15

II. Courts Widely Recognize Fourth Amendment Protections for Digital Communications and Other Stored Documents. 17

III. A Service Provider's TOS Does Not Defeat its Users' Reasonable Expectations of Privacy in their Email or Digital Papers. 20

A. Monitoring Policies Do Not Extinguish a User's Reasonable Expectations of Privacy. 20

B. The Appellate Court's Reasoning Could Leave all Cloud-Stored Files,Not Just Contraband Material, Unprotected by the Fourth Amendment. 23

IV. The Minnesota Constitution Provides Even Greater Protections for Cloud-Stored "Papers and Effects." 24

V. The Lower Court Decision Conflicts with Federal Court Opinions. 27

CONCLUSION 29

CERTIFICATION OF LENGTH OF DOCUMENT 31

TABLE OF AUTHORITIES

Cases

Ascher v. Comm'r of Pub. Safety,
519 N.W.2d 183 (Minn. 1994) 24, 25

Bubis v. United States,
384 F.2d 643 (9th Cir. 1967) 18

Carpenter v. United States,
138 S. Ct. 2206 (2018)..... 7, 9, 19

Chapman v. United States,
365 U.S. 610 (1961)..... 19

City of Ontario v. Quon,
560 U.S. 746 (2010)..... 17, 28

In re Grand Jury Subpoena, JK-15-029,
828 F.3d 1083 (9th Cir. 2016) 9

In re Welfare of B.R.K.,
658 N.W.2d 565 (Minn. 2003) 26

Kahn v. Griffin,
701 N.W.2d. 815 (Minn. 2005) 25, 26

Katz v United States,
389 U.S. 347 (1967)..... 18

Michigan Dept. of State Police v. Sitz,
496 U.S. 444 (1990)..... 25

O'Connor v. Johnson,
287 N.W.2d 400 (Minn. 1979) 26

Rakas v. Illinois,
439 U.S. 128, 142 (1978)..... 22

Riley v. California,
573 U.S. 373 (2014)..... 17, 28

Smith v. Maryland,
442 U.S. 735 (1979)..... *passim*

State v. Askerooth,
681 N.W.2d 353 (Minn. 2004) 25

State v. Cripps,
533 N.W.2d 388 (Minn. 1995) 26

State v. Gray,
456 N.W.2d 251 (Minn. 1990) 19

State v. Leonard,
943 N.W.2d (Minn. 2020) 26

State v. Pauli,
2020 WL 7019328, (Nov. 30, 2020)..... 8, 20, 23, 27

State v. Perkins,
582 N.W.2d 876 (Minn. 1998) 23

State v. Perkins,
588 N.W.2d 491 (Minn. 1999) 23

State v. Russell,
477 N.W.2d 886 (Minn. 1991) 25

Stoner v. California,
376 U.S. 483 (1964)..... 19

United States v. Ackerman,
296 F.Supp.3d 1267 (D. Kan. 2017)..... 27

United States v. Ackerman,
804 Fed.Appx. 900 (10th Cir. 2020)..... 27

United States v. Byrd,
138 S. Ct. 1518 (2018)..... *passim*

United States v. Henderson,
241 F.3d 638 (9th Cir. 2000) 9

United States v. Irving,
347 F.Supp.3d 615 (D. Kan. 2018)..... 27

United States v. Jacobsen,
466 U.S. 109 (1984)..... 18, 24

United States v. Miller,
425 U.S. 435 (1976)..... 20

United States v. Owens,
782 F.2d 146 (10th Cir. 1986) 23, 24

United States v. Stratton,
229 F.Supp.3d 1230 (D. Kan. 2017)..... 27

United States v. Thomas,
447 F.3d 1191 (9th Cir. 2006) 22

United States v. Warshak,
631 F.3d 266 (6th Cir. 2010) ..... *passim*

Women of the State of Minn. by Doe v. Gomez, 542 N.W.2d 17 (Minn. 1995) 24

Constitutional Provisions

Minn. Const. art. I, sec.10 25

Other Authorities

Alex Hern, *Your Fitness Tracker Knows You're Pregnant Before You Do*, Guardian (Feb. 8, 2016) 14

Alexa Hulth & James Cebula, *The Basics of Cloud Computing*, U.S. Comput. Emergency Readiness Team 7

Amanda Watts, *Cops Use Murdered Woman's Fitbit to Charge Her Husband*, CNN (Apr. 26, 2017) 14

Amazon Photos Terms of Use (effective Jun. 1, 2020) 16

Amy Wang, *"I'm in Your Baby's Room": A Hacker Took Over a Baby Monitor and Broadcast Threats, Parents Say*, Wash. Post (Dec. 20, 2018) 13

Antonio Regalado, *Who Coined 'Cloud Computing'?*, MIT Tech. Rev. (Oct. 31, 2011) 10

Apple iCloud and Conditions for the United States, Canada, and Puerto Rico 16

Benny Evangelista, *Smart Toothbrushes the Latest Internet of Things Battleground*, SFGate (June 9, 2016) 13

Brooke Auxier, *What We've Learned About Americans' Views of Technology During the Time of COVID-19*, Pew Rsch. Ctr. (Dec. 18, 2020) 14

Bruce Lee, *How a Fitbit Told Jane Slater That Her Partner Was Cheating*, Forbes (Dec. 7, 2019) 14

Christine Hauser, *Police Use Fitbit Data to Charge 90-Year-Old Man in Stepdaughter's Killing*, N.Y Times (Oct. 3, 2018) 14

David Priest, *Ring Adds Geofencing to All of Its Products*, CNET (Feb. 17. 2021) 13

Dropbox Investor Relations 10

Dropbox Terms of Service (effective Feb. 10, 2017) 15

Dropbox Terms of Service (effective Sept. 24, 2019) 15

Dropbox, *Choose the Right Dropbox for You* 11

Dropbox, *Dropbox Business: Choose the Right Dropbox for You* 11

Dropbox, *How Much is 1 TB of Storage?* 11

Dropbox, *Simplify PC and Mac Backup* 11

Farhad Manjoo, *A Future Where Everything Becomes a Computer Is as Creepy as You Feared*, N.Y. Times (Oct.10, 2018) 12

