Court of Appeals Docket No. 2025-00202
Appellate Division, First Judicial Department Index Number 2022-05781

Court of Appeals
State of New York

THE PEOPLE OF THE STATE OF NEW YORK,

Respondent,

-against-

TYSHAWN MORRIS,

Defendant-Appellant.

BRIEF OF AMICI CURIAE THE ELECTRONIC PRIVACY INFORMATION CENTER, THE LEGAL AID SOCIETY, THE AMERICAN CIVIL LIBERTIES UNION, THE NEW YORK CIVIL LIBERTIES UNION, THE CENTER FOR DEMOCRACY & TECHNOLOGY, AND THE ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF DEFENDANT-APPELLANT

Laura Moraff
Brett Max Kaufman
Nathan Freed Wessler
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street,
18th Floor
New York, NY 10004
Tel.: (212) 549-2500
lauramoraff@aclu.org

Daniel R. Lambright
NEW YORK CIVIL LIBERTIES UNION FOUNDATION
125 Broad St.
19th Floor
New York, NY 10004
Tel.: (202) 607-3300
dlambright@nyclu.org

Dated: June 25, 2026
New York, New York

(Additional Counsel on Next Page)

Jerome D. Greco
THE LEGAL AID SOCIETY
49 Thomas Street
New York, NY 10013
Tel.: (212) 298-3075
jgreco@legal-aid.org

Jeramie Scott
Thomas McBrien
ELECTRONIC PRIVACY
INFORMATION CENTER
1519 New Hampshire Ave. NW
Washington, DC 20036
Tel.: (202) 483-1140
scott@epic.org

Counsel for Amici Curiae

RULES OF PRACTICE 500.1(f) AND 500.23 DISCLOSURE STATEMENTS

Pursuant to 22 N.Y.C.R.R. Part 500.1(f), the Electronic Privacy Information Center ("EPIC") hereby discloses that it is a non-profit 501(c)(3) organization with no parent, subsidiaries, or affiliates.

The Legal Aid Society ("LAS") discloses that it is a non-profit organization with no parent, subsidiaries, or affiliates.

The American Civil Liberties Union ("ACLU") hereby discloses that it is a non-profit 501(c)(4) entity organization. The ACLU has 54 affiliates throughout the 50 states, the District of Columbia, and Puerto Rico.

The New York Civil Liberties Union ("NYCLU") hereby discloses that it is a non-profit 501(c)(4) entity organization and is the New York State affiliate of the American Civil Liberties Union.

The Center for Democracy & Technology ("CDT") hereby discloses that it is a non-profit 501(c)(3) organization with no parent or subsidiary and no affiliate as that term is defined under New York law. CDT has a sister organization based in Brussels, Belgium, the Centre for Democracy & Technology (CDT) Europe, which has a common mission, and some overlap in the boards of directors.

The Electronic Frontier Foundation ("EFF") hereby discloses that it is a non-profit organization with no parent, subsidiaries, or affiliates.

No other person or entity has contributed to the preparation or submission of this brief. Additionally, no party or party's counsel contributed money that was intended to fund preparation or submission of this brief.

STATEMENT OF RELATED LITIGATION PURSUANT TO RULE 500.13(a)

Amici curiae state that they are not aware of any related litigation.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Other Authorities

INTERESTS OF AMICUS CURIAE

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C., established in 1994 to protect privacy, freedom of expression, and democratic values in the information age. EPIC regularly participates as amicus curiae in cases concerning emerging privacy issues, the Fourth Amendment, and searches of digital devices and data. (*See e.g.* brief of Amici Curiae EPIC et al. in *United States v Chatrie*, 136 F4th 100 [4th Cir 2025], *cert granted* 2026 WL 120676 [Jan 16, 2026, No. 25-112]; brief of Amici Curiae EPIC et al. in *Carpenter v United States*, 585 US 296 [2018]; brief of Amici Curiae EPIC et al. in *Riley v. California*, 573 US 373 [2014]; brief of Amicus Curiae EPIC in *O.W. v Carr*, 172 F4th 337 [4th Cir 2026]).

The Legal Aid Society ("LAS") is a nonprofit New York corporation. The organization has provided free legal services to low-income families and individuals since 1876. As the primary public defender in New York City, LAS employs over 800 public defenders and provides representation to thousands of people arrested and accused of crimes every year. LAS has appeared before the New York Court of Appeals, the New York Appellate Divisions, the United States Supreme Court, and other courts to represent its clients and as amicus curiae on issues that affect its clients and their communities.

