

**SUPPLEMENTAL
APPENDIX**

**MAKING WARRANTS GREAT AGAIN: AVOIDING GENERAL SEARCHES IN THE
EXECUTION OF WARRANTS FOR ELECTRONIC DATA**

Jennifer S. Granick

CONTENTS OF THE SUPPLEMENTAL APPENDIX

Brief of the ACLU et al. as Amici Curiae Supporting Defendant-Appellant,
State v. Turay, No. S068894 (Or. argued May 3, 2022)..... SUPPL. APPENDIX 1

Brief of the ACLU et al. as Amici Curiae Supporting Defendant-Appellant,
State v. Mefford, 517 P.3d 210 (Mont. 2022) SUPPL. APPENDIX 53

State v. Mefford, 517 P.3d 210 (Mont. 2022) SUPPL. APPENDIX 84

Brief of the ACLU et al. as Amici Curiae Supporting Plaintiff-Appellant,
Facebook v. State, No. A-61-21/A-7-22
(N.J. argued Mar. 13, 2023)..... SUPPL. APPENDIX 122

Brief of the ACLU et al. as Amici Curiae Supporting Appellant-Defendant,
State v. Missak, No. A-000193-22T4
(N.J. Super. Ct. App. Div. argued Mar. 15, 2023)..... SUPPL. APPENDIX 198

Case No. S068894

IN THE SUPREME COURT OF THE STATE OF OREGON

STATE OF OREGON,)	
)	
Plaintiff–Respondent,)	Washington County Circuit
<i>Petitioner on Review,</i>)	Court
)	Case No. 17CR59493
v.)	
)	Court of Appeals
AHMED GBANABOM TURAY,)	Case No. A166973
)	
Defendant–Appellant,)	Supreme Court
<i>Respondent on Review.</i>)	Case No. S068894
)	
)	

**BRIEF OF AMICI CURIAE THE AMERICAN CIVIL LIBERTIES UNION
AND THE AMERICAN CIVIL LIBERTIES UNION OF OREGON IN
SUPPORT OF DEFENDANT–APPELLANT TURAY**

Review of the Decision of the Court of Appeal from a Judgment
of the Circuit Court for Washington County
Hon. OSCAR GARCIA, Judge

Kelly K. Simon, OSB#154213
Rachel Dallal, TPN# T22032103
(temporarily licensed in Oregon,
barred in Washington)
AMERICAN CIVIL LIBERTIES
UNION OF OREGON
P.O. BOX 40585
Portland, OR 97240
Telephone: (503) 444-7015
E-mail: ksimon@aclu-or.org

Jennifer Stisa Granick*
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
39 Drumm Street
San Francisco, CA 94111
Telephone: (415) 343-0758
E-mail: jgranick@aclu.org

** Pro hac vice application forthcoming*

*Counsel for Amici Curiae The American Civil Liberties Union & American Civil
Liberties Union of Oregon*

Additional counsel listed on following page.

March 2022

Ellen F. Rosenblum, OSB#753239
Attorney General
Benjamin Gutman, OSB#160599
Solicitor General
Peenesh Shah, OSB#112131
Assistant Attorney General
1162 Court Street NE
Salem, OR 97301-4096
Telephone: (503) 378-4402
E-mail: peenesh.h.shah@doj.state.or.us

Attorneys for Petitioner on Review

Ernest Lannet, OSB#013248
Chief Defender
Eric R. Johansen, OSB#822919
Deputy Public Defender
Office of Public Defense Services
1175 Court Street NE
Salem, OR 97301
Telephone: (503) 378-3349
E-mail: eric.r.johansen@opds.state.or.us

Attorneys for Respondent on Review

TABLE OF CONTENTS

TABLE OF AUTHORITIES ii

INTERESTS OF AMICI CURIAE 1

FACTUAL BACKGROUND 2

INTRODUCTION AND SUMMARY OF ARGUMENT 5

ARGUMENT 10

I. THE STATE’S PROPOSED RULES OF LAW VIOLATE THE
FEDERAL AND STATE CONSTITUTIONS..... 10

II. CELL PHONES CONTAIN AN IMMENSE AMOUNT OF
PRIVATE, SENSITIVE DATA. 13

III. WARRANTS CAN LIMIT LAW ENFORCEMENT SEARCHES BY
CATEGORY OF DATA..... 17

A. *Mansor* recognizes that warrants must be particular and not
overbroad, especially when authorizing searches of digital
devices..... 17

B. Use restrictions, while essential, are not enough on their own to
shield private and sensitive digital data..... 19

C. A general requirement that warrants identify relevant file types
is reasonable and effective for law enforcement..... 22

D. Under careful judicial supervision, forensic tools enable highly
effective and properly scoped searches and seizures of digital
material..... 26

E. Warrants can effectively limit by data category government
searches and seizures of social media account information..... 31

IV. THIS COURT SHOULD HOLD THAT WHERE SOME OF
THE WARRANT IS INVALID, ANY EVIDENCE ACTUALLY
OBTAINED PURSUANT TO THOSE PROVISIONS SHOULD
BE SUPPRESSED..... 38

CONCLUSION 41

TABLE OF AUTHORITIES

Cases

<i>Berger v. New York</i> , 388 U.S. 41 (1967)	33
<i>Burns v. United States</i> , 235 A.3d 758 (D.C. Cir. 2020)	24
<i>Carpenter v. United States</i> , 138 S. Ct. 2206 (2018).....	1
<i>Demaree v. Pederson</i> , 887 F.3d 870 (9th Cir. 2018)	18
<i>Elkins v. United States</i> , 364 U.S. 206 (1960)	39
<i>In re Search of Black iPhone 4</i> , 27 F. Supp. 3d 74 (D.D.C. 2014).....	26
<i>In re United States of America’s Application for a Search Warrant to Seize and Search Elec. Devices from Edward Cunnius</i> , 770 F. Supp. 2d 1138 (W.D. Wash. 2011)	24
<i>In the Matter of Applications for Search Warrants for Info. Associated with Target Email Accounts/Skype Accounts</i> , Nos. 13–MJ–8163–JPO, 13–MJ–8164–DJW, 13–MJ–8165–DJW, 13–MJ–8166–JPO, 13–MJ–8167–DJW, 2013 WL 4647554 (D. Kan. Aug. 27, 2013).....	36
<i>In the Matter of the Search of Info. Associated with [redacted]@mac.com that Is Stored at Premises Controlled by Apple, Inc.</i> , 13 F. Supp. 3d 145 (D.D.C. 2014), <i>order vacated</i> , 13 F. Supp. 3d 157 (D.D.C. 2014).....	36
<i>In the Matter of the Search of Info. Associated with Email Addresses Stored at Premises Controlled by the Microsoft Corp.</i> , 212 F. Supp. 3d 1023 (D. Kan. 2016).....	36
<i>In the Matter of the Search of Premises Known as: Three Hotmail Email Accounts</i> , No. 16-MJ-8036-DJW, 2016 WL 1239916 (D. Kan. Mar. 28, 2016).....	36
<i>People v. Herrera</i> , 357 P.3d 1227 (Colo. 2015).....	25

<i>People v. Hughes</i> , 506 Mich. 512, 958 N.W.2d 98 (2020)	1
<i>People v. Musha</i> , 131 N.Y.S.3d 514 (N.Y. Sup. Ct. 2020)	24
<i>Riley v. California</i> , 573 U.S. 373 (2014)	6, 13, 14, 15, 16, 17, 23
<i>State v. Bock</i> , 310 Or. App. 329, 485 P.3d 931 (2021)	24, 40, 41
<i>State v. Davis</i> , 295 Or. 227, 666 P.2d 802 (1983)	38, 39
<i>State v. Johnson</i> , 335 Or. 511, 73 P.3d 282 (2003)	39
<i>State v. Laundry</i> , 103 Or. 443, 206 P. 290 (1922) (en banc)	39
<i>State v. Mansor</i> , 363 Or. 185, 421 P.3d 323 (2018)	3, 5, 6, 7, 8, 17, 18, 19, 20, 41
<i>State v. McLawhorn</i> , 636 S.W.3d 210 (Tenn. Crim. App. 2020)	24
<i>State v. Pittman</i> , 367 Or. 498, 479 P.3d 1028 (2021) (en banc)	1
<i>State v. Turay</i> , 313 Or. App. 45, 493 P.3d 1058 (2021), <i>rev. allowed</i> , 369 Or. 69 (Dec. 9, 2021)	3, 4, 5
<i>Taylor v. State</i> , 260 A.3d 602 (Del. 2021)	24
<i>Terry v. Ohio</i> , 392 U.S. 1 (1968)	39
<i>United States v. Adjani</i> , 452 F.3d 1140 (9th Cir. 2006)	28
<i>United States v. Blake</i> , 868 F.3d 960 (11th Cir. 2017), <i>cert. den. sub nom.</i> <i>Blake v. United States</i> , 138 S. Ct. 1580 (2018)	32
<i>United States v. Comprehensive Drug Testing, Inc.</i> , 621 F.3d 1162 (9th Cir. 2010) (en banc)	18

<i>United States v. Galpin</i> , 720 F.3d 436 (2d Cir. 2013)	17
<i>United States v. Ganas</i> , 824 F.3d 199 (2d Cir. 2016) (en banc)	1
<i>United States v. Hasbajrami</i> , 945 F.3d 641 (2d Cir. 2019)	1
<i>United States v. Mohamud</i> , 843 F.3d 420 (9th Cir. 2016)	2
<i>United States v. Morton</i> , 984 F.3d 421 (5th Cir. 2021), <i>reh'g en banc granted</i> , 996 F.3d 754 (5th Cir. May 18, 2021)	23
<i>United States v. Otero</i> , 563 F.3d 1127 (10th Cir. 2009)	18
<i>United States v. Pineda-Moreno</i> , 688 F.3d 1087 (9th Cir. 2012)	2
<i>United States v. Ross</i> , 456 U.S. 798 (1982)	34
<i>United States v. Shipp</i> , 392 F. Supp. 3d 300 (E.D.N.Y. 2019)	33, 34
<i>United States v. Warshak</i> , 631 F.3d 266 (6th Cir. 2010)	1
<i>Wheeler v. State</i> , 135 A.3d 282 (Del. 2016)	7, 19
Other Authorities	
AccessData, <i>Forensic Toolkit User Guide</i> (2017)	27, 28
App Annie, <i>The State of Mobile 2021</i> (2021)	14
Blink, <i>Blink Home Monitor App</i>	16
Computer Crime & Intellectual Prop. Sect., Crim. Div., U.S. Dep't of Just., <i>Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations</i> (2009)	28
Diane Thieke, <i>Smartphone Statistics: For Most Users, It's 'Round-the- Clock' Connection</i> , ReportLinker (Jan. 26, 2017)	14
Jehiel Keeler Hoyt, <i>The Cyclopedia of Practical Quotations</i> (1896)	22

Geoffrey A. Fowler & Heather Kelly, <i>Amazon’s New Health Band Is the Most Invasive Tech We’ve Ever Tested</i> , Wash. Post (Dec. 10, 2020)	15
Google, <i>About Google Photos</i>	37
Grindr, <i>About Grindr</i>	16
Guidance Software, <i>EnCase Forensic User Guide Version 8.07</i> (2018).....	27
Hum. Rights Watch, <i>Dark Side: Secret Origins of Evidence in U.S. Criminal Cases</i> (Jan. 9, 2018)	21
Jack Nicas, Mike Isaac, & Shira Frenkel, <i>Millions Flock to Telegram and Signal as Fears Grow Over Big Tech</i> , N.Y. Times (Jan. 13, 2021).....	16
Jenna McLaughlin, <i>FBI Told Cops to Recreate Evidence from Secret Cell-Phone Trackers</i> , The Intercept (May 2016)	21
Jennifer Granick, <i>American Spies</i> (2017)	22
Jessica Glenza & Nicky Woolf, <i>StingRay Spying: FBI’s Secret Deal with Police Hides Phone Dragnet From Courts</i> , The Guardian (Apr. 10, 2015)	21
John Koetsier, <i>We’ve Spent 1.6 Trillion Hours on Mobile So Far in 2020</i> , Forbes (Aug. 17, 2020).....	13
John Shiffman & Kristina Cooke, <i>Exclusive: U.S. Directs Agents to Cover Up Program Used to Investigate Americans</i> , Reuters (Aug. 5, 2013).....	21
Justin McCarthy, <i>One in Five U.S. Adults Use Health Apps, Wearable Trackers</i> , Gallup (Dec. 11, 2019).....	15
Kinkoo, <i>Kinkoo</i>	16
Mary Meeker, <i>Internet Trends 2019</i> , Bond Capital (June 11, 2019).....	16
Microsoft, <i>Search for eDiscovery Activities in the Audit Log</i> , Microsoft Docs (Jan. 7, 2022)	29
Mitch Strohm, <i>Digital Banking Survey: 76% of Americans Bank Via Mobile App—Here Are the Most and Least Valuable Features</i> , Forbes (Feb. 24, 2021).....	16
Orin S. Kerr, <i>A User’s Guide to the Stored Communications Act—And a Legislator’s Guide to Amending It</i> , 72 Geo. Wash. L. Rev. 1208 (2004).....	33

Orin S. Kerr, <i>Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data</i> , 48 <i>Tex. Tech. L. Rev.</i> 1 (2015)	20
Orin S. Kerr, <i>Searches and Seizures in a Digital World</i> , 119 <i>Harv. L. Rev.</i> 531 (2005).....	28
Pew Rsch. Ctr., <i>Mobile Fact Sheet</i> (Apr. 7, 2021)	13
Sarah Silbert, <i>All the Things You Can Track with Wearables</i> , <i>Lifewire</i> (Dec. 2, 2020)	15
Sudip Bhattacharya et al., <i>NOMOPHOBIA: NO Mobile Phone PhoBIA</i> , 8 <i>J. Fam. Med. Prim. Care</i> 1297 (2019)	14
Upturn, <i>Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones</i> (Oct. 2020)	30, 31
Constitutional Provisions	
Or. Const., Art. I, sect. 9	1, 5, 6, 16, 38, 39, 40
U.S. Const. amend. IV	1, 38

INTERESTS OF AMICI CURIAE

The American Civil Liberties Union (“ACLU”) is a nationwide, nonprofit, nonpartisan organization dedicated to the principles of liberty and equality embodied in the Constitution and our nation’s civil rights laws. The American Civil Liberties Union of Oregon (“ACLU of Oregon”) is the Oregon state affiliate of the national ACLU.

Since its founding in 1920, the ACLU has frequently appeared before the Supreme Court and other state and federal courts in numerous cases implicating Americans’ right to privacy in the digital age, including as counsel in *Carpenter v. United States*, 138 S. Ct. 2206 (2018) and as amicus in *State v. Pittman*, 367 Or. 498, 479 P.3d 1028 (2021) (en banc), *People v. Hughes*, 506 Mich. 512, 958 N.W.2d 98 (2020), *United States v. Ganius*, 824 F.3d 199 (2d Cir. 2016) (en banc), *United States v. Hasbajrami*, 945 F.3d 641 (2d Cir. 2019), and *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010). The ACLU of Oregon has appeared frequently before this Court and federal courts advocating for the right to privacy and free speech in digital media and the right to privacy generally under the Fourth Amendment to the U.S. Constitution and Article I, section 9 of the Oregon Constitution, including in *Pittman*, 367 Or. 498, 479 P.3d 1028, *United*

States v. Mohamud, 843 F.3d 420 (9th Cir. 2016), and *United States v. Pineda-Moreno*, 688 F.3d 1087 (9th Cir. 2012).

FACTUAL BACKGROUND

Detectives in Beaverton were investigating advertisements listed on the website Backpage offering sex with a minor, J, individually or with an adult woman named Gregg. Police arranged a “date” with J, who was dropped off by an unknown man. J eventually identified Turay, the defendant in this case, as the person who dropped her off. Officers located and stopped Turay in his car, seizing several cell phones, a pack of condoms, and a motel room key from the vehicle. They then sought and obtained a warrant to search the contents of the seized phones. The warrant specified nine categories of information to be “searched, seized, and analyzed”:

1. Any and all communications (voice, email, text, or otherwise) between [J, Gregg, and/or defendant].
2. Evidence related to the relationship between [J, Gregg, and/or defendant].
3. Evidence regarding any communications (voice, email, text, or otherwise) involving prostitution related activities.
4. Any photos of [J, defendant, or Gregg] that show an association with prostitution including any profiting from prostitution.
5. Images, videos and/or data which depict [J or Gregg] in sexually explicit positions or conduct that relate to internet postings or advertisements.

6. Any evidence related to use of internet sites associated with prostitution, including backpage.com for a period of time 06/15/2017 to 09/06/2017.

7. Any evidence related to the use of Uber or other ride-sharing or taxicab companies.

8. Any evidence regarding the locations, including geolocation information, of the phones for a period of time from 06/15/2017 to 09/06/2017.

9. Any other evidence related to the crimes of Prostitution (ORS 167.007), Promoting Prostitution (ORS 167.012) and/or Compelling Prostitution (ORS 167.017).

See ER at 3–4.

Turay moved to suppress all information obtained as a result of these searches, arguing that the affidavit filed in support of the warrant application failed to establish probable cause or, in the alternative, was insufficiently particular and was overbroad under Article I, section 9. The trial court denied the motion and admitted the evidence. Turay was convicted of one count of compelling prostitution, ORS 167.017. *State v. Turay*, 313 Or. App. 45, 493 P.3d 1058 (2021), *rev. allowed*, 369 Or. 69 (Dec. 9, 2021).

The appellate court rejected Turay’s probable cause claim. With respect to the particularity and overbreadth claims, however, the court applied *State v. Mansor*, 363 Or. 185, 421 P.3d 323 (2018), this Court’s landmark case holding, in part, that a warrant authorizing a search of digital data must specify both *what* information is sought and—to the extent

possible—*when* that information was created (*e.g.*, by providing date ranges to narrow the search). Under the *Mansor* framework, the appellate court concluded that:

The first two search commands lacked particularity because they included no restrictions as to the time or subject matter of the information sought and could therefore be read to authorize a “general search” for “anything incriminating.”

The **seventh and ninth search commands lacked particularity**, since J’s mention of ride-sharing app was part of a conceded lie to protect the defendant, and because neither command included date or location limitations despite the availability of such limiting information to law enforcement.

The eighth command—for *all* geolocation data over a three-month period—likewise lacked the requisite specificity because it did not include descriptions of locations or activities that would reasonably limit what police could seek. (The court described this provision as “amount[ing] to a general hunt through the phone for its whereabouts for three months” *Turay*, 313 Or. App. at 59).

Finally, while a closer case, the court held that the **fourth command was defective** for its use of the vague phrase “association with prostitution” to narrow the type of information police could seek. Because the rest of the affidavit did not provide any saving context that would narrow this phrase to only that information supported by probable cause, the court held that the fourth search command was also insufficiently particular.

The court held that only the third, fifth, and sixth commands were sufficiently particular.

The appellate court next addressed the question of what a court should do when it concludes that some, but not all, of a digital data warrant is insufficiently particular. The court rejected the State’s suggestion that any data that *could* have resulted from a lawful section of the warrant should stand, emphasizing that Article I, section 9 rights hinge on how the search was actually conducted—not how it *might* have been conducted. *Turay*, 313 Or. App. at 65. Therefore, it held, courts in these situations must hold a hearing wherein the State must establish that the evidence sought to be utilized was actually discovered through a search or forensic analysis responsive to the surviving, constitutional portion of the warrant. *Id.* at 66. The court then remanded for the district court to make this factual finding. *Id.*

This Court granted review. *Turay*, 369 Or. 69. The State has conceded in its brief on the merits that the second, seventh, and ninth search commands were invalid. *See* Pet’r Br. at 13, 22–23, 28–29, 32. That leaves the first, fourth, and eighth commands in dispute before this Court.

INTRODUCTION AND SUMMARY OF ARGUMENT

This Court has recognized that cell phones today generate and store a huge amount of extremely revealing information about the people who use them. *Mansor*, 363 Or. at 209–10 (citing the “unique characteristics of the

cell phone described in *Riley* [*v. California*, 573 U.S. 373 (2014)]”).

Warrants for cell-phone searches must closely adhere to the probable cause showing, lest authority to search a device for evidence of one crime mutate into authority to search the entirety of the device for evidence of any crime—a prohibited general search. In *Mansor*, this Court held that warrants meet the probable cause obligation by describing what *information* related to the alleged criminal conduct may be found on the device, as well as by imposing a *temporal limitation* on the search, if one is available and relevant. 363 Or. at 216–17. The Court also held that, because even a narrowly drawn search term will mean that law enforcement examines some information that is not responsive to probable cause, Article I, section 9 does not allow the State to use that information. *Id.* at 221.

These are critical provisions for ensuring that searches of extensive and sensitive personal data do not overstep constitutional bounds. But here, the State seeks to roll back *Mansor*’s protections by advocating for broad and imprecise rules that will not effectively guide issuing courts. Pet’r Br. at 2–3. The Court should reject the State’s proposed rules of law, which neither provide adequate guidance to courts nor ensure that warrants issued in accordance with the proposed rules will be constitutional. Warrants must not permit rummaging searches through any data on a device, an outcome that

the State’s proposed rules would allow. The State’s proposals muddle rather than improve on the rule this Court cites in *Mansor*: A “warrant must identify, as specifically as reasonably possible in the circumstances, the information to be searched for, including, if relevant and available, the time period during which that information was created, accessed, or otherwise used.” 363 Or. at 218.

Further, in *Mansor*, the Court did not address the conditions under which warrants must identify the *type* of computer file to be sought,¹ although it suggested that such a requirement would be “unworkable.” *Id.* at 215. Amici request that the Court consider the question in this case, and hold that warrants usually can and—where possible—*should* limit police searches by relevant file type.

It is true that an issuing judge can only “describe what investigating officers believe will be found on electronic devices with as much specificity as possible under the circumstances.” *Id.* at 216 (quoting *Wheeler v. State*, 135 A.3d 282, 304 (Del. 2016)). And in some cases, courts may not be able to describe a specific *file or type* of digital evidence supported by probable

¹ The defendant in *Mansor* did not make this argument before this Court. 363 Or. at 341 (“Defendant clarifies that that element [of what investigating officers believe will be found on the electronic devices] does not necessarily mean the type of computer file, such as an email, text, or photograph.”)

cause. However, that will not usually be the case. Indeed, courts often will have sufficient context to limit search warrants to types of computer files, such as images, text messages, word-processing documents authored by the computer owner, or similar. These categories can be further refined by keyword searches, restricting police access to chats only between suspects, for example.

The rules amici propose do not limit *where* on a device law enforcement may search for relevant information,² but they do ensure that a search is narrowly tailored to capture only the *type* of data supported by probable cause, wherever it may be stored. For instance, modern forensic tools are designed to identify relevant data even if it is housed in unexpected places throughout the hard drive, whether innocently or due to an intentional effort to conceal its whereabouts. Deployment of these forensic capabilities reduces or eliminates the need to search digital files indiscriminately in order to uncover hidden evidence. Forensic tools also enable effective judicial oversight, as courts can require forensic analysts to keep a query log demonstrating their search procedures, thereby allowing judges to verify that

² In *Mansor*, this Court rejected the defendant's argument that warrants must identify places or specific locations where evidence is likely to be found on the computer. 363 Or. at 216–17.

evidence was not acquired through inappropriate rummaging.

Additionally, where the data targeted by a digital search is stored by an Internet communication service, such as a social media platform, an effective warrant can even more easily specify the type of data relevant to the inquiry. This is because third-party platforms house and organize data independently of their users, meaning that a criminal suspect *cannot* disguise one type of data (such as device location history) as another (such as tagged photos) on, for instance, a Facebook account in the same way that is theoretically possible, at least for a sophisticated user, on a hard drive. Therefore, if it is clear in a given case that communications between two social media accounts are likely to be relevant, it is probably unnecessary for a search warrant to authorize seizure of all those accounts' posted videos, for which there is no probable cause, as well.

It is worth noting that the three search commands the appellate court held were valid already tend to define permissible searches by something like file type. Command (3) permits a search for communications and specifies that this means voice, email, text, or other forms of communication. Command (5) identifies the permissible types of files to search as images, videos, or “data which depict[s]” J or Gregg engaged in conduct related to the charges. Command (6) permits a search of any

evidence related to use of internet sites associated with prostitution, specifically backpage.com. This could be rephrased as permitting a search of relevant “internet search and/or browser history.”

Finally, when searches happen pursuant to invalid warrant provisions, as apparently happened here, the evidence from those searches must be suppressed, even if the information *could* have been searched for and discovered under a valid provision.

ARGUMENT

I. THE STATE’S PROPOSED RULES OF LAW VIOLATE THE FEDERAL AND STATE CONSTITUTIONS.

The State argues for two rules of law regarding particularity requirements for warrants for electronic searches. First, the State proposes that a warrant’s search command is sufficiently particular if it provides a “reasonable degree of certainty [as to] whether a particular piece of data falls within the scope of that search command, **no matter how broad that scope is.**” Pet’r Br. at 2–3 (emphasis added). Second, the State proposes that a search command is not overbroad so long as it is “within the scope of the probable cause supporting it. . . . Even if that description **is not certain or precise enough to meet the specificity standard.**” *Id.* at 3 (emphasis added). Alone or together, these rules do not adequately guide judges issuing

warrants and are insufficiently protective of privacy in electronic information stored on a cell phone or hard drive.

The State’s proposed rules of law would lead judges in Oregon to issue unconstitutional warrants. Assume that police presented an affidavit establishing probable cause to believe that the defendant took photographs on his cell phone of paraphernalia associated with selling illegal drugs on June 12. The corresponding warrant would authorize a search of “all data stored on the defendant’s phone for photos related to drug sales on June 12.” That warrant would satisfy the *temporal* limitation requirement of *Mansor*. But it is not particular and would allow extensive rummaging through *all* data on the phone. Yet, under the State’s proposed rules, the government could argue that the warrant is sufficiently particular because it identifies the information sought—photos related to drug sales on June 12. As such, the warrant arguably specifies the data subject to search—even though, in this case, that means *all* data from a particular date. Further, the State’s proposed rules would treat this warrant as not overbroad, because the police would know to a “reasonable degree of certainty” that the drug paraphernalia photos must fall within the specified category of information to search—because that category includes *everything* on the phone.

But this is not what either the state or federal constitution allows.

Valid warrants must, to the extent possible, limit the personal data accessed and reviewed by investigators to specifically that for which there is probable cause.³ There will rarely, if ever, be probable cause to believe that *all data* stored on a given device, even with a date limitation, will relate to whatever crime is under investigation. The State’s malleable proposed rules, however, would permit warrants to authorize these sweeping searches.

The Court should reject the State’s arguments. As the logic of *Mansor*—and that of other privacy-protective opinions from courts around the country—demonstrates, warrants for digital data should to the extent possible describe the data sought, the relevant time frame, and the types or categories of files likely to contain the desired evidence. And as the facts of *Mansor* show, warrants *can* effectively limit searches by category of data, such as Internet search history, without leaving police investigations at the mercy of the changeable nature of electronic data. Modern forensic techniques and the practical logistics of digital searches enable and require that police narrow their focus in searching cell phones and other computers. The warrant can and must guide that search to be constitutional.

³ It is not clear whether the State’s “reasonable degree of certainty” is more, less, or the same as probable cause, which the Constitution requires.

II. CELL PHONES CONTAIN AN IMMENSE AMOUNT OF PRIVATE, SENSITIVE DATA.

Smartphones are ubiquitous, highly portable devices that “place vast quantities of personal information literally in the hands of individuals.” *Riley*, 573 U.S. at 386. Americans use their phones for a wide variety of purposes and, as a result, smartphones contain a voluminous and varied collection of data. While data is often organized by application or file type, even discrete categories of information—alone or in combination with each other—comprise a “digital record of nearly every aspect of [our] lives.” *Id.* at 375.

Cell phone use is now deeply entrenched in the fabric of daily life. Ninety-seven percent of Americans own a cell phone and 85% own a smartphone specifically.⁴ These devices are “such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude that they were an important feature of the human anatomy.” *Riley*, 573 U.S. at 385. Mobile devices have become the screen that people access first and most often.⁵ Nearly half of Americans check their smartphones as soon as

⁴ Pew Rsch. Ctr., *Mobile Fact Sheet* (Apr. 7, 2021), <https://www.pewinternet.org/fact-sheet/mobile/>.

⁵ John Koetsier, *We’ve Spent 1.6 Trillion Hours on Mobile So Far in 2020*, *Forbes* (Aug. 17, 2020),

they wake up in the morning.⁶ People proceed to spend an average of four hours a day using various apps on their phones.⁷ Cell phone use is so persistent that the medical field has adopted a term to describe the intense anxiety many people experience when they fear being separated from their cell phones: *NOMOPHOBIA: NO MOBILE PHONE PHOBIA*.⁸

Americans' dependency on smartphones has, intentionally and inadvertently, resulted in our phones containing vast troves of our personal information. Indeed, cell phones "differ in both a quantitative and a qualitative sense" from other objects because of "all [the personal information] they contain and all they may reveal." *Riley*, 573 U.S. at 393, 403. The "immense storage capacity" of smartphones allows them to function as "cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers," and to store

<https://www.forbes.com/sites/johnkoetsier/2020/08/17/weve-spent-16-trillion-hours-on-mobile-so-far-in-2020/>.

⁶ Diane Thieke, *Smartphone Statistics: For Most Users, It's 'Round-the-Clock' Connection*, ReportLinker (Jan. 26, 2017), <https://www.reportlinker.com/insight/smartphone-connection.html>.

⁷ App Annie, *The State of Mobile 2021* 7 (2021), available at <https://www.appannie.com/en/go/state-of-mobile-2021/>.

⁸ Sudip Bhattacharya et al., *NOMOPHOBIA: NO Mobile Phone PhoBIA*, 8 J. Fam. Med. Prim. Care 1297 (2019), available at <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6510111/>.

extensive historical information related to each functionality. *Id.* at 393.

Because a cell phone “collects in one place many distinct types of information”—for example, an address, a note, a prescription, a bank statement, or a video— cell-phone data “reveal much more in combination than any isolated record,” *id.* at 394, and they reveal much more about “an individual’s private interests or concerns.” *Id.* at 395.

The broad range of applications available to cell phone users and the ever-increasing amount of storage on new-generation devices mean that digital searches today implicate more data than ever before. For instance, one in five Americans currently use health-related smartphone apps—sometimes linked to wearable devices—to track information related to their location, movement and sleep patterns, heart rate, nutrition, menstrual cycles, and other sensitive health data.⁹ Other apps may monitor home security cameras, facilitate dating (and thereby reveal the user’s sexual

⁹ Justin McCarthy, *One in Five U.S. Adults Use Health Apps, Wearable Trackers*, Gallup (Dec. 11, 2019), <https://news.gallup.com/poll/269096/one-five-adults-health-apps-wearable-trackers.aspx>; Sarah Silbert, *All the Things You Can Track with Wearables*, Lifewire (Dec. 2, 2020), <https://www.lifewire.com/what-wearables-can-track-4121040/>; Geoffrey A. Fowler & Heather Kelly, *Amazon’s New Health Band Is the Most Invasive Tech We’ve Ever Tested*, Wash. Post (Dec. 10, 2020), <https://www.washingtonpost.com/technology/2020/12/10/amazon-halo-band-review/>.

orientation), track a household's budget, manage financial accounts, or send encrypted messages.¹⁰ Coupled with devices' rapidly increasing storage capacities, these apps mean that any given person's cell phone may reveal a comprehensive portrait of their health, their location history, their sexual preferences, their private conversations, their photos, their finances, their social and professional networks, and a myriad of other things from taste in music to political beliefs. In short, cell phones produce "a digital record of nearly every aspect of [users'] lives—from the mundane to the intimate." *Riley*, 573 U.S. at 395. While a single app or type of data can reveal an extraordinary amount about a person, the combination of the many different types of data on a phone can essentially reconstruct a person's life.

¹⁰ See, e.g., Blink, *Blink Home Monitor App*, <https://blinkforhome.com/blink-app> (last visited Mar. 29, 2022); Grindr, *About Grindr*, <https://www.grindr.com/about/> (last visited Mar. 29, 2022); Kinkoo, *Kinkoo*, <https://www.kinkoo.app/> (last visited Mar. 29, 2022); Mitch Strohm, *Digital Banking Survey: 76% of Americans Bank Via Mobile App—Here Are the Most and Least Valuable Features*, *Forbes* (Feb. 24, 2021), <https://www.forbes.com/advisor/banking/digital-banking-survey-mobile-app-valuable-features/>; Mary Meeker, *Internet Trends 2019*, Bond Capital, at 168 (June 11, 2019), available at <https://www.bondcap.com/report/itr19/>; Jack Nicas, Mike Isaac, & Shira Frenkel, *Millions Flock to Telegram and Signal as Fears Grow Over Big Tech*, *N.Y. Times* (Jan. 13, 2021), <https://www.nytimes.com/2021/01/13/technology/telegram-signal-apps-big-tech.html>.

Therefore, as this Court has recognized, Article I, section 9, “must be read in light of the ever-expanding capacity of individuals and the government to gather information by technological means.” *Mansor*, 363 Or. at 373.

III. WARRANTS CAN LIMIT LAW ENFORCEMENT SEARCHES BY CATEGORY OF DATA.

A. *Mansor* recognizes that warrants must be particular and not overbroad, especially when authorizing searches of digital devices.

The text and principles of Article I, section 9, can be traced directly to the Fourth Amendment to the United States Constitution. Under both provisions of law, it is axiomatic that officers must have probable cause to support the search of a cell phone. *See generally Mansor*, 363 Or. 185; *Riley*, 573 U.S. 373. Further, probable cause to search or seize *some* data on the phone cannot justify access to the totality of the phone’s contents; instead, warrants must offer sufficiently particular instructions and avoid giving law enforcement license to search an overly broad swath of information. Given the vast amounts of personal data stored on phones, and all that can be gleaned from that data, strict limits on digital searches and seizures are crucial to preserve privacy. *See, e.g., United States v. Galpin*, 720 F.3d 436, 447 (2d Cir. 2013) (discussing the need for “heightened sensitivity to the particularity requirement in the context of digital searches” due to the vast

amount of information that digital devices contain); *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1176 (9th Cir. 2010) (en banc) (per curiam), *overruled in part on other grounds by Demaree v. Pederson*, 887 F.3d 870 (9th Cir. 2018) (discussing the “serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant”); *United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir. 2009) (ability of a computer to store “a huge array” of information “makes the particularity requirement that much more important”).

In *Mansor*, this Court held that “warrant[s] must identify, as specifically as reasonably possible in the circumstances, the information to be searched for, including, if relevant and available, the time period during which that information was created, accessed, or otherwise used.” 363 Or. at 187–88. Further, *Mansor* held that warrants must describe, to the greatest degree of specificity possible, the information that law enforcement is authorized to search and seize—in other words, the data for which there exists probable cause. As this Court has emphasized, law enforcement may not “rummag[e]” indiscriminately through the vast amount of sensitive information stored on cell phones. *Id.* at 220.

The question remains, however, whether warrants should limit digital

searches by *file type* (for instance, authorizing the search and seizure of text messages, but not photos, from a specific time period). The *Mansor* Court did not reach this issue because the defendant did not pursue it. Thus, while the Court rejected the contention that warrants for digital devices should limit *where* investigators may search, such as a “My Documents” or “Downloads” folder, *id.* at 216, the Court did not consider whether they should require a list of relevant file *categories*. *Id.* (“Defendant clarifies that that element [of what investigating officers believe will be found on the electronic devices] does not necessarily mean the type of computer file, such as an email, text, or photograph.”). However, this Court suggested that it agreed with the court in *Wheeler*, 135 A.3d at 305, that limitations on types of files officers could search would be “unworkable.” *Mansor*, 363 at 215.

This is the question *amici* ask the court to address in this case.

B. Use restrictions, while essential, are not enough on their own to shield private and sensitive digital data.

Use restrictions on non-responsive data obtained pursuant to a lawful warrant are an essential Fourth Amendment protection for the reasons this Court stated in *Mansor*. The intermingled nature of digital data means that “[e]ven a reasonable search authorized by a valid warrant necessarily may require examination of at least some information that is beyond the scope of the warrant.” *Id.* at 220. As this Court recognized, this means that there is

always a risk that search warrants for digital devices could inadvertently become the electronic equivalent of general warrants, sanctioning the “undue rummaging that the particularity requirement was enacted to preclude.” *Id.* (internal quotation marks omitted). Thus, even where warrants authorize, and officers conduct, only reasonable searches, “individual privacy interests preclude the state from benefiting from that necessity by being permitted to use that evidence at trial.” *Id.* at 220–21. The State may not use information obtained in a computer search if the warrant did not authorize the search for that information, unless some other warrant exception applies. *Id.* at 221 (citing Orin S. Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 *Tex. Tech. L. Rev.* 1, 24 (2015) (advocating for use restrictions for data “nonresponsive” to the warrant)).

This rule instantiating use restrictions is privacy protective and disincentivizes police overreach—law enforcement would be disinclined to search too broadly if courts will exclude nonresponsive or inappropriately obtained evidence. However, use restrictions do not fully protect a person’s privacy and are at best an incomplete remedy. When a law enforcement cellphone search exceeds the scope of probable cause, investigators learn intimate information about the individual’s life, *regardless* of whether that

data is ultimately excluded at trial. Further, if an overbroad search leads to useful information, investigators will be incentivized to use “parallel construction,” an opaque and controversial (if not always illegal) technique whereby the government manufactures an alternative, valid discovery route for evidence obtained through illegal means or via techniques the government would rather not have publicly known or reviewed by a court. *See* Hum. Rights Watch, *Dark Side: Secret Origins of Evidence in U.S. Criminal Cases* (Jan. 9, 2018), <https://www.hrw.org/report/2018/01/09/dark-side/secret-origins-evidence-us-criminal-cases>; John Shiffman & Kristina Cooke, *Exclusive: U.S. Directs Agents to Cover Up Program Used to Investigate Americans*, Reuters (Aug. 5, 2013), <https://www.reuters.com/article/us-dea-sod/exclusive-u-s-directs-agents-to-cover-up-program-used-to-investigate-americans-idUSBRE97409R20130805> (parallel construction used to protect the DEA’s use of information from intelligence intercepts, wiretaps, and a massive database of telephone records); Jenna McLaughlin, *FBI Told Cops to Recreate Evidence from Secret Cell-Phone Trackers*, *The Intercept* (May 2016), <https://theintercept.com/2016/05/05/fbi-told-cops-to-recreate-evidence-from-secret-cell-phone-trackers/>; Jessica Glenza & Nicky Woolf, *StingRay Spying: FBI’s Secret Deal with Police Hides Phone Dragnet From*

Courts, The Guardian (Apr. 10, 2015), <https://www.theguardian.com/us-news/2015/apr/10/stingray-spying-fbi-phone-drag-net-police>; Jennifer Granick, *American Spies* 178, 224 (2017).

There is also the danger that, with enough information, police could concoct a story to support their prosecution of the original crime, even if the evidence for such a crime was sparse at the time the warrant was issued. “If you give me six lines written by the hand of the most honest of men, I will find something in them which will hang him.” Armand Jean du Plessis, Cardinal-Duc de Richelieu et de Fronsac as cited in Jehiel Keeler Hoyt, *The Cyclopedia of Practical Quotations* 763 (1896).

Finally, use restrictions do not protect an individual’s privacy in any instance where that person is not ultimately charged with a crime.

In sum, use restrictions—while a critical tool to ensure that illegally obtained information is not used to convict a defendant—are insufficient to protect the full extent of the substantial privacy interests at stake in digital searches.

C. A general requirement that warrants identify relevant file types is reasonable and effective for law enforcement.

Warrants can limit searches for electronic evidence by file type as well as by description and time without unduly interfering with law enforcement investigations. If there is probable cause to believe that co-

conspirators texted each other, there is no reason in the first instance to search photos. If investigators learn that suspicious texts attach photos, then the search can expand to those (and related) photos, either pursuant to a second warrant, or under the first warrant, as overseen by the issuing judge. This is not a heavy lift.

Widely used forensic software is capable of limiting searches to particular categories of data, which can then be sub-searched for the information approved in the warrant. As with e-discovery tools, such forensic software can also generate query or audit logs that supervising officers, prosecutors, magistrates, and defense attorneys can review to ensure that searches were performed in a narrow and constitutional manner.

