Dillon Reisman (374142021)
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-Appellant*, v. ZAK A. MISSAK, *Defendant-Respondent*.	: Criminal Action : No. A-2602-23T4 : : : : : Trial No. SOM-21-000879 : : Sat Below: : Hon. Peter J. Tober, P.J. Cr.

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

Dillon Reisman (374142021)
Jeanne LoCicero (024052000)
AMERICAN CIVIL LIBERTIES UNION
OF NEW JERSEY FOUNDATION
[redacted]
Post Office Box 32159
Newark, NJ 07102
Tel: (973) 854-1714
dreisman@aclu-nj.org
jlocicero@aclu-nj.org

Jennifer Stisa Granick*
Nathan Freed Wessler*
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
[redacted]
San Francisco, CA 94104
Tel: (415) 343-0758
jgranick@aclu.org
nwessler@aclu.org

* *Pro hac vice* pending

Attorneys for Amici Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES ii

INTERESTS OF AMICI CURIAE 1

PRELIMINARY STATEMENT 2

FACTUAL BACKGROUND 4

ARGUMENT. 7

I. Cell Phones Contain an Immense Amount of Private, Sensitive Data 7

II. Warrants Must Specifically Limit Law Enforcement Searches. 12

A. Where possible, warrants must limit digital searches by time frame. 13

B. Warrants should limit digital searches by the substance and type of data sought. 16

III. The State's New Justifications for a General Search of all Content on the Phone are Inadequate. 19

A. Forensic tools are able to find and meaningfully present relevant evidence for review, even if the data has been hidden or deleted. 20

B. The State fails to justify a search for the kinds of information it says it seeks. 25

C. Courts agree that searches of all content on a cell phone are impermissible general searches and are not allowed without exceptional circumstances not present here. 28

D. The State's authority does not support its argument. 31

CONCLUSION 34

TABLE OF AUTHORITIES

Cases

Burns v. United States,
235 A.3d 758 (D.C. Cir. 2020) 21

Carpenter v. United States,
585 U.S. 296 (2018)..... 1, 4, 32

Commonwealth v. Snow,
160 N.E.3d 277 (Mass. 2021) 18

In re [REDACTED]@gmail.com,
62 F. Supp. 3d 1100 (N.D. Cal. 2014) 17

In re Search of Google Email Accounts Identified in Attachment A,
92 F. Supp. 3d 944 (D. Alaska 2015).....17

In re Search of Info. Associated with Email Addresses Stored at Premises Controlled by Microsoft Corp.,
212 F. Supp. 3d 1023 (D. Kan. 2016) 20

In re United States' Application for a Search Warrant to Seize and Search Elec. Devices from Edward Cunnius,
770 F. Supp. 2d 1138 (W.D. Wash. 2011).....22

Lipsky v. N.J. Ass'n of Health Plans, Inc.,
474 N.J. Super. 447 (App. Div. 2023).....14

Marron v. United States,
275 U.S. 192 (1927).....23

Matter of People,
189 N.Y.S.3d 923 (N.Y. Crim. Ct. 2023) 38

People v. Carson,
No. 355925, 2024 WL 647964 (Mich. App. Feb. 15, 2024).....37

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) 22

People v. Thompson,
178 A.D.3d 457 (N.Y. App. Div. 2019).....18

Richardson v. State,
282 A.3d 98 (Md. 2022) 35, 36

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

Stanford v. Texas,
379 U.S. 476 (1965).....35

State v. Bock,
485 P.3d 931 (Or. Ct. App. 2021)..... 21, 34

State v. Boone,
232 N.J. 417 (2017) 24

State v. Burnett,
42 N.J. 377 (1964).....7

State v. Earls,
214 N.J. 564 (2013) 2, 14

State v. Feliciano,
224 N.J. 351 (2016) 35

State v. Irelan,
375 N.J. Super. 100 (App. Div. 2005).....7, 26

State v. Lunsford,
226 N.J. 129 (2016) 2

State v. Mansor,
421 P.3d 323 (Or. 2018) ..... *passim*

State v. Marshall,
199 N.J. 602 (2010) 24

State v. McLawhorn,
636 S.W.3d 210 (Tenn. Crim. App. 2020) 22

State v. Missak,
476 N.J. Super. 302 (App. Div. 2023) ..... *passim*

State v. Reid,
194 N.J. 386 (2008) 2

State v. Smith,
278 A.3d 481 (Conn. 2022) 36

State v. Turay,
532 P.3d 57 (Or. 2023) 16, 40

Taylor v. State,
260 A.3d 602 (Del. 2021) 22, 39, 40

Terreros v. State,
312 A.3d 651 (Del. 2024) 38

Thomas v. State,
305 A.3d 683 (Del. 2023) 39

United States v. Abboud,
438 F.3d 554 (6th Cir. 2006) 17

United States v. Brown,
828 F.3d 375 (6th Cir. 2016) 24, 25

United States v. Comprehensive Drug Testing, Inc.,
621 F.3d 1162 (9th Cir. 2010) 16