Google Drive Additional Terms of Service (effective Mar. 31, 2020) 16

Google One, *One Membership to Get More Out of Google* 11

Hope Reese, *Wi-Fi-enabled 'Hello Barbie' Records Conversations with Kids and Uses AI to Talk Back*, Tech. Republic (Nov. 10, 2015) 13

iCloud Storage Plans and Pricing 11

iCloud—The best place for all your photos, files, and more 10

Janet Morrissey, *The Instant, Custom, Connected Future of Medical Devices*, N.Y. Times (Feb. 14, 2019) 13

Janna Anderson et al., *Experts Say the 'New Normal' in 2025 Will Be Far More Tech-Driven, Presenting More Big Challenges*, Pew Rsch. Ctr. (Feb. 18, 2021) 15

Jen Booton, *Under Armour's New HOVR Smart Shoe Will Automatically Track Your Run*, SportTechie (Jan. 26, 2018) 13

Lawyer Monthly, *Why Do Companies Continuously Update Their Terms & Conditions?* (Jan. 31, 2017) 15

Liam Tung, *Google: G Suite Now Has 2 Billion Users*, ZDNet, (Mar. 13, 2020) 11

Martin Backman, *Smart Homes and Home Automation*, Berg Insight 12

Michael Potuck, *Apple Hits 1.5 Billion Active Devices with ~80% of Recent iPhones and iPads running iOS 13*, 9to5Mac (Jan. 28, 2020) 10

Microsoft Services Agreement (effective Oct. 1, 2020) 16

Microsoft Terms of Use (effective Jun. 24, 2015) 9, 16

Nat. Net. to End Domestic Violence, *Smart Cars & Driverless Vehicles: Safety and Privacy Concerns*, Technology Safety 13

Onstar, *User Terms* (effective May 1, 2018) 16

Rani Molla, *Amazon, Apple, and Google Are Working Together So That Your Smart Home Works Better*, Vox (Dec. 18, 2019) 12

Ring Terms of Service (effective Dec. 8, 2020) 16

Samsung, *Terms of Service* (effective Mar. 8, 2019) 17

Samuel Gibbs, *How Did Email Grow from Messages Between Academics to a Global Epidemic?*, Guardian (Mar. 7, 2016) 10

Sarah Halzack, *Privacy Advocates Try to Keep 'Creepy,' 'Eavesdropping' Hello Barbie from Hitting Shelves*, Wash. Post (Mar. 11, 2015) 13

STATEMENT OF INTEREST[1]

Amicus curiae the Electronic Frontier Foundation ("EFF") is a member-supported, non-profit civil liberties organization that has worked to protect free speech and privacy rights in the online and digital world for thirty years. With roughly 35,000 active donors, EFF represents technology users' interests in court cases and broader policy debates, and actively encourages and challenges the government and courts to support privacy and safeguard individual autonomy as emerging technologies become more prevalent in society. EFF regularly participates as amicus in the Supreme Court, this Court, and other courts in cases addressing the Fourth Amendment and its application to new technologies. *See, e.g.*, *Carpenter v. United States,* 138 S. Ct. 2206 (2018); *Riley v. California*, 573 U.S. 373 (2014); *City of Ontario v. Quon*, 560 U.S. 746 (2010); *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010); *Webster v. Hennepin Cty*., 910 N.W.2d 420 (Minn. 2018).

The American Civil Liberties Union ("ACLU") is a nationwide, nonprofit, nonpartisan organization dedicated to defending the principles embodied in the Federal Constitution and our nation's civil rights laws. The ACLU of Minnesota is the local affiliate of the ACLU. Since its founding in 1920, the ACLU has frequently appeared before the U.S. Supreme Court, other federal courts, and this Court in numerous cases implicating Americans' right to privacy, including as counsel in *Carpenter v. United*

[1] Pursuant to Minnesota Rule of Court 129.03, amici certify that no counsel for a party authored this brief in whole or in part, and no person other than amici or their counsel has made any monetary contributions to fund the preparation or submission of this brief. This Court granted leave to file this brief on March 11, 2021.

States, and as amicus in *United States v. Warshak*; *Webster v. Hennepin Cty.*; and *State v. Leonard*, 943 N.W.2d 149 (Minn. 2020).

INTRODUCTION

The Fourth Amendment protects electronic documents and other files—the modern-day equivalent of papers and effects. *See Carpenter*, 138 S. Ct. at 2222. Electronic papers, especially those stored with a service like Dropbox for communication to and collaboration with others, are no different from email, which "is the technological scion of tangible mail, and it plays an indispensable part in the Information Age." *Warshak*, 631 F.3d at 286. Since *Warshak*, courts have routinely held that individuals have a reasonable expectation of privacy in their communications held in accounts operated by third party providers. The Supreme Court has agreed, at least in dicta. In *United States v. Carpenter*, every Justice authored or joined an opinion acknowledging that the Fourth Amendment protects the content of stored digital files. *See* 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).

Cloud computing, broadly defined, is any service that allows users to store and access their digital personal effects online.[2] Cloud computing services store people's most personal information, and all inform their users that the service reserves the right to

[2] Alexa Hulth & James Cebula, *The Basics of Cloud Computing*, U.S. Comput. Emergency Readiness Team, https://us-cert.cisa.gov/sites/default/files/publications/CloudComputingHuthCebula.pdf.

access that information to protect the interests, rights, and property of that business.

Yet, the appellate court in this case opined that when people "agree" to an online service provider's terms of service ("TOS") stating that the provider may monitor or analyze user accounts for illegal or unwanted behavior, they lose their reasonable expectation of privacy in any content stored in that account. *State v. Pauli*, 2020 WL 7019328, *3 (Nov. 30, 2020). This analysis, if correct, would apply to any and all emails, files, photos, attachments and other electronic "papers and effects" maintained with any service provider, not just Dropbox, because all service providers impose terms of service similar to those at issue here. Not only would this vitiate Fourth Amendment and Minnesota state constitutional protections for the millions of people who use these services, it would mean that a private company's TOS trumps Fourth Amendment protections for *all* content maintained with the provider. This is inconsistent with public expectations, well-recognized Fourth Amendment case law, and Supreme Court dicta. If adopted by this Court, it would undermine fundamental privacy protections in communications media used by nearly all Americans.