There is U.S. Supreme Court precedent to support limiting searches by file type or category. *Riley* explicitly discussed the invasiveness of law enforcement access to different “categories,” “areas,” “types” of data, and “apps.” 573 U.S. at 395, 396, 399. The Court also pointed out that “certain types of data are also qualitatively different” from others in terms of privacy. *Id.* at 395. As the Fifth Circuit recently put it, the lesson of *Riley* is that “distinct types of information, often stored in different components of the phone, should be analyzed separately.” *United States v. Morton*, 984 F.3d

421, 425 (5th Cir. 2021), *reh'g en banc granted*, 996 F.3d 754 (5th Cir. May 18, 2021).

With increasing frequency, courts have followed *Riley* to hold that looking at the right categories of data, not all data, is the only plan that makes sense and complies with the Constitution. *See, e.g., State v. Bock*, 310 Or. App. 329, 335, 485 P.3d 931 (2021) (warrants may not authorize searches through any and all contents of electronic files that may contain circumstantial evidence about the owner or evidence of identified criminal offenses); *Burns v. United States*, 235 A.3d 758, 775 (D.C. Cir. 2020) (warrant authorizing search for categories of data for which there was no probable cause was “constitutionally intolerable”); *People v. Musha*, 131 N.Y.S.3d 514 (N.Y. Sup. Ct. 2020) (in child abuse case, there was probable cause to search the phone’s photographs, but not to examine web search history); *State v. McLawhorn*, 636 S.W.3d 210, 239–44 (Tenn. Crim. App. 2020) (officers cannot search entirety of phone to determine whether device has flashlight function); *Taylor v. State*, 260 A.3d 602 (Del. 2021) (warrant permitting search and seizure of “any/all data stored by whatever means” failed the Fourth Amendment and state constitutions’ particularity requirements); *In re United States of America’s Application for a Search Warrant to Seize and Search Elec. Devices from Edward Cunnius*, 770 F.

Supp. 2d 1138, 1147–1151 (W.D. Wash. 2011) (application to search and seize “all electronically stored information . . . contained in any digital devices seized from [defendant’s] residence for evidence relating to the crimes of copyright infringement or trafficking in counterfeit goods” was improper because it sought “the broadest warrant possible,” and did not propose to use a search technique that foreclosed the plain view doctrine’s application to digital materials). As these cases demonstrate, even when there is probable cause to search a device for *something*, courts routinely hold that file types that are not connected to the probable cause showing may not be accessed or examined.

To be clear, warrants should limit searches based on time frame, information sought, *and* file type—especially when authorizing searches of sensitive categories of data such as personal conversations. For example, in *People v. Herrera*, 357 P.3d 1227 (Colo. 2015), the Colorado Supreme Court suppressed evidence contained in a text message involving a third party not named in the warrant. The court held that the government’s argument that *any* text message folder could be searched because of the abstract possibility that the folder might contain indicia of who owned the phone, or might have been deceptively labeled, would result in an unconstitutional limitless search. *Id.* at 1230, 1233–34. Thus, the appropriate

search criteria would have identified the relevant file type (text messages) *and* the text conversations relevant to the inquiry (those involving the individuals named in the warrant). These functional limitations can be constitutionally required, as the law is clear that police cannot get a warrant to seize or search categories of data for which there is no probable cause. *See, e.g., In re Search of Black iPhone 4*, 27 F. Supp. 3d 74, 79 (D.D.C. 2014).

D. Under careful judicial supervision, forensic tools enable highly effective and properly scoped searches and seizures of digital material.

Search features, as well as forensic tools, can narrow down the information an investigator seeks to only that which is responsive to key terms—just as one might use Google to search the web—and can display information about the results and their location on the device. Investigators can refine their queries using keyword searches, including Boolean queries like those lawyers use in a Westlaw search. Moreover, the power of these tools makes it far more difficult, perhaps impossible, for the casual computer user to effectively hide, obscure, or mislabel evidence.

The tools also perform targeted searches, which enable investigators to comprehensively and efficiently home in on the digital evidence most likely to be warrant-responsive, while ignoring other information.

Investigators can limit a search to a particular date range, allowing analysts to obtain files within temporal proximity of the relevant crime.¹¹ Forensic tools can also search based on file category or type. For example, EnCase Forensic Software (“EnCase”) is a law enforcement search tool for hard drives and mobile devices. EnCase can be configured to search for specific files or types of data on a computer—such as emails, Internet searches,¹² photographs,¹³ documents,¹⁴ files over a specified size,¹⁵ files with a particular extension,¹⁶ files containing personal identifying information (such as email addresses and credit card, Social Security, and phone numbers),¹⁷ or files containing certain keywords.¹⁸ Law enforcement widely

¹¹ See, e.g., AccessData, *Forensic Toolkit User Guide* 102 (2017), available at https://ad-pdf.s3.amazonaws.com/ftk/FTK%206.1/FTK_UG.pdf (FTK User Guide) (“Refine evidence further by making the addition of evidence items dependent on a date range or file size that you specify. However, once in the case, filters can also be applied to accomplish this.”).

¹² Guidance Software, *EnCase Forensic User Guide Version 8.07* 64–65 (2018), available at <http://encase-docs.opentext.com/documentation/encase/forensic/8.07/Content/Resources/External%20Files/EnCase%20Forensic%20v8.07%20User%20Guide.pdf>.

¹³ *Id.* at 62.

¹⁴ *Id.*

¹⁵ *Id.*

¹⁶ *Id.*

¹⁷ *Id.* at 338.

¹⁸ *Id.* at 143, 246.

uses these forensic tools because they search regardless of how the information is stored or named. For example, while file extension search filters are imperfect (since a suspect could disguise a photo by resaving a “.jpg” to a “.doc” extension),¹⁹ “file header” functionalities on EnCase can determine a file’s format regardless of filename or extension.²⁰ Forensic software programs can also detect embedded file images—that is, photographs hidden inside of Microsoft Word documents.²¹ And while keyword searches can be imperfect,²² today Optical Character Recognition (“OCR”)—a common forensic tool which automatically extracts text contained in graphic files, such as images or non-searchable PDFs—

¹⁹ Computer Crime & Intellectual Prop. Sect., Crim. Div., U.S. Dep’t of Just., *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* 36 (2009), available at <https://perma.cc/VP23-RZTJ> (DOJ Manual) (quoting *United States v. Adjani*, 452 F.3d 1140, 1150 (9th Cir. 2006)).

²⁰ Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 545 (2005).

²¹ See, e.g., AccessData, *Forensic Toolkit User Guide* 139 (2017), https://ad-pdf.s3.amazonaws.com/ftk/FTK%206.1/FTK_UG.pdf (FTK User Guide) (“To recover embedded or deleted files, the case evidence is searched for specific file headers. . . . Embedded or deleted items can be found as long as the file header still exists.”).

²² DOJ Manual at 79.

addresses that challenge.²³ EnCase can also automatically identify illegal files (such as child pornography) without a human investigator needing to open the file.

Forensic tools may also have a search history feature, just as eDiscovery tools do.²⁴ Such query or audit logs facilitate a post-search review to ensure law enforcement complied with the dictates of the warrant. With such logs, judges could better understand the precise steps that law enforcement took when search a cell phone. In particular, these logs could equip judges to better assess the reasonableness of the search technique and ascertain if the search was sufficiently narrowly tailored to the warrant. If courts were to insist upon the production of digital audit logs created by the forensic tool upon the return of a search warrant, tool vendors that do not already provide this functionality would rapidly develop this feature.

²³ FTK User Guide at 95 (“The [OCR] process lets you extract text that is contained in graphics files. The text is then indexed so that it can be[] searched[] and bookmarked.”).

²⁴ See, e.g., Microsoft, *Search for eDiscovery Activities in the Audit Log*, Microsoft Docs (Jan. 7, 2022), <https://docs.microsoft.com/en-us/microsoft-365/compliance/search-for-ediscovery-activities-in-the-audit-log?view=o365-worldwide> (Content search and eDiscovery-related activities are logged in the audit log when creating, starting, and editing Content searches, and performing search actions, such as previewing, exporting, and deleting search results, among other activities.).

There are many such products on the market and available to law enforcement at the state and local level, as well as to the FBI. For instance, similar tools include Forensic ToolKit and Cellebrite. Research by the firm Upturn shows that mobile device forensic tools are widely available even to smaller law enforcement agencies, which either purchase them outright, obtain them through federal grants, or work with larger local law enforcement agencies that conduct extractions of data at the smaller agencies' request. Upturn, *Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones* (Oct. 2020), available at <https://perma.cc/7DCK-PGMQ>.

In sum, forensic search tools can therefore make searches limited by file type workable, while also being effective for law enforcement. Certainly, limiting searches by file category or type will not always be possible. But it often is, and in those situations, this Court should require that warrants indicate, and officers observe, that limitation.

File-type limitations are not, however, a panacea—and they require judicial regulation to be used both effectively and lawfully. Like any search technique, forensic search tools can be over- or under-inclusive. And forensic tools can extract more and different types of data than manual searches, and analyze that data far more efficiently than human reviewers

acting alone. Indeed, they can even reveal information that the owner does not know is there, and, by gathering hidden and deleted files, exacerbate the potential for indiscriminate and overbroad searches. As with manual searches, forensic searches potentially expose substantial amounts of irrelevant info to manual review by investigators. For this reason, some technical experts have warned that forensic search tools “are simply too powerful in the hands of law enforcement and should not be used.”²⁵

However, proper warrants and judicial oversight can ensure that these powerful tools are used in ways that reduce rummaging, limit law enforcement agents’ exposure to non-responsive information, and enable judicial oversight and auditing of the search process.

E. Warrants can effectively limit by data category government searches and seizures of social media account information.

Seizures and searches of information stored in social media or other online accounts are different from those seeking data stored on a phone or hard drive. In the latter case, officers will typically seize computer hardware,

²⁵ Upturn, *Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones* 5. The Upturn report recommends at a minimum banning consent searches of mobile devices, abolishing the plain view exception for digital searches, and requiring easy-to-understand audit logs, enacting robust data deletion and sealing requirements, and requiring clear public logging of law enforcement use.

which contains all data on a device, and then extract that data for forensic analysis. The vast majority of the extracted data is irrelevant to the case, and highly intimate. This is why having a warrant effectively narrow the search is so important.

In contrast, obtaining every bit of information in an online account will usually be unnecessary, because it is relatively simple to identify, request, and seize only the categories of data relevant to the inquiry. For instance, providers preserve account data after the receipt of a warrant, so spoliation is less of a concern than when officers must seize a device from the suspect's possession. In addition to being able to preserve data, service providers have the capability of filtering out irrelevant data as directed by a warrant. Investigators can work with providers to ensure that only responsive information, as defined by the warrant, is ultimately disclosed.

Notably, it is not currently possible to hide evidence in the context of a Facebook or other social media account in the same way as a sophisticated computer user might be capable of on a hard drive or other local storage. *United States v. Blake*, 868 F.3d 960, 974 (11th Cir. 2017), *cert. den. sub nom. Blake v. United States*, 138 S. Ct. 1580 (2018). Information associated with an online account is stored, categorized, and sorted by the company—not by the user. Providers are able to effectively distinguish images from

text, find material by date, and filter conversations by participant or even keyword. Even sophisticated criminals cannot effectively hide evidence behind misleading file names or types online. “[T]here is no possibility that a user could have filed an incriminating photo as a ‘poke,’ and there is no chance that an incriminating message will be stored as a third-party password or a rejected friend request.” *United States v. Shipp*, 392 F. Supp. 3d 300, 309 (E.D.N.Y. 2019). The platform organizes the information in such a way that even a technologically sophisticated criminal cannot effectively conceal information in a different category of information, making broad searches especially unnecessary.

Further, seizing the entirety of online account data raises cybersecurity and oversight concerns as well as privacy considerations. Many of the information demands that we have seen officials list as part of common boilerplate warrants should almost never be permitted, such as passwords and PIN codes. This sensitive information can be used to prospectively spy on account holders, a technique that likely requires a wiretap warrant, not a Rule 41 warrant (or its state-law equivalent).²⁶ It risks

²⁶ The Fourth Amendment requires safeguards beyond traditional search warrants where surveillance consists of “a series [of intrusions] or a continuous surveillance” and not “one limited intrusion.” *Berger v. New York*, 388 U.S. 41, 57 (1967); *See also* Orin S. Kerr, *A User’s Guide to the Stored Communications Act—And a Legislator’s Guide to Amending It*, 72

abuse by enabling officers to repeatedly access accounts without judicial oversight. Passwords can also be misused to send fake messages, impersonate the account holder, or even create false evidence—and it is a rare scenario where the password itself will constitute relevant evidence supported by probable cause.

In *Shipp*, 392 F. Supp. 3d 300, for example, a search warrant to Facebook demanded all of the suspect’s personal information, activity logs, photos and videos, as well as materials posted by others that tagged the suspect, all postings, private messages, and chats, all friend requests, groups and applications activity, all private messages and video call history, check-ins, IP logs, “likes,” searches, use of Facebook Marketplace, payment information, privacy settings, blocked users, and tech-support requests. *Id.* at 303–06. This list was not limited to the types of information likely to provide evidence of the specific crime under investigation. And the district court expressed “serious concerns regarding the breadth of [the] Facebook warrants.” *Id.* at 307. Warrant-issuing courts “can and should take particular care to ensure that the scope of searches involving Facebook are ‘defined by

Geo. Wash. L. Rev. 1208, 1232 (2004) (stating it is the functional equivalent of a wiretap if an agent installs software that copies incoming messages a few milliseconds after they arrive).

the object of the search and the places in which there is probable cause to believe that it may be found.”” *Id.* (citing *United States v. Ross*, 456 U.S. 798, 824 (1982)). If, for example, a case involves a conspiracy to sell drugs, the police do not need passwords, tagged posts, or “likes.” In *Shipp*, the “all-content” warrant far exceeded those limits in purporting to authorize seizure of all this information.

To limit up front the information to which the government gets access, courts should reject “all-data,” “all-content,” or boilerplate service-provider warrants containing comprehensive lists of types of data in favor of a defined list of relevant categories of data tailored to the investigation at hand. For example, if the allegations are that a suspect sent photos of guns to prospective buyers over WhatsApp, the warrant can authorize a search of WhatsApp chats and associated photos sent through the application—passwords, location history, and other account data would be irrelevant. Keyword searches may be an option to further limit the data that a service provider discloses to law enforcement. The government must be required to narrow the data it seizes from online service providers by asking the provider to limit disclosures based on keywords, such as the name of a co-conspirator, a bank account number used for illegal proceeds, or reference to the address where a burglary took place.

For example, officers could limit the warrant to demand only messages between co-conspirators. If Bob and Alice are collaborating, Google may be able to parse just emails between those two, just as account holders can do when they search their inboxes. The government should also limit its acquisition to messages sent by the suspect, or exclude emails between suspects and their employers, identified attorneys, clergy, or spouses, or notifications from social media entities like Facebook or Twitter.

In the Matter of the Search of Premises Known as: Three Hotmail Email Accounts, No. 16-MJ-8036-DJW, 2016 WL 1239916, at *7, *14 (D. Kan. Mar. 28, 2016) (suggesting that warrants could direct an online service provider to produce responsive material in a manner devoid of the exercise of investigatory skill or discretion).²⁷ See also *In the Matter of the Search of Info. Associated with [redacted]@mac.com that Is Stored at Premises Controlled by Apple, Inc.*, 13 F. Supp. 3d 145 (D.D.C. 2014), order vacated, 13 F. Supp. 3d 157 (D.D.C. 2014); *In the Matter of Applications for Search Warrants for Info. Associated with Target Email Accounts/Skype Accounts*,

²⁷ The magistrate was overturned by the District Court, which ruled that the “seize first, search second” process did not require these limitations. *In the Matter of the Search of Info. Associated with Email Addresses Stored at Premises Controlled by the Microsoft Corp.*, 212 F. Supp. 3d 1023, 1037 (D. Kan. 2016).

Nos. 13–MJ–8163–JPO, 13–MJ–8164–DJW, 13–MJ–8165–DJW, 13–MJ–8166–JPO, 13–MJ–8167–DJW, 2013 WL 4647554 (D. Kan. Aug. 27, 2013).

Images may be another area where providers’ built-in search capabilities enable more tailored data seizures. For instance, Google Photos is designed to do image searches. Google, *About Google Photos*, <https://www.google.com/photos/about/> (last visited Mar. 29, 2022) (explaining that photos saved to Google photos “are automatically organized and searchable” by their associated geolocation information and the things in them). Investigators might seek from Google only those photos that were taken at a particular location or that contain the image of a particular person of interest.

The main objection to having online service providers search for and disclose only a portion of online account data is that providers are poorly positioned to conduct investigations for law enforcement. Providers do not know the facts of the investigation and are not trained law enforcement actors. However, warrants with specifications such as data category limitations, time frames, email to/from limits, and photo location- or content-searches mean that providers need not understand the investigation or exercise any investigatory discretion in providing responsive information. The search terms should be clear, set by the investigators, and overseen by

the issuing magistrate or judge. Often, executing these advanced searches is well within the capability of the provider and requires no investigatory expertise. And investigators can then follow up on any leads by obtaining a second warrant.

IV. THIS COURT SHOULD HOLD THAT WHERE SOME OF THE WARRANT IS INVALID, ANY EVIDENCE ACTUALLY OBTAINED PURSUANT TO THOSE PROVISIONS SHOULD BE SUPPRESSED.

The appellate court rejected the State's suggestion that any data that *could* have resulted from a lawful section of the warrant should stand, and emphasized that Article I, section 9 rights hinge instead on how the search was *actually* conducted. This Court's jurisprudence and the principles underlying the Fourth Amendment support the appellate court's conclusion and this Court should adopt it.

“[R]ules of law designed to protect citizens against unauthorized or illegal searches or seizures of their persons, property, or private effects are to be given effect by denying the state the use of evidence secured in violation of those rules against the persons whose rights were violated.” *State v. Davis*, 295 Or. 227, 237, 666 P.2d 802 (1983). One purpose of rules requiring the suppression of evidence gathered in violation of the Oregon Constitution is to restore the parties to the position they would have been in

had the violation not occurred. The exclusionary rule of section 9 is predicated on the personal right of a criminal defendant to be free from an “unreasonable search, or seizure.” *Id.* at 231–37; *State v. Laundry*, 103 Or. 443, 494, 206 P. 290 (1922) (en banc).

Another goal of the suppression remedy is “to deter—to compel respect for the constitutional guaranty in the only effectively available way—by removing the incentive to disregard it.” *Elkins v. United States*, 364 U.S. 206, 217 (1960). “A ruling admitting evidence in a criminal trial ... has the necessary effect of legitimizing the conduct which produced the evidence, while an application of the exclusionary rule withholds the constitutional imprimatur.” *Terry v. Ohio*, 392 U.S. 1, 13 (1968).

Evidence is not inadmissible under Article I, section 9, simply because it was obtained after unlawful police conduct. But to save the evidence, the State must establish that the disputed evidence did not derive from the illegality. *State v. Johnson*, 335 Or. 511, 520–21, 73 P.3d 282 (2003). The test is not whether the disputed evidence *could have* be obtained lawfully, but rather whether *was* or *inevitably would have* been. *Id.* (in relevant part, state must prove that the police *inevitably* would have obtained the disputed evidence through lawful procedures even without the violation of the defendant's rights under Article I, section 9).

The State's proposed rule of law is to the contrary. It suggests that evidence obtained pursuant to invalid portions of a warrant may be admitted regardless of police conduct so long as there exists some theory under which the evidence could have fallen within the scope of a different, valid search command. This rule would not serve the purpose of the suppression remedy, which is, in part, to deter police misconduct. Police should not be applying for or executing unconstitutional searches. But the State's rule would invite them to do just that by blessing these illegal searches in at least some cases. The rule also conflicts with this Court's holding in *Johnson*, which requires that the acquisition of the evidence have been inevitable, not merely conceivable.

As in *State v. Bock*, 310 Or. App. 329, the State's argument is unworkable, and fails to serve the purpose of the exclusionary rule. Courts cannot retrace the forensic investigator's steps to determine whether a different search *might* have captured the same evidence. *Id.* at 340. Guessing what might have happened if the warrant terms were valid is a speculative enterprise beyond the scope of evidentiary proof.

Nor does such a rule provide the remedy required by Article I, section 9—making the defendant whole. As the appellate court explained, in the context of the plain view exception:

Although it might have been “expected” that state agents would examine each photo on defendant's cell phone in searching for location data, that fact does not make the search for those photos somehow less invasive. The state still had to conduct a broad search of defendant’s cell phone to find those photos to search them for location data in the first place. The breadth of the search is what renders the plain view doctrine inapplicable; the alternative would sanction the sort of general warrant that the plain view doctrine was never meant to authorize.

Id. (citing *Mansor*, 363 Or. at 220).

The court’s insight is no less true here. The State’s rule would bless an overbroad search pursuant to an unconstitutional warrant despite the lack of guidance to the police, and the improper review of private information.

CONCLUSION

The judgment of the Court of Appeals should be affirmed.

Dated: March 29, 2022

Respectfully Submitted,

/s/ Kelly K. Simon

Kelly K. Simon, OSB#154213

Rachel Dallal, TPN# T22032103

(temporarily licensed in Oregon,
barred in Washington)

AMERICAN CIVIL LIBERTIES

UNION OF OREGON

P.O. BOX 40585

Portland, OR 97240

Telephone: (503) 444-7015

E-mail: ksimon@aclu-or.org

Counsel continued on following page.

Jennifer Stisa Granick*
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
39 Drumm Street
San Francisco, CA 94111
Telephone: (415) 343-0758
E-mail: jgranick@aclu.org

** Pro hac vice application
forthcoming*

*Attorneys for Amici Curiae The
American Civil Liberties Union &
American Civil Liberties Union of
Oregon*

CERTIFICATE OF COMPLIANCE

I HEREBY CERTIFY that this brief complies with the word-count limitation in ORAP 5.05(1)(b)(ii)(B) because the word count on this brief (as described in ORAP 5.05(1)(d)(i)) is 8,876 words.

I certify that the size of the type in this brief is not smaller than fourteen points for both the text of the brief and footnotes, as required under ORAP 5.05(3)(b)(ii).

Dated: March 29, 2022

/s/ Kelly K. Simon

Kelly K. Simon, OSB#154213

American Civil Liberties

Union of Oregon

P.O. BOX 40585

Portland, OR 97240

Telephone: (503) 444-7015

E-mail: ksimon@aclu-or.org

*Attorney for Amici Curiae The
American Civil Liberties Union &
American Civil Liberties Union of
Oregon*

CERTIFICATE OF FILING AND SERVICE

I HEREBY CERTIFY that on March 29, 2022, I caused the foregoing Brief of Amici Curiae The American Civil Liberties Union and The American Civil Liberties Union of Oregon in Support of Defendant–Appellant Turay to be electronically filed with the State Court Administrator, Records Section, by using the Court’s electronic filing system.

I FURTHER CERTIFY that on March 29, 2022, I electronically served the foregoing Brief of Amici Curiae The American Civil Liberties Union and The American Civil Liberties Union of Oregon in Support of Defendant–Appellant Turay upon Ernest Lannet and Eric Johansen, attorneys for Appellant, and Peenesh Shah, Ellen F. Rosenblum, and Benjamin Guttman, attorneys for Petitioner, using the Court’s electronic filing system.

Dated: March 29, 2022

/s/ Kelly K. Simon

Kelly K. Simon, OSB#154213

American Civil Liberties

Union of Oregon

P.O. BOX 40585

Portland, OR 97240

Telephone: (503) 444-7015

E-mail: ksimon@aclu-or.org

*Attorney for Amici Curiae The American
Civil Liberties Union & American Civil
Liberties Union of Oregon*

IN THE SUPREME COURT OF THE STATE OF MONTANA

No. DA 20-0330

STATE OF MONTANA

Plaintiff–Appellee,

v.

BRADLEY MEFFORD,

Defendant–Appellant.

**BRIEF OF AMICI CURIAE AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF MONTANA AND AMERICAN CIVIL LIBERTIES
UNION FOUNDATION IN SUPPORT OF DEFENDANT–APPELLANT
BRADLEY MEFFORD**

On Appeal from the Montana Second Judicial District Court,
Silver Bow County, the Honorable Kurt Krueger, Presiding

Brett Max Kaufman
ACLU Foundation
125 Broad Street, 18th Fl.
New York, NY 10004
(212) 549-2500

Alex Rate
Akilah Lane
ACLU of Montana Foundation
P.O. Box 1968
Missoula, MT 59806
(406) 224-1447
ratea@aclumontana.org

Counsel for Amici Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES	iii
STATEMENT OF INTEREST OF AMICI	1
INTRODUCTION	2
ARGUMENT	6
I. CELL PHONES GENERATE, STORE, AND PROVIDE ACCESS TO VAST QUANTITIES OF SENSITIVE PERSONAL INFORMATION THAT REQUIRE HEIGHTENED CONSTITUTIONAL PROTECTIONS AGAINST WARRANTLESS SEARCHES, ANALYSIS, AND STORAGE.....	6
A. Cell phone searches raise significant privacy concerns because they provide access to vast amounts of personal information	6
B. Law enforcement is easily and cheaply able to extract, analyze, and store the entire contents of cell phones using advanced forensic tools, especially exacerbating privacy harms from warrantless, unjustified searches	8
II. CONSENT-BASED SEARCHES OF DIGITAL DATA MUST BE NARROWLY SCOPED TO THE OWNER’S EXPLICIT PERMISSION.....	13
A. The search in this case exceeded the scope of Mefford’s consent.....	13
B. A reasonable person would understand consent to search their cell phone as limited to common-sense categories of relevant information	16
C. Limitations on consent are particularly important because consent searches of cell phones raise unique concerns about law enforcement coercion	20
CONCLUSION.....	21
CERTIFICATE OF COMPLIANCE	

CERTIFICATE OF SERVICE

TABLE OF AUTHORITIES

CASES

<i>Arizona v. Gant</i> , 556 U.S. 332 (2009)	4, 13
<i>Carpenter v. United States</i> , 138 S. Ct. 2206 (2018)	2, 8
<i>Collins v. Virginia</i> , 138 S. Ct. 1663 (2018)	13
<i>Coolidge v. New Hampshire</i> , 403 U.S. 443 (1971)	4
<i>Florida v. Jimeno</i> , 500 U.S. 248 (1991)	17
<i>Florida v. Royer</i> , 460 U.S. 491 (1983)	13
<i>Katz v. United States</i> , 389 U.S. 347 (1967)	13
<i>Leaders of a Beautiful Struggle v. Balt. Police Dep’t</i> , 2 F.4th 330 (4th Cir. 2021)	2
<i>Payton v. New York</i> , 445 U.S. 573 (1980)	14
<i>People v. Hughes</i> , 958 N.W.2d 98 (Mich. 2020)	2
<i>Riley v. California</i> , 573 U.S. 373 (2014)	<i>passim</i>
<i>Stanford v. Texas</i> , 379 U.S. 476 (1965)	16
<i>State v. Allies</i> , 186 Mont. 99, 606 P.2d 1043 (1979)	14

<i>State v. Bailey</i> , 2010 ME 15, 989 A.2d 716	16
<i>State v. Cope</i> , 250 Mont. 387, 819 P.2d 1280 (1991)	15
<i>State v. Goetz</i> , 2008 MT 296, 345 Mont. 421, 191 P.3d 489	17, 18
<i>State v. Seader</i> , 1999 MT 290, 297 Mont. 60, 990 P.2d 180	4
<i>State v. Stone</i> , 2004 MT 151, 321 Mont. 489, 92 P.3d 1178	13
<i>State v. Thomas</i> , 2020 MT 222, 401 Mont. 175, 471 P.3d 733	17
<i>United States v. Blocker</i> , 104 F.3d 720 (5th Cir. 1997)	17
<i>United States v. Bosse</i> , 898 F.2d 113 (9th Cir.1990)	17
<i>United States v. Chandler</i> , No. 20-20476, 2021 WL 5233289 (E.D. Mich. November 10, 2021)	18
<i>United States v. Jones</i> , 565 U.S. 400 (2012)	2
<i>United States v. Washington</i> , 490 F.3d 765 (9th Cir. 2007)	20
<i>Walter v. United States</i> , 447 U.S. 649 (1980)	14, 18

CONSTITUTIONAL PROVISIONS

Mont. Const. art II, § 11	4, 13
---------------------------------	-------

OTHER AUTHORITIES

Alan Butler, <i>Get a Warrant: The Supreme Court’s New Course for Digital Privacy Rights After Riley v. California</i> , 10 Duke J. Const. L. & Pub. Pol’y 83 (2014)	7
Apple, <i>Compare iPhone Models</i>	7
Apple, <i>iCloud</i>	7
Assoc. Press, <i>Your Next iPhone Could Have 1 Terabyte of Storage</i> , NPR (Sept. 14, 2021).....	7
Devon W. Carbado, <i>(E)Racing the Fourth Amendment</i> , 100 Mich. L. Rev. 946 (2002)	20
Dropbox, <i>How Much is 1 TB of Storage?</i>	7
iClick, <i>How Big Is a Gig?</i>	7
J.D. Biersdorfer, <i>Getting Alerts from a Digital Pill Box</i> , N.Y. Times (June 5, 2017).....	21
Janice Nadler, <i>No Need to Shout: Bus Sweeps and the Psychology of Coercion</i> , 2002 Sup. Ct. Rev. 153 (2002).....	20
Logan Koepke et al., Upturn, <i>Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones</i> (Oct. 2020).....	10, 11, 12, 19
Marcy Strauss, <i>Reconstructing Consent</i> , 92 J. Crim. L. & Criminology 211 (2002)	20
Montana DOJ Attorney General, <i>Experts Use Digital Forensics to Crack Down on Cyber Crime</i> (Feb. 25, 2014).....	11
Ric Simmons, <i>Not “Voluntary” But Still Reasonable: A New Paradigm for Understanding the Consent Searches Doctrine</i> , 80 Ind. L. J. 773 (2005).....	12
App Annie, <i>The State of Mobile 2021</i> (2021).....	8

STATEMENT OF INTEREST OF AMICI

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 Montana is the local affiliate of the ACLU. The ACLU and the ACLU of Montana have frequently appeared before courts—including this one—throughout the country advocating for Americans’ right to privacy based on the Constitutions of both the United States and of Montana, both as direct counsel and as amici curiae. *See e.g., Carpenter v. United States*, 138 S. Ct. 2206 (2018); *People v. Hughes*, 958 N.W.2d 98 (Mich. 2020); *United States v. Wilson*, 13 F.4th 961 (9th Cir. 2021); *In re Search Warrant to Google for All Records Associated with Google Account scottarcla@gmail.com*, No. 20CCPC0020 (Cal. Super. Ct., L.A. Cnty. Nov. 12, 2020); *State v. Burch*, 961 N.W.2d 314 (Wisc. 2021); *People v. McCavitt*, No. 125550, 2021 WL 4898748 (Ill. Oct. 21, 2021).

Amici write to address only Issue One raised in the Brief of Appellant, whether the Fourth Amendment and the Montana Constitution prohibit warrantless intrusions into a person’s cell phone absent a recognized exception. BoA, filed Oct. 29, 2021, p. 1. In particular, we address the proper scope of searches based on consent, and not whether there was reasonable cause to search Mefford’s phone as a probationary search.

INTRODUCTION

Today, virtually everyone carries an electronic device that contains more personal information than could be found in the traditionally most constitutionally protected space—their own homes. *See Riley v. California*, 573 U.S. 373, 395–97 (2014). The more than eighty percent of Americans who own smartphones “keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate.” *Id.* at 395. For that reason, the United States Supreme Court, along with other federal courts and state high courts around the country, have over the past decade begun to recognize that more stringent protections against unjustified searches of digital data are necessary to ensure that the public’s constitutional rights are not overtaken and undermined by advancing technologies. *Carpenter v. United States*, 138 S. Ct. 2206 (2018) (cell-site location information); *Riley*, 573 U.S. 373 (electronic device search incident to arrest); *United States v. Jones*, 565 U.S. 400 (2012) (warrantless GPS tracking); *People v. Hughes*, 958 N.W.2d 98 (Mich. 2020) (overbroad cell phone searches); *Leaders of a Beautiful Struggle v. Balt. Police Dep’t*, 2 F.4th 330 (4th Cir. 2021) (city-wide aerial surveillance).

This case illustrates why exceedingly strong protections against unreasonable searches—including reading the scope of consent-based searches narrowly—are necessary in the digital age. Appellant Mefford’s parole officer

asked to view Mefford's phone to confirm Mefford's explanation for why he had committed a technical parole violation—sitting in his apartment complex's parking lot after curfew to obtain Wi-Fi Internet service and talk to his daughter on a messaging app. Mefford agreed to show his text messages with his daughter from that night, and the parole officer reviewed the relevant app data, which confirmed that Mefford was talking to a female person that evening. At that point, the search should have concluded. Instead, the officer exceeded the scope of the consensual search by failing to return Mefford's phone and continuing to look through Mefford's phone to examine Mefford's photo files. The officer did so on his own hunch, and his own say-so. Extending the search beyond the terms of the consent that Mefford gave amounts to unconstrained searching of private digital papers beyond any reasonable interpretation of consent in this case.

When a search is based on consent, that search can go no farther than the consent actually given, even if the officers' purpose in extending the investigation is to look for evidence of the same offense. A consent search is lawful only because the suspect agrees to it. Mefford agreed only to review of his in-app messaging conversation with a specific person on a specific date and time. In order to continue searching beyond the bounds of Mefford's consent, the officer needed to ask for additional consent, get a warrant, or have another exception to the warrant requirement apply.

The Fourth Amendment’s purpose is to avoid “giving police officers unbridled discretion to rummage at will among a person’s private effects.” *Arizona v. Gant*, 556 U.S. 332, 345 (2009); *see also State v. Seader*, 1999 MT 290, ¶¶ 11, 14, 297 Mont. 60, ¶¶ 11, 14, 990 P.2d 180, ¶¶ 11, 14 (discussing Mont. Const. art II, § 11). Narrow permission or justification to search for specific information on an individual’s cell phone does not authorize the State to search through *any other* information on the phone. Contrary logic would open the door to just such “general, exploratory rummaging” as the “‘general warrant’ abhorred by the colonists.” *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971). Consent must be read very narrowly, or the State will be permitted to rummage at will among a person’s most personal and private information on the thinnest of justifications. This Court should reject that position.

Moreover, broadening the scope of an individual’s consent beyond the bounds of the permission the person expressed and would have reasonably understood to have given opens the door to expansive law enforcement access, copying and storage of an individual’s most private information. This expansion would be based solely on an officer’s assertion that the subsequent searches and seizures were justified because he wanted to investigate further. As such, it has the potential to eviscerate constitutional protections for privacy and against

unreasonable searches that have heretofore been narrowly and delicately circumscribed.

This Court should ensure that law enforcement is not able to invade Montanans' most private domains without strictly satisfying an exception to the warrant requirement, and it should make clear that the scope of consent to search a cell phone is limited to what a reasonable person would believe from the totality of the circumstances, and nothing more.

ARGUMENT

I. **CELL PHONES GENERATE, STORE, AND PROVIDE ACCESS TO VAST QUANTITIES OF SENSITIVE PERSONAL INFORMATION THAT REQUIRE HEIGHTENED CONSTITUTIONAL PROTECTIONS AGAINST WARRANTLESS SEARCHES, ANALYSIS, AND STORAGE.**

Modern cell phones contain a wealth of sensitive information that would never have been accessible to law enforcement before the digital age. And today, government agencies have advanced forensic tools that can extract and analyze all of the data stored on a cell phone, including data that the user might not even know exists. When law enforcement searches and analyzes an individual's cell phone data, it invades that individual's expectation of privacy protected by the U.S. and Montana Constitutions, and it must obtain a warrant—or an exception to the warrant requirement, narrowly circumscribed to avoid unmerited intrusion into the vast amounts of personal information now stored on digital devices, must apply.

A. **Cell phone searches raise significant privacy concerns because they provide access to vast amounts of personal information.**

A smartphone is a palm-sized portal into an individual's personal life, as smartphones “place vast quantities of personal information literally in the hands of individuals.” *Riley*, 573 U.S. at 386. In *Riley*, the U.S. Supreme Court recognized that cell phone searches “implicate privacy concerns far beyond those implicated” by the search of any other object and thus require heightened constitutional protections. *Id.* at 393. This is partly because cell phones have become “such a

pervasive and insistent part of daily life”—so much so that they appear almost “an important feature of human anatomy.” *Id.* at 385; *see also* Alan Butler, *Get a Warrant: The Supreme Court’s New Course for Digital Privacy Rights After Riley v. California*, 10 *Duke J. Const. L. & Pub. Pol’y* 83, 89–91 (2014).

Cell phone searches involve a quantitatively different privacy intrusion than do searches of physical items because of cell phones’ “immense storage capacity.” *Riley*, 573 U.S. at 393. And that disparity is only getting more dramatic. In 2014, when the U.S. Supreme Court decided *Riley*, the top-selling smartphone could store sixteen gigabytes of data. *Id.* at 394.¹ The minimum storage on Apple’s current line of iPhones is 128 gigabytes and up to one terabyte, equal to roughly twenty continuous days of high definition video, 250,000 personal photos, or six million pages of documents spanning 1,300 physical filing cabinets.² Off-device cloud storage services expand capacity even further.³ Storage capacities increase

¹ Sixteen gigabytes equals about 3,686 songs, 8,672 digital copies of *War and Peace*, 9,830 digital photos, or ten feature-length movies. *See* iClick, *How Big Is a Gig?*, <https://perma.cc/32XX-B3QP>.

² Apple, *Compare iPhone Models*, <https://perma.cc/LH9K-BEGC> (last visited Jan. 18, 2022). Assoc. Press, *Your Next iPhone Could Have 1 Terabyte of Storage*, NPR (Sept. 14, 2021), <https://perma.cc/FZZ6-EGKQ>; Dropbox, *How Much is 1 TB of Storage?*, <https://perma.cc/SM5K-CUWU> (last visited Jan. 18, 2022).

³ Apple, *iCloud*, <https://perma.cc/5UMQ-NV3K> (last visited Jan. 18, 2022) (providing up to 2TB of remote storage).

every year, as does the sheer volume of personal data stored on—and accessible from—cell phones.

Cell phones are also qualitatively different from other objects because they “collect[] in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record.” *Riley*, 573 U.S. at 394. Along with more traditional data like text messages, phone calls, and emails, the proliferation of smartphone apps⁴ for social media, health and activity, dating, video streaming, mobile shopping, banking, and password storage have created novel types of records that can “reveal an individual’s private interests or concerns.” *Id.* at 395. Location information in particular is “detailed, encyclopedic, and effortlessly compiled” by apps whenever a “cell phone faithfully follows its owner . . . into private residences, doctor’s offices, political headquarters, and other potentially revealing locales.” *Carpenter*, 138 S. Ct. at 2216, 2218.

B. Law enforcement is easily and cheaply able to extract, analyze, and store the entire contents of cell phones using advanced forensic tools, especially exacerbating privacy harms from warrantless, unjustified searches.

While this case involved a manual search of a cell phone into areas outside

⁴ See App Annie, *The State of Mobile 2021* (2021), <https://www.appannie.com/en/go/state-of-mobile-2021> (gathering the most popular apps of 2020).

the bounds of the legitimate object of the search, the district court opinion’s expansive interpretation of consent could have profound implications given modern advances in law enforcement surveillance technologies. In recent years, law enforcement agencies across the country have acquired powerful new tools to conduct detailed forensic searches of cell phones. These forensic search techniques are problematic because of how much additional personal information the searches can reveal when *all* of the data from a phone is extracted, organized, and categorized in unexpected ways, stored indefinitely, and available to generate leads in cases completely unrelated to the original search.

As discussed above, a police officer’s manual search of areas of a phone beyond an individual’s limited consent can reveal a great deal of private information. Perusing a person’s map data can reveal where and when somebody went to their place of worship, or whether they attended a recent political protest. Clicks on some photographs, a financial app, or a message thread can reveal private medical data. And a scroll through a person’s email inboxes, or even a contacts list, can expose a person’s other private associations, preferences, or the like.

With technology, access to and analysis of this sensitive information becomes even easier—and even more frightening for privacy. Mobile device forensic tools (“MDFTs”) enable law enforcement to first extract and then analyze

a complete copy of a cellphone’s contents. Logan Koepke et al., Upturn, *Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones* 1–2 (Oct. 2020) [hereinafter Upturn Report], <https://perma.cc/7DCK-PGMQ>.⁵ MDFTs extract “the maximum amount of information possible” from a phone, including a user’s contacts, call logs, text conversations, photos, videos, saved passwords, GPS location records, phone usage records, online account information, and app data. *Id.* at 10, 16. MDFTs can access data stored remotely in the cloud and even data (like messages and photos) that the user previously deleted. *Id.* at 16–17, 21–23. MDFTs can also use login credentials stored on a phone to extract data from apps and services that are otherwise password-protected. *Id.* at 17–20.