United States v. Diaz,
841 F.2d 1 (1st Cir. 1988) 17

United States v. Galpin,
720 F.3d 436 (2d Cir. 2013).....15

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

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

United States v. Hill,
459 F.3d 966 (9th Cir. 2006).....27

United States v. Holcomb,
No. CR21-75-RSL, 2022 WL 1539322 (W.D. Wash. May 16, 2022).....18

United States v. Warshak,
631 F.3d 266 (6th Cir. 2010).....2

United States v. Wey,
256 F. Supp. 3d 355 (S.D.N.Y. 2017) 34

United States v. Zemlyansky,
945 F. Supp. 2d 438 (S.D.N.Y. 2013) 19, 20

Warden Penitentiary v. Hayden,
387 U.S. 294 (1967).....24

Wheeler v. State,
135 A.3d 282 (Del. 2016)..... 15, 16, 18

Statutes

N.J.S.A. 2C:5-1A(1).....5

N.J.S.A. 2C:13-6A.....5

N.J.S.A. 2C:14-2C(4) 5

Other Authorities

App Annie, *The State of Mobile 2021* 7 (2021) 10

Apple, *iPhone 16* 11

Blink, *Blink Home Monitor App* 13

Brief of Upturn Inc. as Amicus Curiae, *State v. Smith*, 278 A.3d 481 (Conn. 2022) (No. SC 20600) 30

Diane Thieke, *Smartphone Statistics: For Most Users, It's a 'Round-the-Clock' Connection*, ReportLinker (Jan. 26, 2017) 10

Geoffrey A. Fowler & Heather Kelly, *Amazon's New Health Band Is the Most Invasive Tech We've Ever Tested*, Wash. Post (Dec. 10, 2020) 12

Grindr, *About Grindr* 13

Jack Nicas, Mike Isaac & Shira Frenkel, *Millions Flock to Telegram and Signal as Fears Grow Over Big Tech*, N.Y. Times (Jan. 13, 2021) 13

John Koetsier, *We've Spent 1.6 Trillion Hours on Mobile So Far in 2020*, Forbes (Aug. 17, 2020) 10

Justin McCarthy, *One in Five U.S. Adults Use Health Apps, Wearable Trackers,* Gallup (Dec. 11, 2019) 12

Kinkoo, *Kinkoo* 13

Laurent Sacharoff, *The Fourth Amendment Inventory*, 105 Iowa L. Rev. 1643 (2020). 27

Logan Koepke et al., *Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones*, Upturn (Oct. 21, 2020) 30, 41

Mary Meeker, Founder, Bond Capital, Vox/Recode Code Conference Presentation: Internet Trends 2019 (June 11, 2019) 13

Mitch Strohm, *Digital Banking Survey: 76% of Americans Bank Via Mobile App—Here Are the Most and Least Valuable Features*, Forbes (Feb. 24, 2021).....13

Paulette Keheley, *How Many Pages in a Gigabyte? A Litigator's Guide*, Digital War Room: Blog (Apr. 2, 2020) 11

Pew Rsch. Ctr., *Mobile Fact Sheet* (Apr. 7, 2021) 10

Sarah Silbert, *All the Things You Can Track with Wearables*, Lifewire (Dec. 2, 2020).....12

Sudip Bhattacharya et al., *NOMOPHOBIA: NO Mobile Phone PhoBIA*, 8 J. Fam. Med. Primary Care 1297 (2019).....11

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. For over 60 years, the ACLU-NJ has defended liberty and justice guided by the vision of a fair and equitable New Jersey for all.

Since its founding in 1920, the ACLU has frequently appeared before the U.S. 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*, 585 U.S. 296 (2018), as amicus (with the ACLU-NJ) at an earlier stage in this case, *State v. Missak*, 476 N.J. Super. 302 (App. Div. 2023), and 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).

PRELIMINARY STATEMENT

In this appeal, the State seeks approval of a warrant to search all content on a cellphone. This Court has already held such a warrant in this case to be a prohibited and overbroad general search because it aims to search for any data on an entire device, rather than just for data for which there is probable cause. The State returns not with a narrowed warrant, but with broad and generic additions to its affidavit. But as the State forthrightly admits, its new rationale would allow an unlimited search not just of this phone, in this case, but of anyone's phone, in any criminal investigation. Were this Court to adopt the State's reasoning, it would be a huge and unjustified rejection of current constitutional protections under both the Fourth Amendment and Article I, Paragraph 7 of the New Jersey Constitution.