The appellate court opined that the specific language in Dropbox's TOS prohibiting illegal activity, permitting the company to review user activity and content, and to report violations of their terms and other law to third parties, diminished Mr. Pauli's objectively reasonable expectation of privacy. *Id*. at *3. While a TOS may govern the relationship between the provider and the user, such form contracts cannot extinguish a user's constitutional rights as against the government. *United States v. Byrd*, 138 S. Ct. 1518, 1529 (2018). A provider's mere ability to access its users'

content does not extinguish those rights. *Warshak*, 631 F.3d at 286–87; *In re Grand Jury Subpoena, JK-15-029*, 828 F.3d 1083, 1090 (9th Cir. 2016).

Although this case involves child pornography, the appellate court's rationale cannot be cabined to child pornography cases. Providers reserve the right to review accounts for many reasons unrelated to child pornography, including if content is merely "inappropriate" or violates copyrights.[3] Applying the appellate court's rationale, a service provider would have the ultimate power to determine individuals' constitutional privacy and property interests in their personal documents. To the contrary, as with rental cars, individuals retain a reasonable expectation of privacy in their private papers and property, even if they violate the contract. *See, e.g.*, *Byrd*, 138 S. Ct. 1518 (reasonable expectation of privacy in rental car despite violation of rental contract); *United States v. Henderson*, 241 F.3d 638, 647 (9th Cir. 2000) (lessee maintains a reasonable expectation of privacy in a rental car even after the rental agreement has expired). Under the lower court's rationale, Fourth Amendment protections would rise and fall depending on take-it-or-leave-it notices drafted by dominant communications platforms and the unilateral actions the companies take pursuant to those notices. This would lead to absurd results and would be contrary to *Warshak* and to Supreme Court dicta in *Carpenter*.

This Court should make clear that people have a reasonable expectation of privacy in their uploaded documents, photos, and electronic files, even if contraband,

[3] *See, e.g.,* Microsoft, *Microsoft Terms of Use* (effective June 24, 2015), https://www.microsoft.com/en-us/legal/intellectualproperty/copyright#o9.

despite private companies' monitoring warnings in their terms of service.

ARGUMENT

I. Cloud-Based Technology is Part of Day-to-Day Life

Three and a half decades separate the world's first e-mail message[4] from the vast storage and communicative capacities of cloud computing.[5] With cloud computing, previously unimaginable troves of information—including private photos, voice recordings, videos, documents, diaries, correspondence, appointments, medical records and more—are stored and can be accessed by an owner at any time, using any device bearing an internet connection.

In recent years, the use of cloud-based services for digital storage has skyrocketed. Since its advent in 2007, Dropbox's user-base has soared to more than 700 million registered users.[6] Apple offers free iCloud storage to users of its more than 1.5 billion active phones, tablets, laptops, and other devices around the world.[7] And the popular Google G Suite—which includes both Gmail and cloud storage Google Drive (offering

---

[4] Samuel Gibbs, *How Did Email Grow from Messages Between Academics to a Global Epidemic?*, Guardian (Mar. 7, 2016), https://www.theguardian.com/technology/2016/mar/07/email-ray-tomlinson-history.

[5] Antonio Regalado, *Who Coined 'Cloud Computing'?*, MIT Tech. Rev. (Oct. 31, 2011), https://www.technologyreview.com/2011/10/31/257406/who-coined-cloud-computing/(noting 2006 as the year Google's Eric Schmidt introduced the term to an industry conference, with the term quickly gaining popularity after).

[6] Dropbox, *Dropbox Investor Relations*, https://investors.dropbox.com/.

[7] Apple, *iCloud—The best place for all your photos, files, and more*, https://www.apple.com/icloud/; Michael Potuck, *Apple Hits 1.5 Billion Active Devices with ~80% of Recent iPhones and iPads running iOS 13*, 9to5Mac (Jan. 28, 2020), https://9to5mac.com/2020/01/28/apple-hits-1-5-billion-active-devices-with-80-of-recent-iphones-and-ipads-running-ios-13/.

access to stored and shareable documents, spreadsheets, photos, slide presentations, videos, and more)—enjoys 2 billion monthly active users.[8]

Today's most popular cloud storage platforms allow personal users to store massive quantities of personal information on their servers. Dropbox, Apple, and Google all offer their users several gigabytes storage of data for free and up to two terabytes of storage by subscription.[9] According to Dropbox, each terabyte of cloud storage totals over 250,000 personal photos, nearly 21 continuous days of high-definition video, or the equivalent of 6.5 million pages of documents spanning 1,300 physical filing cabinets.[10] For media groups and other businesses, Dropbox offers plans with five terabytes up to as much storage space as is needed.[11]

With many cloud-based services, including Dropbox, users can set up their systems so that their personal data and files are instantaneously and automatically transmitted from their local computer or hard drive, and stored on remote servers.[12] The owner can then access such files, share access with others, and maintain control across

---

[8] Liam Tung, *Google: G Suite Now Has 2 Billion Users*, ZDNet, (Mar. 13, 2020), https://www.zdnet.com/article/google-g-suite-now-has-2-billion-users/.

[9] Dropbox, *Choose the Right Dropbox for You*, https://www.dropbox.com/individual/plans-comparison; Apple, *iCloud Storage Plans and Pricing*, https://support.apple.com/en-us/HT201238; Google One, *One Membership to Get More Out of Google* https://one.google.com/about.

[10] Dropbox, *How Much is 1 TB of Storage?*, https://www.dropbox.com/features/cloud-storage/how-much-is-1tb.

[11] Dropbox, *Dropbox Business: Choose the Right Dropbox for You*, https://www.dropbox.com/business/pricing.

[12] Dropbox, *Simplify PC and Mac Backup*, https://www.dropbox.com/features/cloud-storage/computer-backup.

platforms over who has editing access or viewing rights.