MDFTs enable law enforcement to organize and draw connections in extracted data. They can aggregate data from different apps and sort it by GPS location, file type, or the time and date of creation, enabling police to view the data in ways a phone user cannot and to gain insights that would be impossible if the data were siloed by application. *Id.* at 12. Police can use a MDFT’s data-sorting capability to make sense of reams of data and tell a particular story about a person,

⁵ Upturn is a 501(c)(3) organization that works in partnership with many of the nation’s leading civil rights and public interest organizations to promote equity and justice in the design, governance, and use of digital technology.

including by revealing where they were (and what they were doing), when, with whom, and even why.

Today, law enforcement agencies of all sizes in all fifty states and the District of Columbia have access to these powerful data extraction and analysis tools and use them frequently, placing “[e]very American [] at risk of having their phone forensically searched by law enforcement.” *Id.* at 32. At least 2,000 law enforcement agencies nationwide, including in Montana, have purchased MDFTs, while agencies without their own MDFTs often access them through partnerships with MDFT-equipped departments or through federal forensic laboratories. *Id.* at 32, 35, 39; Montana DOJ Attorney General, *Experts Use Digital Forensics to Crack Down on Cyber Crime* (Feb. 25, 2014), <https://perma.cc/85UN-3JN7>. Many police departments readily admit that they consider MDFTs a standard investigatory tool and use them daily. Upturn Report at 47. At least 50,000 cell phone extractions took place between 2015 and 2019 among the forty-four agencies that reported statistics to Upturn. *Id.* at 41. This is a “*severe undercount*” of the national number, as the vast majority of the agencies that currently use MDFTs did not respond to Upturn’s inquiries or did not track MDFT use statistics at all or for the full period covered in the report. *Id.*

Despite the outcome of *Riley*, 573 U.S. at 386, many MDFT searches occur without warrants. Upturn’s recent report shows that police frequently conduct

detailed, warrantless forensic searches of cell phone data based on users’ purported consent. *Id.* at 46–47.⁶ Some examples are striking: of the 1,583 cell phones on which the Harris County, Texas Sheriff’s Office performed extractive searches from August 2015 to July 2019, 53 percent were consent searches or searches of “abandoned/deceased” phones. *Id.* at 46. Of the 497 cell phone extractions performed in Anoka County, Minnesota between 2017 to May 2019, 38 percent were consent searches. *Id.* at 47.

Once law enforcement extracts cell phone data, it has the technological capability to store the data forever and search it at will. In this way, through simple consent, the State could come to possess massive amounts of information about a person that, unless subject to legal limitations, could be retained indefinitely and searched at a later date. This is a patently unreasonable power for police to wield—and this Court should make clear that the U.S. and Montana Constitutions do not permit such abuse.

⁶ Consent has become an increasingly common justification for searches of physical evidence as well. *See, e.g.,* Ric Simmons, *Not “Voluntary” But Still Reasonable: A New Paradigm for Understanding the Consent Searches Doctrine*, 80 Ind. L. J. 773 (2005) (more than 90 percent of warrantless searches are accomplished through the use of consent).

II. CONSENT-BASED SEARCHES OF DIGITAL DATA MUST BE NARROWLY SCOPED TO THE OWNER’S EXPLICIT PERMISSION.

Warrantless searches are “per se unreasonable under the Fourth Amendment” unless they fall within one of the “few specifically established and well-delineated exceptions” to the warrant requirement. *Gant*, 556 U.S. at 338 (quoting *Katz v. United States*, 389 U.S. 347, 357 (1967)); *State v. Stone*, 2004 MT 151, ¶ 18, 321 Mont. 489, ¶ 18, 92 P.3d 1178, ¶ 18 (discussing Mont. Const. art II, § 11). Once an exception to the warrant requirement is invoked, courts must ensure that its application is “limited in scope to that which is justified by the particular purposes served by the exception.” *Florida v. Royer*, 460 U.S. 491, 500 (1983); accord *Collins v. Virginia*, 138 S. Ct. 1663, 1671–72 (2018) (a warrantless search must not be “untether[ed] . . . from the justifications underlying it” (cleaned up)). In the context of searches of electronic devices, the “vast quantities of personal information” at stake make it all the more critical to ask whether application of the exception “to this particular category of effects would ‘untether the rule from the justifications underlying the . . . exception.’” *Riley*, 573 U.S. at 386 (quoting *Gant*, 556 U.S. at 343).

A. The search in this case exceeded the scope of Mefford’s consent.

Here, the record shows that Mefford gave consent only to a limited search of a single message thread in a specific app, to corroborate that at the time of

Mefford’s curfew violation, he was in the parking lot chatting with his daughter. Order at 2; *see* 1/7/19 Tr. at 11; D.C. Doc. 36 at 2. Miller “saw messages between Mefford and his daughter during the hours of concern.” Order at 2; *see* 1/7/19 Tr. at 11; D.C. Doc. 36 at 2. But Miller went further, developing his own, unannounced rationale to search through Mefford’s photos app. Order at 2; *see* 1/7/19 Tr. at 11; D.C. Doc. 36 at 2.⁷ A reasonable person would have understood Mefford’s consent to mean that he was granting Miller permission to search his phone so that he could “show him the messages from the time and date that was of concern.” 1/7/19 Tr. at 21. It was only after this that Miller took matters into his own hands.

Like warrant-based searches, consent searches are “limited by the terms of [their] authorization.” *Walter v. United States*, 447 U.S. 649, 656 (1980). This requirement helps avoid the indiscriminate searches and seizures that were the “immediate evils” motivating adoption of the Fourth Amendment. *Id.* at 657 (citing *Payton v. New York*, 445 U.S. 573, 583 (1980)). It is black letter law that searches and seizures conducted on the basis of consent are reasonable only if conducted within the scope of the consent: “Where items are seized which go beyond the scope of the consent given by a defendant, a successful arrest and prosecution

⁷ As Mefford’s brief explains, the State never even attempted to introduce evidence supporting Miller’s purported justification for expanding his search. App. Br. 7.

based on those items seized cannot pass constitutional muster.” *State v. Allies* (1979), 186 Mont. 99, 135, 606 P.2d 1043, 1062 (Shea, J., concurring in part and dissenting in part), *abrogated on other grounds by State v. Cope* (1991), 250 Mont. 387, 819 P.2d 1280. Given that cell phone searches can reveal voluminous amounts of people’s most sensitive information, and the enormous privacy implications of allowing broad law enforcement access to this data, courts must narrowly interpret the scope of consent when a cell phone search is in question.

With those principles in mind, and contrary to the district court’s reasoning, a reasonable person in Mefford’s position would consider their consent to search a cell phone to extend only to categories of data explicitly discussed with law enforcement in lay terms—not a search of other areas of phone. Here, a reasonable person would consider their consent to extend only to the probation officer viewing Mefford’s message application to find his conversation with his daughter on the night in question. 1/7/19 Tr. at 23. Mefford did not consent to the officer searching other data on the phone, for that purpose or for any other. 1/7/19 Tr. at 23, 31; App. Br. 8–9, 11–12.

Given the breadth and sensitivity of data on cell phones—the exact kind of information the U.S. Supreme Court said required heightened constitutional protections in *Riley*, 573 U.S. 373—the risks of an overbroad “consent” search to the device owner are severe. And consent searches are especially problematic

because they are conducted without judicial authorization or oversight. Allowing law enforcement to engage in hunch-based searches beyond the reasonably understood bounds of consent would mean that the government could invade any individual's privacy (including victims' and witnesses') without a warrant or other legal justification based only on an officer's mere assertion that his motivation was to search for additional, related evidence.

B. A reasonable person would understand consent to search their cell phone as limited to common-sense categories of relevant information.

As with the search-incident-to-arrest exception analyzed in *Riley*, this Court must assess how to apply a doctrine that originated “in the context of physical objects” such as luggage and vehicles, to this new context involving the “digital content on cell phones” or other electronic devices. 573 U.S. at 386. Consent searches remain permissible in the context of electronic devices, but to avoid narrow grants of consent from enabling sweeping searches of highly sensitive personal data, police and courts must interpret the scope of consent with “scrupulous exactitude.” *Cf. Stanford v. Texas*, 379 U.S. 476, 485 (1965). A reasonable person would not believe that giving consent to search a texting app on their cell phone would mean they were giving the police permission to perform a search of photos on the phone (or, even less, to use MDFTs to extract and store all of the phone's data). *See State v. Bailey*, 2010 ME 15, 989 A.2d 716 (a police

officer exceeded the scope of a suspect’s consent to search his computer for evidence of another person using his computer without authorization by running a general search of all video files on his computer).

Consent searches have always been limited by the scope of the permission granted. *Florida v. Jimeno*, 500 U.S. 248, 252 (1991); see *United States v. Blocker*, 104 F.3d 720, 728 (5th Cir. 1997) (Inspections are “limited to the purposes contemplated by the [consenting] suspect.” (alteration in original) (quoting *United States v. Bosse*, 898 F.2d 113, 115 (9th Cir. 1990))). Especially given the unique nature of digital data and the powerful tools law enforcement agencies now possess, it is objectively reasonable to define consent to search a cell phone as including only a limited, manual search of data relevant to the immediate matter, at least in the absence of clear and unambiguous evidence to the contrary. Otherwise, voluminous and intimate data could be readily subject to indiscriminate police review. The consent exception, which was largely developed prior to the advent of phones that store enormous amounts of data, should not be used to expand access to digital data, which the U.S. Supreme Court has held should be subject to more, not less, Fourth Amendment protection. *Riley*, 573 U.S. at 393.⁸

⁸ Moreover, “the range of warrantless searches which may be conducted pursuant to Montana’s Constitution is narrower than the corresponding range of searches which may be lawfully conducted under the Fourth Amendment to the U.S. Constitution.” *State v. Thomas*, 2020 MT 222, ¶ 13, 401 Mont. 175, ¶ 13, 471 P.3d 733, ¶ 13 (citing *State v. Goetz*, 2008 MT 296, ¶ 14, 345 Mont. 421, ¶ 14, 191 P.3d

With that in mind, common knowledge about how cell phones work would limit consensual access to particular categories of data found on a device. When a person looks for information on their own cell phone, they commonly open a particular app, such as text messages or email. They then search that specific category of data, either by scrolling through messages or by typing a query term in the search bar and pressing “Enter.” The owner reasonably expects the same common-sense “search” when giving consent to police.

Under the circumstances of this case, the layperson’s common-sense understanding that consent applies to particular categories of data on a device, and not to all information, should control. The U.S. Supreme Court’s decision in *Riley* rested in part on the observation that “a cell phone’s capacity allows even just one type of information to convey far more than previously possible.” 573 U.S. at 394. As a result, distinct types of information, usually stored in different parts of a phone, should be analyzed separately. *United States v. Chandler*, No. 20-20476, 2021 WL 5233289, *4–5 (E.D. Mich. November 10, 2021). Just as “[c]onsent to search a garage would not implicitly authorize a search of an adjoining house,” *Walter*, 447 U.S. at 656–57, consent to search text messages from last Tuesday

489, ¶ 14). And the State bears the burden to establish an exception to the warrant requirement. *Goetz*, ¶ 40.

would not implicitly authorize a search of text messages from last month, let alone photos or a contact list.

This limitation on the categories of data that can be searched would also apply to deleted information, information stored in the cloud, and data, such as incoming messages, that did not exist when law enforcement first received consent to search. Individuals generally do not give consent to a search for information they did not know or expect to be on the phone. For one, accessing data stored on the cloud and not actually resident on the device dramatically expands the scope of a search. *Riley*, 573 U.S. at 397. As the *Riley* Court explained, “[t]reating a cell phone as a container whose contents may be searched incident to an arrest is a bit strained as an initial matter. . . . But the analogy crumbles entirely when a cell phone is used to access data located elsewhere, at the tap of a screen.” *Id.* (citations omitted). Further, an ordinary person does not know that data they delete from their device is still “on” it and does not expect that anyone in possession of the phone can access deleted information. *See* Upturn Report at 21–22. When a person deletes data from their phone, they clearly indicate that they do not want anyone, including law enforcement, to look at the data, thus excluding it from the scope of consent. Finally, information like incoming text messages or emails that is received while the phone is in law enforcement’s possession cannot be considered within the scope of the original consent.

C. Limitations on consent are particularly important because consent searches of cell phones raise unique concerns about law enforcement coercion.

People may feel coerced to offer consent when law enforcement seizes or threatens to search their cell phones. Scholars and practitioners have long criticized the consent exception to the Fourth Amendment's warrant requirement on policy grounds, often referencing the inherently coercive nature of law enforcement "requests." *See, e.g.,* Marcy Strauss, *Reconstructing Consent*, 92 J. Crim. L. & Criminology 211, 236 (2002) ("most people would not feel free to deny a request by a police officer"); Janice Nadler, *No Need to Shout: Bus Sweeps and the Psychology of Coercion*, 2002 Sup. Ct. Rev. 153, 156 (2002) ("the fiction of consent in Fourth Amendment jurisprudence has led to suspicionless searches of many thousands of innocent citizens who 'consent' to searches under coercive circumstances"). Many have also observed that coercion is particularly present for people of color, and especially Black Americans, who may fear physical harm if they decline a request from a law enforcement officer. *See, e.g.,* Devon W. Carbado, *(E)Racing the Fourth Amendment*, 100 Mich. L. Rev. 946, 971–73, 972 n.121 (2002); *United States v. Washington*, 490 F.3d 765, 768–69, 773 (9th Cir. 2007) (finding recent incidents of white police officers shooting African Americans during traffic stops pertinent to assessment of voluntariness of consent).

In the cell phone context, people may feel additional coercion to consent to a

search just to get their device back. Cell phones perform many essential functions, serving as prescription drug reminders,⁹ and lifelines to app-based services such as Uber and Lyft. People who find themselves questioned by law enforcement may feel pressured to acquiesce to search requests to quickly regain access to the device, for example to call the babysitter and say that they've been delayed and will be home late. The inherent coerciveness of consent requests makes it all the more important that the scope of consent be narrowly construed.

CONCLUSION

For these reasons this Court should hold that Mefford's consent to allow the probation officer to see his text messages from the evening in question did not extend to photos on his phone and that the evidence discovered there was obtained unconstitutionally.

⁹ J.D. Biersdorfer, *Getting Alerts from a Digital Pill Box*, N.Y. Times (June 5, 2017), <https://perma.cc/M4DR-DABR>. (“The App Store stocks several pharmaceutical apps designed to organize your pills, schedule doses and remind you to take your medicine.”).

DATED this 19th day of January 2022

Brett Max Kaufman
ACLU Foundation
125 Broad Street, 18th Fl.
New York, NY 10004
(212) 549-2500

Alex Rate
Akilah Lane
ACLU of Montana Foundation
P.O. Box 1968
Missoula, MT 59806
(406) 224-1447
ratea@aclumontana.org

Counsel for Amici Curiae

CERTIFICATE OF COMPLIANCE

Pursuant to Rule 11 of the Montana Rules of Appellate Procedure, I certify that this brief is printed with a proportionately-spaced, 14-point Times New Roman typeface; is double spaced (excluding footnotes, quoted, and indented material); has margins of 1-inch; and has a word count of 4,797 words, excluding the exempted Table of Contents, Table of Authorities, Certificate of Compliance, and Certificate of Service.

DATED this 19th day of January 2022

/s/ Alex Rate

Alex Rate
ACLU of Montana Foundation
P.O. Box 1968
Missoula, MT 59806
(406) 224-1447
ratea@aclumontana.org

Counsel for Amici Curiae

CERTIFICATE OF SERVICE

I hereby certify that on the 19th day of January 2022, I served true and accurate copies of the foregoing Brief of Amici Curiae ACLU Foundation of Montana and ACLU Foundation on the following individuals:

Chad Wright (Counsel for Defendant–Appellant)
Office of State Public Defender
Appellate Defender Division
P.O. Box 200147
Service Method: eService

Eileen Joyce (Counsel for Plaintiff–Appellee)
155 W. Granite Street
Butte, MT 59701
Service Method: eService

Austin Miles Knudsen (Counsel for Plaintiff–Appellee)
215 N. Sanders
Helena, MT 59620
Service Method: eService

Electronically signed by Krystal Pickens on behalf of Alex Rate
DATED this 19th day of January 2022

CERTIFICATE OF SERVICE

I, Alexander H. Rate, hereby certify that I have served true and accurate copies of the foregoing Brief - Amicus to the following on 01-19-2022:

Eileen Joyce (Attorney)
155 W. Granite Street
Butte MT 59701
Representing: State of Montana
Service Method: eService

Austin Miles Knudsen (Govt Attorney)
215 N. Sanders
Helena MT 59620
Representing: State of Montana
Service Method: eService

Kristen Lorraine Peterson (Attorney)
Office of the Appellate Defender
555 Fuller Avenue
Helena MT 59620
Representing: Bradley Mefford
Service Method: eService

Jonathan Mark Krauss (Govt Attorney)
215 N. Sanders
P.O. Box 201401
Helena MT 59620
Representing: State of Montana
Service Method: eService

Electronically signed by Krystel Pickens on behalf of Alexander H. Rate
Dated: 01-19-2022

DA 20-0330

IN THE SUPREME COURT OF THE STATE OF MONTANA

2022 MT 185

STATE OF MONTANA,

Plaintiff and Appellee,

v.

BRADLEY MEFFORD,

Defendant and Appellant.

APPEAL FROM: District Court of the Second Judicial District,
In and For the County of Butte/Silver Bow, Cause No. DC 18-183
Honorable Kurt Krueger, Presiding Judge

COUNSEL OF RECORD:

For Appellant:

Chad Wright, Appellate Defender, Kristen L. Peterson, Assistant
Appellate Defender, Helena, Montana

For Appellee:

Austin Knudsen, Montana Attorney General, Jonathan M. Krauss,
Assistant Attorney General, Helena, Montana

Eileen Joyce, Butte-Silver Bow County Attorney, Samm Cox, Deputy
County Attorney, Butte, Montana

For Amici American Civil Liberties Union Foundation of Montana and
American Civil Liberties Union Foundation:

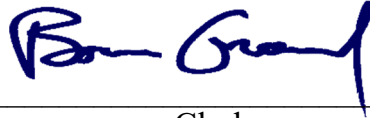
Alex Rate, ACLU of Montana Foundation, Missoula, Montana

Brett Max Kaufman, ACLU Foundation, New York, New York

Submitted on Briefs: June 29, 2022

Decided: September 27, 2022

Filed:

A handwritten signature in blue ink that reads "Ben Grand". The signature is written in a cursive style with a large initial "B".

Clerk

Justice Beth Baker delivered the Opinion of the Court.

¶1 Bradley Mefford appeals his conviction of Sexual Abuse of Children in the Montana Second Judicial District Court, Butte-Silver Bow County. Mefford asserts that the court should have suppressed the evidence his parole officer discovered when he conducted a warrantless search of Mefford's phone. He claims the officer's search was unreasonable because it exceeded the scope of Mefford's consent and because the parole officer lacked reasonable cause to conduct the additional search. Because the search exceeded the scope of any valid exception to the warrant requirement, we reverse.

FACTUAL AND PROCEDURAL BACKGROUND

¶2 In November 2016, Mefford was on parole from a 2006 Flathead County conviction for Criminal Possession with Intent to Distribute, Criminal Endangerment, and Assault with a Weapon. Mefford had been placed under the supervision of Butte Probation and Parole and was required to wear a Global Positioning System (GPS) monitor on his ankle and to adhere to a 10:00 p.m. curfew.

¶3 On November 26, 2016, Probation and Parole Officer Jake Miller observed through the GPS tracker that Mefford was in his apartment's parking lot after 10:00 p.m. Miller, along with Mefford's supervising officer Jerry Finley, conducted a home visit on November 29, 2016, to investigate Mefford's curfew violation. Mefford advised the officers that, because the service on his cellular phone was disconnected and he could access the internet only from his parking lot, he sat in his car to message his sixteen-year-old daughter through the Facebook Messenger application on his phone. Miller asked to

see Mefford's phone so he could verify his story, and Mefford gave him permission to use it. Mefford asked his girlfriend, with whom he lived, to get his phone from upstairs and give it to Miller. Mefford gave Miller his daughter's name and told him to look for their conversation on Facebook Messenger.

¶4 Miller opened Facebook Messenger and confirmed that Mefford was telling the truth—that he in fact was engaged in a Facebook Messenger conversation, with a person bearing the name Mefford provided, at the time that Mefford violated his curfew on November 26, 2016. He believed, however, that Mefford was messaging a woman older than his daughter, based on the person's profile picture on Facebook Messenger. Without asking any other questions, Miller opened the digital photo gallery application on Mefford's phone and discovered several photos depicting what he believed was child pornography. The officers detained Mefford and seized his phone. The Board of Pardons and Parole revoked Mefford's parole and returned him to the Montana State Prison to continue serving the active portion of his 2006 sentence.

¶5 Nearly a year later, Detective Sergeant Jeff Williams obtained a search warrant for the phone.¹ Williams turned the phone over to a forensic examiner, who determined that Mefford's phone contained approximately thirty images depicting child pornography or child erotica. The examiner also conducted a forensic extraction of the phone and

¹ A previous search warrant was issued, but the phone had been returned to law enforcement custody without analysis. Williams testified that the reason for the delay in reapplying for a warrant was that he did not become a detective until January 2017, and Mefford's case was part of a number of "outstanding" cases he was assigned after his promotion, sometime in October 2017.

determined that the photos most likely were downloaded from a file-sharing website. In July 2018, the State charged Mefford with Sexual Abuse of Children, in violation of § 45-5-625(1)(e), MCA, for knowingly possessing a visual medium “in which a child is engaged in sexual conduct, actual or simulated.”

¶6 Mefford moved to suppress the evidence and to dismiss the charge on the ground that Miller’s search was unlawful because it exceeded the scope of Mefford’s consent. The District Court held a suppression hearing. Miller testified that he requested permission to use Mefford’s phone “to confirm his story of being on the phone.” Miller said he opened the photo gallery to look for an image of Mefford’s daughter and compare it to the profile picture of the person Mefford was messaging, to confirm that she actually was his daughter. Mefford testified that his consent was limited to the Facebook Messenger application: “I told him, just go to the Messenger app . . . you should be able to see the conversation and the time. . . . I consented to him opening the Messenger app for . . . my daughter, to view the conversation I was having.” He added that he did not give Miller permission to search other areas of the phone; that Miller never asked him what his daughter looked like; and that Miller never asked Mefford if he could look through the photo gallery.

¶7 The District Court denied Mefford’s motion, finding that Miller’s warrantless search of the phone was a valid probationary search and that he did not exceed the scope of Mefford’s consent when he opened the photo gallery application.² The case went to trial,

² In the prosecutor’s affidavit for leave to file charges, he cited Miller’s November 2016 discovery of photos on Mefford’s phone. The affidavit also referred to information reported by Mefford’s prison cellmate months after Mefford’s phone was seized and he had been returned to custody for his parole revocation. There was no mention of this information at the suppression hearing, and

and a jury found Mefford guilty of Sexual Abuse of Children, under § 45-5-625(1)(e), MCA. The District Court sentenced Mefford to five years in the Montana State Prison, with no time suspended.

STANDARD OF REVIEW

¶8 “We review the denial of a motion to suppress to determine whether the district court’s findings of fact are clearly erroneous and whether its legal conclusions are correct.” *State v. Thomas*, 2020 MT 222, ¶ 9, 401 Mont. 175, 471 P.3d 733 (citation omitted). “Findings of fact are clearly erroneous if not supported by substantial credible evidence, if the court misapprehended the effect of the evidence, or if this Court’s review leaves a definite or firm conviction a mistake has been made.” *Thomas*, ¶ 9 (citation omitted).

DISCUSSION

¶9 *Whether the District Court erroneously rejected Mefford’s claim that his parole officer lacked a valid exception to the warrant requirement.*

¶10 The Fourth Amendment to the United States Constitution and Article II, Section 11, of the Montana Constitution guarantee individuals the right to be free from unreasonable government searches. U.S. Const. amend. IV; Mont. Const. art. II, § 11; *State v. Peoples*, 2022 MT 4, ¶ 12, 407 Mont. 84, 502 P.3d 129; *State v. Staker*, 2021 MT 151, ¶ 10 n.9, 404 Mont. 307, 489 P.3d 489; *Thomas*, ¶ 13. Both the Fourth Amendment and Article II, Section 11, provide that no warrant shall issue absent probable cause and a particular

the State made no claim that the warrant was issued on any factual basis other than the photos Miller saw on the phone in November 2016. The State makes no such argument on appeal.

description of the place to be searched. U.S. Const. amend. IV; Mont. Const. art. II, § 11; *Peoples*, ¶ 15.

¶11 Apart from Article II, Section 11, and its federal counterpart, the Montana Constitution provides an express right to individual privacy against government intrusion. Mont. Const. art. II, § 10; *State v. Smith*, 2021 MT 324, ¶ 12, 407 Mont. 18, 501 P.3d 398. Article II, Section 10, states that “[t]he right of individual privacy . . . shall not be infringed without the showing of a compelling state interest.” Mont. Const. art. II, § 10. “Together, Article II, Sections 10-11, provide a heightened state right to privacy, broader where applicable than the privacy protection provided under the Fourth and Fourteenth Amendments to the United States Constitution.” *Staker*, ¶ 9 (citations omitted).

¶12 A “search” occurs, within the meaning of the United States and Montana Constitutions, when “government action intrudes or infringes upon an individual’s reasonable expectation of privacy.” *Staker*, ¶ 10; *see also United States v. Jacobsen*, 466 U.S. 109, 113, 104 S. Ct. 1652, 1656 (1984). A “reasonable expectation of privacy” exists when “an individual has [(1)] a subjective expectation of privacy that is [(2)] objectively reasonable in society.” *Staker*, ¶ 11 (citing *Katz v. United States*, 389 U.S. 347, 361, 88 S. Ct. 507, 516 (1967) (Harlan, J., concurring)) (other citations omitted). “Whether an individual had a subjective expectation of privacy, and whether such expectation was objectively reasonable in society, are mixed questions of fact and law under the totality of the circumstances of each case.” *Staker*, ¶ 11 (citations omitted). If an individual demonstrates a reasonable expectation of privacy, thus triggering the protections of Article II, Sections 10 and 11, we turn to the nature of the State’s intrusion

to determine whether the search was “reasonable under the circumstances.” *State v. Goetz*, 2008 MT 296, ¶ 38, 345 Mont. 421, 191 P.3d 489.

¶13 Whether an individual had an actual, subjective expectation of privacy depends on various factors, including “the nature and circumstances of the location and setting at issue and the extent to which the subject overtly or implicitly assumed, considered, desired, or endeavored to ensure that the subject activity or information would remain concealed or undisclosed to others.” *Staker*, ¶ 21 (citations omitted); *see also Goetz*, ¶ 29 (“What a person knowingly exposes to the public is not protected, but what an individual seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.”) (citations omitted). The determination necessarily depends on “the particular facts of the case.” *Goetz*, ¶ 29.

¶14 Mefford maintains he had a subjective expectation of privacy in his phone’s digital photo gallery because of the vast quantity of personal information it contained. Mefford manifested this expectation when he gave Miller permission to open Facebook Messenger on his phone and told him what conversation to read. Miller implicitly recognized Mefford’s expectation of privacy by asking for permission to see his phone. The State does not dispute that Mefford had a subjective expectation of privacy in his photos. We agree.

¶15 The State similarly does not dispute Mefford’s argument that his expectation of privacy was objectively reasonable. We have recognized a reasonable expectation of privacy in cell phone communications. *See, e.g., State v. Stewart*, 2012 MT 317, ¶ 42, 367 Mont. 503, 291 P.3d 1187; *State v. Allen*, 2010 MT 214, ¶ 57, 357 Mont. 495, 241 P.3d 1045 (“society is willing to recognize as reasonable the expectation that private

cell phone conversations are not being surreptitiously monitored and recorded by government agents”). Cell phones have become storage devices for all manner of private information. As Amici highlight, “[a] smartphone is a palm-sized portal into an individual’s personal life,” which may contain up to “250,000 personal photos” and information about a person’s “health and activity, dating, video streaming, mobile shopping, banking, and password storage.” The United States Supreme Court recognized the unique privacy implications of modern cell phones in *Riley v. California*:

[A] cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form.

573 U.S. 373, 396-97, 134 S. Ct. 2473, 2491 (2014) (emphasis in original) (holding that police may not search the contents of a cell phone without a warrant and that the search incident to arrest exception did not apply to the photos and videos on the defendant’s phone). *See also State v. Neiss*, 2019 MT 125, ¶ 58, 396 Mont. 1, 443 P.3d 435, (analogizing a computer to a “container—for example a filing cabinet[] . . . capable of storing vast amounts of documents”). We agree with Mefford that his expectation of privacy in the information stored on his cell phone is one society recognizes as objectively reasonable. Miller’s action of accessing and viewing the contents of Mefford’s phone thus constituted a government search, triggering constitutional protections.

¶16 We consider the nature of the State’s intrusion to determine whether the search was reasonable under the circumstances. To be reasonable, the government intrusion must be justified by a compelling state interest and supported by “procedural safeguards such as a

properly issued search warrant” or a warrant exception. *Goetz*, ¶ 27; *see also Staker*, ¶ 13. Warrantless searches are “*per se* unreasonable except under certain recognized and narrowly delineated exceptions to the warrant requirement.” *Peoples*, ¶ 15 (citations omitted). “[B]ased on the heightened individual right to privacy under Article II, Section 10, the government must generally utilize the least intrusive means available to effect a warrantless search under a recognized exception to the warrant requirement of Article II, Section 11.” *Staker*, ¶ 12 (citations omitted). We have recognized “only a few ‘specifically established and well-delineated’” exceptions to the Article II, Section 11 search warrant requirement, *Nichols v. DOJ*, 2011 MT 33, ¶ 20, 359 Mont. 251, 248 P.3d 813 (quoting *State v. Loh*, 275 Mont. 460, 468, 914 P.2d 592, 597 (1996)), including, as pertinent here, the “consent” and “probation search” exceptions. *See Peoples*, ¶ 17; *State v. Dupree*, 2015 MT 103, ¶ 19, 378 Mont. 499, 346 P.3d 1114.

¶17 Mefford does not dispute the State’s compelling interest in the supervision of probationers and parolees but argues that the State lacked a valid warrant exception to search his phone beyond the messages needed to confirm his explanation. The State contends that Miller’s search was reasonable because it was justified by the “consent” and “probation search” exceptions to the warrant requirement.

Consent

¶18 Consent to search “is a recognized exception to the warrant requirement.” *State v. Snell*, 2004 MT 269, ¶ 9, 323 Mont. 157, 99 P.3d 191. To qualify as a valid exception, consent must be “given knowingly and voluntarily by an individual with the ability to consent.” *State v. Parker*, 1998 MT 6, ¶ 20, 287 Mont. 151, 953 P.2d 692. “When an

official search is properly authorized—whether by consent or by the issuance of a valid warrant—the scope of the search is limited by the terms of the authorization.” *State v. Graham*, 2004 MT 385, ¶ 22, 325 Mont. 110, 103 P.3d 1073 (quoting *Walter v. United States*, 447 U.S. 649, 656-57, 100 S. Ct. 2395, 2401-02 (1980)); see also *Florida v. Jimeno*, 500 U.S. 248, 251, 111 S. Ct. 1801, 1804 (1991) (“The scope of a search is generally defined by its expressed object.”). Whether the search came within the terms of authorization is a question of “objective reasonableness.” *Parker*, ¶ 21. We ask whether the state actor could have “reasonably . . . understood” an individual’s consent “to extend to a particular” area. *Parker*, ¶¶ 21-22.

¶19 We held in *Parker*, ¶¶ 21-22, that a person’s consent to search a vehicle authorized the police to search containers within the vehicle. There, an officer initiated a traffic stop, suspecting that the occupants of the vehicle possessed “weapons, drugs, or drug paraphernalia.” *Parker*, ¶ 5. The owner of the vehicle gave consent when the officer asked to search the vehicle; the district court concluded that the owner “did not limit the scope of the search.” *Parker*, ¶¶ 5, 17. The officer opened a purse located on the passenger floor, where he found drugs and drug paraphernalia. *Parker*, ¶ 7. He also discovered a fanny pack in the rear deck of the vehicle, of which all occupants denied ownership. *Parker*, ¶ 8. The officer then searched the fanny pack and discovered more drugs and drug paraphernalia. *Parker*, ¶ 9. We concluded that it was objectively reasonable for the officer to believe that the owner’s consent to search the vehicle extended to closed items inside the vehicle as well. *Parker*, ¶ 22.

¶20 We held in *State v. Pearson*, by contrast, that a defendant’s consent to search his vehicle did not extend to his fanny pack, which was on his person outside the vehicle. 2011 MT 55, ¶ 22, 359 Mont. 427, 251 P.3d 152. Pearson was on probation when an officer extended a traffic stop upon suspicion of drug activity. *Pearson*, ¶¶ 5-8. The officer initially conducted a lawful pat-down and searched his fanny pack but did not discover any contraband. *Pearson*, ¶ 8. Pearson subsequently consented to a search of his vehicle, and the officers searched his fanny pack a second time, where they discovered methamphetamine. *Pearson*, ¶ 9. We held that, because Pearson consented only to a search of his vehicle, the officers exceeded the scope of his consent when they searched the fanny pack a second time. *Pearson*, ¶ 22. We affirmed the district court’s denial of Pearson’s suppression motion, however, on the doctrine of inevitable discovery. *Pearson*, ¶ 34.

¶21 Mefford argues that Miller’s search of his photos exceeded the scope of his consent, which he limited to only one conversation on Facebook Messenger. He contends that the search of a cell phone is quantitatively and qualitatively unique in this context because a person can switch from one application to another within a few seconds and with the tap of a screen. This, he asserts, is the physical equivalent of searching through a person’s mail, bedroom, place of business, storage facility, vehicle, and call records. Traditional scope-of-consent principles, therefore, while instructive, do not fully account for the differences between physical searches and digital searches. The State argues that substantial evidence supports the court’s finding that Mefford consented to a search of the entire phone and not to only a specific application.

¶22 Based on the testimony at the suppression hearing, we agree with Mefford that Miller's search of his photos exceeded the scope of his consent. Both Mefford's and Miller's testimonies indicate that the purpose of the search was to confirm that Mefford was on his phone when he said he was. Miller testified:

I asked the defendant if I could view the phone *to confirm his story of being on the phone*. The reason for that is, besides trying to contact the defendant that prior weekend about him being in the parking lot, I tried to call the cell phone number that he had provided, and it said it was disconnected.

. . .

The defendant gave me consent to view the phone. And I did confirm there were messages at that time frame like the defendant said.

The photo of the person sending the message didn't appear to be his daughter; didn't appear to be a younger female like he had described.

(Emphasis added.) Miller admitted that he asked to view Mefford's phone to confirm that he was on the phone when he said he was and that he did in fact confirm that Mefford was on the phone. Mefford's testimony was consistent with Miller's understanding of the scope of the search:

I said, look, I can verify when I was out past curfew, okay? I mean, *I was talking to my daughter through Messenger on my phone*, and I had to go a little bit outside my house and sit in my car to pick up wifi, you know, to use the Messenger app. I said, look, *I can verify the time and the date*, and I don't have a problem with that, you know.

. . .

I told [my girlfriend], hey, can you go upstairs and grab the phone for me so I can show him the messages from the time and date that was of concern.

She did. She went and got the phone. She handed it to him.

I told him, *just go to the Messenger app*; her name is [F.]; and, you should be able to see the conversation and the time.

(Emphasis added.) Mefford’s testimony clearly corroborates Miller’s: Mefford agreed to give Miller his phone so he could confirm that Mefford was on the phone at the time of his curfew violation. Miller said his purpose in asking for the phone was to “confirm [Mefford’s] story of being on the phone,” and Mefford said the purpose was to “verify when [he] was out past curfew,” “verify the time and the date,” and to “see the conversation and the time.” There was no discussion about confirming the identity of Mefford’s daughter or about accessing any different applications on Mefford’s phone. Based on their consistent testimonies, Miller and Mefford discussed only a search of the phone limited to confirming that Mefford was using it at the time he violated curfew. The record does not substantiate the District Court’s finding that Mefford gave Miller blanket approval to search the contents of his phone.

¶23 Based on the circumstances of the interaction between Mefford and the officers, Miller could not have “reasonably . . . understood” Mefford’s consent to extend to his digital photo gallery. *See Parker*, ¶ 21. It was no more reasonable for Miller to believe that he had permission to search Mefford’s photos to corroborate the identity of his daughter than it would have been for him to search through a photo album in Mefford’s bedroom or a rolodex on Mefford’s office desk for information regarding Mefford’s daughter. Each of those searches similarly would not have been permitted by Mefford’s consent. The terms of Mefford’s authorization limited Miller’s search to “look at the conversation” with Mefford’s daughter—a specific purpose—and it was not objectively

reasonable for Miller to believe that Mefford's consent extended to other areas of the phone. The District Court's finding was clearly erroneous.

¶24 Our holding in *Parker* is distinguishable both because of the facts of that case and because of the unique privacy implications of cell phones. In *Parker*, the owner did not limit the scope of her consent when the officer asked to search the vehicle, and it was objectively reasonable for the officer to believe that the owner's consent extended to smaller compartments within the vehicle. See *Parker*, ¶¶ 5-8. Mefford, unlike the vehicle owner in *Parker*, directed his consent to one application on his phone—equivalent to consenting to a search of an item or container within a vehicle. Mefford told Miller to “go to the Messenger app,” where he “should be able to see the conversation and the time.” Unlike the situation in *Parker*, Mefford's consent reasonably did not extend to other areas of his phone. The limited capacity of a fanny pack or even a vehicle, moreover, is not comparable to the vast storage capabilities of a modern cell phone or cell phone application, thus rendering this a unique case. By searching a cell phone, an officer can discover highly sensitive and private information about the owner of the phone and every person with whom the owner associates. Such information is not ordinarily discoverable during the search of a vehicle or its contents.

¶25 The situation here is more comparable to *Pearson*, where the defendant consented to a search of his vehicle but not to his fanny pack. *Pearson*, ¶¶ 8-9. It was objectively reasonable for both Pearson and the officer to expect that Pearson's consent to search his vehicle did not include permission to search his fanny pack, which he wore on his person. Similarly, when Mefford authorized Miller to read his conversation on Facebook

Messenger, he could not have expected that his consent extended to browsing the photo gallery on his phone, nor was it reasonable for Miller to think it did.

¶26 Relevant to this discussion is the scope of a search pursuant to a valid search warrant. Clearly, a search conducted pursuant to a warrant is not per se unreasonable; but we have stated that the scope of the search similarly is limited “by the terms of the authorization.” *Graham*, ¶ 22. *See also United States v. Strickland*, 902 F.2d 937, 941 (11th Cir. 1990) (“The scope of the actual consent restricts the permissible boundaries of a search in the same manner as the specifications in a warrant.”). We held in *Graham* that authorization to search the defendant’s garage pursuant to a search warrant did not extend to a search of his home. *Graham*, ¶ 27. There, officers obtained a search warrant for the defendant’s property based on probable cause that the defendant was operating a clandestine methamphetamine laboratory inside an unattached garage on his property. *Graham*, ¶¶ 8-9. The search of the garage yielded no evidence, but the officers found a methamphetamine laboratory in the defendant’s home, which they also searched pursuant to the same warrant. *Graham*, ¶ 10. We rejected the State’s assertion that, based on a “reasonable inference,” the officers believed they were authorized to search the defendant’s home for contraband. *Graham*, ¶ 22. We concluded that the officers’ search of the defendant’s home exceeded the scope of their expressed authorization to search the garage pursuant to the search warrant. *Graham*, ¶¶ 26-27.

¶27 Our holding in *Graham* is analogous to the case before us. In *Graham*, the search warrant limited the scope of the search to a specific physical location, and the officers exceeded the parameters of the warrant when they searched a separate structure on the

defendant's property. *Graham*, ¶¶ 8-9, 22. Though here we are dealing with digital, not physical, "locations," the scope of Mefford's consent similarly was limited. Just as in *Graham*, where it was unreasonable for the officers to believe that the warrant implicitly authorized them to search other structures on the defendant's property, it was unreasonable for Miller to infer that he had permission to access other applications on Mefford's phone.