The information stored on desktop computers, laptops, and cell phones is far more vast, diverse, and sensitive than information stored in a filing cabinet, or even an entire home. *See infra* Section I. These characteristics make it critical that warrants for cell phone searches closely adhere to Fourth Amendment and

Article I, Paragraph 7 requirements, lest grounds to search particular information on a device for evidence of one crime mutate into authority to search the entirety of the device for evidence of any crime. Electronic device searches must be limited to files and folders for which the affidavit in support of the warrant provides probable cause. Departing from that rule would be particularly problematic in the context of digital information, which the Supreme Court has recognized as deserving of more protection than low-tech or analog versions of the same information. *Carpenter v. United States*, 585 U.S. 296 (2018); *Riley v. California*, 573 U.S. 373 (2014). This is a context where the invasion of privacy would be astoundingly acute. *See infra* Section II.

In this case, nothing in the State's revamped affidavit justifies a search beyond the categories of data and the date range likely to contain evidence of the crime under investigation. The Second Warrant application does not provide any case-specific justification for a plenary search, instead offering vague proffers and rampant speculation, and dismissing privacy interests, not just of Mr. Missak, but also of his friends and family who have communicated with him over that device. (*See infra* Section III). Because that falls far short of the requirements of the Fourth Amendment and Article I, Paragraph 7, amici respectfully urge the Court to affirm the court's ruling below.

FACTUAL BACKGROUND

In December 2021, 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 by the New Jersey Internet Crimes Against Children Task Force. At the same time, officers seized an Apple iPhone 12 Pro Max that Missak had with him.

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) (Pa1–Pa3). The affidavit related the details of the State's investigation and requested the "ability and opportunity to access all information contained within the [phone]." (Pa11–Pa12).

A judge issued a search warrant authorizing 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 any other stored information on said mobile device that will assist in the continuation of this investigation.
>
> [(Pa11).]

The State did not search (and still has not searched) the phone, representing that it first needs Missak to provide his passcode in order to enable investigators to access to the phone data.

On June 24, 2022, 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. (Pa31–Pa35).

After granting review, this Court reversed the trial court's order and quashed the search warrant. *State v. Missak*, 476 N.J. Super 302 (App. Div. 2023) (*Missak I*) (Pa38). It held that the affidavit in support of the warrant lacked probable cause that the phone's text messages, calls, communications, GPS data, or other data created or existing prior to defendant's alleged initial communications with the undercover officer on December 8, 2021, would contain evidence of the two crimes for which law enforcement expressly sought the search warrant. *Id.* at 321–22 (Pa62–63). The Court held that the State could not establish probable cause through its mere assertion that "individuals '*may*'

seek to alter computer files to disguise what they contain and '*may*' thereby avoid the State's recovery of information and data for which probable cause has otherwise been established." *Id.* at 320–2 (Pa62–63) (emphases added). And because there were no facts in the record establishing that information on the phone predating the date of the offense would constitute evidence of Missak's use of the phone "around the time" of the crime, the warrant application did "not provide sufficient facts supporting the expansive search warrant for all the data and information on the seized cellular phone." *Id.* at 321–22 (citing *State v. Irelan*, 375 N.J. Super. 100, 118 (App. Div. 2005) and *State v. Burnett*, 42 N.J. 377, 386-87 (1964)) (Pa62–63) ("Probable cause requires more than a mere hunch or bare suspicion."). Though it rejected the State's warrant, the panel explained that "[t]he State [was] free to seek a new search warrant based on whatever facts are available to it that establish probable cause to believe the various information and data the State requests to search contain evidence pertaining to the criminal charges pending against defendant." *Id.* at 323 (Pa63).

Taking this Court up on the opportunity, on September 12, 2023, the State obtained a Search Warrant/Communications Data Warrant (the "Second Warrant") that would permit the State to search defendant's phone in its entirety. (Pa65–67). The application for the Second Warrant included new language intended to support a search of *all* content on the phone. (Pa72); Appellant Br.

at 12–13. Those justifications included new claims purportedly requiring a search of all content on the phone due to law enforcement's technological incapacity to otherwise find evidence. (Pa71–72).

The State's new justifications also included claims about the types of evidence the State believed it has probable cause to search for. The State asserted that it must look at all contents of the device, even photos of the device owner's family and friends, as probative of mental intent and ownership and control of the device. (Pa72–73).

On March 5, 2024, the trial court quashed the Second Warrant. It held that this warrant, like the first one, lacked sufficient probable cause to support a search of the phone in its entirety. In particular, it found that the State failed to identify any precise data or information that would reveal evidence of the perpetrator's intent, and that there was insufficient justification for searching beyond data from the applications used to commit the crimes charged to demonstrate ownership. (Pa99–101). The State has appealed that quashal order to this Court.

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.[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 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 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

---

[1] Pew Rsch. Ctr., *Mobile Fact Sheet* (Apr. 7, 2021) (attached at Amicus Appendix (hereafter, "Aa") 185).

[2] John Koetsier, *We've Spent 1.6 Trillion Hours on Mobile So Far in 2020*, Forbes (Aug. 17, 2020) (Aa68).