Beyond basic digital storage, cloud computing also makes possible the collection of massive troves of personal data other than documents, photos, and messages. Cars, televisions, home surveillance cameras, and other everyday objects are increasingly being upgraded with the ability to connect to the internet and store data in the cloud with third party service providers. When connected and working in concert, these objects are able to amass reams of data regarding our intimate, offline lives, forming a vivid picture of our personal preferences, associations, political orientations, spending habits, and daily behaviors so as to present even more targeted ads and data for building future products.[13] Nowhere is this phenomenon more common than in objects in the home. Experts estimate nearly one in three American homes now qualify as "smart homes," where Wi-Fi–connected technology "control[s], monitor[s], and automat[es] functions" and makes them remotely accessible through smartphone apps and online portals.[14]

Information about our homes is extremely sensitive. Today's so-called smart devices are capable of watching both front porches and sleeping infants. They sleeplessly track the books we read, the questions we research online, when we leave home, and

---

[13] Farhad Manjoo, *A Future Where Everything Becomes a Computer Is as Creepy as You Feared*, N.Y. Times (Oct.10, 2018), https://www.nytimes.com/2018/10/10/technology/future-internet-of-things.html; Rani Molla, *Amazon, Apple, and Google Are Working Together So That Your Smart Home Works Better*, Vox (Dec. 18, 2019), https://www.vox.com/recode/2019/12/18/21028232/amazon-apple-google-connectivity-standard-project-connected-home.

[14] Martin Backman, *Smart Homes and Home Automation*, Berg Insight, http://www.berginsight.com/ReportPDF/ProductSheet/bi-sh8-ps.pdf.

where we go once we do.[15] Cloud-connected technologies are in our cars, identifying things like the number of other passengers in the vehicle and even allowing anxious parents to track teen drivers through GPS and live reports on driving behavior.[16] The same technology is in toys, recording children's conversations,[17] and medical devices: monitoring heart rate, predicting future blood sugar levels, and even sensing from within our bodies when we have not taken our medications and alerting our doctor accordingly.[18] Even today's wristwatches harness the cloud to continuously track and record our whereabouts, as well as intuit when we are awake or at rest. The technology,

---

[15] *See* Amy Wang, *"I'm in Your Baby's Room": A Hacker Took Over a Baby Monitor and Broadcast Threats, Parents Say*, Wash. Post (Dec. 20, 2018), https://www.washingtonpost.com/technology/2018/12/20/nest-cam-baby-monitor-hacked-kidnap-threat-came-device-parents-say/; Jen Booton, *Under Armour's New HOVR Smart Shoe Will Automatically Track Your Run*, SportTechie (Jan. 26, 2018), https://www.sporttechie.com/under-armour-new-hovr-connected-shoe-run/; David Priest, *Ring Adds Geofencing to All of Its Products*, CNET (Feb. 17. 2021), https://www.cnet.com/home/security/ring-adds-geofencing-to-all-of-its-products/; Benny Evangelista, *Smart Toothbrushes the Latest Internet of Things Battleground*, SFGate (June 9, 2016), https://www.sfgate.com/business/article/Smart-toothbrushes-the-latest-Internet-of-Things-7971669.php.

[16] Nat. Net. to End Domestic Violence, *Smart Cars & Driverless Vehicles: Safety and Privacy Concerns*, Technology Safety, https://www.techsafety.org/connectedcars.

[17] Hope Reese, *Wi-Fi-enabled 'Hello Barbie' Records Conversations with Kids and Uses AI to Talk Back*, Tech. Republic (Nov. 10, 2015), https://www.techrepublic.com/article/wi-fi-enabled-hello-barbie-records-conversations-with-kids-and-uses-ai-to-talk-back/; Sarah Halzack, *Privacy Advocates Try to Keep 'Creepy,' 'Eavesdropping' Hello Barbie from Hitting Shelves*, Wash. Post (Mar. 11, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/03/11/privacy-advocates-try-to-keep-creepy-eavesdropping-hello-barbie-from-hitting-shelves/.

[18] Janet Morrissey, *The Instant, Custom, Connected Future of Medical Devices*, N.Y. Times (Feb. 14, 2019), https://www.nytimes.com/2019/02/14/business/smart-medical-devices-implants.html.

also able to track elevated heart rates—from physical exercise, emotional distress, infidelity, or even pregnancy[19] —is being used by law enforcement in criminal investigations.[20]

A. The Global Pandemic Has Increased Reliance on Technology for Everyday Activities

Society's reliance on digital communication has only grown in the last decade. However, experts now predict a paradigm shift following the global pandemic, which has forced millions to rely on digital devices and online communication to remotely work, attend classes, schedule and check into medical appointments, as well as stay in close touch with friends and family.[21] Indeed, a 2021 Pew Research Center study surveyed over 900 leaders in technology, business, and policy, with respondents "nearly universal[ly]" agreeing that by 2025, "larger segments of the population [will] come to

---

[19] Bruce Lee, *How a Fitbit Told Jane Slater That Her Partner Was Cheating*, Forbes (Dec. 7, 2019), https://www.forbes.com/sites/brucelee/2019/12/07/how-a-fitbit-told-jane-slater-that-her-partner-was-cheating/?sh=15e19d8e182f; Alex Hern, *Your Fitness Tracker Knows You're Pregnant Before You Do*, Guardian (Feb. 8, 2016), https://www.theguardian.com/technology/2016/feb/08/fitness-tracker-pregnant-fitbit.

[20] *See*, *e.g.*, Christine Hauser, *Police Use Fitbit Data to Charge 90-Year-Old Man in Stepdaughter's Killing*, N.Y Times (Oct. 3, 2018), https://www.nytimes.com/2018/10/03/us/fitbit-murder-arrest.html; Amanda Watts, *Cops Use Murdered Woman's Fitbit to Charge Her Husband*, CNN (Apr. 26, 2017), https://www.cnn.com/2017/04/25/us/fitbit-womans-death-investigation-trnd.

[21] Brooke Auxier, *What We've Learned About Americans' Views of Technology During the Time of COVID-19*, Pew Rsch. Ctr. (Dec. 18, 2020), https://www.pewresearch.org/fact-tank/2020/12/18/what-weve-learned-about-americans-views-of-technology-during-the-time-of-covid-19/ ("A month into the COVID-19 outbreak, 87% of U.S. adults said the internet had been at least important for them personally during the outbreak, including 53% who deemed the internet as 'essential'…").

rely . . . on digital connections for work, education, health care, daily commercial transactions and essential social interactions." [22]

B. Cloud-Computing Services Come with Terms of Service Drafted to Protect the Providers' Business Interests, Including by Permitting Some Access to Stored Customer Data.