¶28 Other jurisdictions considering the search of electronic devices have scrutinized the extent of the owner's consent to determine the permissible scope of the search. *See, e.g., United States v. Lopez-Cruz*, 730 F.3d 803, 811 (9th Cir. 2013) (holding that consent to search a cell phone does not extend to answering incoming calls on the cell phone); *Wisconsin v. Jereczek*, 961 N.W.2d 70, 72 (Wis. Ct. App. 2021) (forensic extraction of computer's hard drive exceeded the scope of defendant's consent, which was limited to a search of only his son's user account); *Maine v. Bailey*, 989 A.2d 716, 725 (Me. 2010) (consent to search a computer for the purpose of determining whether someone was impermissibly gaining access to it did not extend to a search of the defendant's videos on the computer); *Illinois v. Prinzing*, 907 N.E.2d 87, 99 (Ill. App. Ct. 2009) (where detective limited search of a computer to "viruses," searching for images on the computer exceeded the scope of the defendant's consent). These cases, like the case before us, are distinguishable from cases in which defendants signed general consent forms to search all the contents of, e.g., a cell phone or a computer. *See, e.g., United States v. Gallegos-Espinal*, 970 F.3d 586, 591-92 (5th Cir. 2020) (upholding the warrantless search of a phone where the defendant signed a consent form authorizing a "complete" search of his iPhone); *United States v. Thurman*, 889 F.3d 356, 368-69 (7th Cir. 2018) (upholding a

forensic search of the defendant's phone, where the defendant gave "unlimited" consent to search the phone).

¶29 These cases, like our analogous precedent, demonstrate that whether an officer exceeds the scope of consent in a cell phone search must be determined on a case-by-case basis, under the standard of objective reasonableness we have applied in similar cases. *See Parker*, ¶ 21. On the suppression hearing record in this case, we conclude that Mefford's consent to search Facebook Messenger for the limited purpose of confirming that he was on the phone during his curfew violation did not give Miller permission to access Mefford's digital photo gallery on his phone. Miller's excursion into other areas of the phone exceeded the scope of Mefford's consent under Article II, Sections 10 and 11, of the Montana Constitution.

Probation Search

¶30 The District Court held in the alternative that Miller's search was a permissible probation search. The State reasserts that argument on appeal.

¶31 The Department of Corrections (DOC) supervises probationers and parolees. Sections 46-23-1001(4), -1002(1)-(4), -1012, -1021(1), MCA. The DOC may "adopt rules for the conduct of persons placed on parole." Section 46-23-1002(3), MCA. "At any time during the release on parole," probation and parole officers are authorized to "arrest . . . the parolee for violation of any of the conditions of release or a notice to appear to answer to a charge of violation." Section 46-23-1023(1), MCA. Pursuant to the DOC's regulations, parolees are subject to the same search requirements as probationers. *See Admin. R. M. 20.7.1101 (2008)*.

¶32 Parolees are subject to warrantless searches of their homes and property when: (1) “such searches are generally authorized by an established state law regulatory scheme that furthers the special government interests in rehabilitating probationers and protecting the public from further criminal activity by ensuring compliance with related conditions of probation and the criminal law”; (2) the probation officer has reasonable cause to suspect that the probationer may be in violation of the probationer’s conditions of supervision or the criminal law; and (3) “the warrantless search is limited in scope to the reasonable suspicion that justified it in the first instance except to the extent that new or additional cause may arise within the lawful scope of the initial search.” *Peoples*, ¶ 17.

¶33 Regarding the first requirement of the exception, Mefford does not dispute that he was supervised by Probation and Parole at the time of the search. The DOC authorizes searches of parolees pursuant to Admin. R. M. 20.7.1101(7)-(8) (2008):

Upon reasonable suspicion that the offender has violated the conditions of supervision, a probation and parole officer may search the person, vehicle, and residence of the offender, and the offender must submit to a search.

. . .

The offender must comply with all municipal, county, state, and federal laws and ordinances and shall conduct himself/herself as a good citizen.

¶34 Regarding the second requirement, the “reasonable cause” standard is “substantially less than the probable cause standard required by the Fourth Amendment because of the probationer’s diminished expectation of privacy.” *State v. Burchett*, 277 Mont. 192, 195-96, 921 P.2d 854, 856 (1996); *see also State v. Moody*, 2006 MT 305, ¶ 12, 334 Mont. 517, 148 P.3d 662. At a minimum, however, it “require[s] some specific and

articulable factual basis known to the probation officer upon which to reasonably suspect, based on the probationer’s criminal and probation compliance history and the officer’s knowledge of his or her life, character, and circumstances, that the probationer may be in possession of contraband in violation of his or her probation or the criminal law.” *Peoples*, ¶ 18 (citing *State v. Fischer*, 2014 MT 112, ¶¶ 10-17, 374 Mont. 533, 323 P.3d 891) (other citations omitted).

¶35 Under the third requirement, the scope of the search must be limited “to the reasonable suspicion that justified it in the first instance except to the extent that new or additional cause may arise within the lawful scope of the initial search.” *Peoples*, ¶ 17. The officer’s suspicion cannot be a generalized suspicion of wrongdoing; “the decision to search must be based on ‘specific facts.’” *Peoples*, ¶ 18 (quoting *United States v. Hill*, 967 F.2d 902, 910 (3d Cir. 1992)).

¶36 Mefford does not dispute that Miller had reasonable cause to suspect that he violated curfew on November 26, 2016. He argues, however, that Miller did not reasonably suspect that Mefford was in possession of contraband on his phone and that he therefore exceeded the scope of his search when he opened another application. The State argues that Miller’s suspicion that Mefford was out past curfew gave him the authority to search Mefford’s phone based on the “flexibility” of supervisory powers that probation officers possess.³

³ The State argues also that Mefford did not preserve this argument for appeal because his motion to suppress was based solely on the assertion that Miller exceeded the scope of Mefford’s consent. Though we do not permit parties to raise new issues or change their legal theories on appeal, “[w]e of course permit parties to bolster their preserved issues with additional legal authority or to make further arguments within the scope of the legal theory articulated at trial.” *State v. Strizich*, 2021 MT 306, ¶ 32, 406 Mont. 391, 499 P.3d 575 (citations and alterations omitted). Mefford

¶37 The parties agree that Miller and Finley went to Mefford’s home on November 29, 2016, to investigate a potential parole violation based on their suspicion that Mefford violated curfew three days earlier. That suspicion was based on Mefford’s GPS ankle monitor, which indicated that Mefford was in his apartment parking lot after 10:00 p.m. Upon questioning Mefford, the officers learned that he in fact had been out past curfew. Mefford admitted to the officers that he violated his curfew, but he claimed it was because he was communicating with his sixteen-year-old daughter, who resided in California, through Facebook Messenger. To substantiate his account, Mefford agreed to the officers’ review of his recent Facebook Messenger history. At that point, the officers’ suspicion was confirmed: Mefford violated a condition of his parole by leaving his apartment after 10:00 p.m. on November 26, 2016. The District Court concluded that Miller had reasonable cause to look further once the profile picture raised questions about whether Mefford was conversing with his daughter or with someone else.

¶38 Probationers and parolees “have significantly diminished subjective and objective expectations of privacy.” *Peoples*, ¶ 17. Mefford does not dispute that his expectation of privacy was diminished, as he was subject to the supervision of the DOC. Even the search of a probationer with a diminished expectation of privacy, however, “is limited in scope to

argued that the State violated his Fourth Amendment and Article II, Sections 10 and 11 rights by conducting an illegal search of his phone. The burden then shifted to the prosecution to “prove that the search c[ame] within a recognized exception to the warrant requirement.” *State v. Heath*, 2000 MT 94, ¶ 18, 299 Mont. 230, 999 P.2d 324. It was not Mefford’s burden to preemptively refute every possible warrant exception the State might raise to justify its warrantless search. The District Court’s Order, moreover, contradicts the State’s assertion that Mefford did not raise this argument until now: “The Defense argues that even under a probationary search a warrant was required to search the phone because a cell phone does not fall under the resident, person, or vehicle requirement.” Mefford’s argument on appeal thus is properly preserved.

the reasonable suspicion that justified it in the first instance,” unless new or additional cause arises “within the lawful scope of the initial search.” *Peoples*, ¶ 17. Without Mefford’s consent, in order to conduct an additional search of Mefford’s digital photo gallery, Miller needed “reasonable cause” to expand the search. But Miller did not identify a “specific and articulable factual basis” upon which to suspect that Mefford had violated the criminal law or a condition of his parole. *See Peoples*, ¶ 18. Miller’s initial reason for searching Facebook Messenger (“to confirm [Mefford’s] story of being on the phone”) no longer provided an articulable basis to search because he already confirmed that Mefford was on the phone when he said he was. The only reason Miller gave for searching Mefford’s photos was that he wanted to confirm that the person with whom Mefford was communicating was his daughter. Aside from this being unrelated to Mefford’s admitted curfew violation, Miller articulated nothing about Mefford’s alleged daughter’s profile picture that gave rise to further suspicion of a crime or a parole violation. Miller believed that the person with whom Mefford was communicating was “too old” to be Mefford’s daughter. He did not suspect that Mefford was engaged in an inappropriate conversation with a minor over Facebook Messenger. Miller identified nothing within the substance of Mefford’s Facebook Messenger conversation that alerted him to the possibility of a crime or a suspected parole violation that could be substantiated by viewing Mefford’s digital photo gallery. Miller likewise did not connect the additional search to Mefford’s criminal history, Mefford’s parole compliance history, or the circumstances of the curfew violation. *See Peoples*, ¶ 18. And finally, Miller did not identify any “new or additional” cause that

would amount to a “specific and articulable factual basis” to search further. *See Peoples*, ¶ 18.

¶39 The State asserts that Miller had reasonable cause to suspect that Mefford violated his curfew and therefore reasonably suspected that Mefford was involved in “suspicious activity.” Miller said no such thing. Neither the “circumstances” of the parole violation nor Mefford’s “criminal and probation compliance history” gave rise to a suspicion that Mefford possessed contraband of the kind discovered on his phone. *See Peoples*, ¶ 18. And a “generalized suspicion” or an “undeveloped hunch” of suspicious activity is never sufficient to supply a “specific and articulable factual basis . . . upon which to reasonably suspect” that a crime has been committed. *Peoples*, ¶ 18; *State v. Reeves*, 2019 MT 151, ¶¶ 11-13, 396 Mont. 230, 444 P.3d 394; *State v. Hoover*, 2017 MT 236, ¶¶ 18-19, 388 Mont. 533, 402 P.3d 1224. Mefford’s substantiated curfew violation did not provide an articulable factual basis for a search of Mefford’s photos.

¶40 The State cites *State v. Burke*, 235 Mont. 165, 766 P.2d 254 (1988), for the proposition that probation officers have “flexibility” in supervising parolees, and therefore Mefford’s suspicious behavior authorized Miller to exceed the scope of the initial probation search. In *Burke*, an officer observed “various persons leave [a] bar,” walk to the defendant’s car, which the defendant occupied, and return to the bar. 235 Mont. at 166, 766 P.2d at 255. When he approached the defendant, the officer noticed the odor of marijuana and saw cigarette rolling papers in plain view. *Burke*, 235 Mont. at 166, 766 P.2d at 255. The defendant was on probation, and his probation officer gave the officer permission to search the vehicle, where the officer discovered marijuana. *Burke*,

235 Mont. at 166-67, 766 P.2d at 255. The probation officer then gave the officer permission to search the defendant's house, pursuant to Admin. R. M. 20.7.1101(11) (1978), which permitted the warrantless search of a probationer's house upon "reasonable cause." *Burke*, 235 Mont. at 167, 169-70, 766 P.2d at 255, 257. We held that the search of the defendant's home was lawful under the probation search exception to the warrant requirement. *Burke*, 235 Mont. at 171, 766 P.2d at 258. We rejected the defendant's argument on appeal that a standard more stringent than "reasonable grounds" should apply, based, in part, on the "degree of flexibility [that] must be accorded the probation officer," considering the probation officer's "knowledge," "expertise," and "continued experience" with the probationer/parolee. *Burke*, 235 Mont. at 168-69, 766 P.2d at 256.

¶41 *Burke* does not elevate the "flexibility" of probation officers to a stand-alone warrant exception. On the contrary, it is consistent with our holding here. In *Burke*, the probation officer had reasonable cause to believe that the defendant violated a condition of supervision by possessing marijuana, which authorized the probation officer to order a search of the defendant's home. The scope of the search was limited to the reasonable suspicion that justified the initial search (i.e., that the defendant possessed marijuana). It was reasonable to assume that the defendant would possess marijuana in his home as well as in his vehicle. Here, by contrast, Miller had reasonable cause that Mefford violated his curfew. His reasonable cause was confirmed when Mefford admitted that he violated his curfew. His search of Facebook Messenger corroborated Mefford's story that Mefford was on his phone during his curfew violation. At that point, Miller's initial articulable suspicion (that Mefford violated his curfew) no longer was relevant to his subsequent search of

Mefford's photos. Nothing that Miller reasonably could have expected to discover in Mefford's photos would have provided further evidence of a curfew violation, nor would it have confirmed or dispelled his suspicion that Mefford violated his curfew on November 26, 2016, or anything else Miller reasonably suspected from the new information he learned. The facts of *Burke* thus are distinguishable from the present case.

¶42 In short, a probation and parole officer's flexibility to supervise probationers with a diminished expectation of privacy does not vitiate the requirements for a probation search exception. *See Peoples*, ¶ 17 (explaining the three elements of the probation search exception). There are many cases affirming the warrantless search of a probationer that illustrate the proper exercise of a probation officer's supervisory flexibility. In these cases, the scope of the search was within the articulable factual basis that gave rise to the officer's initial reasonable cause or was properly extended after the officer learned new information "within the lawful scope of the initial search." *Peoples*, ¶ 17. *See, e.g., State v. Conley*, 2018 MT 83, ¶¶ 3-6, 25, 391 Mont. 164, 415 P.3d 473 (upholding a warrantless search of the defendant-probationer's vehicle based on reasonable cause that the defendant was in possession of drugs because the defendant was on probation for a drug offense, admitted to prior methamphetamine use, had multiple other probation violations, and admitted that he had been awake all night); *Fischer*, ¶¶ 2-6, 17 (upholding a warrantless search of the defendant's purse for narcotic pills because the defendant was on probation for a drug offense, admitted that her pill count was "off," and failed to report it to Probation and Parole as required by her conditions of supervision); *State v. Charlie*, 2010 MT 195, ¶¶ 25-26, 357 Mont. 355, 239 P.3d 934 (upholding a warrantless probation search of a

vehicle where the defendant ran a stop sign, appeared nervous, spoke rapidly, and was observed reaching around the inside of the car during the traffic stop); *State v. Fritz*, 2006 MT 202, ¶¶ 4-7, 11, 333 Mont. 215, 142 P.3d 806 (upholding a probation search of the defendant’s vehicle after the defendant drove to a residence where officers discovered evidence of drug use and drug paraphernalia, and the owner of the residence informed them that the defendant possessed chemicals commonly used in the manufacture of methamphetamine); *State v. Stone*, 2004 MT 151, ¶¶ 8-10, 42, 321 Mont. 489, 92 P.3d 1178 (upholding a warrantless search of the defendant’s home under the probation search exception, where officers received a report that there were “dead” and “dying” animals on the defendant’s property, and where officers observed dead rabbits in cages around the defendant’s home); *State v. Roper*, 2001 MT 96, ¶¶ 6-7, 19, 305 Mont. 212, 26 P.3d 741 (upholding a probation search of the defendant’s home where the defendant was on probation for selling drugs, two probationers reported that the defendant was still using and selling drugs, and the probation officer learned that a drug task force was investigating the defendant for drug distribution); *State v. Beaudry*, 282 Mont. 225, 226-27, 231, 937 P.2d 459, 460, 462 (1997) (upholding a probation search of the defendant’s home on the ground that the probation officer had reasonable cause to suspect the defendant possessed contraband after the defendant tested positive for illicit drugs four times, admitted that he consumed alcohol, frequented bars, and possessed stolen firearms); *State v. Burchett*, 277 Mont. 192, 194-95, 197, 921 P.2d 854, 855, 857 (1996) (upholding a probation search where the probation officer suspected that the defendant burglarized his place of previous employment because the manager reported that it was an “inside job”

and that another employee witnessed firearms and the stolen merchandise in the defendant's home); *State v. Boston*, 269 Mont. 300, 302-03, 305, 889 P.2d 814, 815-17 (1994) (upholding a warrantless search of a parolee's residence and storage garage when the parole officer learned of evidence linking the defendant to an arson fire); *State v. Hall*, 249 Mont. 366, 816 P.2d 438 (1991) (holding that a probation officer had reasonable cause to search the defendant's home pursuant to the probation search exception because an informant advised the drug task force that the defendant was selling drugs, and an undercover detective subsequently notified the probation officer that he purchased drugs from the defendant's residence); *State v. Small*, 235 Mont. 309, 310-12, 767 P.2d 316, 317-18 (1989) (upholding a probation search of the defendant's home after the probation officer received a tip from a confidential informant that the defendant, who was on probation for a drug conviction, was selling marijuana at her residence).

¶43 Each of these cases reveals specific facts upon which the officer reasonably suspected violations of probation or the criminal law. In sharp contrast, nothing that Miller expected to discover in Mefford's photo gallery had any connection to the initial crime that landed him on parole or to the admitted curfew violation that Miller and Finley were investigating. Mefford was paroled on drug and assault convictions, not for sex crimes or crimes involving minors. The contents of his photo gallery bore no relation to the reasons for his parole. Miller did not articulate any suspicion that Mefford was conversing with a prostitute, with someone younger than his daughter, or that Mefford's Facebook Messenger conversation revealed evidence of some other crime or some other parole violation.

Miller's stated purpose thus exceeded "the suspicion that justified [the search of Mefford's phone] in the first instance." *See Peoples*, ¶ 17.

¶44 The Dissent posits that the officers had reasonable suspicion that Mefford was lying about the identity of the person with whom he was communicating and may have committed an additional parole violation by drinking. Dissent, ¶¶ 54-56. First though, Officer Finley did not testify at the suppression hearing, and Miller said nothing at the hearing about any additional suspected violations. Second, even if Miller may have had a reasonable suspicion that Mefford was not being truthful about who he had been texting, Miller did not explain how randomly scrolling through the photos in Mefford's private cell phone photo gallery could provide evidence confirming his suspicion. It was, furthermore, unreasonable for Miller to assume that, by engaging in a generalized scrolling through Mefford's photos, he could confirm the identity of Mefford's daughter without: (a) knowing what Mefford's daughter looked like; (b) asking Mefford if he had pictures of his daughter on his phone; (c) knowing whether Mefford's daughter used her own photograph as her profile picture on Facebook; or (d) considering that, even if Mefford had personal photos that matched the profile picture of the person with whom he was communicating on Facebook, it still would not confirm whether she actually was Mefford's daughter. Miller did not ask any such questions or seek additional information to ascertain whether Mefford was lying. The expedition into Mefford's photo gallery had no connection to Mefford's curfew violation or to any new reasonable cause that Miller articulated and was otherwise unconnected to Mefford's "criminal history," "[parole] compliance history," or "[Miller's] knowledge of [Mefford's] life, character, and circumstances." *See Peoples*, ¶ 18.

¶45 Had Mefford been communicating with a younger child through Facebook Messenger; had Mefford’s Facebook Messenger conversation revealed that he was having an inappropriate conversation with his “daughter”; or had Miller seen evidence of some other crime, such as prostitution or the sale of drugs, this would be a completely different case, and Miller almost certainly would have had new reasonable cause to conduct an additional search. Similarly, had Mefford been on parole for a sex crime or for abuse of children, those facts could cast the circumstances of Miller’s search under a different light. But those facts are not before the Court in this appeal. On this record, we conclude that Miller’s warrantless search of Mefford’s digital photo gallery was not a valid probation search under Article II, Sections 10 and 11, of the Montana Constitution.

Application of Exclusionary Rule

¶46 Pursuant to the exclusionary rule, “evidence discovered as the result of a constitutionally invalid search or seizure is generally inadmissible against the accused in subsequent proceedings.” *State v. Zeimer*, 2022 MT 96, ¶ 54, 408 Mont. 433, 510 P.3d 100 (citations omitted). The purpose of the rule is to “deter illegal police conduct and to preserve judicial integrity.” *State v. Long*, 216 Mont. 65, 71, 700 P.2d 153, 157 (1985). The State bears the burden of proving that an exception to the exclusionary rule applies. *Zeimer*, ¶ 54. The State does not argue, nor did it before the District Court, that any exception to the exclusionary rule should apply if the search of Mefford’s photo gallery were held unlawful. We have recognized, however, “that the question of whether evidence would have been inevitably discovered is one we can answer *sua sponte*, provided there is

a sufficient record before us to make that determination.” State v. Ellis, 2009 MT 192, ¶ 47, 351 Mont. 95, 210 P.3d 144 (emphasis added).

¶47 We consider whether there is a sufficient record of “inevitable discovery” to answer the question sua sponte. *See Ellis, ¶¶ 47-48.* Though the Application for Leave to File an Information included additional facts to support probable cause, there is no record evidence suggesting that this information would have been “inevitably discovered” but for Miller’s warrantless search of the phone. *See Ellis, ¶ 47.* The inevitable discovery exception applies when “the tainted evidence would have inevitably been discovered through lawful means.” *Ellis, ¶ 49.* The critical question under the exception is whether the untainted evidence “was the result of the exploitation of the initial illegal search[.]” *State v. Laster, 2021 MT 269, ¶ 45, 406 Mont. 60, 497 P.3d 224 (alterations omitted).*

¶48 Here, the only additional evidence is that Mefford’s cellmate reported to a detective that, while incarcerated in the Montana State Prison, Mefford admitted that he engaged in “sex acts that involved children.” His cellmate made this report during the period that Mefford was incarcerated due to his parole revocation, which resulted from Miller’s illegal search of his phone. The only reason Mefford was incarcerated and his phone seized was because of Miller’s search on November 29, 2016. The record therefore does not substantiate that the inevitable discovery exception would apply, even if the State had argued for the exception. Because there is not a sufficient record to make this determination, we do not sua sponte consider the question.

¶49 The record clearly indicates that Miller’s illegal search of Mefford’s phone served as the basis for the warrant application, the Information, and the evidence presented at

Mefford's trial. The record shows, therefore, that the images of child pornography that were extracted from Mefford's phone would not have been discovered but for Miller's illegal search of his photos. Detective Williams would not have obtained a warrant to extract the images had Miller not searched Mefford's phone on November 29, 2016. Those photos served as the evidentiary basis upon which Mefford was convicted. They are, therefore, subject to suppression under the exclusionary rule. As "fruit of the poisonous tree," the contraband discovered as a consequence of Miller's unlawful search should have been suppressed under the exclusionary rule. *See Zeimer*, ¶ 54.

CONCLUSION

¶50 We conclude that Miller's warrantless search of Mefford's digital photo gallery on his phone was unlawful because it was not executed pursuant to a valid warrant exception and therefore was not reasonable within the meaning of the Montana and United States Constitutions. We reverse the District Court's Order Denying Defendant's Motion to Suppress and Dismiss and vacate its Corrected Judgment and Order of Commitment.

/S/ BETH BAKER

We Concur:

/S/ LAURIE McKINNON
/S/ INGRID GUSTAFSON
/S/ DIRK M. SANDEFUR

Justice James Jeremiah Shea, concurring and dissenting.

¶51 I concur with the Majority's conclusion that the scope of Miller's search exceeded Mefford's consent and did not fall within the consent exception to the warrant requirement for a lawful search. Opinion, ¶ 29. I dissent from the Majority's conclusion that the search of Mefford's photo gallery was not a permissible probationary search. Opinion, ¶ 44. I would hold the totality of the circumstances in this case provided reasonable cause to search Mefford's photo gallery.

¶52 The probation search exception allows a probation or parole officer to search a parolee's property "without a warrant or probable cause for evidence of violation of a probation condition or the criminal law if: (1) such searches are generally authorized by an established state law regulatory scheme that furthers the special government interests in rehabilitating probationers and protecting the public from further criminal activity by ensuring compliance with related conditions of probation and the criminal law; (2) the probation officer has reasonable cause to suspect, based on awareness of articulable facts, under the totality of the circumstances that the probationer may be in violation of his or her probation conditions or the criminal law; and (3) the warrantless search is limited in scope to the reasonable suspicion that justified it in the first instance except to the extent that new or additional cause may arise within the lawful scope of the initial search." *Peoples*, ¶ 17. "The reasonable cause standard is substantially less than the probable cause standard required by the Fourth Amendment because of the probationer's diminished expectation of privacy." *Burchett*, 277 Mont. at 195-96, 921 P.2d at 856 (internal quotations omitted).

An officer need not necessarily “be certain, or even ultimately correct, that a person is engaged in criminal activity.” *See Hoover*, ¶ 18.

¶53 The Majority assesses this encounter through the narrow lens of Mefford’s curfew violation. The Majority fails to consider all of the circumstances attendant to the encounter between Mefford and the parole officers that culminated in the search of Mefford’s photo gallery. In this case, the totality of the circumstances prior to Miller’s search of Mefford’s photo gallery are these:¹ (1) Miller and Finley conducted a home visit because Mefford violated his parole by being out well after his curfew; (2) the home visit was necessary because Mefford instructed his girlfriend to call Finley that morning to tell him that he would not be reporting to the probation and parole office as required because he injured his back; (3) Finley thought Mefford had been drinking in violation of his parole and thought Mefford “was trying to dodge him” which is why Mefford had his girlfriend call Finley to tell him he was not going to report as required, instead of calling Finley himself; (4) a previous search of Mefford’s residence revealed he had beer in his possession; (5) Mefford’s explanation for his curfew violation was that he was messaging his sixteen-year-old daughter until 3:00 a.m.; (6) Mefford could tell that Miller also thought he was lying so Mefford offered to verify his explanation by asking his girlfriend to retrieve his phone to show it to Miller; (7) although the messages confirmed Mefford was communicating with *someone* at 3:00 a.m., well after his curfew and in violation of his probation, the profile photograph of the individual with whom Mefford was messaging did

¹ Unless otherwise noted, the facts set forth are taken from Miller’s and Mefford’s uncontroverted testimony at the suppression hearing.

not appear to Miller to be a sixteen-year-old girl; and (8) rather than the messages confirming Mefford's story as to why he was violating his curfew, Miller now suspected Mefford was lying to him about the identity of the individual with whom he was communicating at 3:00 a.m. in violation of his parole.

¶54 In summary, at the point at which Miller opened Mefford's photo gallery, Finley and Miller knew that Mefford had violated his parole by being out well after curfew the preceding weekend; they suspected Mefford may have committed an additional parole violation by drinking because he failed to report to their office as required and did not call them himself to explain why he was failing to report; and, rather than Mefford's explanation for his curfew violation allaying their suspicions, it exacerbated them because it appeared to them that Mefford was lying about who he was messaging at 3:00 a.m. So what are they to do with their suspicions as to Mefford's activities? According to the Majority—nothing. The Majority holds that at this point, “the officers’ suspicion was confirmed: Mefford violated a condition of his parole by leaving his apartment after 10:00 p.m. on November 26, 2016.” Opinion, ¶ 37. But that was not the basis for Miller's search of Mefford's photo gallery. The officers' suspicions regarding Mefford's curfew violation had been confirmed even before Mefford offered up his phone to substantiate the reason for this violation. When Miller reviewed the messages and saw the profile picture that did not appear to comport with Mefford's description of a sixteen-year-old girl, this gave rise to new suspicions that Mefford was lying to them about who he was communicating with, constituting new or additional cause which arose within the lawful

scope of the initial search that allowed Miller to further investigate why, in his estimation, Mefford was lying to him about who he was communicating with. *See Peoples*, ¶ 17.

¶55 It makes no sense to hold, as the Majority does, that Mefford can offer an explanation for a parole violation, offer his phone to verify his explanation, but when his explanation appears to raise even more suspicions of compliance, the officer is just supposed to disregard these new suspicions and stand down. Further investigation in this situation does not vitiate the warrant requirement, as the Majority suggests. *See Opinion*, ¶ 42. The totality of the circumstances presented in this case, and the probation and parole officers' actions in light of those circumstances, necessarily falls squarely within the "degree of flexibility" we accord probation and parole officers when determining how to exercise their supervisory powers. *State v. Conley*, 2018 MT 83, ¶ 18, 391 Mont. 164, 415 P.3d 473 (citing *Burke*, 235 Mont. at 169, 766 P.2d at 256).

¶56 The Majority suggests that Miller had only a "generalized suspicion" of wrongdoing because he did not articulate the specific facts that gave him reasonable cause to search Mefford's photo gallery and no specific facts "gave rise to a suspicion that Mefford possessed contraband of the kind discovered on his phone." *Opinion*, ¶¶ 38-39. But Miller did not open Mefford's photo gallery for the purpose of searching for contraband. Miller opened Mefford's photo gallery for the express purpose of either confirming or dispelling his suspicion that Mefford was lying to him about Mefford's proffered explanation for his curfew violation. Miller was not required to connect his reasonable suspicion that a crime was being committed to the specific types of crime germane to Mefford's conviction and parole. More broadly, Miller was not even required to be certain or correct as to whether

there was criminal activity or a parole violation. *See Hoover*, ¶ 18. Rather, the probation search exception allowed Miller to search Mefford’s photo gallery when he had reasonable cause to suspect, based on his awareness of numerous articulable facts, under the totality of the circumstances that Mefford *may* be in violation of his parole conditions when the explanation Mefford offered raised more suspicions because he appeared to be lying about who he was messaging. *See Peoples*, ¶ 17.

¶57 While acknowledging that Miller may have had a reasonable suspicion that Mefford was lying about the identity of the person with whom he was communicating, the Majority nevertheless concludes that Miller did not explain how searching through Mefford’s photo gallery “could provide evidence confirming his suspicion.” Opinion, ¶ 44. But was it necessary to connect these dots? Common sense and life experience tell us that people have photos of their children on their phones, and those photos often provide context as to the identity of the persons in them. If, for example, Mefford’s photo gallery included a photograph of him with the young woman he had been messaging at a party where she is blowing out sixteen candles on a birthday cake, Miller’s suspicions would have been allayed. On the other hand, if there were photos of Mefford with the young woman drinking in a bar, Miller’s suspicions would have been confirmed.

¶58 It also bears noting that nobody, including Mefford, has questioned Miller’s stated motive for looking in Mefford’s photo gallery. There is absolutely no suggestion that Miller’s stated suspicion that Mefford was not really messaging his daughter was a pretext to rifle through Mefford’s phone. Miller did not use his suspicion of Mefford’s dishonesty to go searching through Mefford’s banking apps or emails on some unfettered fishing

expedition. Miller merely opened Mefford's photo gallery to confirm whether Mefford was being honest about his volunteered explanation for his curfew violation or whether Mefford's suspected dishonesty required further investigation. Indeed, Mefford himself acknowledged that Miller wanting to see a photo of his daughter to confirm her identity was reasonable. In response to questioning from his attorney, Mefford testified:

Q. [H]ad [Miller] said, hey, Brad, can I see a picture of [your daughter] to confirm that this is actually her on this Messenger app, what would you have said?

A. I would have said, sure, no problem, you know.

In light of the photos Mefford had on his phone, it is no wonder that he would have preferred to pull up a photo of his daughter himself rather than allow Miller to look for one. But it is incongruous to hold that a parolee with significantly diminished subjective and objective expectations of privacy, can acknowledge the reasonable basis for a search, yet have the fruits of that search suppressed based on the manner in which it was conducted.

¶59 Miller's search of the photo gallery in Mefford's phone was justified under the totality of the circumstances. Within the context of those circumstances, Miller's search was a reasonable response to either confirm or dispel his suspicion that Mefford was being dishonest about who he was messaging in violation of his curfew and whether that warranted further investigation. On that basis I would affirm the District Court's order denying Mefford's motion to suppress evidence and dismiss the charges against him.

/S/ JAMES JEREMIAH SHEA

Chief Justice Mike McGrath and Justice Jim Rice join the Concurrence and Dissent of Justice James Jeremiah Shea.

/S/ MIKE McGRATH

/S/ JIM RICE

Alexander Shalom (BAR No. 021162004)
AMERICAN CIVIL LIBERTIES UNION
OF NEW JERSEY FOUNDATION
570 Broad Street, 11th Fl.
Post Office Box 32159
Newark, NJ 07102

SUPREME COURT OF NEW JERSEY

FACEBOOK, INC., <i>Plaintiff,</i>	: Criminal Action
	: No. 087054
	:
	: Superior Court of New Jersey,
	: Appellate Division
	: Nos. A-3350-20, A-0119-21
	:
	:
	:
	:
	:
	: Sat Below:
	: Hon. Jack M. Sabatino, P.J.A.D.
	: Hon. Garry S. Rothstadt, J.A.D.
	: Hon. Jessica R. Mayer, J.A.D.
	:
	:

STATE OF NEW JERSEY
Defendant.

IN THE MATTER OF THE APPLICATION
OF THE STATE OF NEW JERSEY FOR A
COMMUNICATIONS DATA WARRANT
AUTHORIZING THE OBTAINING OF
THE CONTENTS OF RECORDS FROM
FACEBOOK, INC.

**BRIEF OF *AMICI CURIAE* AMERICAN CIVIL LIBERTIES UNION &
AMERICAN CIVIL LIBERTIES UNION OF NEW JERSEY**

Alexander Shalom (BAR No. 021162004)
Jeanne LoCicero (BAR No. 024052000)
AMERICAN CIVIL LIBERTIES UNION
OF NEW JERSEY FOUNDATION
570 Broad Street, 11th Fl.
Post Office Box 32159
Newark, NJ 07102
Tel: (973) 854-1714
ashalom@aclu-nj.org
jlocicero@aclu-nj.org

Jennifer Stisa Granick*
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
2101 Webster Street #1300
Oakland, CA 94612
Tel: (415) 343-0758
jgranick@aclu.org

* *Pro hac vice* pending

Attorneys for Amici Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES ii

PRELIMINARY STATEMENT 1

STATEMENT OF FACTS AND PROCEDURAL HISTORY 3

ARGUMENT 4

 I. Today’s data surveillance is far more invasive even than eavesdropping
 and wiretaps of old. 4

 II. Under *Berger*, the Fourth Amendment requires that warrants seeking
 ongoing access to future private communications contain special
 safeguards, like those enshrined in Title III and the NJWESCA, regardless
 of whether acquisition is contemporaneous or not. 8

 III. If the Court disagrees that the proposed series of ongoing acquisitions of
 electronic communications are an “interception”, the *Berger* and
 subsequent electronic search cases nevertheless require strict adherence to
 Fourth Amendment safeguards. 13

 IV. The New Jersey Constitution also requires these safeguards, as it is more
 protective than the federal Constitution. 19

CONCLUSION 22

APPENDIX OF *AMICI CURIAE* Aai

TABLE OF AUTHORITIES

CASES

<i>Anderson v. Maryland</i> , 427 U.S. 463 (1976).....	20
<i>Berger v. New York</i> , 388 U.S. 41 (1967).....	passim
<i>California v. Greenwood</i> , 486 U.S. 35 (1988).....	26
<i>Carpenter v. United States</i> , 138 S. Ct. 2206 (2018)	11, 12, 19, 27
<i>Facebook, Inc. v. State</i> , 251 N.J. 378 (2022)	9
<i>Facebook, Inc. v. State</i> , 252 N.J. 36 (2022)	9
<i>Facebook, Inc. v. State</i> , 471 N.J. Super. 430 (App. Div. 2022)	8
<i>Florida v. Bostick</i> , 501 U.S. 429 (1991).....	26
<i>Heien v. North Carolina</i> , 574 U.S. 54 (2014).....	26
<i>In re [REDACTED]@gmail.com</i> , 62 F. Supp. 3d 1100 (N.D. Cal. 2014)	22
<i>In re Grand Jury Subpoena</i> , 828 F.3d 1083 (9th Cir. 2016)	12
<i>In re Search of Google Email Accounts identified in Attachment A</i> , 92 F. Supp. 3d 944 (D. Alaska 2015).....	22
<i>In re Search of Info. Associated With Four Redacted Gmail Accounts</i> , 371 F. Supp. 3d 843 (D. Or. 2018).....	23
<i>In re Three Hotmail Email Accounts</i> , No. 16-MJ-8036-DJW, 2016 WL 1239916 (D. Kan. Mar. 28, 2016)	21

<i>Osborn v. United States</i> , 385 U.S. 323 (1966).....	15
<i>Rakas v. Illinois</i> , 439 U.S. 128 (1978).....	25
<i>Richardson v. State</i> , No. 46, 2022 WL 3711713 (Md. August 29, 2022).....	21
<i>Riley v. California</i> , 573 U.S. 373 (2014).....	11, 12, 20
<i>Schneckloth v. Bustamonte</i> , 412 U.S. 218 (1973).....	26
<i>Smith v. Maryland</i> , 442 U.S. 735 (1979).....	27
<i>State v. Alston</i> , 88 N.J. 211 (1981)	25
<i>State v. Ates</i> , 217 N.J. 253 (2014)	24
<i>State v. Carter</i> , 247 N.J. 488 (2021)	25
<i>State v. Carty</i> , 170 N.J. 632 (2002)	26
<i>State v. Cooke</i> , 163 N.J. 657 (2000)	25
<i>State v. Domicz</i> , 188 N.J. 285 (2006)	26
<i>State v. Earls</i> , 214 N.J. 564 (2013)	27
<i>State v. Fairley</i> , 457 P.3d 1150 (Wash. Ct. App. 2020).....	21
<i>State v. Feliciano</i> , 224 N.J. 351 (2016)	24
<i>State v. Hempele</i> , 120 N.J. 182 (1990)	25, 26

<i>State v. Johnson</i> , 68 N.J. 349, 353–54 (1975).....	26
<i>State v. McAllister</i> , 184 N.J. 17 (2005)	26
<i>State v. Novembrino</i> , 105 N.J. 95 (1987)	25
<i>State v. Reid</i> , 194 N.J. 386 (2008)	27
<i>State v. Smith</i> , 278 A.3d 481 (Conn. 2022).....	21
<i>United States v. Abboud</i> , 438 F.3d 554 (6th Cir. 2006).....	22
<i>United States v. Christie</i> , 624 F.3d 558 (3d Cir. 2010).....	27
<i>United States v. Comprehensive Drug Testing, Inc.</i> , 621 F.3d 1162 (9th Cir. 2010)	11, 24
<i>United States v. Diaz</i> , 841 F.2d 1 (1st Cir. 1988)	22
<i>United States v. Espudo</i> , 954 F. Supp. 2d 1029 (S.D. Cal. 2013).....	16
<i>United States v. Griffith</i> , 867 F.3d 1265 (D.C. Cir. 2017).....	23
<i>United States v. Leon</i> , 468 U.S. 897 (1984).....	25
<i>United States v. Miller</i> , 425 U.S. 435 (1976).....	26
<i>United States v. Shipp</i> , 392 F. Supp. 3d 300 (E.D.N.Y. 2019).....	12, 21
<i>United States v. Warshak</i> , 631 F.3d 266 (6th Cir. 2010).....	12
<i>United States v. Wey</i> , 256 F. Supp. 3d 355 (S.D.N.Y. 2017).....	21, 22

STATUTES

New Jersey Wiretapping and Electronic Surveillance Act, 7, 8, 18
 N.J.S.A. 2A:156A-12.....7
 N.J.S.A. 2A:156A-1–2625
 N.J.S.A. 2A:156A-2.....7
Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. 90-351, Title III,
 18 U.S.C. §§ 2510–20 7, 8, 18

OTHER AUTHORITIES

Antonio Regalado, *Who Coined ‘Cloud Computing’?*,
 MIT Tech. Rev. (Oct. 31, 2011)9
Apple, *iCloud Storage Plans and Pricing*10
Dropbox, *Choose the Right Dropbox for You*10
Dropbox, *How Much is 1 TB of Storage?*10
Google One, *One Membership to Get More Out of Google*10
Microsoft 365, *OneDrive PC folder backup*10
Microsoft, *OneDrive Personal Cloud Storage*.....10
Samuel Gibbs, *How Did Email Grow from Messages Between Academics to a
 Global Epidemic?*, Guardian (Mar. 7, 2016)9

PRELIMINARY STATEMENT

The Appellate Division concluded that so long as the State makes a single showing of probable cause, the sole limitation on the State's ability to surveil an individual's prospective private communications is Rule 3:5-5(a), which requires that a warrant be executed within 10 days of issuance. Under the ruling below, therefore, courts can issue warrants for communications and related data (communications data warrants or "CDWs") so long as the surveillance is limited to 10 days' worth of future conversations. This ongoing communications surveillance, the Appellate Division held, is not subject to enhanced safeguards contained in Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510 *et seq.* (hereinafter "Wiretapping and Electronic Surveillance Act" or "Title III")¹, or the equivalent provisions of the New Jersey Wiretapping and Electronic Surveillance Act ("NJWESCA"), N.J.S.A. 2A:156A-2, 2A:156A-12.