[3] Diane Thieke, *Smartphone Statistics: For Most Users, It's a 'Round-the-Clock' Connection*, ReportLinker (Jan. 26, 2017) (Aa49).

[4] App Annie, *The State of Mobile 2021* 7 (2021) (Aa14).

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 16 offers 128 gigabytes of data storage—by some estimates, the equivalent of more than 86 million pages of text—and more expensive versions can store four times that.[6]

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 extensive historical information related to each functionality. *Id.* at 393. Because a cell phone "collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, or a video—[cell phone data] reveal[s] much more in combination

---

[5] Sudip Bhattacharya et al., *NOMOPHOBIA: NO Mobile Phone PhoBIA*, 8 J. Fam. Med. Primary Care 1297 (2019) (Aa199).

[6] Apple, *iPhone 16* (Aa17); *see also* Paulette Keheley, *How Many Pages in a Gigabyte? A Litigator's Guide*, Digital War Room: Blog (Apr. 2, 2020) (Aa180).

than any isolated record," and much more about "an individual's private interests or concerns," *id.* at 394, 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.[7] Other apps might monitor home security cameras, facilitate dating (and thereby reveal the user's sexual orientation and predilections), track a household's budget, manage financial accounts, or send encrypted messages.[8] Coupled with devices' rapidly increasing storage capacities, the proliferation of these apps

---

[7] Justin McCarthy, *One in Five U.S. Adults Use Health Apps, Wearable Trackers,* Gallup (Dec. 11, 2019) (Aa73); Sarah Silbert, *All the Things You Can Track with Wearables*, Lifewire (Dec. 2, 2020) (Aa192); Geoffrey A. Fowler & Heather Kelly, *Amazon's New Health Band Is the Most Invasive Tech We've Ever Tested*, Wash. Post (Dec. 10, 2020) (Aa62).

[8] *See, e.g.*, Blink, *Blink Home Monitor App* (Aa32); Grindr, *About Grindr* (Aa67); Kinkoo, *Kinkoo* (Aa80); Mitch Strohm, *Digital Banking Survey: 76% of Americans Bank Via Mobile App—Here Are the Most and Least Valuable Features*, Forbes (Feb. 24, 2021) (Aa172); Mary Meeker, Founder, Bond Capital, Vox/Recode Code Conference Presentation: Internet Trends 2019 (June 11, 2019) (Aa175); Jack Nicas, Mike Isaac & Shira Frenkel, *Millions Flock to Telegram and Signal as Fears Grow Over Big Tech*, N.Y. Times (Jan. 13, 2021) (Aa70–71).

means 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.

As this Court has recognized, 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. *Missak I*, 476 N.J. Super at 314 (citing *Lipsky v. N.J. Ass'n of Health Plans, Inc*., 474 N.J. Super. 447, 473 (App. Div. 2023)) (noting "the strong privacy interests associated with the contents[] of individuals' personal electronic devices, which often include an extraordinary amount of confidential and even privileged information") (Pa51); *see also 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 interests in cell phone location data (citations omitted)).

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 and Article I, Paragraph 7, it is axiomatic that officers must have probable cause to support the search of a cell phone. *See Riley*, 573 U.S. 373; *Missak I*, 476 N.J. Super. at 316 (Pa53). 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); *State v. Mansor*, 421 P.3d 323, 337–38, 341–43 (Or. 2018); *Wheeler v. State*, 135 A.3d 282, 299 (Del. 2016).

Failure to use available time frames and sought-after file types to cabin a warrant—as this warrant fails 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); *Wheeler*, 135 A.3d at 304; *Mansor*, 421 P.3d at 342–43. Probable cause to search or seize *some* data on the phone cannot justify access to the totality of the phone's contents. *Missak I*, 476 N.J. Super. at 321–22 (Pa62–63).

A. Where possible, warrants must 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 State v. Turay*, 532 P.3d 57, 69 (Or. 2023) ("[W]hen a time-based description of the information sought on a computer is relevant and available to the police, that detail ordinarily should be set out in the affidavit and included in the warrant's description of the evidence sought." (quotation marks omitted) (quoting *Mansor*, 421 P.3d at 342)); *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, 946 (D. Alaska 2015) (application without date restriction denied as overbroad); *see also Wheeler*, 135 A.3d at 304 ("One obvious respect [in which the warrant lacked particularity] was the failure to limit the search to the relevant time frame."); *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, 280 (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) (Aa245)[9] ("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*, 639 F. Supp. 3d 1142 (W.D. Wash. Nov. 8, 2022) (on reconsideration, concluding that the good-faith doctrine applied and suppression was therefore not appropriate, without disturbing the substantive ruling), *appeal docketed,* No. 23-46 (9th Cir. argued Sept. 10, 2024).

[9] Pursuant to *R.* 1:36-3, counsel includes this unpublished opinion in the appendix. Counsel cites the opinion for its value in demonstrating how other courts have applied established legal principles to similar factual situations as the present case, and not because the case constitutes binding law. Counsel is aware of no cases that are contrary to that limited proposition.