All of this data is subject to terms of service similar to the one at issue in this case. Cloud computing, software, and other internet companies use TOS to protect their business interests. These documents offer protection against contractual and litigation risk, protect the business's rights and property, and limit the company's liability.[23] Given the benefits a TOS provides to a business, it is no surprise that company lawyers draft the TOS to give the business broad latitude in its operation. Yet, these reservations of rights are almost never negotiated, and users have no choice but to click "I agree" just to engage in activities fundamental to modern life. *Riley*, 573 U. S. at 385.

As with nearly every commercial service, Dropbox's cloud-computing service comes with a TOS, which permits the company access to its users' stored data.[24] Dropbox's provider-access terms are industry-standard. In its TOS, Google's primary

---

[22] Janna Anderson et al., *Experts Say the 'New Normal' in 2025 Will Be Far More Tech-Driven, Presenting More Big Challenges*, Pew Rsch. Ctr. (Feb. 18, 2021), https://www.pewresearch.org/internet/2021/02/18/experts-say-the-new-normal-in-2025-will-be-far-more-tech-driven-presenting-more-big-challenges.

[23] Lawyer Monthly, *Why Do Companies Continuously Update Their Terms & Conditions?* (Jan. 31, 2017), https://www.lawyer-monthly.com/2017/02/why-do-companies-continuously-update-their-terms-conditions/.

[24] *Compare* Dropbox, *Dropbox Terms of Service* (effective Sept. 24, 2019), https://www.dropbox.com/terms, *with* Dropbox, *Dropbox Terms of Service* (effective Feb. 10, 2017), https://www.dropbox.com/terms2016.

and most popular file storage service, Google Drive, states:

> We may review content to determine whether it is illegal or violates our Program Policies. . . . But that does not necessarily mean that we review content, so please don't assume that we do.[25]

Similarly, Apple's iCloud terms note:

> You acknowledge and agree that Apple may, without liability to you, access, use, preserve and/or disclose your Account information and Content to law enforcement authorities, government officials, and/or a third party, as Apple believes is reasonably necessary or appropriate. . . .[26]

Other widely-used cloud storage services, including Microsoft's OneDrive and Azure as well as Amazon Drive, have near-identical provider access language in their TOS.[27] Similar TOS apply to data gathered by devices such as our cars, televisions, and security cameras.[28] Lawyers advising providers like these will continue to draft TOS to

---

[25] Google Drive, *Google Drive Additional Terms of Service* (effective Mar. 31, 2020), https://www.google.com/drive/terms-of-service/.

[26] Apple, *Apple iCloud and Conditions for the United States, Canada, and Puerto Rico*, https://www.apple.com/legal/internet-services/icloud/en/terms.html.

[27] *Compare* Microsoft, *Microsoft Terms of Use* (effective Jun. 24, 2015), https://www.microsoft.com/en-us/legal/intellectualproperty/copyright#o10 ("Microsoft has no obligation to monitor the Communication Services. However Microsoft reserves the right to review materials posted to the Communication Services and to remove any materials in its sole discretion."), *and* Microsoft, *Microsoft Services Agreement* (effective Oct. 1, 2020), https://www.microsoft.com/en-us/servicesagreement ("When investigating alleged violations of these Terms, Microsoft reserves the right to review Your Content in order to resolve the issue. However, we cannot monitor the entire Services and make no attempt to do so."), *with* Amazon, *Amazon Photos Terms of Use* (effective Jun. 1, 2020), https://www.amazon.com/gp/help/customer/display.html?nodeId=G201376540 ("We may use, access, and retain Your Files in order to provide the Services to you, enforce the terms of the Agreement, and improve our services, and you give us all permissions we need to do so.").

[28] *See, e.g.,* Ring, *Ring Terms of Service* (effective Dec. 8, 2020), https://ring.com/terms (assuring Ring extensive rights to use consumer content shared through the service); Onstar, *User Terms* (effective May 1, 2018), https://www.onstar.com/us/en/user_terms/

include similar data-access language so as to protect their client companies from potential lawsuits.

II. Courts Widely Recognize Fourth Amendment Protections for Digital Communications and Other Stored Documents.

By now, most courts to address the question recognize that users have a Fourth Amendment-protected interest in the contents of their digital communications. Electronic communications have in recent years far surpassed, or even entirely replaced, letters and phone calls as a means of communication for most people and have become "so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification." *Quon*, 560 U.S. at 760. Because people now conduct much, if not all, of their personal and professional correspondence electronically, obtaining access to a person's online messages allows the government to examine not just a handful of selected letters in one's letterbox, but years' worth of communications.

People store sensitive and extensive collections of electronic communications and other documents and files with providers like Dropbox. Like the modern cellphone, online accounts today can contain "a digital record of nearly every aspect of [people's] lives—from the mundane to the intimate." *Riley*, 573 U.S. at 395.

Individuals enjoy an expectation of privacy in digital files even though third

---

(reserving right to access software on cars without additional user knowledge and consent); Samsung, *Terms of Service* (effective Mar. 8, 2019), https://www.samsung.com/us/apps/samsung-members/terms-of-service/ (Company "may, but ha[s] no obligation to monitor your use of the Samsung Services, your accounts, content, and communications….").

parties facilitate the sending and receiving of messages and store the content. That is because merely entrusting digital "papers" and "effects" to an intermediary does not defeat the reasonable expectation that the contents of the materials will remain private. *Smith v. Maryland*, 442 U.S. 735, 741 (1979) (distinguishing constitutional protection for contents of conversation from numbers dialed). This has always been true for physical mail, even though at any point a mail carrier could open a letter and examine its contents. *Warshak*, 631 F.3d at 285 (*citing United States v. Jacobsen*, 466 U.S. 109, 114 (1984)). Likewise, since the Supreme Court's ruling in *Katz v United States,* 389 U.S. 347 (1967), it has been "abundantly clear that telephone conversations . . . are fully protected by the Fourth and Fourteenth Amendments"—even though the telephone company could "listen in when reasonably necessary to 'protect themselves and their properties against the improper and illegal use of their facilities.'" *Warshak,* 631 F.3d at 285, 287 (citing *Smith*, 442 U.S. at 746; *Bubis v. United States*, 384 F.2d 643, 648 (9th Cir. 1967)). As *Warshak* recognized, third-party internet service providers ("ISPs") are the "functional equivalent" of post offices or phone companies; they make "email communication possible." *Warshak*, 631 F.3d at 286.