The Appellate Division's conclusion is wrong, and Meta's argument that a CDW cannot authorize ongoing surveillance of future communications is correct. The Appellate Division's ruling violates *Berger v. New York*, 388 U.S. 41 (1967), with deeply troubling consequences for privacy in modern digital

¹ Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. 90-351, Title III, 18 U.S.C. §§ 2510–20.

communications. In *Berger*, the U.S. Supreme Court held that the sensitivity of and privacy interest in private conversations require enhanced procedural safeguards to cabin executive discretion, minimize the risk of abuse, and avoid the problem of general warrants. *Id.* In response to *Berger*, the U.S. Congress and state legislatures, including New Jersey's, passed comprehensive legislation regulating wiretaps and electronic surveillance. *See* Wiretapping and Electronic Surveillance Act; NJWESCA. These statutes govern prospective, ongoing searches and seizures of communications, and the surveillance at issue here can only be constitutionally conducted with the kinds of safeguards that these statutes provide.

Indeed, regardless of whether the novel surveillance here is labeled an “interception,” the constitutional concerns that motivated the *Berger* Court plainly apply and should guide this Court’s ruling. In the five decades since *Berger*, technological developments have vastly expanded the universe of private communications susceptible to government intrusions and at risk of indiscriminate government rummaging. Service providers now store extensive records of past conversations, far more revealing even than the eavesdropping or wiretapping of old. In 1967, police had to tap into conversations at the right place and the right time, or the conversations instantly disappeared. Now, law enforcement can go back in time, and scour vast repositories of emails, texts,

direct messages, photos, location data, search histories, and more. As with the interception of current or prospective conversations, when law enforcement engages in surveillance of sensitive digital communications content, the Constitution requires scrupulous adherence to the dictates of the Fourth Amendment, especially the particularity requirement, to balance the relationship between the state and the individual and to ensure that police do not abuse the extensive access modern technology affords to intimate matters.

Finally, the New Jersey Constitution provides protections beyond those of the Fourth Amendment, and therefore dictates that this Court hold that the types of protections codified in Title III and the NJWESCA must also apply to the communications surveillance at issue here.

STATEMENT OF FACTS AND PROCEDURAL HISTORY

For the purpose of this brief, *amici* accept the statement of facts and procedural history contained in Meta's Appellate Division brief, adding the following: The Appellate Division affirmed the trial court's quashing of the communication data warrants, but held that wiretap orders were not required. *Facebook, Inc. v. State*, 471 N.J. Super. 430, 436 (App. Div. 2022). The panel imposed certain temporal limitations on the use of communication data warrants. *Id.* Thereafter, Facebook sought leave to appeal, which this Court

granted. *Facebook, Inc. v. State*, 251 N.J. 378 (2022). The State sought and obtained leave to cross-appeal. *Facebook, Inc. v. State*, 252 N.J. 36 (2022).

ARGUMENT

I. Today’s data surveillance is far more invasive even than eavesdropping and wiretaps of old.

Computers and other digital devices contain an immense amount of private, sensitive data. Three and a half decades separate the world’s first e-mail message² from the vast storage and communicative capacities of cloud computing.³ With cloud computing, previously unimaginable troves of information—including private photos, voice recordings, videos, documents, diaries, correspondence, appointments, medical records, and more—are stored by third-party companies and can be accessed by a user at any time, via any device with an Internet connection.

These advances also mean that individuals can engage in an increasing variety and volume of cloud-based electronic communications, including emails, SMS and text messages, chats on messaging apps, and social media messages. Those communications can include not just conversations, but also

² Samuel Gibbs, *How Did Email Grow from Messages Between Academics to a Global Epidemic?*, *Guardian* (Mar. 7, 2016) (Aa29).

³ Antonio Regalado, *Who Coined ‘Cloud Computing’?*, *MIT Tech. Rev.* (Oct. 31, 2011) (Aa2) (noting 2006 as the year Google’s Eric Schmidt introduced the term to an industry conference, with the term quickly gaining popularity after).

all of the kinds of digital files now stored in our devices and on our Internet accounts.

In recent years, the use of cloud-based services for digital storage and communication has skyrocketed. Today's most popular cloud storage platforms allow personal users to store massive quantities of personal information on their servers. Microsoft, Dropbox, Apple, and Google all offer their users several gigabytes of data storage for free and up to two terabytes by subscription.⁴ A 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.⁵

With many cloud-based services, 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.⁶ The owner can then access those files, share access with others, and maintain control across platforms over who has editing access or viewing rights. The low cost of cloud storage also means that social media companies allow users

⁴ Microsoft, *OneDrive Personal Cloud Storage* (Aa25); Dropbox, *Choose the Right Dropbox for You* (Aa12); Apple, *iCloud Storage Plans and Pricing* (Aa8); Google One, *One Membership to Get More Out of Google* (Aai).

⁵ Dropbox, *How Much is 1 TB of Storage?* (Aa17).

⁶ Microsoft 365, *OneDrive PC folder backup* (Aa20).

to constantly add content—conversations, photos, videos, audio recordings, and other files—without having to delete older data, resulting in years of personal and communicative information stored online.

In short, today’s digital platforms store far more information revealing individuals’ private matters than one could obtain from past physical analogs. *See Riley v. California*, 573 U.S. 373, 394–95 (2014); *see also United States v. Comprehensive Drug Testing, Inc.* (hereinafter “*CDT*”), 621 F.3d 1162, 1175 (9th Cir. 2010) (en banc) (per curiam).

Because online accounts “collect[] in one place many distinct types of information”—for example, an address, a note, a prescription, a bank statement, or a video—digital data “reveal much more in combination than any isolated record,” *Riley*, 573 U.S. at 394, and they reveal much more about “an individual’s private interests or concerns.” *Id.* at 395. Moreover, while our garages and desk drawers may fill all the way up with knickknacks, requiring periodic spring cleaning, digital data can pile up and persist indefinitely. Law enforcement access to electronically stored data can expose years’—even decades’—worth of personal information. *See Carpenter v. United States*, 138 S. Ct. 2206, 2218 (2018); *Riley*, 573 U.S. at 394. This combination of volume, depth, and longevity of personal information raises severe privacy risks when it comes to digital searches.

Technology has also given law enforcement the ability to obtain previously unknowable information, *Carpenter*, 138 S. Ct. at 2217–18, such as records of what we read (Internet browsing history), where we’ve gone (location history), what we’ve said (extensive conversations in the form of email or text), and to whom we’ve said it (associational information), along with efficient and centralized access to medical records and other sensitive information. Courts have already recognized some of these categories of information as deserving of particularly stringent privacy protections. *See, e.g., Riley*, 573 U.S. at 395–96 (search and browsing history “could reveal an individual’s private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD”); *United States v. Warshak*, 631 F.3d 266, 286 (6th Cir. 2010) (email); *In re Grand Jury Subpoena*, 828 F.3d 1083 (9th Cir. 2016) (same). As the Ninth Circuit has explained, “searches of computers therefore often involve a degree of intrusiveness much greater in quantity, if not different in kind, from searches of other containers.” *United States v. Payton*, 573 F.3d 859, 862 (9th Cir. 2009).⁷

⁷ In addition, searches of computers or other digital devices that are connected to the Internet present risks that law enforcement searching through a device could access more than locally stored physical media but online accounts, too. *See, e.g., United States v. Shipp*, 392 F. Supp. 3d 300, 308 (E.D.N.Y. 2019) (Police access to social media accounts and online communications services

II. Under *Berger*, the Fourth Amendment requires that warrants seeking ongoing access to future private communications contain special safeguards, like those enshrined in Title III and the NJWESCA, regardless of whether acquisition is contemporaneous or not.

The Supreme Court’s decision in *Berger* governs the ongoing surveillance of future private communications at issue in this case. The State asserts that it may obtain multiple disclosures of future private electronic communications without complying with either the federal or state wiretap and electronic surveillance statutes, solely because the technological means of transmitting information over the Internet involves temporary storage on a provider’s servers. However, the State cannot avoid the constitutional safeguards that *Berger* prescribes by pointing to minor technological differences between how companies facilitated prospective communications surveillance in the 1960s and today.

In *New York v. Berger*, the U.S. Supreme Court held that a New York statute—which authorized the interception of communications based only on reasonable grounds to believe that evidence of crime may be obtained—violated the Fourth Amendment. 388 U.S. 41 (1967). The New York statute

present a “threat [that] is further elevated . . . because, perhaps more than any other location—including a residence, a computer hard drive, or a car—[they] provide[] a single window through which almost every detail of a person’s life is visible.”).

did not require particularity as to the communications, conversations, or discussions to be seized, the facilities where the interception would take place, or the communications that would be obtained. Nor did it require a showing of necessity, minimization of innocent or irrelevant conversations, nor reporting to the judge. *Id.* at 59.

In ruling the New York statute unconstitutional, the Court noted that access to “private discourse” is particularly invasive and susceptible to abuse. *Id.* at 45. Indeed, eavesdropping invades “the innermost secrets of one’s home or office,” *id.* at 63, and presents “inherent dangers.” *Id.* at 60. Eavesdropping “involve[d] an intrusion on privacy that is broad in scope,” *id.* at 56.

In particular, the Court held that the New York statute violated the Fourth Amendment in part because it permitted a single warrant to authorize multiple prospective searches and seizures. The Court stated that eavesdropping for a two-month period was “[the] equivalent of a series of intrusions, searches and seizures pursuant to a single showing of probable cause[,] . . . [and avoids] prompt execution.” *Id.* at 59. The Fourth Amendment requires that continuation of surveillance be based on “*present* probable cause,” and not on the probable cause showing in the original warrant. *Id.* Yet that is exactly what the State seeks to do here.

The Court further noted that the search was unreasonable because of its impact on uninvolved third parties. “During such a long and continuous (24 hours a day) period[,] the conversations of any and all persons coming into the area covered by the device will be seized indiscriminately and without regard to their connection with the crime under investigation.” *Id.* Again, the information the State would obtain should this warrant be enforced will have a broad impact over a much longer period of time than a day.

To illustrate the lack of adequate protections in the New York law, the Court compared warrants authorized by the New York statute to a court order it upheld in another case, *Osborn v. United States*, 385 U.S. 323 (1966). In particular, the Court noted that the *Osborn* warrant “authorized *one limited intrusion*[,] *rather than a series or a continuous surveillance.*” 388 U.S. at 57 (emphasis added). The Court also noted that the *Osborn* officer’s subsequent searches were based on a new probable cause order. Further, the officer executed the warrants “with dispatch, and not over a prolonged and extended period.” *Id.* In contrast, the State here seeks an order permitting a series of intrusions, based on one showing of probable cause, and without need to go back to court to resume or initiate a new search. The surveillance would take place over a prolonged period. Such an order would violate the Fourth Amendment for the same reason that the statute in *Berger* did. *Id.*

The State argues that it need not comply with the dictates of *Berger*, and thus not of the federal or state statutes that apply to wiretaps and electronic surveillance, because it has contrived to avoid an “interception,” which, it says, means only the acquisition of the contents of communications *contemporaneous* with their transmission. The State’s legal argument exploits the “store and forward” nature of the computer protocols underlying the Internet, even though the information it seeks to obtain is functionally indistinguishable from what a wiretap would produce, but without the constitutionally-required safeguards. *Cf. United States v. Espudo*, 954 F. Supp. 2d 1029, 1034–35 (S.D. Cal. 2013) (holding that when the government “obtain[s] cell site location data for forward-looking periods of time,” it must abide by the rules governing real-time surveillance, notwithstanding that the data is “maintained by the cell phone provider, however briefly, before it [is] sent to the Government”).

Moreover, *Berger* does not draw the sharp line between contemporaneous and stored communications that the State says it does. While *Berger* uses the term “intercept,” it does not define it as “contemporaneous acquisition.” To the extent the examples in *Berger* involved contemporaneous access, that is likely because, in 1967, such access was the only reliable way to obtain private conversations. Then, as people talked, the words disappeared

forever unless someone was right there to hear them or had devised physical means to record them.

But nothing in *Berger*'s reasoning turns on whether the intrusions are contemporaneous or delayed by 15 minutes. The *Berger* Court's analysis was based on the invasiveness of government access to private conversations, and not the technology by which police accomplish the surveillance. While legislatures subsequently sought to implement the constitutionally-required safeguards in statutes regulating "wiretaps and electronic surveillance," see *Wiretapping and Electronic Surveillance Act and NJWESCA*, *Berger* itself emphasized how its principles reached a variety of surveillance methods. Indeed, the Court noted how communications surveillance had evolved through the years, from eavesdroppers lurking near windows or walls to intercepting telegraph signals, connecting to a telephone line, planting "bugs," beaming electronic rays at walls or glass windows, using tiny concealed or parabolic microphones, or employing a combination mirror transmitter that transmits images as well as sounds. 388 U.S. at 45–47. It explained that "few threats to liberty exist which are greater than that posed by the use of eavesdropping devices," regardless of the nature of that device. *Id.* at 63.

Berger is clear that law enforcement access to ongoing private electronic communications requires safeguards beyond a traditional warrant. The State

would use a technological wrinkle to gain exactly that kind of broad access on a repeated, prospective basis, with just one probable cause showing and without showing necessity, minimization, or particularity as to conversations or facilities, and without following other procedures acclaimed in *Berger* and codified in statute. But *Berger*'s reasoning does not depend on the technology employed. The *Berger* safeguards enshrined in New Jersey's wiretapping statute apply to conversation surveillance accomplished by ongoing access to today's online accounts, just as much as they do to surveillance accomplished by ongoing access to private communications using older techniques such as telephone surveillance. For these reasons, Meta's view that a CDW is insufficient and the State must comply with Title III and the NJWESCA is correct.

III. If the Court disagrees that the proposed series of ongoing acquisitions of electronic communications are an "interception", the *Berger* and subsequent electronic search cases nevertheless require strict adherence to Fourth Amendment safeguards.

Surveillance that by its nature involves a broad intrusion on conversational privacy requires strict adherence to the Fourth Amendment's requirements. In light of the extraordinary volume and breadth of sensitive information contained in today's electronically stored and transmitted information, warrants must impose clear limitations on law enforcement's electronic searches and seizures so as to avoid unnecessary exposure of our

intimate details to investigators. Even if the Court disagrees that the wiretapping statutes apply to this case, it should nevertheless ensure that the CDWs here specify the category of data, date range, or other fact-specific criteria that will ensure particularity and guard against overbreadth, and not authorize a “printout of everything that the user has”. *State’s Br. in Opp’n to FB’s Mot. to Appeal*, at 2. In addition, courts can and sometimes must require investigators to report back, to segregate non-responsive data through the use of clean teams or other means, to delete irrelevant data, and to comply with other privacy-protecting practices to ensure that searches are constitutional.

The Fourth Amendment is intended “to place obstacles in the way of a too permeating police surveillance.” *Carpenter*, 138 S. Ct. at 2214 (citation and quotation marks omitted). It requires that search warrants particularly describe the places to be searched and the things to be seized (particularity), and prohibits search for or seizure of anything for which there is not probable cause (overbreadth). Even in the context of warrants authorizing the search and seizure of a person’s physical papers, the Supreme Court has long recognized the grave dangers of government access to papers without probable cause. As a result, “responsible officials, including judicial officials, must take care to assure that [searches and seizures] are conducted in a manner that minimizes unwarranted intrusions upon privacy.” *Anderson v. Maryland*, 427 U.S. 463,

482 n.11 (1976). These concerns are especially salient in the face of expanding technological search capabilities, *see Riley*, 573 U.S. at 394–95, and *Berger*'s warnings about the “inherent dangers” of unbounded electronic searches and seizures hold true whether law enforcement seeks to obtain future communications or a complete record of those that have already occurred. 388 U.S. at 58–60.

Critically for the account searches and seizures at issue here, the Fourth Amendment requires that searches and seizures be limited by time frame, to relevant categories of information, and by other case-specific factors to the extent possible. There is no need for—and the Fourth Amendment does not allow—“all-content” CDWs demanding seizure of any account content or digital files that might exist.

First, courts regularly require the government to specify discrete categories of digital information to satisfy particularity and obtain a valid warrant. For example, in one federal investigation of an illegal firearms charge, a search warrant demanded that Facebook provide all the user's personal information, activity logs, photos, videos, posts, private messages, chats, friend requests, video call history, check-ins, IP logs, “likes,” use of Facebook Marketplace, payment information, privacy settings, blocked users, tech support requests, and more. *United States v. Shipp*, 392 F. Supp. 3d 300,

303–06 (E.D.N.Y. 2019). In another, the government sought all financial records, notes, memoranda, records of internal and external communications, correspondence, audio tapes, video tapes, and photographs, among other information. *United States v. Wey*, 256 F. Supp. 3d 355, 364–66 (S.D.N.Y. 2017). Both courts held that warrants for seizure of any category of data without “link[ing] the evidence sought to the criminal activity supported by probable cause” did “not satisfy the particularity requirement.” *Id.* at 387 (citations omitted); *Shipp*, 392 F. Supp. 3d at 307. *See also In re Three Hotmail Email Accounts*, No. 16-MJ-8036-DJW, 2016 WL 1239916 (D. Kan. Mar. 28, 2016), *overruled in part by In re Info. Associated With Email Addresses Stored at Premises Controlled by the Microsoft Corp.*, 212 F. Supp. 3d 1023 (D. Kan. 2016) (denying warrant to search all content of email accounts).

State courts agree with this principle in the context of both social media and cell phone searches and seizures. *See Richardson v. State*, No. 46, 2022 WL 3711713 (Md. August 29, 2022) (“all-content” warrant to search cell phone should have been limited by time frame and categories of data); *State v. Smith*, 278 A.3d 481 (Conn. 2022) (warrant did not sufficiently limit the search of the contents of a cell phone by a description of the areas within the phone to be searched or by a time frame reasonably related to the crimes); *State v. Fairley*, 457 P.3d 1150 (Wash. Ct. App. 2020) (Fourth Amendment’s

particularity requirement is of heightened importance when searching repositories for expressive materials, in the context of cell phones). Thus, courts should authorize seizure of only those categories of data likely to contain evidence of the crime. Without that limitation, a search is overbroad.

Second, seizures of account data should be limited by timeframe. CDWs can easily accomplish this. If an offense allegedly took place in 2021, police should not need obtain email from any other year, never mind a copy of the entire account, as it appears the State is seeking here. *See United States v. Abboud*, 438 F.3d 554, 576 (6th Cir. 2006) (“Failure to limit broad descriptive terms by relevant dates, when such dates are available to the police, will render a warrant overbroad.” (citations omitted)); *United States v. Diaz*, 841 F.2d 1, 4–5 (1st Cir. 1988) (warrant overbroad when authorized seizure records before the first instance of wrongdoing mentioned in the affidavit); *In re [REDACTED]@gmail.com*, 62 F. Supp. 3d 1100, 1104 (N.D. Cal. 2014) (no warrant issued where government did not include a date limitation); *In re Search of Google Email Accounts identified in Attachment A*, 92 F. Supp. 3d 944 (D. Alaska 2015) (application without date restriction denied as overbroad).

Third, when available, courts can and should also use other criteria of digital information to constrain police and ensure that seizures are scoped to

probable cause, and that the warrant particularly describes the proper data to search, and what to search for. *See United States v. Griffith*, 867 F.3d 1265, 1276 (D.C. Cir. 2017) (deeming a warrant’s failure to narrow a search based on ownership of a cell phone to be insufficiently particular). For example, if conversations between the target and known co-conspirator are potential evidence of a crime, the warrant could demand that Facebook turn over only messages between those two people. *In re Search of Info. Associated With Four Redacted Gmail Accounts*, 371 F. Supp. 3d 843, 845 (D. Or. 2018) (warrant for all emails associated with suspect’s account is overbroad because Google is able to disclose only those emails the government has probable cause to search). If investigators’ analysis reveals that another person may be involved, law enforcement can get a warrant to expand the search. But, as *Berger* points out, “conversations of any and all persons” should not be “seized indiscriminately and without regard to their connection with the crime under investigation.” 388 U.S. at 59. Yet, that is what a “snapshot” of a Facebook account does.

Finally, depending on the facts of the investigation, which judges have access to via affidavits in support of warrants, courts may further constrain potentially abusive rummaging through private data. To protect the intermingled information that investigators do not have probable cause to seize

or review, courts can enhance oversight by imposing search protocols or requiring forensic examiners to log queries for later judicial review. Courts might also require law enforcement to use clean teams, and to segregate and delete irrelevant data, or implement other privacy-protecting means as may be appropriate. *CDT*, 621 F.3d at 1177.

In sum, the surveillance here must be conducted under the safeguards prescribed in *Berger* and implemented by Title III and the NJWESCA. *See* Part II *supra*. But if the Court disagrees, a CDW for one or more complete “snapshots” of a Facebook account should only issue if it closely adheres to Fourth Amendment safeguards. Failure to do so can put the target and everyone he or she communicates with at risk of a series of general searches and seizures that could be easily abused.

IV. The New Jersey Constitution also requires these safeguards, as it is more protective than the federal Constitution.

Although New Jersey’s Wiretap and Electronic Surveillance Act, NJWESCA, N.J.S.A. 2A:156A-1–26, was modeled after Title III of the Omnibus Crime and Safe Streets Act, 18 U.S.C. §§ 2510–20, *State v. Ates*, 217 N.J. 253, 266 (2014), courts interpreting the state law must look to the State Constitution to ensure their interpretation “safeguard[s] an individual’s right to privacy.” *State v. Feliciano*, 224 N.J. 351, 370, 372–77 (2016) (*quoting Ates*, 217 N.J. at 268). The United States Constitution, as interpreted by the United

States Supreme Court, provides important guidance for this Court. But as the Court has emphasized before, while those interpretations “may serve to guide us in our resolution of New Jersey issues, ‘we bear ultimate responsibility for the safe passage of our ship.’” *State v. Cooke*, 163 N.J. 657, 666–67 (2000) (quoting *State v. Hempele*, 120 N.J. 182, 196 (1990)). For more than four decades the New Jersey Constitution has protected individuals’ rights where its federal counterpart has not. *See State v. Alston*, 88 N.J. 211, 225 (1981) (discussing divergence from federal constitutional jurisprudence).

New Jersey courts recognize that the State Constitution provides greater protections than its federal counterpart in a host of relevant contexts. For example, New Jersey courts have refused to erect barriers to civilians’ ability to challenge unlawful searches and seizures. *Compare Alston*, 88 N.J. at 228–29 (taking broad view of standing to challenge validity of searches), *with Rakas v. Illinois*, 439 U.S. 128, 134 (1978) (taking narrow view). When a police officer violates a person’s rights, the New Jersey Constitution provides a remedy, regardless of the officer’s subjective intent. *Compare State v. Novembrino*, 105 N.J. 95, 157–58 (1987) (rejecting good-faith exception to the exclusionary rule) *and State v. Carter*, 247 N.J. 488, 532 (2021) (declining, under the State Constitution, to adopt a reasonable mistake of law exception) *with United States v. Leon*, 468 U.S. 897, 905 (1984) (recognizing good-faith

exception) and *Heien v. North Carolina*, 574 U.S. 54, 61 (2014) (finding stop justified even when based on a reasonable mistake about what the law forbids). Similarly, New Jersey Courts have recognized the peril of allowing police to easily circumvent the warrant requirement through a lax view of consent. *Compare State v. Johnson*, 68 N.J. 349, 353–54 (1975) (requiring showing that consent to search was knowingly given) and *State v. Carty*, 170 N.J. 632, 651 (2002) (disallowing routine requests for consent to search in automobile stops) with *Schneckloth v. Bustamonte*, 412 U.S. 218, 225 (1973) (requiring simply that consent to search be voluntary) and *Florida v. Bostick*, 501 U.S. 429, 434 (1991) (approving routine requests for consent without reasonable suspicion).

Most critically here, this Court has found expectations of privacy where the United States Supreme Court and some federal appellate courts have not, recognizing the vast swaths of personal information that would be revealed in a search of curbside garbage (*compare Hempele*, 120 N.J. at 215 (expectation of privacy in curbside trash) with *California v. Greenwood*, 486 U.S. 35, 37 (1988)), bank records (*compare State v. McAllister*, 184 N.J. 17, 26 (2005) (expectation of privacy in bank records) with *United States v. Miller*, 425 U.S. 435, 442 (1976) (no expectation of privacy in bank records)), utility records (*compare State v. Domicz*, 188 N.J. 285, 299 (2006) (acknowledging expectation of privacy in utility records) with *Smith v. Maryland*, 442 U.S.

735, 743–44 (1979) (no expectation of privacy in calling records)), Internet Service Provider subscription records (*compare State v. Reid*, 194 N.J. 386, 389 (2008) (expectation of privacy in Internet Service Provider records) *with, e.g., United States v. Christie*, 624 F.3d 558, 574 (3d Cir. 2010) (no expectation of privacy in Internet Service Provider records)), and cellphone location (*compare State v. Earls*, 214 N.J. 564, 585 (2013) (expectation of privacy in real-time cell phone location data) *with Carpenter*, 138 S. Ct. at 2220 (finding expectation of privacy in historical cell phone location data, but expressing no view on real-time cell tracking)).

As discussed above, the United States Constitution requires at least as much restraint and as many safeguards as a wiretap order for the prospective surveillance the State is asking for here. The New Jersey Constitution requires at least as much as well, if not more.

CONCLUSION

For the reasons set forth above, the Court should hold that the privacy protections codified in Title III and the NJWESCA apply to the communications surveillance at issue here.

Dated: October 5, 2022

Respectfully submitted,



Alexander Shalom (BAR No. 021162004)
Jeanne LoCicero (BAR No. 024052000)
AMERICAN CIVIL LIBERTIES UNION
OF NEW JERSEY FOUNDATION
570 Broad Street, 11th Fl.
Post Office Box 32159
Newark, NJ 07102
Tel: (973) 854-1714
ashalom@aclu-nj.org
jlocicero@aclu-nj.org

Jennifer Stisa Granick*
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
2101 Webster Street #1300
Oakland, CA 94612
Tel: (415) 343-0758
jgranick@aclu.org

* *Pro hac vice* pending

Attorneys for Amici Curiae

**APPENDIX OF *AMICI CURIAE* AMERICAN CIVIL LIBERTIES
UNION & AMERICAN CIVIL LIBERTIES UNION OF NEW JERSEY**

TABLE OF APPENDIX CONTENTS

Google One, <i>One Membership to Get More Out of Google</i> , https://one.google.com/about	Aai
Antonio Regalado, <i>Who Coined ‘Cloud Computing’?</i> , MIT Tech. Rev. (Oct. 31, 2011).....	Aa1
Apple, <i>iCloud Storage Plans and Pricing</i>	Aa7
Dropbox, <i>Choose the Right Dropbox for You</i>	Aa11
Dropbox, <i>How Much is 1 TB of Storage?</i>	Aa16
Microsoft 365, <i>OneDrive PC folder backup</i>	Aa19
Microsoft, <i>OneDrive Personal Cloud Storage</i>	Aa24
Samuel Gibbs, <i>How Did Email Grow from Messages Between Academics to a Global Epidemic?</i> , Guardian (Mar. 7, 2016)	Aa28

MIT Technology Review**Subscribe****MIT Technology Review****Subscribe**

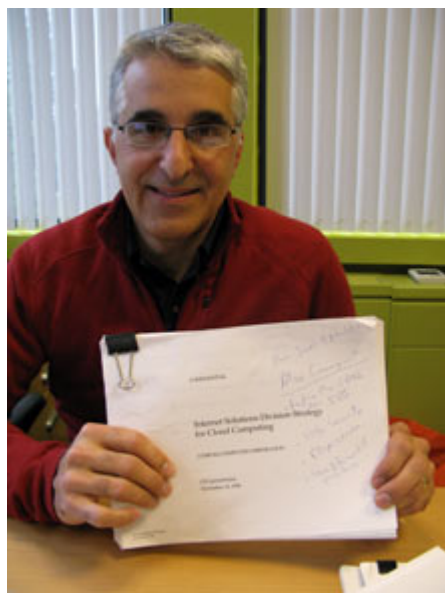
Who Coined 'Cloud Computing'?

Now that every technology company in America seems to be selling cloud computing, we decided to find out where it all began.

By Antonio Regalado

October 31, 2011

Cloud computing is one of the hottest buzzwords in technology. It appears 48 million times on the Internet. But amidst all the chatter, there is one question about cloud computing that has never been answered: Who said it first?



Proof of concept: George Favaloro poses with a 1996 Compaq business plan. The document is the earliest known use of the term “cloud computing” in print (click [here](#) to view).

Some accounts trace the birth of the term to 2006, when large companies such as Google and Amazon began using “cloud computing” to describe the new paradigm in which people are increasingly accessing software, computer power, and files over the Web instead of on their desktops.

But *Technology Review* tracked the coinage of the term back a decade earlier, to late 1996, and to an office park outside Houston. At the time, Netscape's Web browser was the technology to be excited about and the Yankees were playing Atlanta in the World Series. Inside the offices of Compaq Computer, a small group of technology executives was plotting the future of the Internet business and calling it "cloud computing."

Their vision was detailed and prescient. Not only would all business software move to the Web, but what they termed "cloud computing-enabled applications" like consumer file storage would become common. For two men in the room, a Compaq marketing executive named George Favaloro and a young technologist named Sean O'Sullivan, cloud computing would have dramatically different outcomes. For Compaq, it was the start of a \$2-billion-a-year business selling servers to Internet providers. For O'Sullivan's startup venture, it was a step toward disenchantment and insolvency.

See the rest of our Business Impact report on [Business in the Cloud](#).

Cloud computing still doesn't appear in the Oxford English Dictionary. But its use is spreading rapidly because it captures a historic shift in the IT industry as more computer memory, processing power, and apps are hosted in remote data centers, or the "cloud." With billions of dollars of IT spending in play, the term itself has become a disputed prize. In 2008, Dell drew outrage from programmers after attempting to win a trademark on "cloud computing." Other technology vendors, such as IBM and Oracle, have been accused of "cloud washing," or misusing the phrase to describe older product lines.

Like "Web 2.0," cloud computing has become a ubiquitous piece of jargon that many tech executives find annoying, but also hard to avoid. "I hated it, but I finally gave in," says Carl Bass, president and CEO of Autodesk, whose company unveiled a cloud-computing marketing campaign in September. "I didn't think the term helped explain anything to people who didn't already know what it is."

The U.S. government has also had trouble with the term. After the country's former IT czar, Vivek Kundra, pushed agencies to move to cheaper cloud services, procurement officials faced the question of what, exactly, counted as cloud computing. The government asked the National Institutes of Standards and Technology to come up with a definition. Its final draft, released this month, begins by cautioning that "cloud computing can and does mean different things to different people."

"The cloud is a metaphor for the Internet. It's a rebranding of the Internet," says Reuven Cohen, cofounder of Cloud Camp, a course for programmers. "That is why there is a raging debate. By virtue of being a metaphor, it's open to different interpretations." And, he adds, "it's worth money."

August 9, 2006, when then Google CEO Eric Schmidt introduced the term to an industry conference.

“What’s interesting [now] is that there is an emergent new model,” Schmidt said, “I don’t think people have really understood how big this opportunity really is. It starts with the premise that the data services and architecture should be on servers. We call it cloud computing—they should be in a “cloud” somewhere.”

Advertisement

The term began to see wider use the following year, after companies including Amazon, Microsoft, and IBM started to tout cloud-computing efforts as well. That was also when it first appeared in newspaper articles, such as a *New York Times* report from November 15, 2007, that carried the headline “I.B.M. to Push ‘Cloud Computing,’ Using Data From Afar.” It described vague plans for “Internet-based supercomputing.”

Sam Johnston, director of cloud and IT services at Equinix, says cloud computing took hold among techies because it described something important. “We now had a common handle for a number of trends that we had been observing, such as the consumerization and commoditization of IT,” he wrote in an e-mail.

Johnston says it’s never been clear who coined the term. As an editor of the Wikipedia entry for cloud computing, Johnston keeps a close eye on any attempts at misappropriation. He was first to raise alarms about Dell’s trademark application and this summer he removed a citation from Wikipedia saying a professor at Emory had coined the phrase in the late 1990s. There have been “many attempts to coopt the term, as well as various claims of invention,” says Johnston.

That may explain why cloud watchers have generally disregarded or never learned of one unusually early usage—a May 1997 trademark application for “cloud computing” from a now-defunct company called NetCentric. The trademark application was for “educational services” such as “classes and seminars” and was never approved. But the use of the phrase was not coincidental. When *Technology Review* tracked down NetCentric’s founder, O’Sullivan, he agreed to help dig up paper copies of 15-year-old business plans from NetCentric and Compaq. The documents, written in late 1996, not only extensively use the phrase “cloud computing,” but also describe in accurate terms many of the ideas sweeping the Internet today.



Cloud 1.0: Entrepreneur Sean O'Sullivan filed a trademark on “cloud computing” in 1997. He poses at the offices of NetCentric, in Cambridge, Massachusetts during the late 1990s.

At the time, O'Sullivan's startup was negotiating a \$5 million investment from Compaq, where Favaloro had recently been chosen to lead a new Internet services group. The group was a kind of internal “insurgency,” recalls Favaloro, that aimed to get Compaq into the business of selling servers to Internet service providers, or ISPs, like AOL. NetCentric was a young company developing software that could help make that happen.

In their plans, the duo predicted technology trends that would take more than a decade to unfold. Copies of NetCentric's business plan contain an imaginary bill for “the total e-purchases” of one “George Favaloro,” including \$18.50 for 37 minutes of video conferencing and \$4.95 for 253 megabytes of Internet storage (as well as \$3.95 to view a Mike Tyson fight). Today, file storage and video are among the most used cloud-based applications, according to consultancy CDW. Back then, such services didn't exist. NetCentric's software platform was meant to allow ISPs to implement and bill for dozens, and ultimately thousands, of “cloud computing-enabled applications,” according to the plan.

Exactly which of the men—Favaloro or O'Sullivan—came up with the term cloud computing remains uncertain. Neither recalls precisely when the phrase was conceived. Hard drives that would hold e-mails and other electronic clues from those precloud days are long gone.

Favaloro believes he coined the term. From a storage unit, he dug out a paper copy of a 50-page internal Compaq analysis titled “Internet Solutions Division Strategy for Cloud Computing” dated November 14, 1996. The document accurately predicts that enterprise software would give way to Web-enabled services, and that in the future, “application software is no longer a feature of the hardware—but of the Internet.”

O’Sullivan thinks it could have been his idea—after all, why else would he later try to trademark it? He was also a constant presence at Compaq’s Texas headquarters at the time. O’Sullivan located a daily planner, dated October 29, 1996, in which he had jotted down the phrase “Cloud Computing: The Cloud has no Borders” following a meeting with Favaloro that day. That handwritten note and the Compaq business plan, separated by two weeks, are the earliest documented references to the phrase “cloud computing” that *Technology Review* was able to locate.

“There are only two people who could have come up with the term: me, at NetCentric, or George Favaloro, at Compaq ... or both of us together, brainstorming,” says O’Sullivan.

Both agree that “cloud computing” was born as a marketing term. At the time, telecom networks were already referred to as the cloud; in engineering drawings, a cloud represented the network. What they were hunting for was a slogan to link the fast-developing Internet opportunity to businesses Compaq knew about. “Computing was bedrock for Compaq, but now this messy cloud was happening,” says Favaloro. “And we needed a handle to bring those things together.”

Their new marketing term didn’t catch fire, however—and it’s possible others independently coined the term at a later date. Consider the draft version of a January 1997 Compaq press release, announcing its investment in NetCentric, which described the deal as part of “a strategic initiative to provide ‘Cloud Computing’ to businesses.” That phrase was destined to be ages ahead of its time, had not Compaq’s internal PR team objected and changed it to “Internet computing” in the final version of the release.

In fact, Compaq eventually dropped the term entirely, along with its plans for Internet software. That didn’t matter to Favaloro. He’d managed to point Compaq (which later merged with HP) toward what became a huge business selling servers to early Internet providers and Web-page hosters, like UUNet. “It’s ridiculous now, but the big realization we had was that there was going to be an explosion of people using servers not on their premises,” says Favaloro. “I went from being a heretic inside Compaq to being treated like a prophet.”

For NetCentric, the cloud-computing concept ended in disappointment. O’Sullivan gave up using the term as he struggled to market an Internet fax service—one app the spotty network “cloud” of the day could handle. Eventually, the company went belly up and closed its doors. “We got drawn down a rathole, and we didn’t end up launching a raft of cloud computing apps ... that’s something that sticks with me,” says O’Sullivan, who later took a sabbatical from the tech world to attend film school and start a nonprofit to help with the reconstruction of Iraq.

company and, in terms of making us productive, our systems are far better than those of any of our big company. We bring up and roll out new apps in a matter of hours. If we like them, we keep them, if not, we abandon them. We self-administer, everything meshes, we have access everywhere, it's safe, it's got great uptime, it's all backed up, and our costs are tiny," says Favaloro. "The vision came true." **T**

by Antonio Regalado

KEEP READING

MOST POPULAR

This startup wants to copy you into an embryo for organ harvesting

With plans to create realistic synthetic embryos, grown in jars, Renewal Bio is on a journey to the horizon of science and ethics.

By Antonio Regalado

iCloud+ plans and pricing

When you sign up for iCloud, you automatically get 5GB of free storage. If you need more iCloud storage or want access to premium features, you can upgrade to iCloud+ .

About iCloud+

iCloud+ is Apple's premium cloud subscription. It gives you more storage for your photos, files, and backups, and additional features* available only to subscribers:

iCloud+ with 50GB storage

- 50GB of storage
- iCloud Private Relay (Beta)
- Hide My Email
- Custom Email Domain
- HomeKit Secure Video support for one camera

Share everything with up to five other family members.

iCloud+ with 200GB storage

- 200GB of storage
- iCloud Private Relay (Beta)
- Hide My Email
- Custom Email Domain
- HomeKit Secure Video support for up to five cameras

Share everything with up to five other family members.

iCloud+ with 2TB storage

- 2TB of storage
- iCloud Private Relay (Beta)
- Hide My Email
- Custom Email Domain
- HomeKit Secure Video support for an unlimited number of cameras

Share everything with up to five other family members.

You can [upgrade to iCloud+](#) from your iPhone, iPad, iPod touch, Mac, or PC. After you upgrade, you'll be billed monthly.¹ See the monthly pricing and plans per country or region below.