Time frame limitations in warrants guard against searches for evidence of past, unrelated crimes for which there is no probable cause, 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). Use of date-range restrictions or other limitations can thus be a critical and necessary means of minimizing the potential for "general rummaging" when searching electronically stored information. *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"); *Zemlyansky*, 945 F. Supp. 2d at 459–60 (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").

Here, the State knows the exact dates of the criminal activity it is investigating—from December 8, 2021, until Missak's arrest the next day. To

satisfy the Fourth Amendment and Article I, Paragraph 7, any warrant needs to include a date range limiting the search to that period.

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

Warrants can also limit searches for electronic evidence by file type without unduly interfering with law enforcement investigations. For example, if there is only probable cause to believe that co-conspirators texted each other, there is no reason for law enforcement to search photos. Of course, 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 process that complies with constitutional guarantees. *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' 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 through *everything*. They may not access or examine file types that are not reasonably connected to probable cause. Yet in this case, for the second time, the warrant purports to authorize investigators to access *all information*, with no time-frame, app specific, or file-type limitations that would confine the search to the scope of probable cause.

Moreover, the State's warrant suffers an additional defect beyond its overbreadth: it impermissibly delegates unfettered discretion to the investigating officers. 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 gave police officers the discretion to determine which of two apartments the defendant had been associated, inappropriately delegating the "role of the neutral and detached magistrate" to police). That means that the warrant must constrain where and how officers search. This one doesn't, so it must be quashed.

III. The State's New Justifications for a General Search of all Content on the Phone are Inadequate.

It is blackletter law under the Fourth Amendment and Article I, Paragraph 7 that a warrant application must establish a nexus between a proposed search and criminal behavior. *Warden Penitentiary v. Hayden*, 387 U.S. 294, 307 (1967); *State v. Boone*, 232 N.J. 417, 426 (2017); *see, e.g.*, *United States v. Brown*, 828 F.3d 375, 382 (6th Cir. 2016) (requiring that affidavits must set forth "sufficient facts demonstrating why the police officer expects to find evidence in the [place to be searched] rather than in some other place"). The connection "must be specific and concrete, not 'vague' or 'generalized.'" *Brown*, 828 F.3d at 385 (citation omitted).

The State's claims here are generalized in the true meaning of that term: they would apply in every case regardless of the facts. They are also vague. For example, the State claims that it needs to search every file on the phone to find information "probative" of the "mental intent of any actor involved." (Pa72); Appellant Br. at 13. It doesn't identify any possible other "actor" in the offense (other than presumably Mr. Missak). And it doesn't explain what type of information would be probative of mental intent relevant to any element of the charged crimes. Nor does it establish probable cause to believe that evidence of mental intent would be found outside of the relevant date and file type

limitations. Such vague and contextless terms would give officers unguided discretion to rummage through the phone.

A. Forensic tools are able to find and meaningfully present relevant evidence for review, even if the data has been hidden or deleted.

Forensic search tools can make searches limited by date and file type workable. And they are not only effective for law enforcement, but generally will be far *more* effective in identifying responsive evidence than attempting to manually review the voluminous data stored on a phone. 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 officers observe, that limitation, lest searches be unreasonably overbroad and therefore unconstitutional.

Such limitations are eminently appropriate here. The crime in question took place over a known, short period of time. The investigators already have all the conversations between the suspect and the undercover officer, and know exactly what apps were being used. The appropriate reason police are seeking to search the phone is that they want to obtain copies of those messages on the phone that will show that Mr. Missak was a party to the conversations.

The technical allegations in support of the warrant are too speculative to be the basis of probable cause. The application states that "data stored on [ ]

devices *may* be intentionally concealed" or "deleted." (Pa72). There are no facts in the application that would provide probable cause to believe that these obfuscating actions occurred. Speculation that someone in a hypothetical scenario might be able to successfully manipulate cell phone data and hide it from investigators is not probable cause in a particular case. *See Irelan*, 375 N.J. Super. at 118 ("Probable cause requires more than a mere hunch or bare suspicion . . . [I]t requires a well-grounded suspicion."). And relying on that reasoning would cause the exception to swallow 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." Laurent Sacharoff, *The Fourth Amendment Inventory*, 105 Iowa L. Rev. 1643, 1658 (2020). There may be cases where the police have a specific reason to believe that a particular suspect has manipulated a cell phone or other data. 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).[10] But there are no facts suggesting that this obfuscation happened *in this case*.

[10] Requiring a potential extra step poses little to no problem here. The State is especially capable of identifying tampering or other obstacles, since a law enforcement officer was party to all the conversations with the defendant that are relevant to the commission of the alleged crime.

