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, *Plaintiff,* v. ZAK A. MISSAK *Defendant.*	: Criminal Action : No. A-000193-22T4 : : Superior Court of New Jersey, : Appellate Division : : 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

Burns v. United States,
235 A.3d 758 (D.C. Cir. 2020) 16

Carpenter v. United States,
138 S. Ct. 2206 (2018) 1

Commonwealth v. Snow,
160 N.E.3d 277 (Mass. 2021) 13

Demaree v. Pederson,
887 F.3d 870 (9th Cir. 2018) 12

Florida v. Jimeno,
500 U.S. 248 (1991) 11

In re [REDACTED]@gmail.com,
62 F. Supp. 3d 1100 (N.D. Cal. 2014) 13

In re Search of Black iPhone 4,
27 F. Supp. 3d 74 (D.D.C. 2014) 17

In re Search of Google Email Accounts identified in Attachment A,
92 F. Supp. 3d 944 (D. Alaska 2015) 13

In re Search of Info. Associated with Email Addresses Stored at Premises Controlled by Microsoft Corp.,
212 F. Supp. 3d 1023 (D. Kan. 2016) 15

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 (W.D. Wash. 2011) 16

Marron v. United States,
275 U.S. 192 (1927) 20

Marron v. United States,
275 U.S. 192 (1927) 12

Maryland v. Garrison,
480 U.S. 79 (1987) 12

People v. Herrera,
357 P.3d 1227 (Colo. 2015) 17

People v. Hughes,
958 N.W.2d 98 (Mich. 2020) 1

People v. Musha,
131 N.Y.S.3d 514 (N.Y. Sup. Ct. 2020) 16

People v. Thompson,
178 A.D.3d 457 (N.Y. App. Div. 2019) 13

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

State v. Bock,
485 P.3d 931 (Or. Ct. App. 2021) 16

State v. Earls,
214 N.J. 564 (2013).....1, 10

State v. Lunsford,
226 N.J. 129 (2016).....1

State v. Marshall,
199 N.J. 602 (2010).....20

State v. McLawhorn,
636 S.W.3d 210 (Tenn. Crim. App. 2020).....16

State v. Mefford,
517 P.3d 210 (Mont. 2022) 11

State v. Reid,
194 N.J. 386 (2008).....1

Taylor v. State,
260 A.3d 602 (Del. 2021).....16

United States v. Abboud,
438 F.3d 554 (6th Cir. 2006) 13

United States v. Comprehensive Drug Testing, Inc.,
621 F.3d 1162 (9th Cir. 2010) 12

United States v. Diaz,
841 F.2d 1 (1st Cir. 1988) 13

United States v. Galpin,
720 F.3d 436 (2d Cir. 2013) 12

United States v. Ganias,
824 F.3d 199 (2d Cir. 2016) 1

United States v. Hasbajrami,
945 F.3d 641 (2d Cir. 2019) 1

United States v. Hill,
459 F.3d 966 (9th Cir. 2006) 20

United States v. Holcomb, No. CR21-75-RSL,
2022 WL 1539322 (W.D. Wash. May 16, 2022) 14

United States v. Otero,
563 F.3d 1127 (10th Cir. 2009) 12

United States v. Warshak,
631 F.3d 266 (6th Cir. 2010) 1

United States v. Zemlyansky,
945 F. Supp. 2d 438 (S.D.N.Y. 2013) 14

Walter v. United States,
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, *Forensic Toolkit (FTK) User Guide* (Apr. 3, 2017) 22

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 (2015) 18

App Annie, *The State of Mobile 2021* (2021) 8

Apple, *iPhone 12* 8

Brief of Upturn Inc. as Amicus Curiae, *State v. Smith*,
278 A.3d 481 (Conn. 2022) (No. SC 20600) 18, 19, 22

Diane Thieke, *Smartphone Statistics: For Most Users, It's a 'Round-the-Clock' Connection*, ReportLinker (Jan. 26, 2017) 8

Geoffrey A. Fowler & Heather Kelly, *Amazon's New Health Band Is the Most Invasive Tech We've Ever Tested*, Wash. Post (Dec. 10, 2020) 9

Grindr, *About Grindr* 10

John Koetsier, *We've Spent 1.6 Trillion Hours on Mobile So Far in 2020*,
Forbes (Aug. 17, 2020) 7

Justin McCarthy, *One in Five U.S. Adults Use Health Apps, Wearable Trackers,* Gallup (Dec. 11, 2019).....9

Kinkoo, *Kinkoo* 10

Laurent Sacharoff, *The Fourth Amendment Inventory as a Check on Digital Searches*, 105 Iowa L. Rev. 1643 (2020) 19

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

Microsoft, *Search for eDiscovery Activities in the Audit Log*, Microsoft Docs (Jan. 7, 2022) 23

Mitch Strohm, *Digital Banking Survey: 76% of Americans Bank Via Mobile App—Here Are the Most and Least Valuable Features*, Forbes (Feb. 24, 2021) 10

Orin S. Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 Tex. Tech. L. Rev. 1 (2015) 24

Paulette Keheley, *How Many Pages in a Gigabyte? A Litigator's Guide*, Digital War Room (Apr. 2, 2020).....8

Pew Rsch. Ctr., *Mobile Fact Sheet* (Apr. 7, 2021).....7

Sarah Silbert, *All the Things You Can Track with Wearables*, Lifewire (Dec. 2, 2020) 9

Sudip Bhattacharya et al., *NOMOPHOBIA: NO Mobile Phone PhoBIA*, 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. Ganias*, 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 though 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 interestsin 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 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 operatizing 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