* Not all features are available in all countries or regions. HomeKit Secure Video requires a supported iCloud plan, compatible HomeKit-enabled security camera, and HomePod, Apple TV, or iPad running as a home hub. Private Relay is currently in beta. Some websites might have issues like showing content for the wrong region or requiring extra steps to sign in.

iCloud+ pricing

- [North America, South America, Latin America, and the Caribbean](#)
- [Europe, the Middle East, and Africa](#)
- [Asia Pacific](#)

North America, South America, Latin America, and the Caribbean

Brazil (BRL)

50GB: R\$ 3.50

200GB: R\$ 10.90

2TB: R\$ 34.90

Colombia (COP)

50GB: \$2800

200GB: \$8500

2TB: \$27900

Peru (PEN)

50GB: S/.2.90

200GB: S/.9.90

2TB: S/.29.90

Canada (CAD)	Mexico (MXN)	United States ⁴ (USD)
50GB: \$1.29	50GB: \$17	50GB: \$0.99
200GB: \$3.99	200GB: \$49	200GB: \$2.99
2TB: \$12.99	2TB: \$179	2TB: \$9.99

Chile (CLP)
 50GB: \$650
 200GB: \$1900
 2TB: \$6500

Europe, the Middle East, and Africa

Albania ^{2,3} (USD)	Hungary ³ (HUF)	Russia ³ (RUB)
50GB: \$1.19	50GB: 299 Ft	50GB: 59 p.
200GB: \$3.59	200GB: 899 Ft	200GB: 149 p.
2TB: \$11.99	2TB: 2990 Ft	2TB: 599 p.
Armenia ^{2,3}	Iceland ^{2,3} (USD)	Saudi Arabia ³ (SAR)
50GB: \$1.19	50GB: \$1.23	50GB: 3.69 ريال
200GB: \$3.49	200GB: \$3.71	200GB: 10.99 ريال
2TB: \$11.99	2TB: \$12.39	2TB: 36.99 ريال
Belarus ^{2,3} (USD)	Israel (ILS)	South Africa ³ (ZAR)
50GB: \$1.19	50GB: ₪3.90	50GB: R14.99
200GB: \$3.49	200GB: ₪11.90	200GB: R44.99
2TB: \$11.99	2TB: ₪39.90	2TB: R149.99
Bulgaria ³ (BGN)	Nigeria (NGN)	Sweden ³ (SEK)
50GB: 1.99 лв	50GB: ₦300	50GB: 9 kr
200GB: 5.99 лв	200GB: ₦900	200GB: 29 kr
2TB: 18.99 лв	2TB: ₦2900	2TB: 89 kr
Croatia ³ (HRK)	Norway ³ (NOK)	Switzerland ³ (CHF)
50GB: 7.99 kn (0.99 €)	50GB: 10 kr	50GB: CHF 1
200GB: 24.99 kn (2.99 €)	200GB: 29 kr	200GB: CHF 3
2TB: 79.99 kn (9.99 €)	2TB: 99 kr	2TB: CHF 10
Czech Republic ³ (CZK)	Pakistan (PKR)	Tanzania (TZS)
50GB: 25 Kč	50GB: Rs100	50GB: 1900 TSh
200GB: 79 Kč	200GB: Rs300	200GB: 5900 TSh
2TB: 249 Kč	2TB: Rs1000	2TB: 19900 TSh

Denmark³ (DKK)
 50GB: 7 kr
 200GB: 25 kr
 2TB: 69 kr

Poland³ (PLN)
 50GB: 3.99 zł
 200GB: 11.99 zł
 2TB: 39.99 zł

Turkey³ (TRY)
 50GB: 6.49 TL
 200GB: 19.99 TL
 2TB: 64.99 TL

Egypt³ (EGP)
 50GB: £18.99
 200GB: £54.99
 2TB: £189.99

Qatar (QAR)
 50GB: 3.69 ريال
 200GB: 10.99 ريال
 2TB: 36.99 ريال

United Arab Emirates³ (AED)
 50GB: AED 3.69
 200GB: AED 10.99
 2TB: AED 36.99

Euro³ (Euro)
 50GB: 0.99 €
 200GB: 2.99 €
 2TB: 9.99 €

Romania³ (RON)
 50GB: 4.49 lei
 200GB: 12.99 lei
 2TB: 44.99 lei

United Kingdom³ (GBP)
 50GB: £0.79
 200GB: £2.49
 2TB: £6.99

Asia Pacific

Australia³ (AUD)
 50GB: \$1.49
 200GB: \$4.49
 2TB: \$14.99

Japan³ (JPY)
 50GB: ¥130
 200GB: ¥400
 2TB: ¥1300

Republic of Korea (KRW)
 50GB: ₩1,100
 200GB: ₩3,300
 2TB: ₩11,100

China mainland³ (CNY)
 50GB: ¥6
 200GB: ¥21
 2TB: ¥68

Kazakhstan (KZT)
 50GB: ₸349
 200GB: ₸999
 2TB: ₸3490

Singapore (SGD)
 50GB: S\$ 1.28
 200GB: S\$ 3.98
 2TB: S\$ 12.98

Hong Kong (HKD)
 50GB: HK\$ 8
 200GB: HK\$ 23
 2TB: HK\$ 78

Malaysia (MYR)
 50GB: RM3.90
 200GB: RM11.90
 2TB: RM39.90

Taiwan³ (TWD)
 50GB: NT\$ 30
 200GB: NT\$ 90
 2TB: NT\$ 300

India³ (INR)
 50GB: Rs 75
 200GB: Rs 219
 2TB: Rs 749

New Zealand³ (NZD)
 50GB: \$1.69
 200GB: \$4.99
 2TB: \$16.99

Thailand (THB)
 50GB: ฿35
 200GB: ฿99
 2TB: ฿349

Indonesia (IDR)
 50GB: Rp 15000
 200GB: Rp 45000
 2TB: Rp 149000

Philippines (PHP)
 50GB: ₱49
 200GB: ₱149
 2TB: ₱499

Vietnam (VND)
 50GB: ₫19000
 200GB: ₫59000
 2TB: ₫199000

1. For countries and regions where the local currency isn't supported, such as Argentina, storage upgrades are billed in U.S. dollars (USD). [Learn more about countries and regions that bill in U.S. dollars \(USD\).](#)

2. iCloud+ upgrades for Albania, Armenia, Belarus, and Iceland are charged in U.S. dollars (USD), with prices slightly higher due to the Value Added Tax (VAT).

3. Taxes are included in all prices for these countries and regions: Albania, Armenia, Australia, Austria, Belarus, Belgium, Bulgaria, China mainland, Croatia, Cyprus, Czech Republic, Denmark, Egypt, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, India, Ireland, Italy, Japan, Republic of Korea, Latvia, Lithuania, Luxembourg, Malta, Netherlands, New Zealand, Norway, Poland, Portugal, Romania, Russia, Saudi Arabia, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, Taiwan, Turkey, the United Arab Emirates, and the United Kingdom.

4. Residents in some U.S. states have tax added to the monthly payment due to state laws.

Accepted payment methods for iCloud+ upgrades include credit cards, debit cards, and your [Apple Account balance](#). If you don't have enough available funds in your Apple Account balance to complete your upgrade, you'll be charged the remaining amount. Apple Store gift cards aren't accepted as payment for upgrading iCloud+. Learn how to [manage the amount of storage you're using](#).

[Learn how iCloud operates in China mainland.](#)

Published Date: September 01, 2022

Helpful?

Yes

No

Related topics

[Download iCloud for Windows >](#)

[Downgrade or cancel your iCloud+ plan >](#)

[About iCloud Private Relay >](#)

Start a discussion in Apple Support Communities

Ask other users about this article

[Submit my question](#)

[See all questions on this article >](#)






Contact Apple Support




Need more help? Save time by starting your support request online and we'll connect you to an expert.

[Get started >](#)

Choose the right Dropbox for you

Billed monthly
 Billed yearly (Save up to 20%)

<p> For individuals</p> <h2>Plus</h2> <p>\$9.99 / month</p> <p>2 TB (2,000 GB) • 1 user</p> <p>Buy now</p> <ul style="list-style-type: none"> ✓ Unlimited device linking ✓ 30-day file and account recovery ✓ Large file delivery with Dropbox Transfer (up to 2 GB) ✓ 3 free eSignatures per month 	<p> For households</p> <h2>Family</h2> <p>\$16.99 / family / month</p> <p>Shared 2 TB (2,000 GB) • Up to 6 users</p> <p>Buy now</p> <p>Everything in Plus, and:</p> <ul style="list-style-type: none"> ✓ Individual accounts for up to 6 people ✓ Access to Family Room folder for easy group sharing and coordination ✓ A single bill for the whole family 	<p> For solo-workers</p> <h2>Professional</h2> <p>\$16.58 / month</p> <p>3 TB (3,000 GB) • 1 user</p> <p>Try for free</p> <p>or purchase now</p> <p>Everything in Plus, and:</p> <ul style="list-style-type: none"> ✓ 180-day file and account recovery ✓ Advanced sharing controls and file locking ✓ Large file delivery with Dropbox Transfer (up to 100 GB, including customization options)
---	---	--

<p> For growing teams</p> <h2>Standard</h2> <p>\$15 / user / month</p> <p>Shared 5 TB (5,000 GB) • 3+ users</p> <p>Try for free</p> <p>or purchase now</p> <ul style="list-style-type: none"> ✓ Easy to use content protection and external sharing controls ✓ Recover files or restore your entire account up to 180 days ✓ Automatically back up computers—and connected external drives—directly to the cloud 	<p> For complex teams</p> <h2>Advanced</h2> <p>\$24 / user / month</p> <p>As much space as needed • 3+ users</p> <p>Try for free</p> <p>or purchase now</p> <p>Everything in Standard, and:</p> <ul style="list-style-type: none"> ✓ Always-on security monitoring, notifications, and alerts ✓ Large file delivery with Dropbox Transfer (up to 100 GB, including customization options) ✓ Ransomware detection and recovery 	<p> For large organizations</p> <h2>Enterprise</h2> <p>Contact sales for pricing</p> <p>As much space as needed • 3+ users</p> <div style="border: 1px solid black; padding: 5px; text-align: center;"> <p>Contact us</p> </div> <p>Everything in Advanced, and:</p> <ul style="list-style-type: none"> ✓ Enterprise-grade security and visibility tools ✓ Integrations with best-in-class security solutions ✓ Dedicated customer success manager
---	---	---

[Compare all features](#) ↓

Just need 2 GB to store and share your files?

[Sign up for our free plan](#)

Compare all features

	Personal		Business		
	<p>Plus</p> <p>For individuals</p> <div style="border: 1px solid blue; padding: 5px; text-align: center;">Buy now</div>	<p>Family</p> <p>For families</p> <div style="border: 1px solid blue; padding: 5px; text-align: center;">Buy now</div>	<p>Professional</p> <p>For individuals</p> <div style="border: 1px solid blue; padding: 5px; text-align: center;">Try for free</div> <p>or purchase now</p>	<p>Standard</p> <p>For growing teams</p> <div style="border: 1px solid blue; padding: 5px; text-align: center;">Try for free</div> <p>or purchase now</p>	<p>Advanced</p> <p>For complex teams</p> <div style="border: 1px solid blue; padding: 5px; text-align: center;">Try for free</div> <p>or purchase now</p>
Dropbox core features					

SUPPL. APPENDIX 164

Storage	2,000 GB	Share 2,000 GB	3,000 GB	5,000 GB	needed
Users	1 user	Up to 6 users	1 user	3+ users	3+ users
Best-in-class sync technology	✓	✓	✓	✓	✓
Anytime, anywhere access	✓	✓	✓	✓	✓
Easy and secure sharing	✓	✓	✓	✓	✓
256-bit AES and SSL/TLS encryption	✓	✓	✓	✓	✓
Content and accident protection					
Dropbox Backup	✓	✓	✓	✓	✓
File recovery and version history	30 days	30 days	180 days	180 days	1 year
Dropbox Rewind	30-day history	30-day history	180-day history	180-day history	1-year history
Shared link controls	✗	✗	✓	✓	✓
External sharing controls and reporting	✗	✗	✗	✓	✓
Data Classification	✗	✗	✗	✗	✓
Ransomware detection and recovery	✗	✗	✗	✗	✓
Alerts and notifications	✗	✗	✗	✗	✓
Dropbox Passwords	✓	✓	✓	✓	✓
Dropbox Vault	✓	✓	✓	✗	✗
Watermarking	✗	✗	✓	✓	✓
Account transfer tool	✗	✗	✗	✓	✓
Enable multi-factor authentication	✓	✓	✓	✓	✓
Enables HIPAA compliance	✗	✗	✗	✓	✓

Remote device wipe	✓	✓	✓	✓	✓
Device approvals	✗	✗	✗	✓	✓
Productivity and sharing tools					
Family Room	✗	✓	✗	✗	✗
Dropbox Paper	✓	✓	✓	✓	✓
Dropbox Transfer	Send up to 2 GB per Transfer	Send up to 2 GB per Transfer	Send up to 100 GB per Transfer, including customization options	Send up to 2 GB per Transfer	Send up to 100 GB per Transfer, including customization options
HelloSign eSignatures	Send up to 3 documents for eSignature per month	Send up to 3 documents for eSignature per month	Send up to 3 documents for eSignature per month* <i>*Unlimited eSignature bundle available</i>	Send up to 3 documents for eSignature per month	Send up to 3 documents for eSignature per month
File locking	✗	✗	✓	✓	✓
Integrated cloud content	✓	✓	✓	✓	✓
Branded sharing	✗	✗	✓	✓	✓
Web previews and comments	✓	✓	✓	✓	✓
Plus button	✓	✓	✓	✓	✓
File requests	✓	✓	✓	✓	✓
Full text search	✓	✓	✓	✓	✓
Viewer history	✗	✗	✓	✗	✓
Team management					
Admin console	✗	✗	✗	✓	✓
Multi-team admin login	✗	✗	✗	✓	✓
Centralized billing	✗	✓	✗	✓	✓
				SUPPL. APPENDIX 166	

Company-managed groups	✗	✗	✗	✓	✓
Unlimited API access to security platform partners	✗	✗	✗	✓	✓
Unlimited API access to productivity platform partners	✓	✓	✓	✓	✓
1 billion API calls/month for data transport partners	✗	✗	✗	✓	✓
Tiered admin roles	✗	✗	✗	✗	✓
Sign in as user	✗	✗	✗	✗	✓
Audit logs with file event tracking	✗	✗	✗	✗	✓
Single sign-on (SSO) integrations	✗	✗	✗	✗	✓
Invite enforcement	✗	✗	✗	✗	✓
Support					
Priority email support	✓	✓	✓	✓	✓
Live chat support	✓	✓	✓	✓	✓
Phone support during business hours	✗	✗	✗	✓	✓
	For individuals	For families	For individuals	For growing teams	For complex teams

Dropbox

- Desktop app
- Mobile app
- Integrations
- Features
- Solutions
- Do more than store

Products

- Plus
- Professional
- Business
- Enterprise
- HelloSign
- DocSend

Experience Dropbox

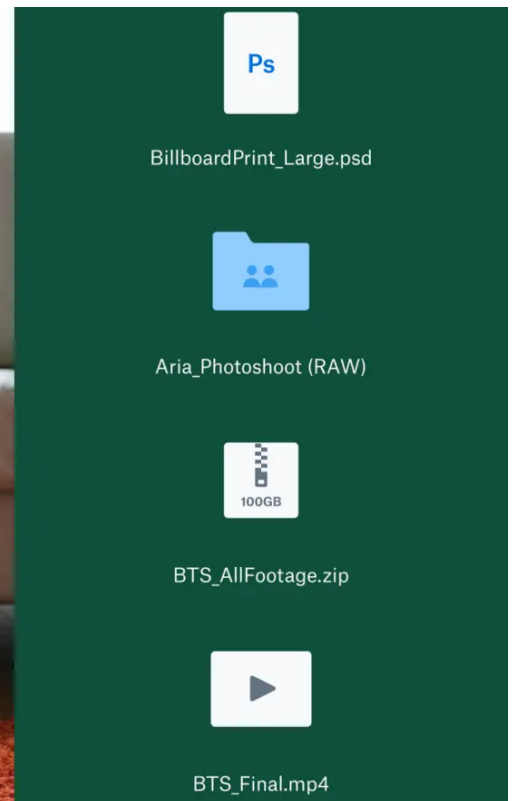
 Search

How much is 1 TB of storage?

1 TB of storage equals 1,000 GB of data—that's about 16 entry-level smartphones.

Share this

[Compare cloud storage plans](#)



What is a terabyte?

When talking about data storage, we often measure whole system storage capacity in terabytes, but most individual files take up megabytes or gigabytes for large files. So how many gigabytes or megabytes are in a terabyte? 1 TB equals 1,000 gigabytes (GB) or 1,000,000 megabytes (MB).

Experience Dropbox

Search

individual external hard drives often start at 1 TB of storage, with larger options going past 32 TB.

How much data can 1 TB hold?

The average user stores a mix of photos, videos, and documents. When you're setting up a cloud storage plan, it's hard to gauge how many photos and videos 1 TB of data can hold. One terabyte gives you the option of storing roughly:

- 250,000 photos taken with a 12MP camera;
- 250 movies or 500 hours of HD video; or
- 6.5 million document pages, commonly stored as Office files, PDFs, and presentations. It's also equal to 1,300 physical filing cabinets of paper!

Store it all in cloud storage

If your phone runs out of space, you're probably not carrying around a second one. When you're running out of storage space on your Apple or Microsoft computer, clunky portable hard drives are fragile, and small flash drives are easy to lose. Plus, the way you connect them to a computer seems to change every year. Your old external USB 3.0 hard drive won't work with a new computer that only has USB-C ports unless you get a special adaptor.

The cloud gives you an easier way to store a large amount of data, including photos, videos, and important files, without ever having to worry about disk space. When you store content in the cloud, you'll be able to do more with it, like:

- Store everything without being picky about what you save. It's also a good idea to follow the 3-2-1 rule: 3 copies of a file on 2 separate medias, with 1 copy off site.
- Access files or work remotely, whenever it's needed—even from mobile devices

Is 1 TB enough data for you?

Experience Dropbox

Search

- [Dropbox Plus](#) comes with 2 TB of storage (for 1 user)
- [Dropbox Family](#) comes with 2 TB of storage (for up to 6 users)
- [Dropbox Professional](#) has 3 TB of storage
- [Dropbox Standard, Advanced, and Enterprise](#) starts at 5 TB of storage (or as much storage as you need depending on your plan) so you don't fret about space

Ready to securely store all of your files in the cloud?

[Compare plans](#) →

Dropbox

Desktop app

Mobile app

Integrations

Features

Solutions

Do more than store

Security

Advance access

Support

Products

Plus

Professional

Business

Enterprise

HelloSign

DocSend

Plans

Product updates

Community



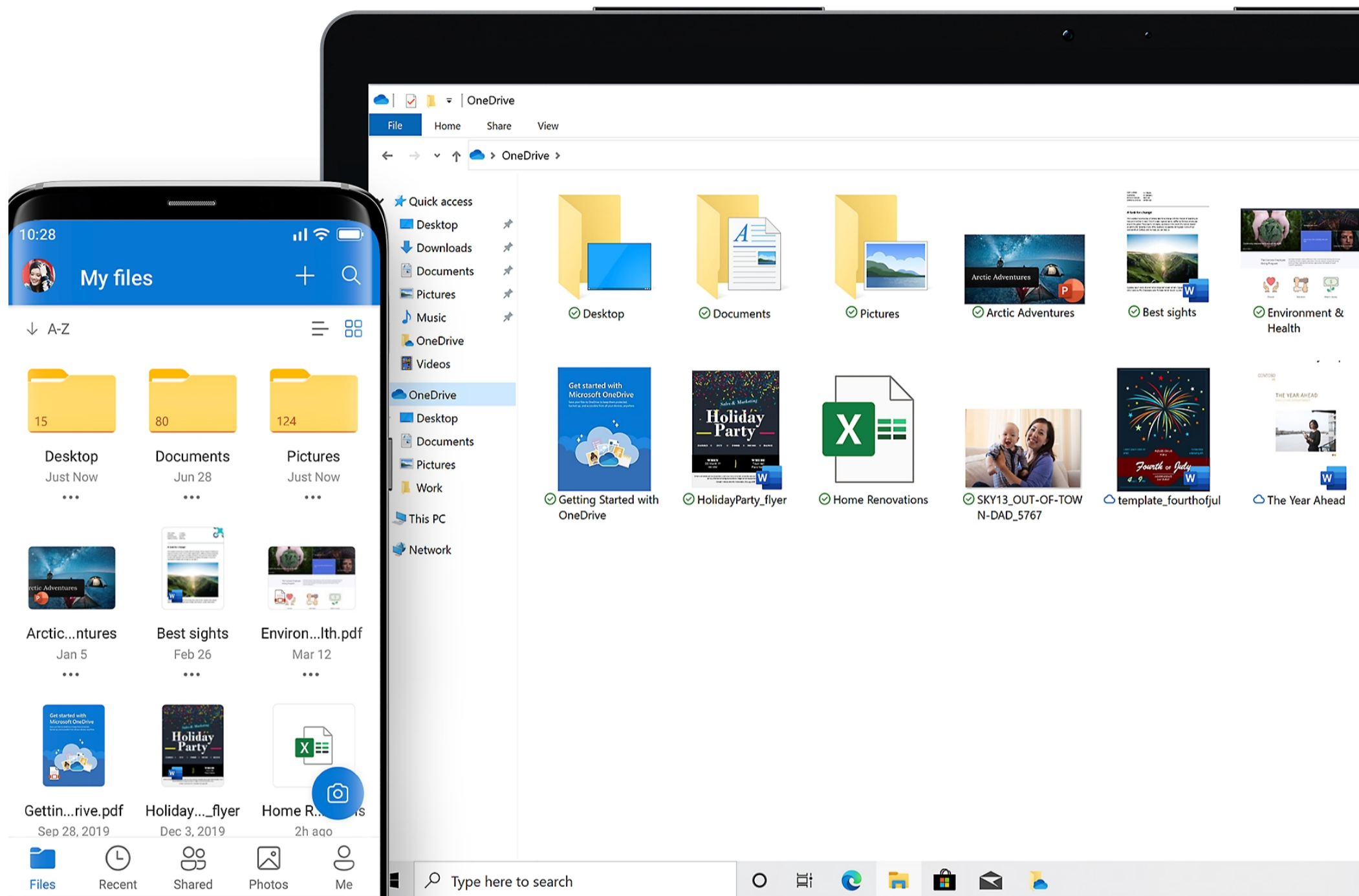
OneDrive PC folder backup

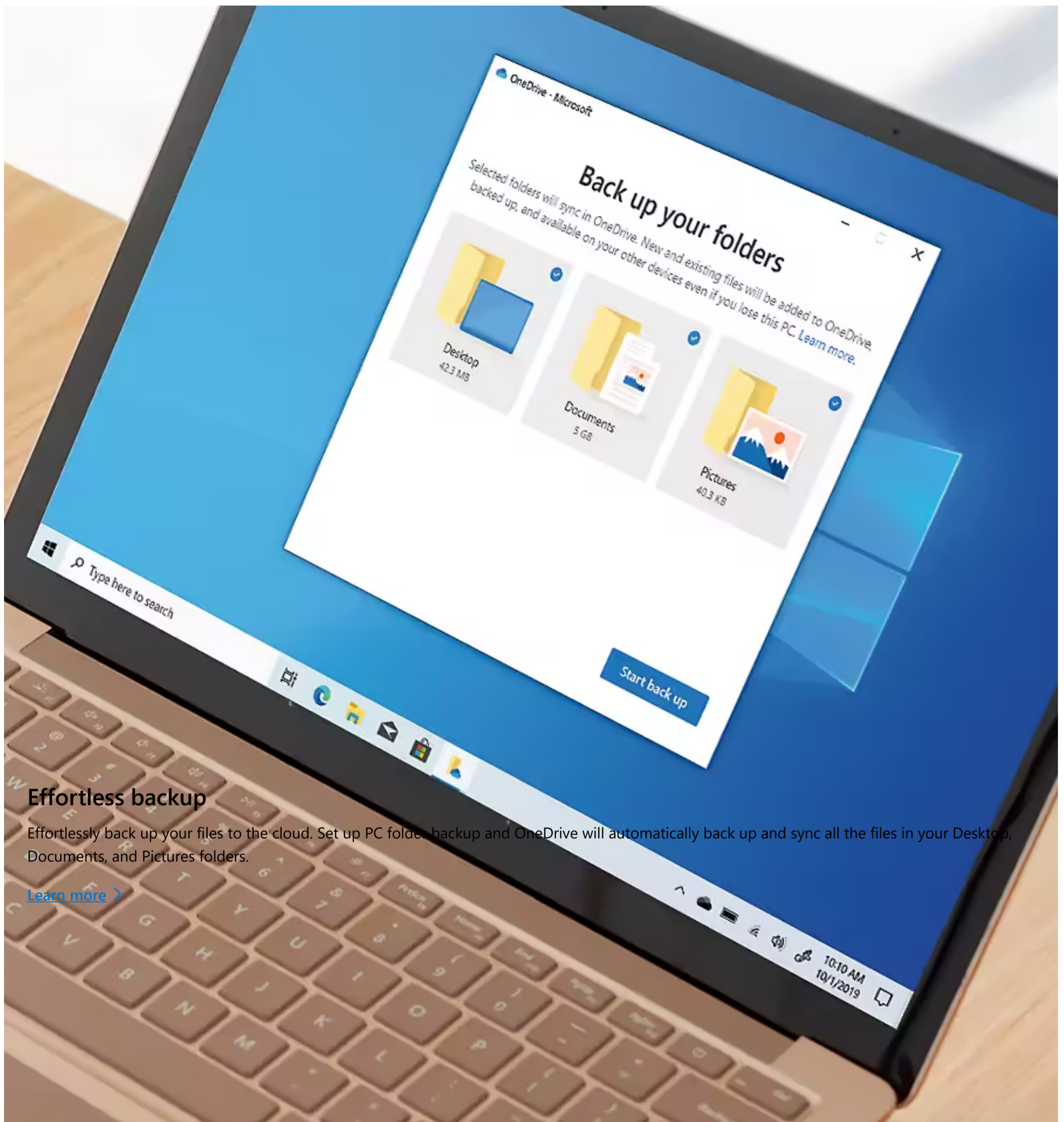
PC folder backup automatically syncs your Desktop, Documents and Pictures folders on your Windows PC to your OneDrive cloud storage. Your files and folders stay protected and are available from any device.

Get started

See it in action

[Don't have OneDrive? Get the free desktop app >](#)





Effortless backup

Effortlessly back up your files to the cloud. Set up PC folder backup and OneDrive will automatically back up and sync all the files in your Desktop, Documents, and Pictures folders.

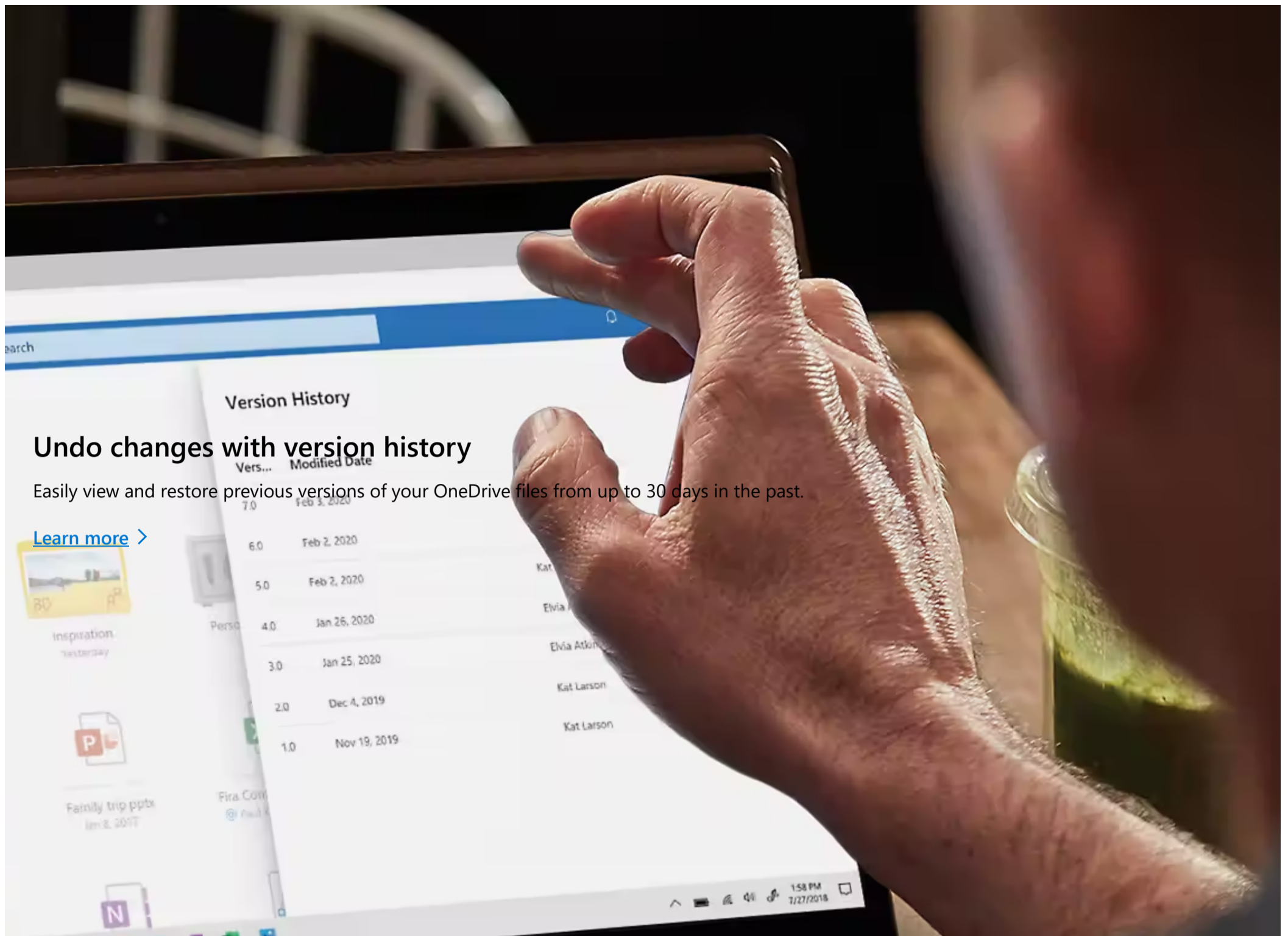
[Learn more >](#)

Access your PC files without your PC

Your backed-up PC folders are available online and in the OneDrive mobile app for you to view or edit files on the go.

[Get the mobile app >](#)

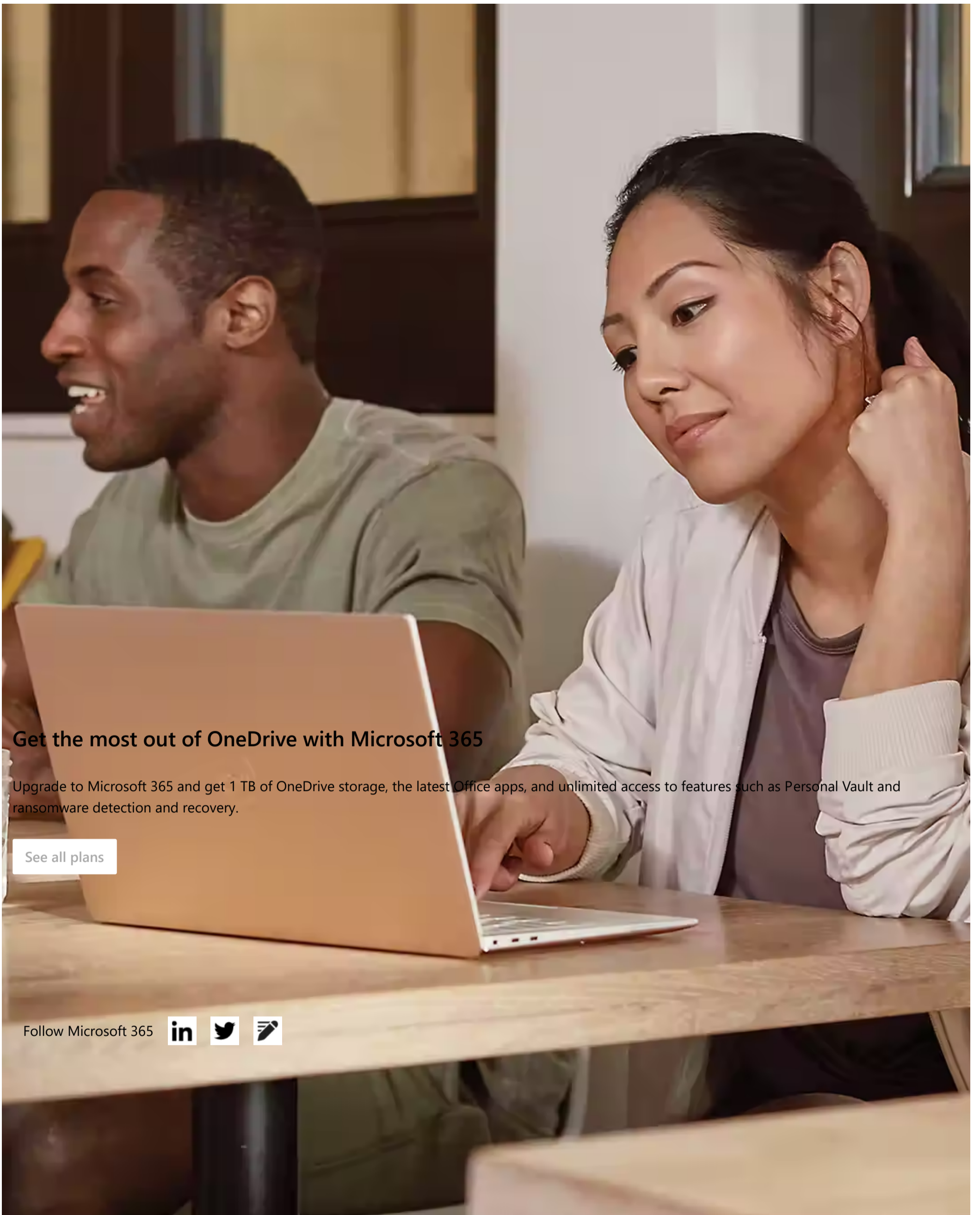




Protect files from ransomware attacks

With a Microsoft 365 subscription, OneDrive will detect ransomware attacks and help restore your files up to 30 days after the attack.

[Learn more >](#)



Get the most out of OneDrive with Microsoft 365

Upgrade to Microsoft 365 and get 1 TB of OneDrive storage, the latest Office apps, and unlimited access to features such as Personal Vault and ransomware detection and recovery.

[See all plans](#)

Follow Microsoft 365



- Surface Laptop Studio
- Surface Pro X
- Surface Go 3
- Surface Duo 2
- Surface Pro 7+
- Windows 11 apps
- Microsoft Store support
- Returns
- Order tracking
- Virtual workshops and training
- Microsoft Store Promise
- Flexible Payments
- Microsoft Teams for Education
- Microsoft 365 Education
- Education consultation appointment
- Educator training and development
- Deals for students and parents
- Dynamics 365
- Microsoft 365
- Microsoft Power Platform
- Microsoft Teams
- Microsoft Industry
- Small Business
- Documentation
- Microsoft Learn
- Microsoft Tech Community
- Azure Marketplace
- AppSource
- Visual Studio
- Company news
- Privacy at Microsoft
- Investors
- Diversity and inclusion
- Accessibility
- Sustainability



Microsoft 365

Products

All Microsoft

OneDrive is turning 15! To celebrate, we've got some surprises for you. [Check out our blog to learn more >](#)

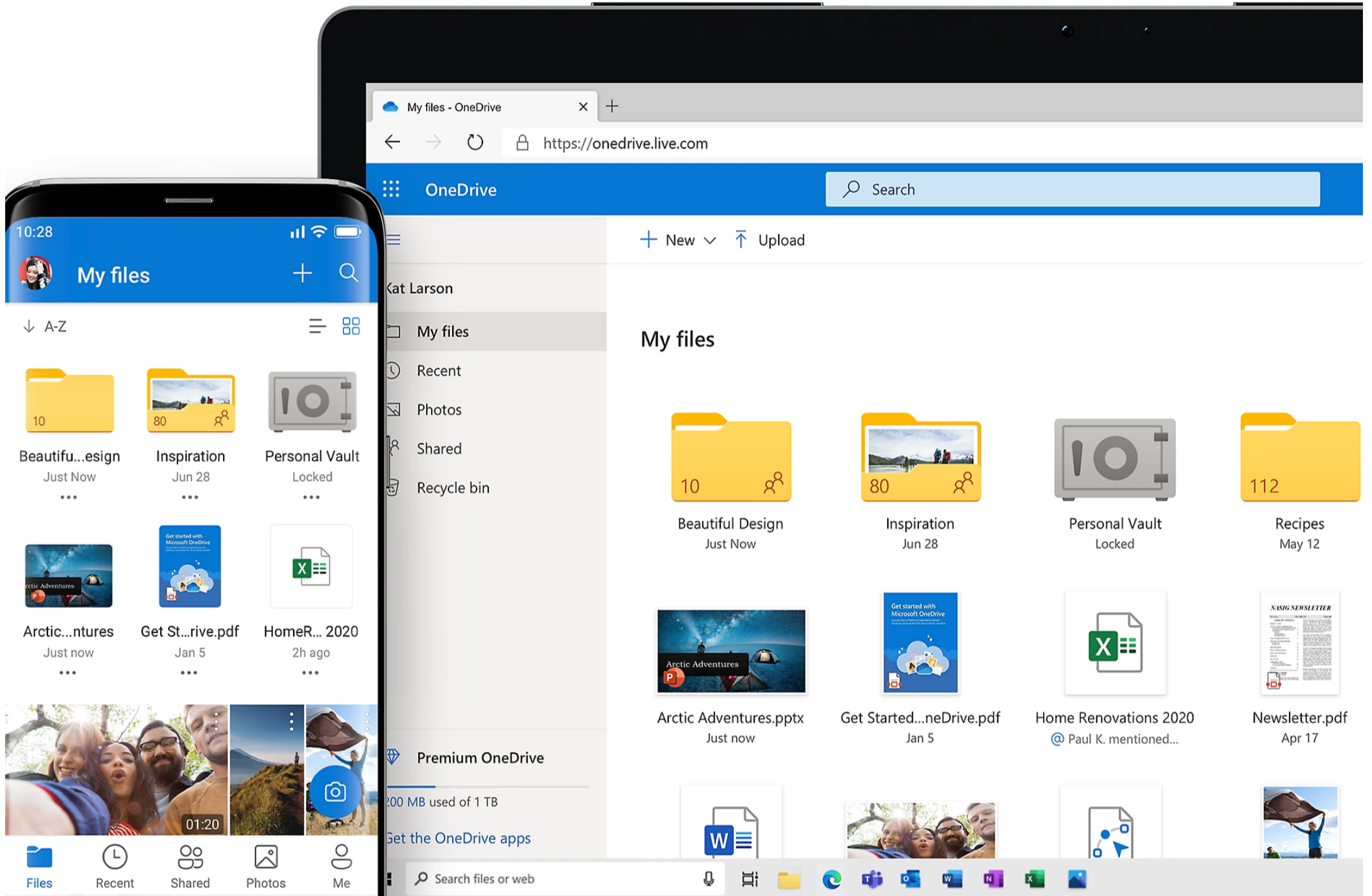
OneDrive Personal Cloud Storage

Save your photos and files to OneDrive and access them from any device, anywhere.

[Create free account](#)

[See plans and pricing](#)

[Already have OneDrive? Sign in >](#)



Organized. Protected. Connected.



Anywhere access

Enjoy the freedom to access, edit, and share your files on all your devices, wherever you are.



Back up and protect

If you lose your device, you won't lose your files and photos when they're saved in OneDrive.



Share and collaborate

Stay connected, share your documents and photos with friends and family, and collaborate in real time with Office apps.



Share and collaborate

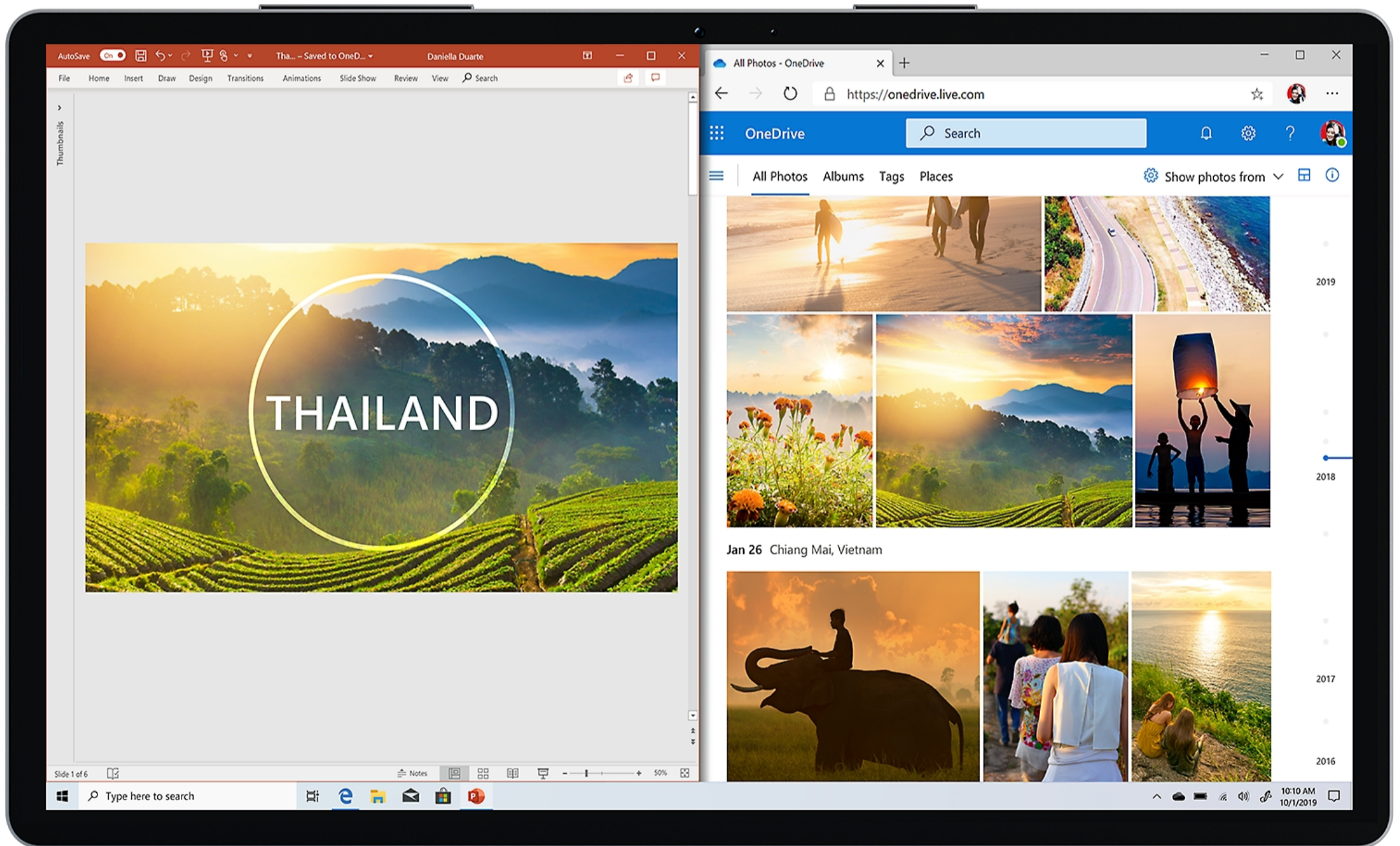
Share files, folders, and photos with friends and family. No more large email attachments or thumb drives—just send a link via email or text.