Nor does an owner's potential deletion of files justify the State's requested unbounded search. The State may need to *extract* or copy all data on the cell phone for forensic analysis to ensure access to relevant-but-deleted files. Appellant's Br. at 28–29; *Mansor*, 421 P.3d at 333. But once the data is secured, investigators have no need to *query* for or *view* files outside of the specified date range in order to find relevant or even deleted information.[11]

A date-targeted search of extracted data using standard forensic search tools will turn up relevant files even if they are stored in chunks, have had their names changed, or are deleted. Forensic tools are powerful enough to locate this information and display it in useful ways without necessitating human review of records outside the scope of a proper warrant.

To the extent the State asserts that it does not have the technical capability to find this information while using a targeted search, those claims are refuted by experts. At the very least, there is enough independent reason to doubt the accuracy of the State's claims such that an evidentiary hearing should be held or a special master appointed before those claims could be the basis of this Court's ruling.

[11] The State calls this the "data reduction phase." Appellant's Br. at 29; *Mansor*, 421 P.3d at 333.

In civil litigation, it is the norm that parties will negotiate—or litigate—over the scope of searches to find discoverable information. Effective searches are a basic functionality of eDiscovery tools. Litigants and their lawyers routinely conduct searches of smartphones and other devices to identify discoverable and relevant evidence.

Forensic tools used in criminal investigations are just as powerful. In 2020, Upturn, a nonprofit technology policy organization with expertise in cell phone forensic tools, published a white paper that refutes the State's claims.[12] The paper documents how the mobile device forensic tools that law enforcement uses organize extracted phone data in an easily navigable and digestible format for law enforcement to more efficiently analyze and explore the information on the device.

First, regardless of how information is stored on a device, in "chunks," fragments, or otherwise, forensic tools readily identify the data and assemble it into a meaningful message, image, or other file type.[13] Of course they can do this. The phone itself can do this, so this capability isn't surprising or difficult.

---

[12] Logan Koepke et al., *Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones* 24, Upturn (Oct. 21, 2020) [hereinafter "*Mass Extraction*"] (Aa91, Aa114).

[13] *Mass Extraction* 24 (Aa114).

As for concealing evidence, Upturn explains that it is difficult — "and in many instances, technically impossible"—to change where data is stored on cellphones, making it much more difficult to hide.[14] "With cellphones in particular, the argument that evidence could be hidden anywhere rings hollow." *Id*.

In addition, "[Mobile device forensic tools or 'MDFTs'] are agnostic toward file organization or file name." They can:

> pick out data that has a particular data type, and 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.
>
> [*See* Brief of Upturn Inc. as Amicus Curiae at 7, *State v. Smith*, 278 A.3d 481 (Conn. 2022) (No. SC 20600) [hereafter, "Upturn Brief"] (Aa35).]

In sum, targeted searches—which include date range and file type capabilities—enable investigators to comprehensively home in on the digital evidence relevant to probable cause, under the supervision of the court, not the discretion of the officers. The State's claims about the technology are inaccurate, or at the very least contentious. This Court should not credit them,

[14] *Mass Extraction* 63 (Aa153).

or in the alternative, should order an evidentiary hearing or appoint a special master with technological expertise to determine these tools' capabilities.

B. The State fails to justify a search for the kinds of information it says it seeks.

The State claims it needs full access to this phone to find evidence of the "mental intent of any actor involved." (Pa72). It also claims it needs to search the full contents of the phone, including non-contraband and innocent photos, to prove ownership and control. (Pa13). But, as the Law Division held, it is not reasonable for law enforcement to seek full access to a defendant's phone simply because evidence could possibly be found anywhere. (Pa101). Investigators can search for these types of information where information for which they have probable cause is located. The State's justifications would result in unbounded warrants authorizing plenary searches of all cell phones in *every* investigation.

1. "Mental Intent"

The State argues that it can search the entire phone because it has probable cause to search for any information "probative" of the "mental intent of any actor involved" in this crime. Appellant's Br. at 13, 37. The term "mental intent" in the context of these facts is too vague to serve as a meaningful guide to investigators. The State has not explained what type of information could be on the phone that might be probative of "mental intent," nor of intent as to what element of the charged offenses, nor why it has probable cause to search for that

kind of evidence unbounded by date. And "probative" is an extremely low standard, much lower than probable cause. *Cf. Carpenter*, 585 U.S. at 298 ("reasonable grounds" for believing that records were "relevant and material to an ongoing investigation" is a standard that "falls well short of the probable cause required for a warrant").

The State also fails to explain why information relevant to the "mental intent" of any other "actor involved" is likely to be on this phone. Indeed, there is no reason to believe that anyone other than the undercover officer was involved in this offense. This catch-all phrase is another indication that the State seeks an overbroad warrant unconstitutionally devoid of any limits.

2. Evidence of Control

The State says it may search the entirety of a device to obtain evidence of control of that device. Appellant's Br. at 15, 37. The State says there is nothing strange about this demand, comparing it to the execution of a search warrant on a residence, where the warrant allows the search for and recovery of utility bills, mail, clothing, identification, and other personal items that tend to establish use and control of the residence.