In 2013, LAS established its Digital Forensics Unit in recognition of the growing use of digital evidence in the criminal legal system. The Unit consists of

two digital forensics labs, digital forensics analysts, and digital forensics attorneys who maintain expertise in digital forensics developments. Besides assisting public defenders with digital forensics and electronic surveillance issues in their cases, the Unit works to educate attorneys, judges, and the general public on issues related to digital forensics, electronic surveillance, and privacy. The Digital Forensics Unit regularly performs extractions of digital devices and has an acute understanding of how forensic tools function.

The American Civil Liberties Union ("ACLU") is a nationwide, nonprofit, nonpartisan organization dedicated to the principles of liberty and equality embodied in federal and state constitutions. 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 *Carpenter v United States*, 585 US 296 [2018] (counsel); *Riley v California*, 573 US 373 [2014] (amicus); *United States v Hasbajrami*, 945 F3d 641 [2d Cir 2019] (amicus); *United States v Ganias*, 824 F3d 199 [2d Cir 2016 en banc] (amicus); *People v Hughes*, 506 Mich 512, 958 NW2d 98 [2020] (amicus); and *State v Missak*, 2025 WL 2528706, *1 [N.J. Super. Ct. App. Div. Sept. 3, 2025, No. A-2602-23] (amicus).

The New York Civil Liberties Union ("NYCLU"), the New York state affiliate of the national ACLU, is a not-for-profit, non-partisan organization with more than 120,000 members and supporters. The NYCLU's mission is to defend and promote

civil rights and liberties as embodied in the United States Constitution, the New York State Constitution, and state and federal law. This mission encompasses defending New Yorkers' rights to be free from unreasonable searches and seizures including in the digital sphere.

The Center for Democracy & Technology ("CDT") is a non-profit, non-partisan, public interest organization that, for over 30 years, has worked to promote the constitutional and democratic values of privacy, equality, free expression, and individual liberty in the digital age. CDT regularly advocates before legislatures, regulatory agencies, and the courts for policies that protect against invasive and unwarranted government surveillance.

The Electronic Frontier Foundation ("EFF") is a non-profit civil liberties organization with more than 35,000 dues-paying members. Founded in 1990, EFF represents the interests of technology users in court cases and broader policy debates surrounding the application of law to technology. EFF regularly participates both as direct counsel and as amicus in the Supreme Court, New York state courts, and other state and federal courts around the country in cases addressing the impact of novel technologies on criminal investigations and the justice system. (*See e.g. Carpenter v United States*, 585 US 296 [2018]; *Riley v California*, 573 US 373 [2014]; *People v Easley*, 38 NY3d 1010 [2022]).

If this Court reaches the question of whether the warrant here satisfied constitutional requirements, this case will have an outsized impact on New Yorkers'

privacy rights in the digital age. Amici respectfully submit this brief to provide the technical and constitutional background necessary to understand the issues present in this case.

PRELIMINARY STATEMENT

This case raises the important and timely question of whether a warrant can validly authorize the search of all files and data on a target cell phone. Given the ubiquity of cell phones in everyday life and the wide breadth of sensitive, personal information they contain, such warrants unreasonably intrude on New Yorkers' privacy rights. They are the modern incarnation of general warrants, in that they give officers limitless discretion to rummage through digital data unrelated to any particularized nexus to probable cause of a crime.

Amici curiae EPIC, LAS, ACLU, NYCLU, CDT, and EFF write to expand upon the arguments presented in Defendant-Appellant's brief by elaborating on caselaw from other jurisdictions that have considered warrants authorizing the search of all data on cell phones, and explaining how modern forensic tools allow for narrower searches of cell phones. While Respondent argues that a "threshold scan" of all data is both lawful and necessary in any cell phone search, (Resp. Br. 32, 39), this position is irreconcilable with the federal and state constitutions, and with the manner in which modern forensic tools analyze data from digital devices. Amici respectfully contend that (I) a warrant to search all data on a cell phone is the modern

equivalent of a general warrant, (II) this warrant's authorization to search all data violated constitutional requirements, and (III) forensic tools reasonably categorize and filter data, making it unnecessary for law enforcement to search through all data from a cell phone.