As the *Warshak* court also noted, Fourth Amendment protection for private documents stored with third parties finds further support "in the application of Fourth Amendment doctrine to rented space." 631 F.3d at 287. *Warshak* recognized:

> Hotel guests, for example, have a reasonable expectation of privacy in their rooms. This is so even though maids routinely enter hotel rooms to replace the towels and tidy the furniture. Similarly, tenants have a legitimate expectation of privacy in their apartments. That expectation persists, regardless of the incursions of handymen to fix leaky faucets.

Id. at 287 (citations omitted). *See Stoner v. California*, 376 U.S. 483, 490 (1964); *Chapman v. United States*, 365 U.S. 610 (1961) (warrantless search of renter's house with only landlord consent was unconstitutional); *State v. Gray*, 456 N.W.2d 251, 255 (Minn. 1990) (holding even "'an unregistered visitor' . . . clearly had a legitimate expectation of privacy in the motel room"); *see also Carpenter*, 138 S. Ct. at 2268 (Gorsuch, J., dissenting) (discussing the law of bailments and noting "the fact that a third party has access to or possession of your papers and effects does not necessarily eliminate your interest in them"). A third party's ability to access private materials does not necessarily defeat the owner's privacy interest in those materials.

For all these reasons, every Justice of the Supreme Court has suggested that the Fourth Amendment protects the content of digital documents stored with third parties. *See Carpenter*, 138 S. Ct. at 2222 (majority op.) ("If the third-party doctrine does not apply to the 'modern-day equivalents of an individual's own 'papers' or 'effects,'' then the clear implication is that the documents should receive full Fourth Amendment protection."); *id*. at 2230 (Kennedy, J., dissenting) (Case law permitting warrantless access to records "may not apply when the Government obtains the modern-day equivalents of an individual's own 'papers' or 'effects,' even when those papers or effects are held by a third party."); *id*. at 2262 (Gorsuch, J., dissenting) ("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. *Smith* and *Miller* teach that the police can review all of this material, on the theory that no one reasonably expects any of it will be kept private. But no one believes that, if they ever did." (citing *Smith*, 442 U.S.

735 and *United States v. Miller*, 425 U.S. 435 (1976))).[29]

III. A Service Provider's TOS Does Not Defeat its Users' Reasonable Expectations of Privacy in their Email or Digital Papers.

The court below held that Mr. Pauli had no constitutionally-protected expectation of privacy in the electronic papers uploaded to his Dropbox account because the company's TOS advised him that it could monitor user accounts for violations of its policies and illegal conduct. *Pauli*, 2020 WL 7019328 at *3. However, while a private document like Dropbox's TOS may govern the provider's relationship with the user, it cannot vitiate the user's Fourth Amendment rights.

A. Monitoring Policies Do Not Extinguish a User's Reasonable Expectations of Privacy.

People have an expectation of privacy in their digital letters, papers, and effects even when their service provider has the ability to monitor these records. *Supra* II. The expectation of privacy analysis is intended to describe "well-recognized Fourth Amendment freedoms," *Smith*, 442 U.S. at 740 n. 5, not the interests of private businesses as advanced by terms that are often buried on a website or in an app. Users' Fourth Amendment-protected expectations of privacy are not upended when third-party providers give notice that they may exercise their capability to access or monitor the

[29] Since *Warshak*, all of the major electronic communications service providers, including Dropbox, require a warrant before they can be compelled to turn over the contents of their users' accounts to the government. And it has been Department of Justice policy since at least 2013 to seek warrants to access the contents of online messages. *See* H.R. Rep. No. 114-528, at 9 (April 26, 2016) (noting, "[s]oon after the [*Warshak*] decision, the Department of Justice began using warrants for email in all criminal cases. That practice became Department policy in 2013.").

user's account. The fact that a private entity reserves the right to interdict illegal activity to protect its own business interests does not enable the government to search emails and documents on the platform without a warrant. For example, in *Warshak*, the email service provider reserved the right to access emails under its Acceptable Use Policy. 631 F.32 at 287. Nevertheless, the Sixth Circuit found that monitoring provision did not impact Warshak's reasonable expectation of privacy in his email. For business reasons, communications companies almost always state in their TOS that the company may conduct private searches as part of its goal to identify and stop illegal activity, or even to merely to protect its business from objectionable conduct or content.[30]

In *United States v. Byrd*, the Supreme Court rejected the assumptions that underlie the appellate court's reasoning. 138 S. Ct. 1518. In *Byrd*, the police stopped and searched a rental car driven by someone who was not on the rental agreement but was given permission to drive by the renter, and discovered heroin. The Court held that drivers have a reasonable expectation of privacy in a rental car even when they are driving the car in violation of the rental agreement. Car-rental agreements, wrote the Court, are filled with long lists of restrictions that have nothing to do with a driver's reasonable expectation of privacy in the car. Even a serious violation of the rental agreement has no impact on an

[30] From another vantage, the appellate court's reasoning stands for the counterproductive proposition that an online service provider must choose between protecting its users' privacy interests and protecting its own business. If a provider chooses to police its platform for illegality or other misconduct, according to the lower court's reasoning, it vitiates its users'expectations of privacy and leaves them open to warrantless and suspicionless searches by the government. But if it chooses the alternative, the company could end up allowing criminal conduct to run on its service unabated.

expectation of privacy. Rental agreements, like terms of service, "concern risk allocation between private parties. . . . But that risk allocation has little to do with whether one would have a reasonable expectation of privacy in the rental car if, for example, he or she otherwise has lawful possession of and control over the car." *Id.* at 1529. Since the defendant in *Byrd* was lawfully in possession of the car, he had an expectation of privacy, despite the fact that he was violating a private agreement. The Fourth Amendment therefore applied to the government's search.