The difference is that in a warranted search of a residence, the scope of the search is already limited. Law enforcement has established probable cause to search the residence, and the warrant specifies particular kinds of records that

may be in the home and are relevant indicia of control.[15] Police could not, for example, also search a person's office without probable cause, merely on the theory that she may have stored utility bills, mail or other indicia there as well. Here, the State fails to identify any precise data or information that will reveal evidence of Mr. Missak's control over the device. (Pa98–99). But the kinds of digital files that might show control are readily identifiable: even simply searching the "settings" app in a cell phone would be likely to show an individual's phone number and email address, and in most cases merely that would suffice for the purposes the State identifies. The State's warrant here, though, has no limits; it permits the State to trawl through *everything* on the basis that *anything* could show Mr. Missak's control over the device.

That is not allowed. For example, in *United States v. Wey*, the Southern District of New York rejected a warrant to search multiple types and categories of information—all "financial records," "notes, memoranda, records of internal and external communications… correspondence, audio tapes[] and video tapes, [and] photographs," among others—that merely pertained to the suspects. 256 F. Supp. 3d 355, 386 (S.D.N.Y. 2017). As the court explained, because every

[15] And, of course, "a cell phone search would typically expose to the government far more than the most exhaustive search of a house." *Riley*, 573 U.S. at 396.

document seized from the suspect pertains to the suspect, the warrants did not impose "meaningful parameters on an otherwise limitless search of a defendant's electronic media," and they failed "to link the evidence sought to the criminal activity supported by probable cause" *Id.* at 387 (citation omitted); *see also Bock*, 485 P.3d at 936 (warrant authorizing the search of a cell phone for circumstantial evidence about the owner and any evidence related to suspected criminal offenses, including unlawful firearm possession, was not sufficiently specific under this state constitution's Fourth Amendment corollary). Like that warrant, the one here is impermissibly broad.

C. Courts agree that searches of all content on a cell phone are impermissible general searches and are not allowed without exceptional circumstances not present here.

Permission to conduct a general search is explicitly the result that the State argues for, but issuance and enforcement of general warrants is a central evil the Fourth Amendment and Article I, Paragraph 7 seek to prevent. *See Stanford v. Texas*, 379 U.S. 476, 481 (1965) (Fourth Amendment protects against general warrants, which were "the worst instrument of arbitrary power . . . that ever was found in an English law book." (quoting founding father James Otis)); *Riley*, 573 U.S. at 403_("Opposition to such searches was in fact one of the driving forces behind the Revolution itself."); *State v. Feliciano*, 224 N.J. 351, 366 (2016).

The Supreme Court of Maryland has stated its expectation that "in appropriate cases, issuing judges will limit searches of cell phones to specific applications and/or types of applications that officers have reason to believe the suspect used in furtherance of the crimes under investigation." *Richardson v. State*, 282 A.3d 98, 118 (Md. 2022). The court added that, "[p]erhaps the most common limitation that issuing judges should consider including in a warrant to satisfy the particularity requirement is a temporal restriction." *Id.* The court gave an example quite similar to the case here:

> If there is probable cause to believe that a suspect used a friend's phone to record a sex crime, the issuing judge reasonably could limit the search of that phone to the recording itself (in the absence of the affiant explaining why there was probable cause to believe that evidence of the crime would be contained in other items on the phone). That would presumably authorize a narrow search of any application on the phone that could have made or stored the recording.
>
> [*Id.*]

Here, there is probable cause to believe that this suspect used this phone to communicate over certain messaging apps and during a specified time period as part of committing the offenses of luring and attempted sexual assault. That is as far as the warrant can go. *See also State v. Smith*, 278 A.3d 481 (Conn. 2022) (warrant did not comply with the particularity requirement in part because it did not limit the search to a reasonably related time frame).

Similarly, in *People v. Carson*, the court held that a reference to the crimes under investigation did not make a warrant to search all content on a cell phone sufficiently particular. No. 355925, 2024 WL 647964 (Mich. App. Feb. 15, 2024) (Aa214)[16], *appeal granted*, No. 166923 (Mich. Sept. 25, 2024). The court noted that "it would have been wholly appropriate to issue a warrant authorizing the police to engage in a search of the phone's contents limited in scope to correspondence between these two regarding the crimes." *Id.* at *8. But "[t]he warrant that was actually issued placed no limitations on the scope of the search and authorized the police to search everything, specifically mentioning photographs and videos." *Id.* The court noted that "[a]uthorization for a search of defendant's photographs and videos, despite there being no evidence suggesting that these files would yield anything relevant, is particularly troubling in light of the tendency of people in our modern world to store compromising photographs and videos of themselves with romantic partners on their mobile devices." *Id.* The State here also seeks to search all of the photos on this device, outside of any time frame and divorced from any facts or

[16] Pursuant to *R.* 1:36-3, counsel includes this unpublished opinion in the appendix. Counsel cites the opinion for its value in demonstrating how other courts have applied established legal principles to similar factual situations as the present case, and not because the case constitutes binding law. Counsel is aware of no cases that are contrary to that limited proposition.

circumstances connected to the crime. *See also Terreros v. State*, 312 A.3d 651, 668 (Del. 2024) (warrant that identified specific categories of data was a general warrant because each category was preceded by 'any and all' language with no temporal limitation); *Matter of People*, 189 N.Y.S.3d 923 (N.Y. Crim. Ct. 2023) (noting that a valid search warrant request for cellular phone data must set forth reasonable date and time restrictions on the data to be searched or provide a reasonable basis for deeming this requirement inapplicable).