[Download Microsoft OneDrive mobile app >](#)

Get more done with Microsoft 365

Create your best work with the latest versions of Word, Excel, and other Office apps. Plus, get 1 TB of cloud storage, document sharing, ransomware recovery, and more with OneDrive.

[Learn more >](#)



Features to make life easier and safer



Files on demand

Access all your OneDrive files in Windows 11 without taking up space on your PC.



Document scanning

Use your mobile device to scan and store documents, receipts, business cards, notes, and more in OneDrive.



Personal Vault

Store important files and photos with an added layer of protection in OneDrive Personal Vault.

Access your photos and files on all your devices

[Sign in](#)

[See plans and pricing](#)

Follow Microsoft 365



What's new

- Surface Laptop Go 2
- Surface Pro 8
- Surface Laptop Studio
- Surface Pro X
- Surface Go 3
- Surface Duo 2
- Surface Pro 7+
- Windows 11 apps

Microsoft Store

- Account profile
- Download Center
- Microsoft Store support
- Returns
- Order tracking
- Virtual workshops and training
- Microsoft Store Promise
- Flexible Payments

Education

- Microsoft in education
- Devices for education
- Microsoft Teams for Education
- Microsoft 365 Education
- Education consultation appointment
- Educator training and development
- Deals for students and parents
- Azure for students

Business

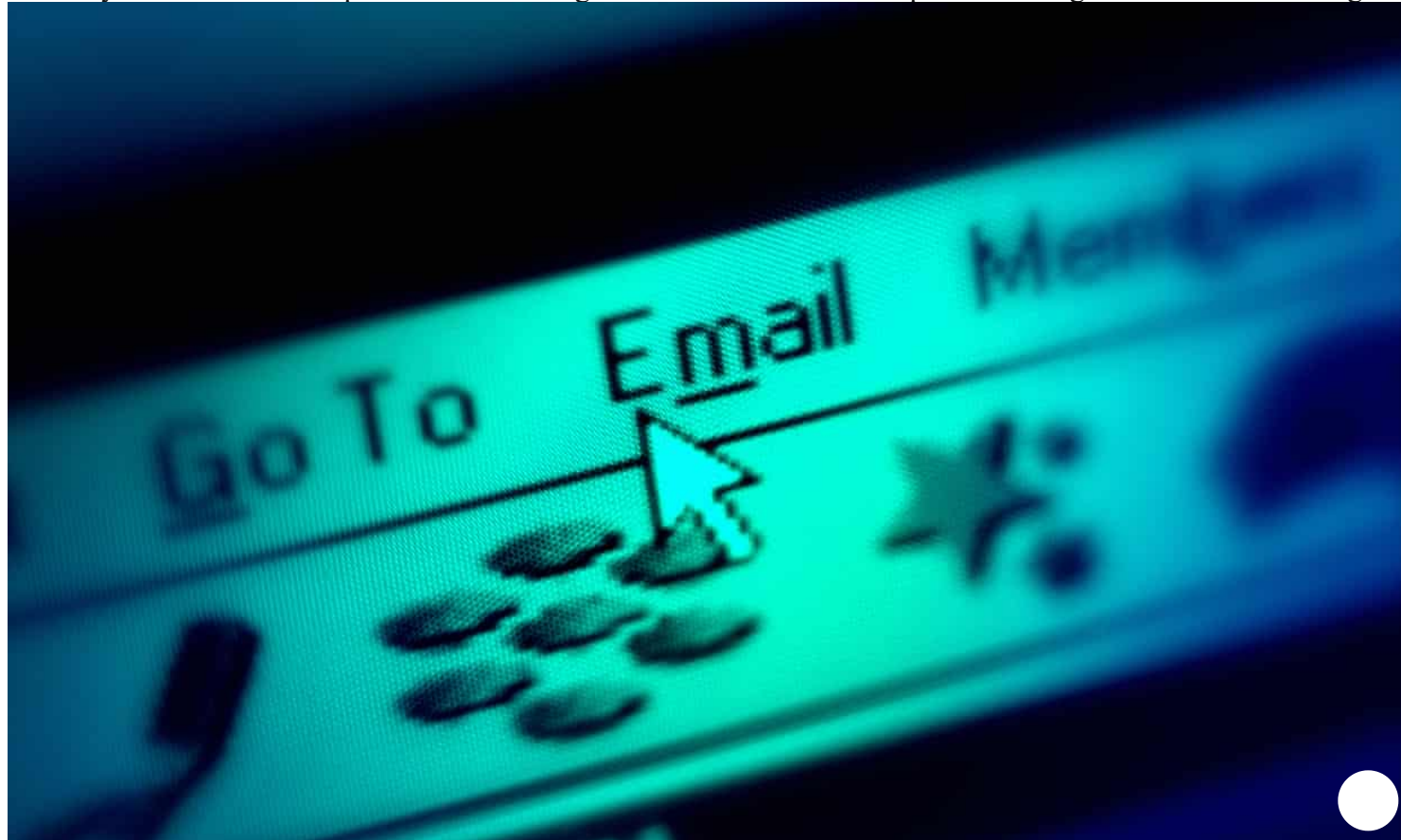
- Microsoft Cloud
- Microsoft Security
- Dynamics 365
- Microsoft 365
- Microsoft Power Platform
- Microsoft Teams
- Microsoft Industry
- Small Business

Developer & IT

- Azure
- Developer Center
- Documentation
- Microsoft Learn
- Microsoft Tech Community
- Azure Marketplace
- AppSource
- Visual Studio

Company

- Careers
- About Microsoft
- Company news
- Privacy at Microsoft
- Investors
- Diversity and inclusion
- Accessibility
- Sustainability



Internet

How did email grow from messages between academics to a global epidemic?

Ray Tomlinson, the man who literally put the @ in email addresses, has died. Here's a brief history of electronic messages, from the Queen's first mail to the triumph of spam

Samuel Gibbs

Mon 7 Mar 2016 10.07 EST

Ray Tomlinson, the man who literally put the “@” in email, [died on Saturday](#), but his invention, which allowed electronic messages to spread across the internet and fill our lives and our inboxes on a daily basis, will live on.

Here is a brief look at what Tomlinson started and the evolution of email through the last half-century.

The first electronic message - 1965



📷 Computers were all about spools of paper and tape back when the first email was sent in the 1960s.
Photograph: H. Armstrong Roberts/ClassicStock/Corbis

The very first version of what would become known as email was invented in 1965 at Massachusetts Institute of Technology (MIT) as part of the university's Compatible Time-Sharing System, which allowed users to share files and messages on a central disk, logging in from remote terminals.

Tomlinson and the @ - 1971



📷 The man who quite literally put the @ sign at the heart of email. Photograph: Handout

American computer programmer Tomlinson arguably conceived the method of sending email between different computers across the forerunner to the internet, Arpanet, at the US Defense Advanced Research Projects Agency (Darpa), introducing the “@” sign to allow messages to be targeted at certain users on certain machines.

Emails become a standard - 1973



📷 Before they were commissioning robots for the battlefield, Darpa started with the internet and email.
Photograph: HO/AFP/Getty Images

The first email standard was proposed in 1973 at Darpa and finalised within Arpanet in 1977, including common things such as the to and from fields, and the ability to forward emails to others who were not initially a recipient.

The Queen sends her first email - 1976



📷 If the Queen had known what email would do to the popularity of her beloved stamps, would she have pressed send? Photograph: Martin Keene/PA

Queen Elizabeth II sends an email on Arpanet, becoming the first head of state to do so.

Eric Schmidt designs BerkNet - 1978



SUPPL. APPENDIX 184

📷 Before Google, Schmidt developed one of the first intranet systems and messaging over serial connections in the world as part of his degree. Photograph: Scott Olson/Getty Images

Eric Schmidt, who would later lead **Google** and oversee the introduction of Gmail, wrote Berkley Network as part of his master's thesis in 1978, which was an early intranet service offering messaging over serial connections.

EMAIL program developed - 1979

At the age of 14, Shiva Ayyadurai writes a program called EMAIL for the University of Medicine and Dentistry of New Jersey, which sent electronic messages within the university, later copyrighting the term in 1982. Whether or not this is the first use of the word email is **up for debate**.

Microsoft Mail arrives - 1988



📷 'Calm down guys, I'm sure this email thing won't catch on. Photograph: Lou Dematteis/Reuters

The first version of **Microsoft** Mail was released in 1988 for Mac OS, allowing users of Apple's AppleTalk Networks to send messages to each other. In 1991, a second version was released for other platforms including DOS and Windows, which laid the groundwork for Microsoft's later Outlook and Exchange email systems.

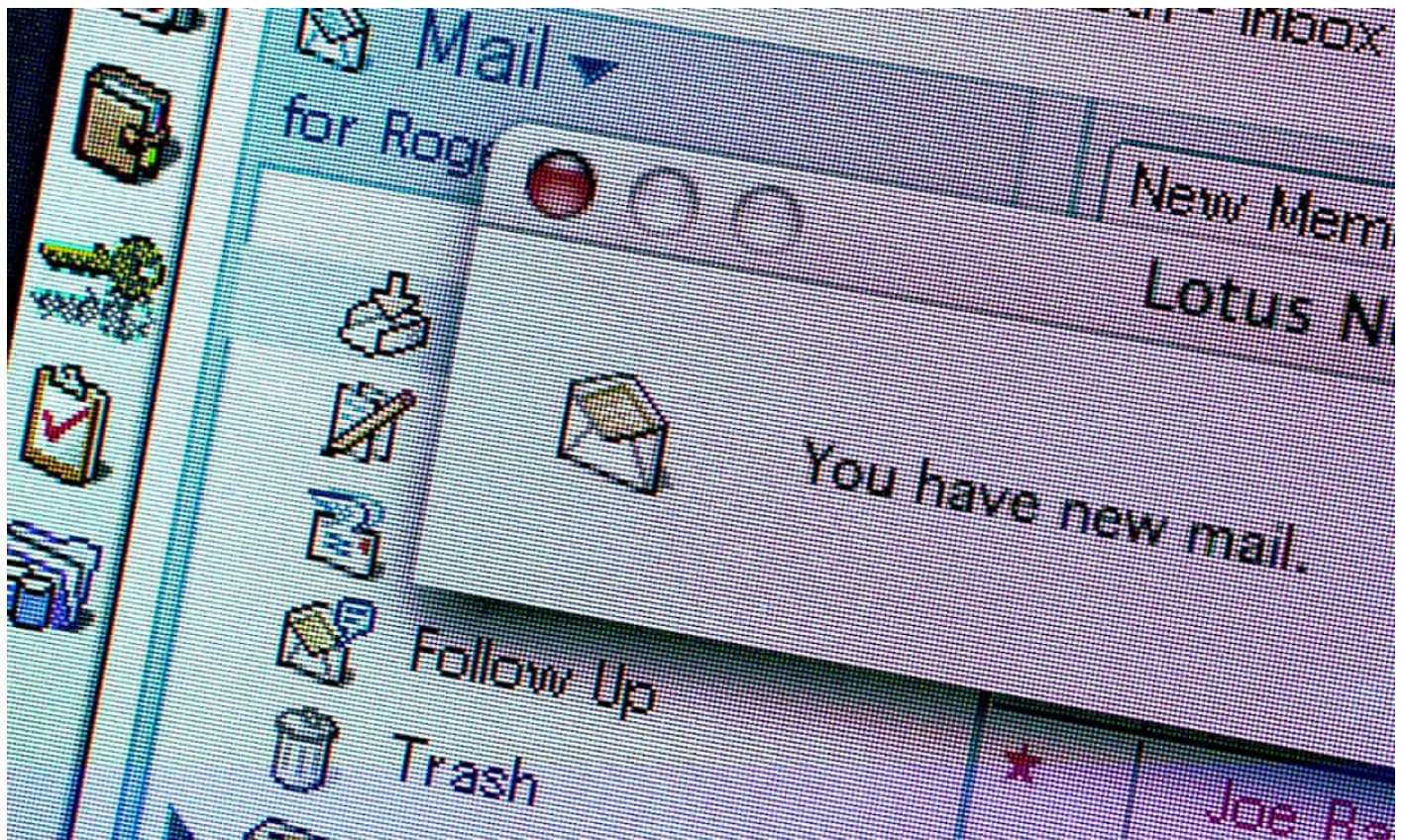
CompuServe starts internet-based email service - 1989



📷 CompuServe became one of the first ISPs to offer email to their customers before it was taken over by AOL.
Photograph: Neal Lauron/Reuters

CompuServe became the first online service to offer internet connectivity via dial-up phone connections, and its proprietary email service allowed other internet users to send emails to each other.

Lotus Notes launched - 1989



Lotus Notes brought joy of email to millions more workers, although it didn't look quite like this in 1989. Photograph: Roger Tooth/The Guardian

The first version Lotus Notes was released in 1989 by Lotus Development Corporation, which was bought by IBM in 1995.

The start of spam - 1990



📷 What's the problem with spam? Photograph: Alamy

The rise of spam can be charted back to the very early days of Arpanet, but it wasn't until the early 1990s that it hit users across the internet, when it was aimed at message boards and later email addresses.

April 1994 is the first recorded business practice of spam from two lawyers from Phoenix, Laurence Carter and Martha Siegel, who ended up writing a book on it.

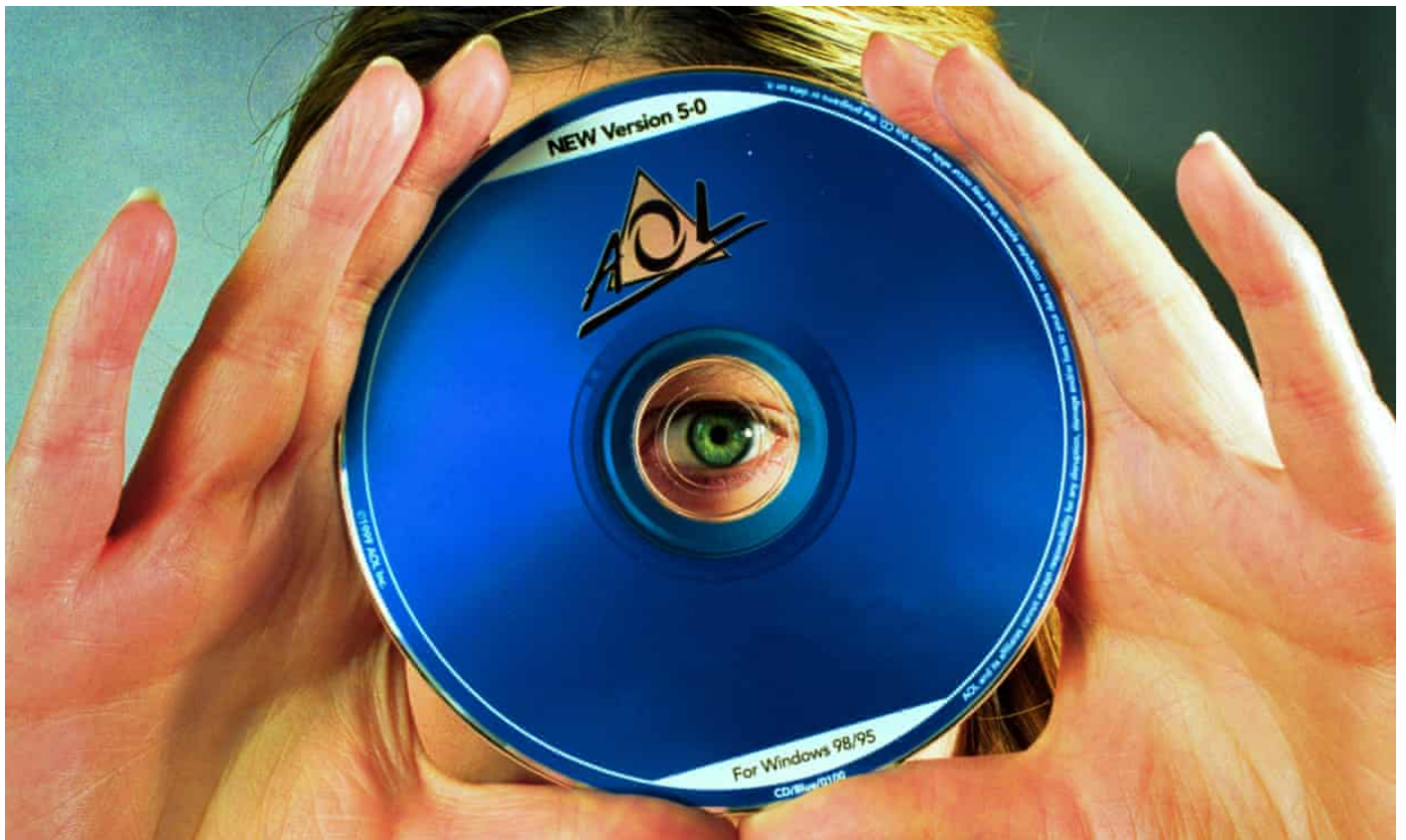
The attachment - 1992



📷 The attachment was born in 1992, another vector for computer viruses such as the Sobig F to spread
Photograph: Roger Tooth/The Guardian

The attachment was born when the Multipurpose [Internet](#) Mail Extensions (Mime) protocol was released, which includes the ability to attach things that are not just text to emails. And so begins the painful exercise of trying to delete emails to make space after someone sends you a massive attachment in the days of limited inbox space.

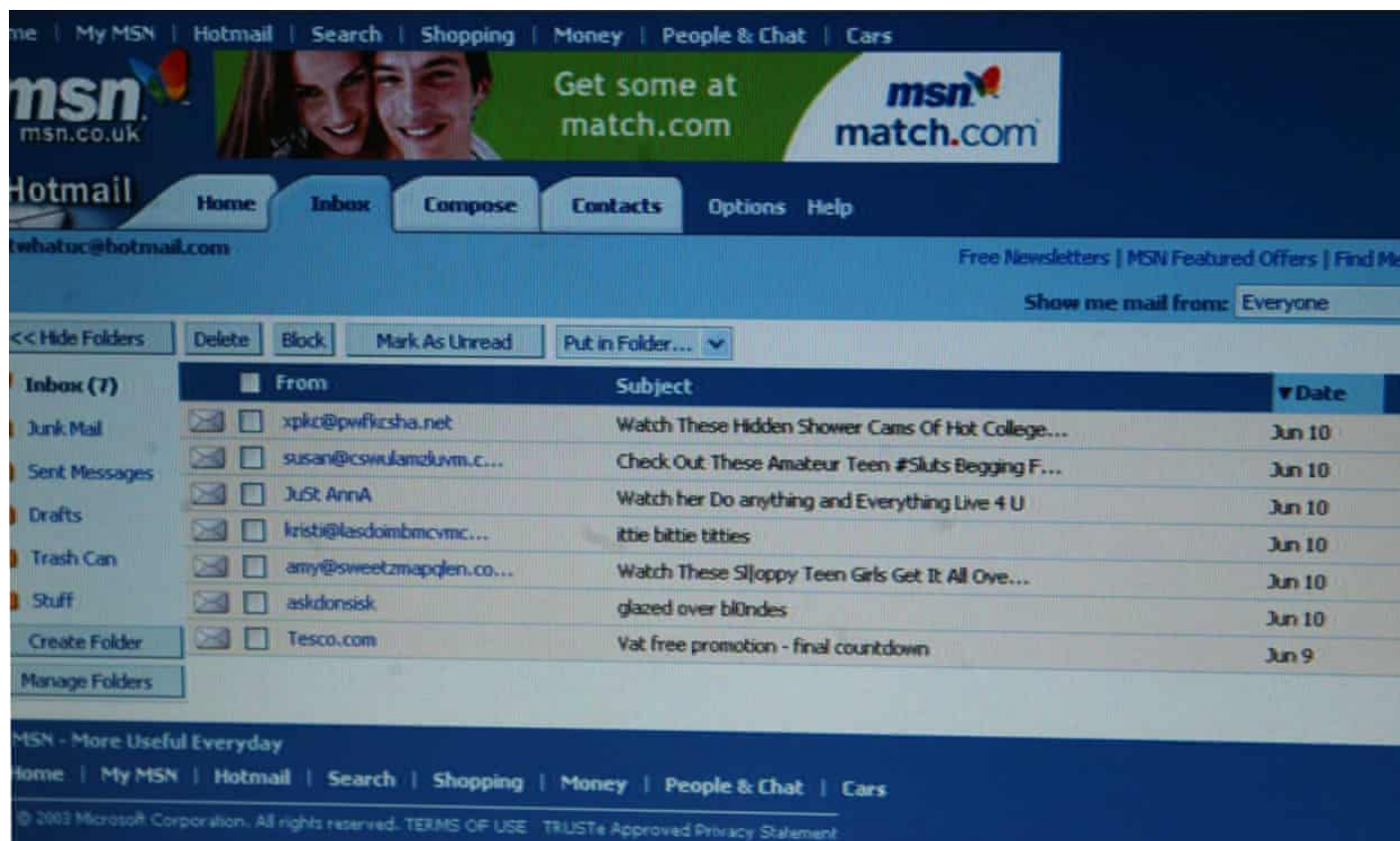
Outlook and Aol - 1993



📷 The iconic AOL CD that cluttered homes for years. Photograph: David Sillitoe/The Guardian

The first version of Microsoft's Outlook was released in 1993 as part of Exchange Server 5.5, while at the same time US internet service providers [AOL](#) and Delphi connected their email systems, paving the way for modern, overloaded email systems we struggle with today.

Hotmail launches - 1996

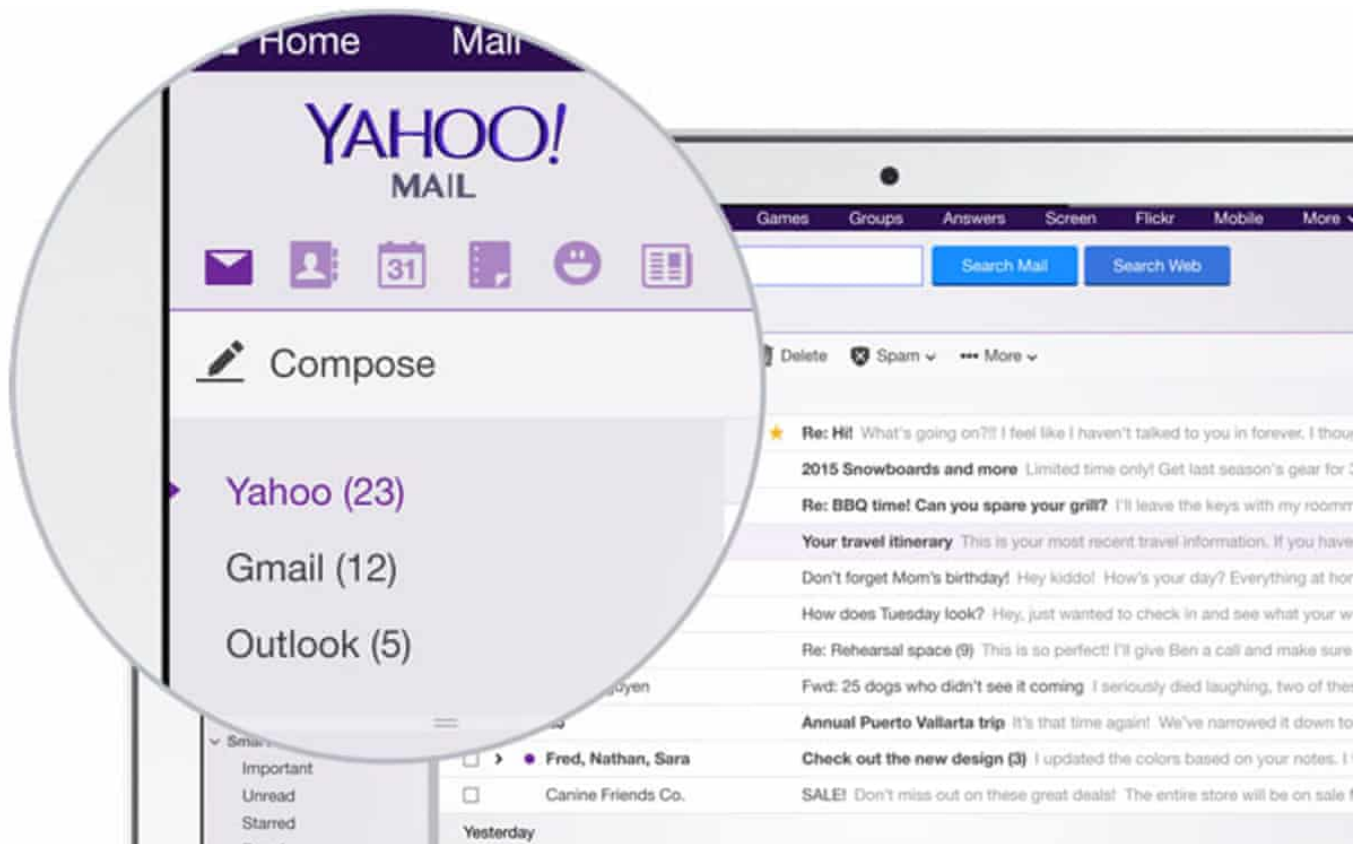


Microsoft's Hotmail was one of the first popular, ISP-agnostic web-based email services. Photograph: Sean Smith/The Guardian

Before Microsoft bought it for \$400m, 1996 saw the launch of one of the first popular webmail email services called HoTMaiL developed by Sabeer Bhatia and Jack Smith. It was one of the first email services not tied to a particular ISP and adopted new HTML-based email formatting - hence the styling of the brand name.

It was bought by Microsoft in 1997, rebranded MSN Hotmail, then Windows Live Hotmail and replaced by Outlook.com in 2013.

Yahoo Mail follows - 1997



📷 Yahoo Mail has been through several revamps in its 9-year history. Photograph: Yahoo

Yahoo Mail was launched the year after Hotmail, which was gaining users by the thousands, and was based on internet company Four11's Rocketmail, which was bought as part of Yahoo's acquisition of the company.

You've Got Mail, and so has everyone else - 1998



📷 Still from the romantic comedy film *You've Got Mail*, starring Tom Hanks and Meg Ryan. Photograph: Warner Bros

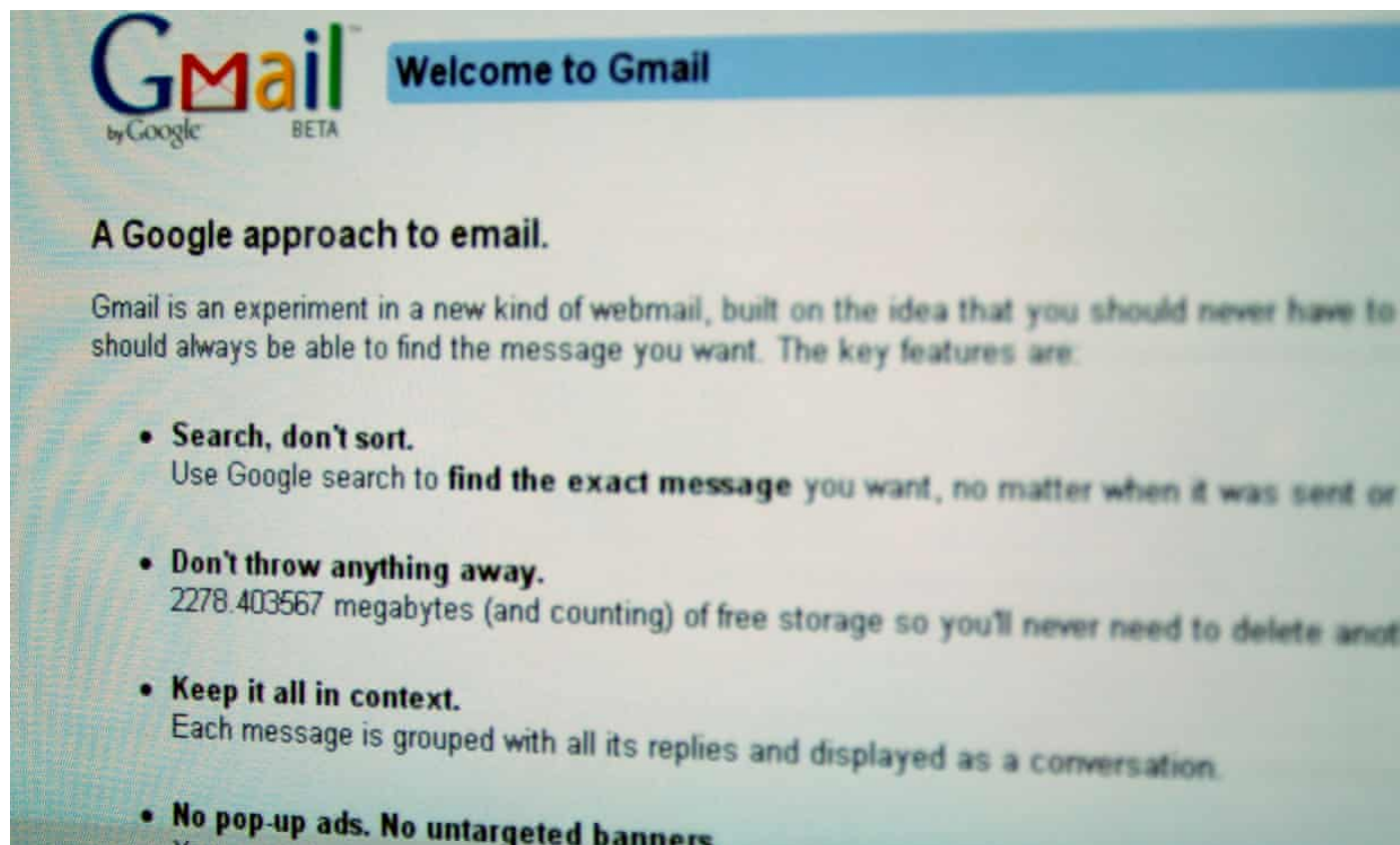
Email was cemented in the public consciousness with the notorious “you’ve got mail” sound of email arriving for AOL users, which formed the cornerstone of the 1998 Tom Hanks and Meg Ryan romantic comedy, [You’ve Got Mail](#).

By the late 1990s spam was becoming a real problem - inducted to the Oxford English Dictionary in 1998 - as more and more marketers jumped on the practically zero-cost outreach proposition and inundated our inboxes.

In 2002, the European Union released its Directive on Privacy and Electronic Communications, which included a section on spam that made it illegal to send unsolicited communications for direct marketing purposes without prior consent of the recipient.

The US passed similar laws in 2004, although neither have been particularly effective at reducing the load.

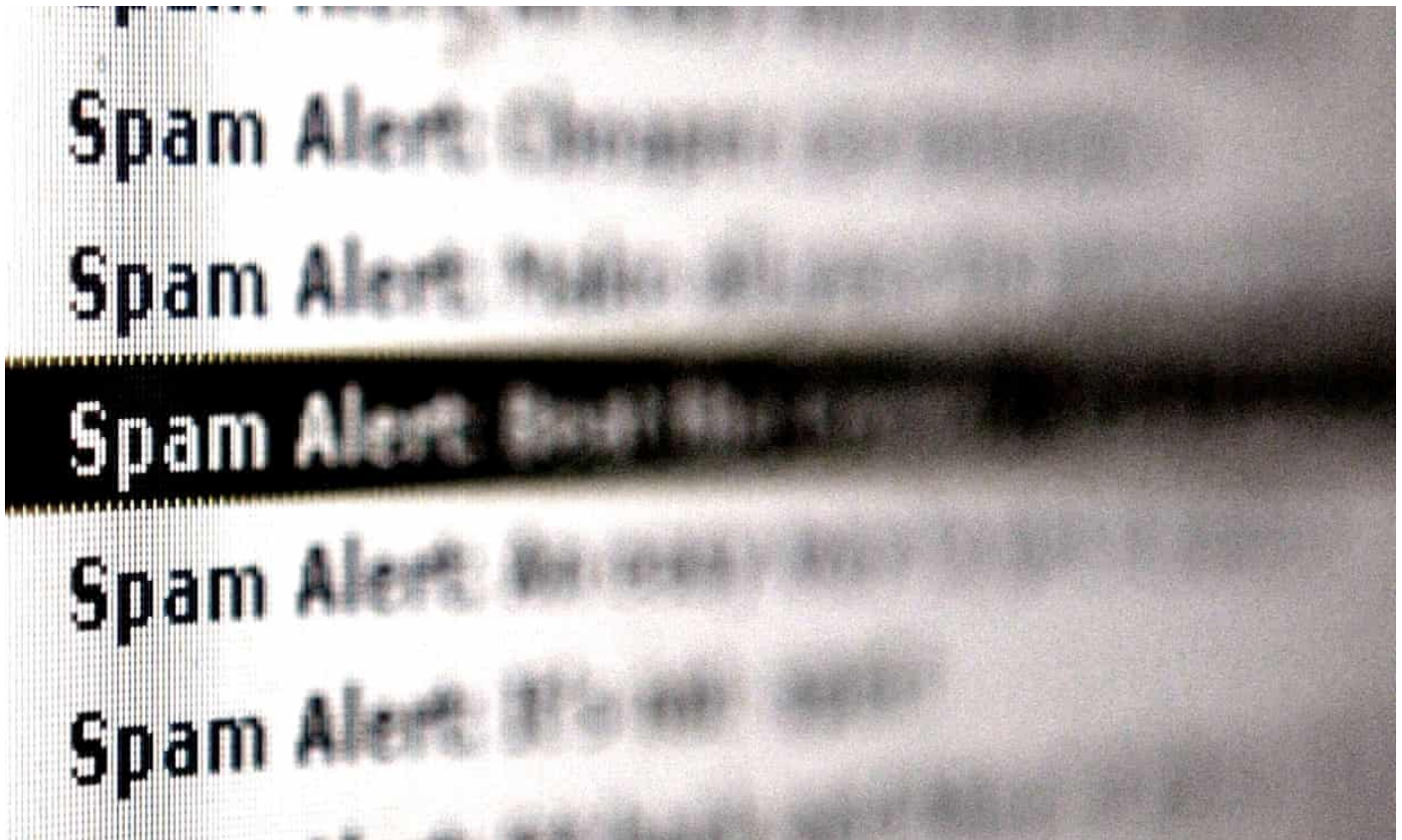
Gmail launches - 2004



📷 Gmail, or Googlemail as it was once known in the olden days. Photograph: Dean Murray / Rex Features

Google's popular email service, [Gmail](#), started life as an internal mail system for Google employees, developed by Paul Buchheit in 2001. It wasn't unveiled to the public until a limited, invite-only beta release in 2004. It was made publicly available in 2007 and dropped its "beta" status in 2009.

Fighting back against spam - 2005



📷 Email protocols started fighting back against spam in the early 2000s. Photograph: Ian Waldie/Getty Images

The first email standard to attempt to fight the deluge of spam by verifying senders was published after a five-year development. Sender Policy Framework was then implemented by a variety of anti-spam programs. A standard of authentication to attempt to prevent email spoofing and phishing was also released called DomainKeys Identified Mail (DKIM).

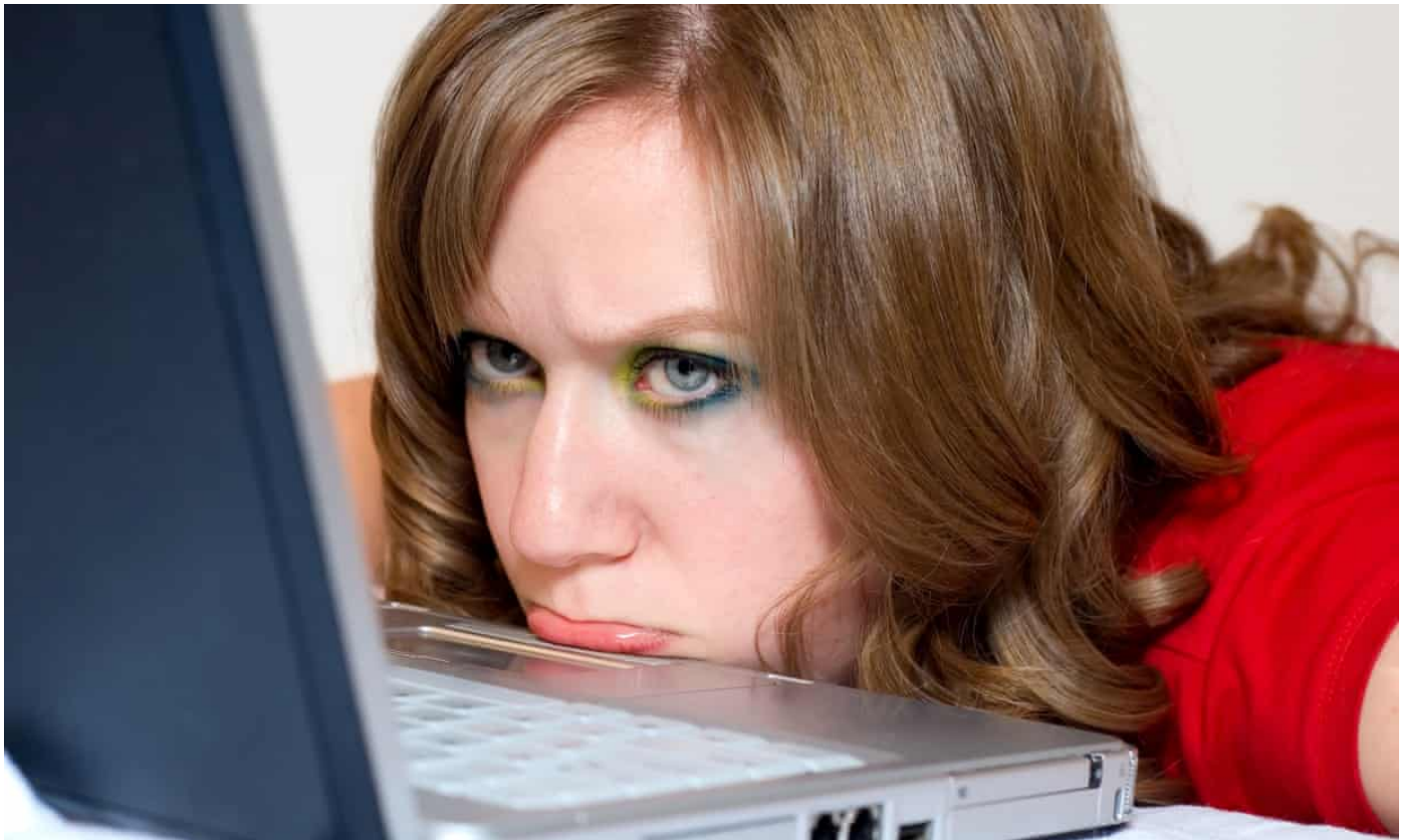
Email goes mobile for casual users - 2007



📷 Little did Steve Jobs know that the Mail icon on the iPhone would forever show thousands unread.
Photograph: Paul Sakuma/AP

Apple's first iPhone was released in 2007, which began to introduce mobile email to the consumer masses. Until that point pre-capacitive consumer smartphones typically had limited email support, while RIM's [BlackBerry](#) had brought the burden of work email to employee palms starting in 2003.

Buried in email - 2015



📷 Buried in email. Photograph: LifeStyleKB / Alamy/Alamy

From humble internal communications beginnings, email now dominates a vast proportion of everyday life. An estimated 4.4bn email addresses are in use worldwide with 205bn emails sent per day in 2015, according to data from market research firm Radicati Group.

That number is set to increase to over 246bn emails a day by the end of 2019.

What was the best (and worst) email you ever received?