ARGUMENT

I. A WARRANT THAT AUTHORIZES A SEARCH OF "ALL FILES AND DATA" ON A CELL PHONE IS AN UNCONSTITUTIONAL GENERAL WARRANT.

The Fourth Amendment to the United States Constitution was crafted to guard against colonial-era writs of assistance and general warrants that "had so bedeviled the colonists" (*Stanford v Texas*, 379 US 476, 481 [1965]). These broad investigatory tools specified only a type of contraband or an offense, and permitted officers to conduct "an unrestrained search for evidence of criminal activity" (*Riley v California*, 573 US 373, 403 [2014]; *Steagald v United States*, 451 US 204, 220 [1981]). They were denounced as "the worst instrument of arbitrary power" because they placed "the liberty of every man in the hands of every petty officer" (*Stanford*, 379 US at 481).

General warrants are also prohibited under Article I, Section 12 of the New York Constitution, which goes even further than the Fourth Amendment in protecting "the search and seizure rights of citizens of New York" (*People v Harris*, 77 NY2d 434, 437 [1991]; *see also People v Weaver*, 12 NY3d 433, 445 [2009] [collecting

cases]). This Court has "not hesitated in the past to interpret article I, § 12 of the State Constitution independently of its Federal counterpart when necessary to assure that our State's citizens are adequately protected from unreasonable governmental intrusions" (*Owner Operator Ind. Drivers Assn., Inc. v. New York State Dept. of Transp.*, 40 NY3d 55, 62–63 [2023], quoting *People v Scott*, 79 NY2d 474, 496–497 [1992]).

This Court, like the United States Supreme Court, has also long recognized the risk that advances in technology will undermine constitutional protections against unconstrained searches (*See People v Washington*, 46 NY2d 116, 121–122 [1978] ["The insidiousness of electronic surveillance threatens the right to be free from unjustifiable governmental intrusion into one's individual privacy to a far greater extent than the writs of assistance and general warrants so dreaded by those who successfully battled for the adoption of the Bill of Rights"]; *Carpenter v United States*, 585 US 296, 305 [2018] ["As technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes, this Court has sought to 'assure [ ] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'"], quoting *Kyllo v United States*, 533 US 27, 34 [2001]).

That risk is especially potent in the context of cell phone searches. Modern cell phone technology was "nearly inconceivable just a few decades ago" but now

allows the majority of American adults to "keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate" (*Riley*, 573 US at 385, 395). A cell phone contains a person's communications, associations, travels, intimate photographs, information about their sexual orientation and religious habits, and much more. Today's cell phones could "just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers" (*id.* at 393). Reading a person's diary is invasive enough—let alone when it comes with photographs, videos, and location history corresponding to each page.

Thus, the search of a cell phone can reveal "[t]he sum of an individual's private life" in ways that analog searches never could (*id.* at 394). Indeed, a cell phone "not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is" (*id.* at 396–397).

Modern developments in artificial intelligence ("AI") make it even easier to derive a complete picture of the user's thoughts and movements from their cell phone data. For example, using GPS coordinates, cell tower logs, Wi-Fi pings, and geotags from a cell phone, AI tools can effortlessly map out a device owner's movements

across weeks or monthslong spans.[1] And by combining data across different messaging and social media apps, AI can build detailed contact networks, and organize the contents of private messages to reveal an individual's thoughts and communications about any given topic.[2] AI can also rapidly filter through databases of tens of thousands of photos and videos and pull up images based on categories such as "nudity," "gathering," "hotel room," and "screenshots."[3] As one vendor describes it, these tools allow police to effectively become a "fly on the wall" and snoop on any moment of the device owner's past.[4]

As discussed in Section III, when used pursuant to a constitutional warrant and with clearly articulated limits as to what is being sought, modern forensic tools can facilitate a properly targeted and reasonably limited search of a device. But unbridled discretion to search all information on a cell phone—especially when coupled with access to extraordinarily powerful AI tools—is a recipe for abuse.

---

[1] *See* Bill Goodwin, *AI Tools Offer 'Near-Real-Time' Analysis of Data from Seized Mobile Phones and Computers*, Computer Weekly [Mar. 18, 2026], https://www.computerweekly.com/news/366640352/AI-tools-offer-near-real-time-analysis-of-data-from-seized-mobile-phones-and-computers [last accessed June 24, 2026]; Cellebrite, *Pathfinder Tutorials*, YouTube [Dec. 11, 2023], at 0:05, https://www.youtube.com/watch?v=ey67StOBby4 [last accessed June 24, 2026].

[2] Cellebrite, *How to Establish a Crime Narrative in Cellebrite Pathfinder's Investigative Analytics Solution*, YouTube [Mar. 13, 2023], at 0:51, https://www.youtube.com/watch?v=tGnGPGBqWzc&t=80s [last accessed June 24, 2026].