Just as the Supreme Court has cautioned "that arcane distinctions developed in property and tort law" ought not to control the analysis of who has a "legally sufficient interest in a place" for Fourth Amendment purposes, *Rakas v. Illinois*, 439 U.S. 128, 142 (1978), courts have repeatedly declined to find private contracts dispositive of individuals' expectations of privacy. In *Smith*, for example, the Supreme Court noted, "[w]e are not inclined to make a crazy quilt of the Fourth Amendment, especially in circumstances where (as here) the pattern of protection would be dictated by billing practices of a private corporation." *Smith*, 442 U.S. at 745. Similarly, in *United States v. Thomas*, the Ninth Circuit held that the "technical violation of a leasing contract" is insufficient to vitiate an unauthorized renter's legitimate expectation of privacy in a rental car. 447 F.3d 1191, 1198 (9th Cir. 2006). And in *United States v. Owens*, the Tenth Circuit did not let a motel's private terms govern the lodger's expectation of privacy, noting, "[a]ll motel guests cannot be expected to be familiar with the detailed internal policies and bookkeeping procedures of the inns where they lodge." 782 F.2d 146, 150

(10th Cir. 1986).[31]

If the appellate court were right in this case, Fourth Amendment protections would rise and fall depending on different courts' interpretations of different service providers' usage policies at different points in time. Customers of one company would enjoy Fourth Amendment rights, while customers of another, including millions of Dropbox users, would not. Supreme Court precedent could be reversed by a commercial TOS. That approach is not workable for the government or the public and cannot be right. *See Smith*, 442 U.S. at 745.

B. The Appellate Court's Reasoning Could Leave all Cloud-Stored Files, Not Just Contraband Material, Unprotected by the Fourth Amendment.

The appellate opinion suggests that Mr. Pauli's expectation of privacy was diminished, specifically in the illegal images he had uploaded. *Pauli*, 2020 WL 7019328, at *4 ("Pauli did not have an objectively reasonable expectation of privacy in the child-pornography content in his Dropbox account… ."). But that is a distinction without a difference. Dropbox advises its users that it may review *any* content for compliance with

[31] *State v. Perkins*, cited by the Court of Appeals in this case, 2020 WL 7019328, at *3, is distinguishable on its facts and does not support a conclusion that Mr. Pauli's use of the Dropbox service constituted behavior that waived his expectation of privacy. 588 N.W.2d 491, 493 (Minn. 1999). In *Perkins*, the defendant motel guest not only physically signed a registration card notifying him he would be asked to leave if he caused a disturbance, he was personally and repeatedly warned by the manager that the party in his room was too loud and if the guests did not stop making noise, they would be evicted. *State v. Perkins*, 582 N.W.2d 876, 879 (Minn. 1998). The party guests did not quit making noise, so Perkins no longer had a right to occupy the hotel room. *Id*. At that point, "the manager summoned the police to assist in the ouster." *Id*. at 879. These facts are very different from the circumstances here where all 700 million Dropbox users must click "agree" to lengthy terms of service they do not read and over which they have no control. *See supra Section I.*

the TOS. *Id*. at *3. If that advisement defeats the user's expectation of privacy, it would do so for *all* documents, photos, and other information in the entire account. Nor does it matter that, when conducting this account monitoring, some files in that account are contraband. The Supreme Court has held that "a warrantless search [can]not be characterized as reasonable simply because, after the official invasion of privacy occurred, contraband is discovered." *Jacobsen*, 466 U.S. at 114. Individuals retain a reasonable expectation of privacy in their papers, effects, and houses even when criminal activity is ongoing. *See e.g. Byrd*, 138 S. Ct. 1518 (reasonable expectation of privacy in rental car containing heroin); *Jacobsen*, 466 U.S. 109 (reasonable expectation of privacy in parcel containing cocaine); *Owens*, 782 F.2d at 150 (reasonable expectation of privacy in hotel room containing cocaine). The same is true with Mr. Pauli's Dropbox account. There is no logical line to draw that leaves evidence of his illegal activity outside of the Fourth Amendment, and the rest of the private, sensitive, intimate details of one's life held in an online account within its protections.

IV. The Minnesota Constitution Provides Even Greater Protections for Cloud-Stored "Papers and Effects."

The Minnesota Supreme Court has found greater protection under the state constitution for Minnesotans' rights to privacy, equal protection, and freedom from unreasonable searches, among other rights. *See, e.g.*, *Ascher v. Comm'r of Pub. Safety*, 519 N.W.2d 183, 186 (Minn. 1994) (invalidating law enforcement sobriety checkpoints as an unreasonable search); *Women of the State of Minn. by Doe v. Gomez*, 542 N.W.2d 17, 30–31 (Minn. 1995) (recognizing greater privacy right to reproductive decisions);

State v. Russell, 477 N.W.2d 886, 889 (Minn. 1991) (establishing more vigorous test for equal protection violations than federal one).

Generally, this Court will interpret the Minnesota Constitution to provide greater protection than its federal counterpart when "a more expansive reading of the state constitution represents the better rule of law." *State v. Askerooth*, 681 N.W.2d 353, 362 n.5 (Minn. 2004). The Minnesota Supreme Court provided a framework in *Kahn v. Griffin*, to explain circumstances that warranted the Court's departure from U.S. Supreme Court precedent. 701 N.W.2d. 815, 828 (Minn. 2005). These circumstances include when the Court:

- "conclude[s] that the United States Supreme Court has made a sharp or radical departure from its previous decisions or approach to the law and when we discern no persuasive reason to follow such a departure."
- "determine[s] that the Supreme Court has retrenched on Bill of Rights issues," or
- "determine[s] that federal precedent does not adequately protect our citizens' basic rights and liberties."

Id. (internal citations omitted).

Minnesota courts have been especially concerned with ensuring that Article I, Section 10 of the Minnesota Constitution adequately protects Minnesotans' right to be free from unreasonable searches and seizures. Article I, Section 10 provides greater protection than the Fourth Amendment does. *See Askerooth*, 681 N.W.2d 353, 362 (Minn. 2004) (principled basis to interpret Article I, Section 10 as providing greater protection than the Fourth Amendment); *Ascher*, 519 N.W.2d 183, 186-87 (Minn. 1994) (declining to follow *Michigan Dept. of State Police v. Sitz*, 496 U.S. 444 (1990) and

holding Article I, Section 10 precludes officers from using road blocks to stop drivers for a short amount of time with no particularized suspicion that the driver had committed any crime). Most recently this Court ruled in *State v. Leonard* that under the Minnesota Constitution, a hotel guest has a reasonable expectation of privacy in the information included in a hotel's guest registry. 943 N.W.2d at 158 ("Exercising our responsibility to safeguard for the people of Minnesota the protections afforded in our Constitution, we now hold that hotel guests have a reasonable expectation of privacy in the sensitive location information found in guest registries.").