12 things today's gamers don't remember about old games

Alexander Shalom (021162004)
AMERICAN CIVIL LIBERTIES UNION
OF NEW JERSEY FOUNDATION
570 Broad Street, 11th Fl.
Post Office Box 32159
Newark, NJ 07102

SUPERIOR COURT OF NEW JERSEY, APPELLATE DIVISION

STATE OF NEW JERSEY,	: Criminal Action
<i>Plaintiff,</i>	: No. A-000193-22T4
	:
v.	: Superior Court of New Jersey,
	: Appellate Division
ZAK A. MISSAK	:
<i>Defendant.</i>	: Trial No. SOM-21-000879
	:
	: Sat Below:
	: Hon. Peter J. Tober, J.S.C.

**BRIEF OF AMICI CURIAE AMERICAN CIVIL LIBERTIES UNION &
AMERICAN CIVIL LIBERTIES UNION OF NEW JERSEY**

Alexander Shalom (021162004)
Jeanne LoCicero (024052000)
AMERICAN CIVIL LIBERTIES UNION
OF NEW JERSEY FOUNDATION
570 Broad Street, 11th Fl.
Post Office Box 32159
Newark, NJ 07102
Tel: (973) 854-1714
ashalom@aclu-nj.org
jlocicero@aclu-nj.org

Jennifer Stisa Granick*
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
39 Drumm Street
San Francisco, CA 94111
Tel: (415) 343-0758
jgranick@aclu.org
* *Pro hac vice* pending
Attorneys for Amici Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES	ii
INTERESTS OF AMICI CURIAE	1
FACTUAL BACKGROUND	2
PRELIMINARY STATEMENT	4
ARGUMENT	7
I. CELL PHONES CONTAIN AN IMMENSE AMOUNT OF PRIVATE, SENSITIVE DATA.....	7
II. WARRANTS MUST SPECIFICALLY LIMIT LAW ENFORCEMENT SEARCHES.	11
A. Warrants should limit digital searches by time frame.....	13
B. Warrants should limit digital searches by the substance and type of data sought.	15
III. THE CONCERN THAT SOPHISTICATED ACTORS COULD POTENTIALLY HIDE EVIDENCE ON CELL PHONES DOES NOT SUPPORT A WARRANT FOR “ALL CONTENT” BECAUSE IT IS DIFFICULT TO HIDE DATA ON CELL PHONES FROM TODAY’S FORENSIC TOOLS.	18
IV. USE RESTRICTIONS, WHILE ESSENTIAL, ARE NOT ENOUGH ON THEIR OWN TO SHIELD PRIVATE AND SENSITIVE DIGITAL DATA.	24
CONCLUSION	25
APPENDIX OF AMICI CURIAE	Aai

TABLE OF AUTHORITIES

Cases

<i>Burns v. United States</i> , 235 A.3d 758 (D.C. Cir. 2020)	16
<i>Carpenter v. United States</i> , 138 S. Ct. 2206 (2018)	1
<i>Commonwealth v. Snow</i> , 160 N.E.3d 277 (Mass. 2021)	13
<i>Demaree v. Pederson</i> , 887 F.3d 870 (9th Cir. 2018)	12
<i>Florida v. Jimeno</i> , 500 U.S. 248 (1991)	11
<i>In re [REDACTED]@gmail.com</i> , 62 F. Supp. 3d 1100 (N.D. Cal. 2014)	13
<i>In re Search of Black iPhone 4</i> , 27 F. Supp. 3d 74 (D.D.C. 2014)	17
<i>In re Search of Google Email Accounts identified in Attachment A</i> , 92 F. Supp. 3d 944 (D. Alaska 2015)	13
<i>In re Search of Info. Associated with Email Addresses Stored at Premises Controlled by Microsoft Corp.</i> , 212 F. Supp. 3d 1023 (D. Kan. 2016)	15
<i>In re United States of America’s Application for a Search Warrant to Seize and Search Elec. Devices from Edward Cunnius</i> , 770 F. Supp. 2d 1138 (W.D. Wash. 2011)	16
<i>Marron v. United States</i> , 275 U.S. 192 (1927)	20
<i>Marron v. United States</i> , 275 U.S. 192 (1927)	12
<i>Maryland v. Garrison</i> , 480 U.S. 79 (1987)	12
<i>People v. Herrera</i> , 357 P.3d 1227 (Colo. 2015)	17
<i>People v. Hughes</i> , 958 N.W.2d 98 (Mich. 2020)	1

<i>People v. Musha</i> , 131 N.Y.S.3d 514 (N.Y. Sup. Ct. 2020)	16
<i>People v. Thompson</i> , 178 A.D.3d 457 (N.Y. App. Div. 2019)	13
<i>Riley v. California</i> , 573 U.S. 373 (2014)	passim
<i>State v. Bock</i> , 485 P.3d 931 (Or. Ct. App. 2021)	16
<i>State v. Earls</i> , 214 N.J. 564 (2013)	1, 10
<i>State v. Lunsford</i> , 226 N.J. 129 (2016)	1
<i>State v. Marshall</i> , 199 N.J. 602 (2010)	20
<i>State v. McLawhorn</i> , 636 S.W.3d 210 (Tenn. Crim. App. 2020)	16
<i>State v. Mefford</i> , 517 P.3d 210 (Mont. 2022)	11
<i>State v. Reid</i> , 194 N.J. 386 (2008)	1
<i>Taylor v. State</i> , 260 A.3d 602 (Del. 2021)	16
<i>United States v. Abboud</i> , 438 F.3d 554 (6th Cir. 2006)	13
<i>United States v. Comprehensive Drug Testing, Inc.</i> , 621 F.3d 1162 (9th Cir. 2010)	12
<i>United States v. Diaz</i> , 841 F.2d 1 (1st Cir. 1988)	13
<i>United States v. Galpin</i> , 720 F.3d 436 (2d Cir. 2013)	12
<i>United States v. Ganius</i> , 824 F.3d 199 (2d Cir. 2016)	1
<i>United States v. Hasbajrami</i> , 945 F.3d 641 (2d Cir. 2019)	1

<i>United States v. Hill</i> , 459 F.3d 966 (9th Cir. 2006)	20
<i>United States v. Holcomb</i> , No. CR21-75-RSL, 2022 WL 1539322 (W.D. Wash. May 16, 2022)	14
<i>United States v. Otero</i> , 563 F.3d 1127 (10th Cir. 2009)	12
<i>United States v. Warshak</i> , 631 F.3d 266 (6th Cir. 2010)	1
<i>United States v. Zemlyansky</i> , 945 F. Supp. 2d 438 (S.D.N.Y. 2013)	14
<i>Walter v. United States</i> , 447 U.S. 649 (1980)	11
Statutes	
N.J.S.A. 2C:13- 6A	2
N.J.S.A. 2C:14-2C(4)	2
N.J.S.A. 2C:5-1A(1)	2
Other Authorities	
AccessData, <i>Forensic Toolkit (FTK) User Guide</i> (Apr. 3, 2017)	22
Andrew D. Huynh, <i>What Comes After Get a Warrant: Balancing Particularity and Practicality in Mobile Device Search Warrants Post-Riley</i> , 101 Cornell L. Rev. 187 (2015)	18
App Annie, <i>The State of Mobile 2021</i> (2021)	8
Apple, <i>iPhone 12</i>	8
Brief of Upturn Inc. as Amicus Curiae, <i>State v. Smith</i> , 278 A.3d 481 (Conn. 2022) (No. SC 20600)	18, 19, 22
Diane Thieke, <i>Smartphone Statistics: For Most Users, It's a 'Round-the-Clock' Connection</i> , ReportLinker (Jan. 26, 2017)	8
Geoffrey A. Fowler & Heather Kelly, <i>Amazon's New Health Band Is the Most Invasive Tech We've Ever Tested</i> , Wash. Post (Dec. 10, 2020)	9
Grindr, <i>About Grindr</i>	10
John Koetsier, <i>We've Spent 1.6 Trillion Hours on Mobile So Far in 2020</i> , Forbes (Aug. 17, 2020)	7

Justin McCarthy, <i>One in Five U.S. Adults Use Health Apps, Wearable Trackers</i> , Gallup (Dec. 11, 2019).....	9
Kinkoo, <i>Kinkoo</i>	10
Laurent Sacharoff, <i>The Fourth Amendment Inventory as a Check on Digital Searches</i> , 105 Iowa L. Rev. 1643 (2020)	19
Logan Koepke et al., <i>Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones</i> , Upturn (Oct. 21, 2020)	21
Microsoft, <i>Search for eDiscovery Activities in the Audit Log</i> , Microsoft Docs (Jan. 7, 2022)	23
Mitch Strohm, <i>Digital Banking Survey: 76% of Americans Bank Via Mobile App—Here Are the Most and Least Valuable Features</i> , Forbes (Feb. 24, 2021)	10
Orin S. Kerr, <i>Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data</i> , 48 Tex. Tech. L. Rev. 1 (2015)	24
Paulette Keheley, <i>How Many Pages in a Gigabyte? A Litigator’s Guide</i> , Digital War Room (Apr. 2, 2020).....	8
Pew Rsch. Ctr., <i>Mobile Fact Sheet</i> (Apr. 7, 2021).....	7
Sarah Silbert, <i>All the Things You Can Track with Wearables</i> , Lifewire (Dec. 2, 2020)	9
Sudip Bhattacharya et al., <i>NOMOPHOBIA: NO Mobile Phone PhoBIA</i> , 8 J. Fam. Med. Primary Care 1297 (2019)	8

INTERESTS OF AMICI CURIAE

The American Civil Liberties Union (“ACLU”) is a nationwide, nonprofit, nonpartisan organization dedicated to the principles of liberty and equality embodied in the Constitution and our nation’s civil rights laws. The American Civil Liberties Union of New Jersey (“ACLU-NJ”) is the New Jersey state affiliate of the national ACLU.

Since its founding in 1920, the ACLU has frequently appeared before the Supreme Court and other state and federal courts in numerous cases implicating Americans’ right to privacy in the digital age, including as counsel in *Carpenter v. United States*, 138 S. Ct. 2206 (2018) and as amicus in *People v. Hughes*, 958 N.W.2d 98 (Mich. 2020), *United States v. Ganius*, 824 F.3d 199 (2d Cir. 2016) (en banc), *United States v. Hasbajrami*, 945 F.3d 641 (2d Cir. 2019), and *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010).

The ACLU-NJ has appeared frequently before this Court and the New Jersey Supreme Court advocating for the rights to privacy and free speech in digital media and the right to privacy generally under the Fourth Amendment to the U.S. Constitution and Article I, paragraph 7 of the New Jersey Constitution. *See, e.g., State v. Lunsford*, 226 N.J. 129 (2016) (telephone billing and toll records); *State v. Earls*, 214 N.J. 564 (2013) (cell phone location data); *State v. Reid*, 194 N.J. 386 (2008) (Internet service provider subscription information).

FACTUAL BACKGROUND

Department of Homeland Security agent Laura Hurley was online posing undercover as an underage child. Defendant Zak A. Missak allegedly contacted Hurley and the two exchanged texts and online messages. Missak subsequently drove to a location, allegedly in an attempt to meet the “child” in person. When he arrived, he was arrested. He had an Apple iPhone 12 Pro Max with him, which officers seized.

The State then filed applications for warrants to search Missak’s vehicle and the phone for evidence of the crimes of luring in violation of N.J.S.A. 2C:13-6A and attempted sexual assault in violation of N.J.S.A. 2C:14-2C(4) and N.J.S.A. 2C:5-1A(1). The affidavit related the details of the investigation and requested the “ability and opportunity to access all information contained within the [phone].” (Pa30–Pa31).

A judge issued a search warrant for the phone, which purported to authorize law enforcement officers to:

access all information contained within the mobile device(s), including, but not limited to stored electronic data, encrypted or password protected files/data, the assigned cellular number, cellular billing number, address book/contact(s) information, all recent calls, to include dialed, received, missed, erased calls, duration of said calls, any Internet access information, incoming and outgoing text messages, text message content, any stored pictures, stored video, calendar information, Global Positioning System (GPS) data, memory or Secure Digital Memory cards (SD cards) and and any

other stored information on said mobile device that will assist in the continuation of this investigation.

(Pa31). The State says it has not yet searched the phone because it first needs Missak to provide his passcode in order to enable investigators to access to the phone data.

Missak moved to quash the warrant. The trial court held that there is a legal presumption that issued warrants are valid, and that, given this presumption, there was sufficient cause to issue the search warrant based on evidence that Missak was in possession of the phone when he texted the undercover officer. (Pa15–Pa16).

Missak also argued that there was no probable cause to search all the data on the phone. Rather, a constitutional warrant must focus on specific, relevant files such as the communications and apps that the State alleges formed the basis of probable cause for the specified crimes. (Pa9). Although the State knows the exact dates and times of the purported communications in which it is interested, the warrant contains no temporal limitations whatsoever.

Characterizing Missak’s argument as a particularity challenge, the court held that the warrant was sufficiently particular. (Pa15). The court concluded that the affidavit in support of the warrant describes why that information can be searched, highlighting the fact that mobile phones can store thousands of pages of information, and that a suspect—though not Missak in particular—may

try to conceal evidence in a “random order” or “with deceptive file names.” (Pa17). Therefore, the court reasoned, authorities may need to examine all the stored data to determine which particular files are evidence or instruments of crimes. (Pa17). The court stated that a narrower warrant could mean that police will not recover hidden or manipulated data, and that the court could address any violation of Missak’s rights by limiting the introduction of “irrelevant or highly prejudicial evidence” at trial. (Pa18).

This Court granted review. *See* Order on Mot. No. M-007129-21, *State v. Missak*, No. AM-000754-21T4 (N.J. Ct. App. Sept. 20, 2022).

PRELIMINARY STATEMENT

Every day, law enforcement agents obtain and execute search warrants for digital materials stored on desktop computers, laptops, and cell phones. The information stored on these devices is vast, diverse, and far more sensitive than information stored in a filing cabinet, or even an entire home. *See Riley v. California*, 573 U.S. 373 (2014).

These characteristics make it all the more important that warrants for cell phone searches closely adhere to Fourth Amendment requirements, lest authority to search a device for evidence of one crime mutate into authority to search the entirety of the device for evidence of any crime—a prohibited general search. Like other searches, electronic device searches must be particularized—that is, cabined by time

frame and limited to files and folders for which the affidavit in support of the warrant provides probable cause. A contrary rule would give investigating officers a free hand to examine any and all files on a mobile device, merely because some files may be subject to search. That would upend the longstanding constitutional baseline rule that searches must be particularized and cannot constitute generalized rummaging through personal and private materials.

The trial court underestimated the amount of data on our mobile devices. It is closer to tens of millions than thousands of pages. The court then took the wrong lesson from the extensive amount of data on cell phones. Far from supporting an all-encompassing search through vast troves of private data, the sheer volume of data on our digital devices means that it is all the more important that warrants carefully steer investigators only towards evidence of the crime under investigation. The mere possibility that evidence *might* be manipulated, by a sophisticated actor, is not a justification to do otherwise—particularly absent any specific evidence that the suspect in the case is capable of doing so. Mobile device data is not nearly as easily altered as the court presumed. Furthermore, today’s powerful forensic tools are capable of identifying, classifying, and aggregating information regardless of order, file name, or other obfuscating techniques. Modern forensic tools are designed to identify relevant data even if it is housed in unexpected places, whether innocently or due to an intentional effort to conceal its whereabouts. Deployment of these

forensic capabilities reduces or even eliminates the purported need to search digital files indiscriminately in order to uncover hidden evidence.

Moreover, the trial court's resolution of Missak's motion to quash the State's warrant should not have relied upon the availability of potential evidentiary rulings that might later limit the introduction of "irrelevant" or "highly prejudicial" information found during an overbroad search. (Pa18). Such routine evidentiary rulings neither remedy constitutional violations nor address concerns underlying the Fourth Amendment's and Article I, paragraph 7's prohibition on general searches. They would not prevent law enforcement from rummaging through private data for which there is no probable cause, nor from searching for evidence of offenses for which there is no probable cause. Nor would they prevent law enforcement from unnecessarily intruding into the private matters of innocent people who happened to have communicated with Missak.

Amici urge the Court to adopt a rule, based in the foundational principles of the Fourth Amendment, that search warrants for cell phone data must be limited to the categories of data that are likely to contain evidence of the crime, and to the relevant time frame of the investigation. This would ensure that a search is narrowly tailored to capture only relevant data supported by probable cause, wherever it may be stored. That potential evidence exists in digital form does not justify departure

from the time-tested guardrails imposed by the Fourth Amendment on law enforcement's efforts to search a person's private papers, effects, and property.

ARGUMENT

I. CELL PHONES CONTAIN AN IMMENSE AMOUNT OF PRIVATE, SENSITIVE DATA.

Smartphones are ubiquitous, highly portable devices that “place vast quantities of personal information literally in the hands of individuals.” *Riley*, 573 U.S. at 386. Americans use their phones for a wide variety of purposes and, as a result, smartphones contain a voluminous and varied collection of data. While data is often organized by application or file type, even discrete categories of information—alone or in combination with each other—comprise a “digital record of nearly every aspect of [our] lives.” *Id.* at 375.

Cell phone use is now deeply entrenched in the fabric of daily life. Ninety-seven percent of Americans own a cell phone and eighty-five percent own a smartphone specifically.¹ These devices are “such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude that they were an important feature of the human anatomy.” *Riley*, 573 U.S. at 385. Mobile devices have become the screen that people access first and most often.² Nearly half of

¹ Pew Rsch. Ctr., *Mobile Fact Sheet*, Apr. 7, 2021 (attached at Amicus Appendix (hereafter, “Aa”) 161).

² John Koetsier, *We've Spent 1.6 Trillion Hours on Mobile So Far in 2020*, *Forbes*, Aug. 17, 2020 (Aa136).

Americans check their smartphones as soon as they wake up in the morning.³ People proceed to spend an average of four hours a day using various apps on their phones.⁴ Cell phone use is so persistent that the medical field has adopted a term to describe the intense anxiety many people experience when they fear being separated from their cell phones: *NOMOPHOBIA: NO MOBILE PHONE PHOBIA*.⁵

Americans' dependency on smartphones has, both intentionally and inadvertently, resulted in our phones containing vast troves of our personal information. The least expensive iPhone 12 offers 64GB of data storage, and more expensive versions can store four times that.⁶ By some estimates, a gigabyte is roughly 678,000 pages of text,⁷ meaning that the trial court underestimated the ratio of private matters to potential evidence approximately by a factor of forty-three thousand.

Indeed, cell phones “differ in both a quantitative and a qualitative sense” from other objects because of “all [the personal information] they contain and all they may reveal.” *Riley*, 573 U.S. at 393, 403. The “immense storage capacity” of

³ Diane Thieke, *Smartphone Statistics: For Most Users, It's a 'Round-the-Clock' Connection*, ReportLinker, Jan. 26, 2017 (Aa183).

⁴ App Annie, *The State of Mobile 2021* 7 (2021) (Aa15).

⁵ Sudip Bhattacharya et al., *NOMOPHOBIA: NO Mobile Phone PhoBIA*, 8 J. Fam. Med. Primary Care 1297 (2019) (Aa33).

⁶ Apple, *iPhone 12* (Aa17).

⁷ Paulette Keheley, *How Many Pages in a Gigabyte? A Litigator's Guide*, Digital War Room, Apr. 2, 2020 (Aa45).

smartphones allows them to function as “cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers,” and to store extensive historical information related to each functionality. *Id.* at 393. Because a cell phone “collects in one place many distinct types of information”—for example, an address, a note, a prescription, a bank statement, or a video—cell phone data “reveal[s] much more in combination than any isolated record,” *id.* at 394, and they reveal much more about “an individual’s private interests or concerns,” *id.* at 395.

The broad range of applications available to cell phone users and the ever-increasing storage capacity of new-generation devices mean that digital searches today implicate more data than ever before. For instance, one in five Americans currently use health-related smartphone apps—sometimes linked to wearable devices—to track information related to their location, movement and sleep patterns, heart rate, nutrition, menstrual cycles, and other sensitive health data.⁸ Other apps might monitor home security cameras, facilitate dating (and thereby reveal the user’s sexual orientation and predilections), track a household’s

⁸ Justin McCarthy, *One in Five U.S. Adults Use Health Apps, Wearable Trackers*, Gallup, Dec. 11, 2019 (Aa141); Sarah Silbert, *All the Things You Can Track with Wearables*, Lifewire, Dec. 2, 2020 (Aa168); Geoffrey A. Fowler & Heather Kelly, *Amazon’s New Health Band Is the Most Invasive Tech We’ve Ever Tested*, Wash. Post, Dec. 10, 2020 (Aa39).

budget, manage financial accounts, or send encrypted messages.⁹ Coupled with devices' rapidly increasing storage capacities, these apps mean that any given person's cell phone may reveal a comprehensive portrait of their health, their location history, their sexual preferences, their private conversations, their photos, their finances, their social and professional networks, and a myriad of other things from taste in music to political beliefs. In short, cell phones produce "a digital record of nearly every aspect of [users'] lives—from the mundane to the intimate." *Riley*, 573 U.S. at 395. While a single app or type of data can reveal an extraordinary amount about a person, the combination of the many different types of data on a phone can essentially reconstruct a person's life. *See State v. Earls*, 214 N.J. 564, 584–85 (2013) (recognizing that the vast amount of private information available through ISP subscriber information, bank records, and phone records can "reveal the most intimate details of a person's life" "provid[ing] a virtual current biography" and additionally protecting privacy interests in cell phone location data (citations omitted)).

⁹ *See, e.g.*, Blink, *Blink Home Monitor App* (Aa37); Grindr, *About Grindr* (Aa44); Kinkoo, *Kinkoo* (Aa50); Mitch Strohm, *Digital Banking Survey: 76% of Americans Bank Via Mobile App—Here Are the Most and Least Valuable Features*, *Forbes*, Feb. 24, 2021 (Aa175); Mary Meeker, *Internet Trends 2019*, Bond Capital, June 11, 2019 (Aa151); Jack Nicas, Mike Isaac & Shira Frenkel, *Millions Flock to Telegram and Signal as Fears Grow Over Big Tech*, *N.Y. Times*, Jan. 13, 2021 (Aa158).

Here, the warrant is not limited in any way. It purports to allow a search of any and all information on the phone, the broadest possible exploration of years and years of Mr. Missak’s life.

II. WARRANTS MUST SPECIFICALLY LIMIT LAW ENFORCEMENT SEARCHES.

Under the Fourth Amendment, it is axiomatic that officers must have probable cause to support the search of a cell phone. *See Riley*, 573 U.S. 373. Further, probable cause to search or seize *some* data on the phone cannot justify access to the totality of the phone’s contents. “When an official search is properly authorized . . . the scope of the search is limited by the terms of the authorization.” *Walter v. United States*, 447 U.S. 649, 656–57 (1980); *see also Florida v. Jimeno*, 500 U.S. 248, 251 (1991) (“The scope of a search is generally defined by its expressed object.”); *accord State v. Mefford*, 517 P.3d 210, 218 (Mont. 2022). Instead, warrants must provide sufficiently particular instructions and avoid giving law enforcement license to search an overly broad swath of information. By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the particularity requirement “ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit.” *Maryland v. Garrison*, 480 U.S. 79, 85 (1987); *see also Marron v. United States*, 275 U.S. 192, 196 (1927) (“The requirement that warrants shall particularly describe the things to be seized makes

general searches under them impossible and prevents the seizure of one thing under a warrant describing another.”).

Given the vast amounts of personal data stored on phones, and all that can be gleaned from that data, strict limits on digital searches and seizures are crucial to preserve privacy. *See, e.g., United States v. Galpin*, 720 F.3d 436, 447 (2d Cir. 2013) (discussing the need for “heightened sensitivity to the particularity requirement in the context of digital searches” due to the vast amount of information that digital devices contain).

Failure to use available time frames to cabin a warrant—as this warrant failed to do—means that the court order will either be overbroad, in that it unreasonably authorizes access to data for which there is no probable cause, or insufficiently particular, in that it fails to guide officers towards relevant evidence and away from unspecified rummaging. *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1176 (9th Cir. 2010) (en banc) (per curiam) (discussing the “serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant”), *overruled in part on other grounds by Demaree v. Pederson*, 887 F.3d 870 (9th Cir. 2018); *United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir. 2009) (ability of a computer to store “a huge array” of information “makes the particularity requirement that much more important”).

As explained below, warrants should limit searches based not only on the information sought, but also on time frame and file type—especially when authorizing searches of sensitive data commonly stored on cell phones.

A. Warrants should limit digital searches by time frame.

Commonly, a warrant can define relevant electronic data subject to search with a limited date range. If possible, it must do so. *See United States v. Abboud*, 438 F.3d 554, 576 (6th Cir. 2006) (“Failure to limit broad descriptive terms by relevant dates, when such dates are available to the police, will render a warrant overbroad.” (citation omitted)); *United States v. Diaz*, 841 F.2d 1, 4–5 (1st Cir. 1988) (warrant overbroad when authorized seizure of records before the first instance of wrongdoing mentioned in the affidavit); *In re [REDACTED]@gmail.com*, 62 F. Supp. 3d 1100, 1104 (N.D. Cal. 2014) (no warrant issued where government did not include a date limitation); *In re Search of Google Email Accounts Identified in Attachment A*, 92 F. Supp. 3d 944 (D. Alaska 2015) (application without date restriction denied as overbroad); *see also People v. Thompson*, 178 A.D.3d 457, 458 (N.Y. App. Div. 2019) (warrant to search defendant’s phones without a time limitation did not satisfy the Fourth Amendment’s particularity requirement); *Commonwealth v. Snow*, 160 N.E.3d 277 (Mass. 2021) (cell phone search warrant presumptively must contain some temporal limit); *United States v. Holcomb*, No. CR21-75-RSL, 2022 WL 1539322, at *6 (W.D. Wash. May 16, 2022) (“Because

law enforcement was aware of the time frame [relevant to the suspected crime], but the [relevant warrant] clause was nonetheless temporally unlimited, [the warrant] lacked particularity.”), *rev'd on other grounds*, 2022 WL 16763686 (W.D. Wash. Nov. 8, 2022).

Time-frame–cabined warrants guard against searches for evidence of past, unrelated crimes as well as against broad searches of innocent and private information based on probable cause for minor crimes. *Riley*, 573 U.S. at 399 (warrant necessary for this purpose). The proper date range should be set forth in the warrant, and not left to the officer’s discretion. “A warrant’s failure to include a time limitation, where such limiting information is available and the warrant is otherwise wide-ranging, may render it insufficiently particular.” *United States v. Zemlyansky*, 945 F. Supp. 2d 438, 459 (S.D.N.Y. 2013) (cleaned up) (finding that the absence of a temporal limit on items to be searched “reinforces the Court’s conclusion that the [] warrant functioned as a general warrant”).

Thus, courts have held that under the Fourth Amendment’s particularity requirement, law enforcement may need to use date-range restrictions or other limitations to prevent the potential for “general rummaging” when searching electronically stored information such as email accounts. *See, e.g., In re Search of Info. Associated with Email Addresses Stored at Premises Controlled by Microsoft*

Corp., 212 F. Supp. 3d 1023, 1037 (D. Kan. 2016) (a warrant must “include[] some limitations (such as a date range) to prevent the potential of a general search”).

Here, the State knew the dates of the criminal activity it was investigating—from December 8, 2021, until Missak’s arrest on December 9. The warrant needed to include that date range to be constitutional.

B. Warrants should limit digital searches by the substance and type of data sought.

Warrants can limit searches for electronic evidence by file type as well as by time frame without unduly interfering with law enforcement investigations. If there is probable cause to believe that co-conspirators texted each other, there is no reason for law enforcement to search photos. If investigators learn that suspicious texts attach photos, then the search can expand to those (and related) photos—either pursuant to a second warrant, or under the first warrant, as overseen by the issuing judge. These and similar guardrails are reasonable given the dangers of overbroad searches through personal and sensitive information.

The U.S. Supreme Court has endorsed this approach. *Riley* explicitly discussed the invasiveness of law enforcement access to different “categories,” “areas,” “types” of data, and “apps.” 573 U.S. at 395, 396, 399. The Court also pointed out that “certain types of data are also qualitatively different” from others in terms of privacy. *Id.* at 395.

With increasing frequency, courts have followed *Riley* to hold that looking at the right categories of data, not all data, is the only plan that makes sense and complies with the Constitution. *See, e.g., State v. Bock*, 485 P.3d 931, 936 (Or. Ct. App. 2021) (warrants may not authorize searches through any and all contents of electronic files that may contain circumstantial evidence about the owner or evidence of identified criminal offenses); *Burns v. United States*, 235 A.3d 758, 775 (D.C. Cir. 2020) (warrant authorizing search for categories of data for which there was no probable cause was “constitutionally intolerable”); *People v. Musha*, 131 N.Y.S.3d 514 (N.Y. Sup. Ct. 2020) (in child abuse case, there was probable cause to search the phone’s photographs, but not to examine Web search history); *State v. McLawhorn*, 636 S.W.3d 210, 239–44 (Tenn. Crim. App. 2020) (officers cannot search entirety of phone to determine whether device has flashlight function); *Taylor v. State*, 260 A.3d 602 (Del. 2021) (warrant permitting search and seizure of “any/all data stored by whatever means” failed the Fourth Amendment and state constitutions’ particularity requirements); *In re United States of America’s Application for a Search Warrant to Seize and Search Elec. Devices from Edward Cunnius*, 770 F. Supp. 2d 1138, 1139, 1147–1151 (W.D. Wash. 2011) (application to search and seize “all electronically stored information . . . contained in any digital devices seized from [defendant’s] residence for evidence relating to the crimes of copyright infringement or trafficking in counterfeit goods” was improper because it

sought “the broadest warrant possible,” and did not propose to use a search technique that foreclosed the plain view doctrine’s application to digital materials). As these cases demonstrate, even when there is probable cause to search a device for *something*, police may not search *everything*. They may not access or examine file types that are not connected to the probable cause.

Critically, the warrant must contain both the substance of the sought-after data and its type. For example, in *People v. Herrera*, 357 P.3d 1227 (Colo. 2015), the Colorado Supreme Court suppressed evidence contained in a text message involving a third party not named in the warrant. The court held that the government’s argument that *any* text message folder could be searched because of the abstract possibility that the folder might contain indicia of who owned the phone, or might have been deceptively labeled, would result in an unconstitutional limitless search. *Id.* at 1230, 1233–34. The appropriate search criteria would have identified the relevant file type (text messages) *and* the text conversations relevant to the inquiry (those involving the individuals named in the warrant). These functional limitations can be constitutionally required, as the law is clear that police cannot get a warrant to seize or search categories of data for which there is no probable cause. *See, e.g., In re Search of Black iPhone 4*, 27 F. Supp. 3d 74, 79 (D.D.C. 2014).

Here, the warrant purports to authorize investigators to access *all information*, with no time-frame, category, or file-type limitations that would confine the search to probable cause.

III. THE CONCERN THAT SOPHISTICATED ACTORS COULD POTENTIALLY HIDE EVIDENCE ON CELL PHONES DOES NOT SUPPORT A WARRANT FOR “ALL CONTENT” BECAUSE IT IS DIFFICULT TO HIDE DATA ON CELL PHONES FROM TODAY’S FORENSIC TOOLS.

Like many courts, the trial court invoked a concern that Missak may have altered or hidden evidence as the primary basis for approving of the “all content” warrant in this case. Because digital data on cell phones may be disguised or manipulated, the court reasoned, investigators will not know where evidence will be located—and as a result, investigators must be able to seize and search everything on a cellphone. This is wrong, both factually and legally.

As Upturn, a nonprofit technology policy organization with expertise in cell phone forensic tools, has explained, most modern cell phones do not give users much ability to control how their files are stored or named. *See* Brief of Upturn Inc. as Amicus Curiae, *State v. Smith*, 278 A.3d 481 (Conn. 2022) (No. SC 20600) (Aa196). “Mobile operating systems are designed for ease of use and do not emphasize user-directed file organization.” Andrew D. Huynh, *What Comes After Get a Warrant: Balancing Particularity and Practicality in Mobile Device Search Warrants Post-Riley*, 101 Cornell L. Rev. 187, 207–08 (2015).

“As any iPhone or Android user can tell, users no longer determine where an app stores its files, because users have no direct access to the file directory.”

Laurent Sacharoff, *The Fourth Amendment Inventory as a Check on Digital Searches*, 105 Iowa L. Rev. 1643, 1660 (2020). These features mean that cell phone users are generally not able to directly manipulate their cell phone data.

Today’s forensic tools are far more powerful than the trial court understood, making it trivial for investigators to search and analyze files regardless of where they are stored or how they are named. Again, Upturn explains today’s mobile device forensic tools, or MDFTs:

MDFTs are agnostic toward file organization or file name. . . . MDFTs can simply traverse through all data on a phone and pick out data that has a particular data type, where file type is distinct from the name of a file (which most cellphone users do not control, anyway). As a result, even in the rare instance in which digital data may be disguised or manipulated, MDFTs can surface files based on their actual content, regardless of how a file is named or where it is located. This means that an image file hidden in an unexpected folder and renamed with a misleading file extension can still be discovered.

Brief of Upturn Inc. as Amicus Curiae, *Smith*, 278 A.3d 481 (Aa205).

Relying on a vague possibility that someone might be able to successfully manipulate cell phone data and hide it from investigators would cause the exception to become the rule. Courts should not “allow[] the very rare prospect of the computer mastermind to drive the entire doctrine, rather than taking the most typical user as the prototype.” Sacharoff, *The Fourth Amendment*

Inventory, 105 Iowa L. Rev. at 1658. There may, of course, be cases where the police have a specific reason to believe that cell phone or other data has been manipulated. In these instances, the state may demonstrate “to the magistrate factually why such a broad search and seizure authority is reasonable in the case at hand.” *United States v. Hill*, 459 F.3d 966, 974–75 (9th Cir. 2006).

Ultimately, the reality is that there is far too much information on modern devices for police officers to comprehensively examine. Cell phone searches inherently entail law enforcement picking and choosing what to look at. Given this reality, the Fourth Amendment requires that investigating officers’ exercise of discretion be defined and overseen by a magistrate. *Marron v. United States*, 275 U.S. 192, 196 (1927); *see also State v. Marshall*, 199 N.J. 602, 606–13 (2010) (finding invalid a warrant that permitted police officers to determine—prior to the search but after the warrant had been issued—with which of two apartments the defendant had been associated because the warrant delegated the “role of the neutral and detached magistrate” to police). That means that the warrant must constrain where and how officers search.

Forensic tools are designed for expansive inspection of data. Mobile device forensics typically consists of data extraction, then analysis. MDFTs accelerate data analysis with powerful visualization tools. Search features also help law enforcement quickly navigate extracted data. Investigators can query

this data, and the search tools will display information responsive to key terms—just as one might use Google to search the Web.

Search features include basic keyword searches, as well as more advanced techniques. Upturn’s survey of MDFTs reveals some of these techniques:

Some mobile device forensic tools now use machine learning-based text and image classification to categorize file contents, including individual frames in a video. For instance . . . Cellebrite offers a “search by face” function, whereby law enforcement can compare an image of a face to all other images of faces found on the phone. Cellebrite also allows law enforcement to define new image categories by feeding its software a small set of example images to search for (for example, searching for hotel rooms by giving the software a set of five images of hotel rooms that were taken from Google images). As another example, Magnet Forensics’ AXIOM can employ text classification models in attempts to detect “sexual conversations,” or to filter conversations by topics ranging from family, drugs, money, and police. Tools also allow law enforcement to search for a specific address on a map and view all “location related” events surrounding a point of interest.

Logan Koepke et al., *Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones* 24, Upturn (Oct. 21, 2020) (Aa77).

Moreover, mobile device forensic tools are widely available even to smaller law enforcement agencies, which either purchase them outright, obtain them through federal grants, or work with larger law enforcement agencies that conduct extractions of data at the smaller agencies’ request. *Id.* at 32–39 (Aa85–92).

“At each stage of the mobile device forensic process there are opportunities to narrow the search. MDFTs can limit what information is copied from the phone or can limit what information will be analyzed. MDFT software has built-in pre- and post-extraction filtering and categorization features, all of which can help narrow the search of a cellphone.” Brief of Upturn Inc. as Amicus Curiae, *Smith*, 278 A.3d 481 (Aa203). Investigators can limit and refine their queries using date limitations, file category limitations, keyword searches, and Boolean queries like those lawyers use in a Westlaw search.

These targeted searches—which include date range and file type capabilities—enable investigators to comprehensively home in on the digital evidence relevant to probable cause.¹⁰ They will nevertheless see a vast amount of private data. Like any search technique, forensic search tools can be over- or under-inclusive. And forensic tools can extract more and different types of data than manual searches, and analyze that data far more efficiently than can human reviewers acting alone. Indeed, forensic tools can even reveal information that even the device’s owner does not know is there and, by gathering hidden and deleted files, exacerbate the potential for indiscriminate and overbroad searches.

¹⁰ See, e.g., AccessData, *Forensic Toolkit (FTK) User Guide* 102 (Apr. 3, 2017) (Aa9) (“Refine evidence further by making the addition of evidence items dependent on a date range or file size that you specify. However, once in the case, filters can also be applied to accomplish this.”).

As with manual searches, forensic searches potentially expose substantial amounts of irrelevant and private information to manual review by investigators.

To facilitate oversight, courts should require that police log their searches to ensure that they are targeted and compliant with the warrant. While it is not clear whether all forensic tool manufacturers have a search history feature, civil eDiscovery tools do.¹¹ It is an easy feature to include. With such logs, judges can better understand the precise steps that law enforcement take when searching a cell phone. In particular, these logs can equip judges to better assess the reasonableness of the search technique and ascertain if the search was sufficiently narrowly tailored to the warrant. If courts were to insist upon the production of digital audit logs created by the forensic tool upon the return of a search warrant, tool vendors that do not already provide this functionality would rapidly develop and provide this feature.

In sum, forensic search tools can make searches limited by date and file type workable, while also being effective for law enforcement. Certainly, limiting searches by date and file type will not always be possible. But it often is, and in those situations, this Court should require that warrants indicate, and

¹¹ See, e.g., Microsoft, *Search for eDiscovery Activities in the Audit Log*, Microsoft Docs (Jan. 7, 2022) (Aa152) (“Content search and eDiscovery-related activities . . . are logged in the audit log” when “[c]reating, starting, and editing Content searches,” and “[p]erforming search actions, such as previewing, exporting, and deleting search results,” among other activities.).

officers observe, that limitation, lest searches be unreasonably overbroad and unconstitutional.

IV. USE RESTRICTIONS, WHILE ESSENTIAL, ARE NOT ENOUGH ON THEIR OWN TO SHIELD PRIVATE AND SENSITIVE DIGITAL DATA.

Use restrictions on non-responsive data obtained pursuant to a lawful warrant are an essential Fourth Amendment protection. *See* Orin S. Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 Tex. Tech. L. Rev. 1, 24 (2015) (advocating for use restrictions for data not responsive to the warrant). However, the use restrictions that the trial court anticipated—imposed through the exclusion of “irrelevant or highly prejudicial” information—are far too narrow. (Pa18). Imposing the regular rules of evidence does nothing to disincentivize the undue rummaging that the particularity requirement was enacted to preclude. Moreover, use restrictions cannot transform an unconstitutionally overbroad or insufficiently particular warrant into a valid one.

While suppression is an evidentiary rule, the Fourth Amendment itself is not. The Fourth Amendment protects privacy—whether or not a police investigation results in a criminal trial. When law enforcement’s search of a cell phone exceeds the scope of probable cause, investigators learn intimate information about the individual’s life, *regardless* of whether that data is ultimately excluded at trial. Use restrictions do not protect an individual’s privacy in any instance where that person

is not ultimately charged with a crime. Nor do they protect the people who communicate with a suspect. While it might be acceptable to invade these people's privacy to reasonably investigate a crime, where the police stray too far, there is no compensation for friends, relatives, and business acquaintances whose privacies of life are also revealed.

In sum, use restrictions—while a critical tool to ensure that illegally obtained information is not used to convict a defendant—are insufficient to protect the full extent of the substantial privacy interests at stake in digital searches.

CONCLUSION

The judgment of trial court should be reversed and the search warrant should be quashed.

Dated: November 17, 2022

Respectfully submitted,



Jennifer Stisa Granick*
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
39 Drumm Street
San Francisco, CA 94111
Tel: (415) 343-0758
jgranick@aclu.org

* *Pro hac vice* pending

Attorneys for Amici Curiae

Alexander Shalom (021162004)
Jeanne LoCicero (024052000)
AMERICAN CIVIL LIBERTIES UNION
OF NEW JERSEY FOUNDATION
570 Broad Street, 11th Fl.
Post Office Box 32159
Newark, NJ 07102
Tel: (973) 854-1714
ashalom@aclu-nj.org
jlocicero@aclu-nj.org