[3] Cellebrite, *How to Use the Media Tags View in the Cellebrite Pathfinder Dashboard*, YouTube [Aug. 24, 2022], at 0:39, https://www.youtube.com/watch?v=lIu62WnUv1c&t=39s [last accessed June 24, 2026].

[4] Cellebrite, *How to Establish a Crime Narrative in Cellebrite Pathfinder's Investigative Analytics Solution*, YouTube [Mar. 13, 2023], at 1:20, https://www.youtube.com/watch?v=tGnGPGBqWzc&t=80s [last accessed June 24, 2026].

Given the vast quantity and sensitive quality of information available on a cell phone, warrants for the search of digital data must be carefully tailored to their justifications. While this Court has yet to opine on the constitutionality of "all-data" cell phone search warrants, other states' high courts have recognized that such warrants are unconstitutional general warrants.

For example, the Supreme Court of Delaware recently held that a warrant to search the defendant's cell phones for "any/all data stored" was an unconstitutional general warrant (*Taylor v State*, 260 A3d 602, 609, 616 [Del 2021]). Although the text of the warrant in *Taylor* included examples of information to be searched and referenced "any other information/data pertinent to this investigation within said scope," and the affidavit referenced the dates of the alleged crimes, the court held that the warrant's authorization to search "any and all data" rendered the warrant unlimited (*id.* at 609, 610, 616). The court reasoned that, instead of limiting the search to "data tied specifically to the probable cause supporting the warrant," (*id.* at 616), the warrant "allowed investigators to conduct an unconstitutional rummaging through all of the contents of [the defendant's] smartphones to find whatever they decided might be of interest to their investigation" (*id.* at 615; *see also Terreros v. State*, 312 A3d

651, 664–66 [Del. 2024] (discussing several other cell phone search warrants that the court treated as unconstitutional general warrants)).

The Michigan Supreme Court has also rejected the government's argument that it is always reasonable to review all data on a digital device, because that rule would "rehabilitate an impermissible *general warrant* that 'would in effect give police officers unbridled discretion to rummage at will among a person's private effects'" (*People v Hughes*, 506 Mich 512, 958 NW2d 98, 117–118 [2020], quoting *Riley*, 573 US at 399 [cleaned up]).

As the cases above illustrate, warrants to authorize the search of all data on a cell phone are contrary to the purposes of the federal and state constitutions. Instead, a warrant to search a cell phone "must specify the particular items of evidence to be searched for and seized from the phone and be strictly limited to the time period and information or other data for which probable cause has been properly established through the facts and circumstances set forth under oath in the warrant's supporting affidavit." (*Burns v United States*, 235 A3d 758, 773 [DC 2020]). A warrant authorizing a search of *all data* on a cell phone is not so limited and therefore cannot issue consistent with the federal and state constitutions.

II. THE WARRANT'S AUTHORIZATION TO SEARCH "ALL FILES AND DATA" RENDERS IT OVERBROAD, INSUFFICIENTLY PARTICULAR, AND UNCONSTITUTIONALLY UNREASONABLE.

A. The warrant's authorization to search all data on the target phone exceeds the probable cause on which it is based and renders it unconstitutionally overbroad.

The warrant at issue here unambiguously orders a search of "all files and data stored in the TARGET DEVICE," (Appendix 58), without probable cause to believe that *all files and data* on the phone constitute evidence of the alleged crimes. In fact, the affidavit provides no reason to believe that Mr. Morris used the target phone in connection with the alleged criminal activity—let alone that he used the phone *only* for that purpose, or that illegality pervaded every corner of the device (*Cf. Voss v Bergsgaard*, 774 F2d 402, 406 [10th Cir. 1985] ["Even if the allegedly fraudulent activity constitutes a large portion, or even the bulk, of the NCBA's activities, there is no justification for seizing records and documents relating to its legitimate activities."]).

While police who are "engaged in the often competitive enterprise of ferreting out crime," (*Johnson v United States*, 333 US 10, 14, [1948]), might wish to exhaustively search every part of a cell phone that has a remote possibility of containing evidence, the federal and state constitutions protect individuals against such overbroad, indiscriminate searches (*See Maryland v Garrison*, 480 US 79, 84

[1987] [The Fourth Amendment requires that warrants be limited to "the specific areas and things for which there is probable cause to search," such that the search is "carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit"]; *People v Gordon*, 36 NY3d 420, 432 [2021] ["[T]he permissible 'scope of [a] search has been carefully limited' by the requirement for probable cause and a particular description of the subjects to be searched"], quoting *People v Dumper*, 28 NY2d 296, 299 [1971]). Thus, "a warrant for the search of the contents of a cell phone must be sufficiently limited in scope to allow a search of only that content that is related to the probable cause that justifies the search" (*State v Henderson*, 289 Neb 271, 854 NW2d 616 [2014]).