Often this Court has taken pains to enumerate a separate state constitutional ground for its decision to ensure that the constitutional principle will stand even if it is later eroded by the U.S Supreme Court's Fourth Amendment jurisprudence. *See e.g. O'Connor v. Johnson*, 287 N.W.2d 400 (Minn. 1979) (warrant authorizing search of attorney's office invalid under both federal and state constitutions); *State v. Cripps*, 533 N.W.2d 388 (Minn. 1995) (holding that underage patron in a bar was seized, within the meaning of Article I, Section 10); *In re Welfare of B.R.K.*, 658 N.W.2d 565, 578 (Minn. 2003) ("[E]ven if short-term social guests do not have a reasonable expectation of privacy under the Fourth Amendment, their expectation is legitimate under Article I, Section 10 of the Minnesota Constitution."). Notably, the *In re Welfare of B.R.K.* Court noted that their result was necessary to "fully protect the privacy interest an individual has in his or her home." *Id*. at 578.

In this case, if the Court determines "that federal precedent does not adequately protect our citizens' basic rights and liberties," *Kahn*, 701 N.W.2d. at 828, it should still

find Article I, Section 10 protects Mr. Pauli's records stored with Dropbox, despite the monitoring terms in Dropbox's TOS.

V. The Lower Court Decision Conflicts with Federal Court Opinions.

The court below cited the district court opinion in *United States v. Ackerman*, to suggest that there may be some terms of service that could obviate a reasonable expectation of privacy. *Pauli*, 2020 WL 7019328, at *3, *citing* 296 F.Supp.3d 1267, 1272 (D. Kan. 2017). But in *Ackerman*, the government actually agreed that the defendant had an expectation of privacy in his email account. *Id.* at 1271. The Department of Justice took a far narrower position than the appellate court here, asserting that the defendant did not have a reasonable expectation of privacy only after AOL terminated the account for violating its TOS. *Id*. at 1272. That holding was wrong, but it certainly does not support the broad reach of the appellate court's holding here. Further, *Ackerman* was appealed to the Tenth Circuit, and that court assumed that Ackerman *had* shown a constitutional violation. It affirmed the district court on the grounds that the search was in good faith and not subject to the exclusionary rule. 804 Fed.Appx. 900, 903 (10th Cir. 2020). The Tenth Circuit neither agreed nor disagreed with the district court opinion.

The appellate court also cited *United States v. Stratton*, 229 F.Supp.3d 1230 (D. Kan. 2017). *Pauli*, 2020 WL 7019328, at *3. That opinion improperly expands the scope of cases involving the workplace or an employer/employee relationship in a manner contrary to federal law, including U.S. Supreme Court analysis, as explained above. *See also United States v. Irving*, 347 F.Supp.3d 615 (D. Kan. 2018) (disagreeing with

Stratton where TOS was more narrow and provider had not terminated account). Even in the workplace context, the U.S. Supreme Court has cautioned against broad holdings that would define employees' privacy expectations in messages transmitted with employer-provided equipment. *See Quon*, 560 U.S. 746. In *Quon*, the Court refrained from defining the plaintiff's expectation of privacy in his pager messages despite his employer police department's, clear policy to the contrary, which stated "[u]sers should have no expectation of privacy or confidentiality when using" city resources. *Id*. at 758.

Society, technology, and the law have evolved. Widespread adoption of electronic communications and storage services hosted by third party service providers has led to a societal recognition that these materials are extremely private. That recognition goes hand-in-hand with the longstanding possessory interest people have in their electronic papers and effects. Influenced by this trend, the Supreme Court has rejected mechanical application of older Fourth Amendment rules to new technologies. *See Riley*, 573 U.S. 373.

Should this Court adopt the appellate court's reasoning, it would go against the prevailing legal authority and create a patchwork of legal protections for cloud storage users. It would be a challenge to implement for both law enforcement and for email service providers who operate across the entire United States. *See Riley*, 573 U.S. at 398 (Fourth Amendment favors "clear guidance to law enforcement through categorical rules"). Further, users of one service would be subject to warrantless government searches, while users of a similar service, but where different lawyers wrote the TOS,

would enjoy constitutional protections.[32] This is untenable.

CONCLUSION

For the reasons above, the Court should decline to adopt either the appellate court's or the government's reasoning and hold that Mr. Pauli had a reasonable expectation of privacy in his Dropbox account.

Respectfully submitted,

Dated: April 22, 2021

s/ Scott M. Flaherty
Scott M. Flaherty (MN Bar No. 388354)
TAFT, STETTINIUS & HOLLISTER LLP
2200 IDS Center
80 South 8th Street
Minneapolis, MN 55402-2157
Tel: 612.977.8400
Fax: 612.977.8650
SFlaherty@Taftlaw.com

Counsel for amici curiae

Jennifer Lynch, *pro hac vice*
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Tel: 4415.436.9333
jlynch@eff.org

[32] Following the appellate court's rule would also mean that only the rare individual who knows how to set up and run their own private server would maintain a reasonable expectation of privacy in their shared documents and photos. That position would come as a surprise to the hundreds of millions of Americans who rely on commercial cloud-based services. *See supra* Section I.

Teresa Nelson (MN Bar No. 269736)
AMERICAN CIVIL LIBERTIES UNION OF MINNESOTA
P.O. Box 14720
Minneapolis, MN 55414
Tel: 651.529.1692
tnelson@aclu-mn.org

Jennifer S. Granick
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
39 Drumm Street
San Francisco, CA 94103
Tel: 415.621.2493
jgranick@aclu.org

CERTIFICATION OF LENGTH OF DOCUMENT

I hereby certify that the foregoing Brief Amici Curiae of Electronic Frontier Foundation, American Civil Liberties Union, and American Civil Liberties Union of Minnesota conforms to the requirements of Minnesota Rule of Court 132.01, Subd. 3(c)(1) and is produced with a proportional 13 point Times New Roman font and is 6,452 words and was prepared using Microsoft Word, version 2016.

Dated: April 22, 2021

s/ Scott M. Flaherty
Scott M. Flaherty (MN Bar No. 388354)
TAFT, STETTINIUS & HOLLISTER LLP
2200 IDS Center
80 South 8th Street
Minneapolis, MN 55402-2157
Tel: 612.977.8400
Fax: 612.977.8650
SFlaherty@Taftlaw.com

Counsel for Amici Curiae