Like those courts, this Court should hold that warrants that purport to allow searches of all content on a cell phone are overbroad and lack particularity.

D. The State's authority does not support its argument.

The State cobbles together cases in support of its broad argument, but they do not withstand scrutiny. Instead, those cases stand for the proposition that warrants to search cell phones must be narrowly tailored to the facts before the Court. The reasoning of those decisions is fatal to the State's assertion of a broad and plenary right to examine cell phone data.

The State cites the Delaware Supreme Court's decision in *Thomas v. State*, 305 A.3d 683, 697–99 (Del. 2023) for the proposition that a search need only be as specific as the circumstances allow. Appellant's Br. at 42. But *Thomas* required a warrant that closely adhered to case-specific facts establishing probable case, even though the State's same "circumstances" regarding the

possibility of evidence deletion or obfuscation were equally present there. The *Thomas* court held that the warrant was overbroad because it permitted a search that would surpass the time frame in which the crime occurred and did not limit the calls and messages to those involving the victims. The warrant needed to be narrowed to be lawful. *Thomas*, 305 A.3d at 703.

Thomas reiterated the principle, set out in earlier Delaware cases, that warrants may not authorize the search and seizure of "any/all data stored by whatever means." *Taylor v. State*, 260 A.3d 602, 609 (Del. 2021) (citation omitted). In *Taylor*, the state supreme court explained that "[t]he free-ranging search for anything 'pertinent to the investigation' undermines the essential protections of the Fourth Amendment—that a neutral magistrate approve in advance, based on probable cause, the places to be searched and the parameters of the search." *Id*. at 616.

The State also cites *Turay*, 532 P.3d at 67 for the proposition that "there is no way to know what data a file contains without opening it." Appellant Br. at 29. *Turay* held under the Oregon Constitution that a warrant was overbroad when it purported to authorize searches exactly like the ones at issue here. A warrant that would permit examination of "[a]ny and all communications," and which lacked restrictions "on the time or subject matter of the information that [was] sought," failed the particularity requirement. *Turay*, 532 P.3d at 76. The

court reiterated its adherence to the principle that a warrant must include, if available and relevant, temporal and nontemporal limiting details—of course governed by a standard of reasonableness in the circumstances. *Id.* at 74 (citing *Mansor*, 421 P.3d 323).

The earlier decision of the Oregon Supreme Court in *Mansor* explicitly rejects the State's position. 421 P.3d 323. The State argues that *Mansor* rejected the view that a warrant must limit a search to those specified areas such as "internet browsing history, document files, hard drive, emails, call logs, and varying application folders." Appellant's Br. at 32 (citing *Mansor*, 421 P.3d at 342). But *Mansor* supports time frame limitations, saying that "to meet the particularity requirement of [the state Constitution], the 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." *Mansor*, 421 P.3d at 343. It upheld the warrant there because its text limited the search to only the single day of the crime. The police, however, searched outside of that time frame. Because no exception to the warrant requirement applied, the court suppressed the fruits of the overbroad search. *Id.*

In ruling here, this Court should take these authorities into account, and note that forensic tools that allow targeted and bounded searches are far more

powerful today than they were in some earlier cases, and will continue to improve.[17]

This Court should decline the State's invitation to veer in the opposite direction of traditional Fourth Amendment and Article I, Paragraph 7 law, as well as the Supreme Court's modern cases protecting electronic data even more comprehensively than analog.

CONCLUSION

For these reasons, the judgment of trial court should be reversed and the search warrant should be quashed.

Dated: October 18, 2024

Respectfully submitted,

Dillon Reisman (374142021)
Jeanne LoCicero (024052000)
AMERICAN CIVIL LIBERTIES UNION OF NEW JERSEY FOUNDATION
[redacted]
Post Office Box 32159
Newark, NJ 07102
Tel: (973) 854-1714
dreisman@aclu-nj.org
jlocicero@aclu-nj.org

Jennifer Stisa Granick*
Nathan Freed Wessler*
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
[redacted]
San Francisco, CA 94104
Tel: (415) 343-0758
jgranick@aclu.org
nwessler@aclu.org

* *Pro hac vice* pending

Attorneys for Amici Curiae

[17] *Mass Extraction* (Aa91).