The "constitutional infirmity" of a warrant to search all data on a cell phone lies in its authorization to search files for which there is no probable cause (*see Gibbs v United States*, 355 A3d 206, 219 [DC 2026]). Given the sheer quantity of data stored on a phone, most of it will be unrelated to the particular crime under investigation. Thus, even if officers do not know "exactly" where the evidence they seek will be located, they must still limit the search to include only those applications, filetypes, and timeframes for which there is probable cause to search (*see id.* ["we can say with some certainty that [officers] would not find evidence of a stabbing on say: [the defendant's] Southwest Airlines application, the Uber

application, the Amazon application, or any of the various applications without a messaging function that are stored on his phone"]). The mere possibility that evidence might exist in unexpected locations on a cell phone does not provide probable cause to search the entire phone.

While Respondent argues that investigators needed to search the entire device to confirm the absence of malware "so as to rebut any claim that the data on the device was inserted by malicious software or a third party" (Resp. Br. 42), the affidavit provides no reason to believe that the device contained any malware, and it provides no case-specific facts indicating that files on the phone might have been maliciously inserted. Should such probable cause develop, law enforcement could easily seek another warrant to search the extraction of the device for malware. But a preemptive, unrestricted search of all data is unreasonable. Permitting officers to review all data on a cell phone simply because it is *possible* that data was maliciously inserted or distorted "would effectively nullify the particularity requirement of the Fourth Amendment" (*Hughes*, 958 NW2d at 117–118).

Respondent has also attempted to justify the overbroad search by asserting that it is "impossible to know in advance all the unique words or phrases investigative subjects will use in their records and communications" (Appendix 55). A warrant need not prescribe which keywords officers should use to conduct the search, and it

need not limit officers to a single search methodology. But it must particularly describe the things to be seized.

A warrant that authorizes a search for all data effectively permits any type of search using any filters or search terms. The federal and state constitutions do not condone such unrestrained rummaging.

The unfortunate reality is that there may not be a *definitive* way to ensure that any given cell phone search will turn up *all* relevant evidence. But that is true in traditional searches, too. An officer cannot definitively know that they have uncovered every piece of evidence in a house without exhaustively searching every inch of every room, closet, and cupboard. Even so, "probable cause to believe that a stolen lawnmower may be found in a garage will not support a warrant to search an upstairs bedroom" and "[p]robable cause to believe that a container placed in the trunk of a taxi contains contraband or evidence does not justify a search of the entire cab" (*United States v Ross*, 456 US 798, 824 [1982]). That is not because it is impossible to find a lawnmower in an upstairs bedroom, or contraband in other parts of the cab. It is because the Fourth Amendment balances the need for evidence against individual privacy and the evils of overbroad warrants; the probability that the evidence sought will actually be found in the place to be searched must be high enough to render the state intrusion constitutionally reasonable. By authorizing a

search of all data on Mr. Morris's phone, the warrant here extended the scope of the search far beyond any probable cause to support it.

B. The warrant's authorization to search all data on the phone violates the particularity requirement, because it leaves the executing officers with discretion to decide which places to search and which items to seize.

Manually searching all data on a modern cell phone is practically impossible. The Supreme Court of the United States recognized cell phones' "immense storage capacity" over a decade ago, when the top-selling smart phone's standard capacity was 16 gigabytes—and was available with up to 64 gigabytes of storage (*Riley*, 573 US at 393–394). Modern smartphones can now store between 64 gigabytes and 2 terabytes of data—thirty-one times more than the devices contemplated in *Riley*.[5] That is more than 15,000 photographs,[6] 12,000 songs,[7] or 64 million 100-character text messages.[8] These numbers will only grow. Forensic tools allow examiners to filter and sort massive amounts of data so that they need not manually search through everything (*see* Section III, *supra* at 21).

---

[5] Kathleen Walsh, *How Many GB Do I Need on My iPhone: Storage Sizing Guide*, Simply Mac [Oct. 8, 2025], https://www.simplymac.com/iphone/how-many-gb-do-i-need-on-my-iphone [last accessed June 24, 2026].

[6] Travis Sharrow, *Unlocking the Magic: Discover How Many iPhone Pictures 64GB Can Store*, Soft Hand Tech [Mar. 17, 2025], https://softhandtech.com/how-many-iphone-pictures-can-64gb-hold/ [last accessed June 24, 2026].

[7] John Elmore, *How Much Is 64GB of Music?* The Techy Life [Apr. 14, 2024], https://thetechylife.com/how-much-is-64gb-of-music/ [last accessed June 24, 2026].

[8] *See* Voye Global Team, *How Much Data iMessage Uses and How to Check Your Usage*, Voye Global [Mar. 17, 2025], https://voyeglobal.com/how-much-data-does-imessage-use/ [last accessed June 24, 2026].

A warrant that authorizes the search of *everything* on a cell phone—even though such a search is entirely impracticable—effectively leaves officers to decide for themselves where to search and what to search for. That discretion is precisely what the particularity requirement forbids: "[T]he Fourth Amendment requires that the Judge's directive be specific enough to leave no discretion to the executing officer" (*People v Darling*, 95 NY2d 530, 537 [2000]). A warrant must be specific enough that the examiners know what to look for, such that "it is the magistrate, and not the police officer, who determines the scope of the search conducted pursuant to a warrant" (*Gordon*, 36 NY3d at 433; *see also People v Potwora,* 48 NY2d 91, 94 [1979] ["With its origins in the Colonials' abhorrence of the general warrant and writ of assistance, the warrant requirement of the State and Federal Constitutions was designed to interpose 'the detached and independent judgment of a neutral Magistrate' between police officers and citizenry" (quoting *People v Hanlon*, 36 NY2d 549, 558 [1975])]).

For these reasons, several other states have invalidated warrants that authorize a search of all data on a cell phone. For example, recognizing "the magnitude of the privacy interests at stake" in a cell phone search, the Michigan Supreme Court noted that it "must jealously guard the requirements of the Fourth Amendment, including the particularity requirement." (*People v Carson*, 2025 WL 2177501, *5, 8 [Mich July 31, 2025, No. 166923]). A warrant that authorized the search of "any and all

data" on a cell phone lacked "instruction on the scope, breadth, or focus of the search," and thus failed to "sufficiently inform an executing officer how to reasonably conduct a limited and constitutionally particular search" (*id.* at *8).

The Nebraska Supreme Court similarly recognized that "the privacy interests at stake in a search of a cell phone" demand sensitivity to the particularity requirement (*State v Henderson*, 854 NW2d at 633). Although the warrants at issue in *Henderson* "listed types of data, such as cell phone calls and text messages," the court held that they violated the particularity requirement by authorizing a search of "[a]ny and all information" on the devices. (*Id.* at 290).

The Delaware Supreme Court likewise recognized that "warrants issued to search electronic devices call for particular sensitivity given the 'enormous potential for privacy violations' that 'unconstrained searches of cell phones' pose" (*Buckham v State*, 185 A3d 1, 18 [Del 2018], quoting *Wheeler v State*, 135 A3d 282, 299 [Del 2016]). The court thus invalidated a warrant authorizing a search of "'[a]ny and all store[d] data contained within the internal memory of the cellular phones [sic], including but not limited to, incoming/outgoing calls, missed calls, contact history, images, photographs and SMS (text) messages' for evidence of 'Attempted Murder 1st Degree'" (*id.* at 15, 18).

Several other states have followed the same logic. (*See Richardson v State*, 481 Md 423, 282 A3d 98, 120 [2022] ["With respect to most cell phone search

warrants, given the privacy interests at stake as explained in *Riley*, the particularity requirement is not satisfied by authorizing officers to search for any and all items that are evidence of a particular crime or crimes."]; *State v Correa*, 353 Conn 338, 341 A3d 910, 914, 920–921 [2025] [warrant authorizing a search of "all data" on defendant's phone "including, but not limited to, all call logs of calls placed and received, [short message service (SMS)] and [multimedia message service (MMS)] [t]ext messaging, telephone numbers stored, address book, calendar, email, video files, and graphic files" violated Fourth Amendment]; *see also United States v Otero*, 563 F3d 1127, 1132 [10th Cir 2009] ["Wisely, the government does not contest that a warrant authorizing a search of 'any and all information and/or data' stored on a computer would be anything but the sort of wide-ranging search that fails to satisfy the particularity requirement."]). This Court should do the same.

C. The warrant's authorization to search all data is unconstitutionally unreasonable.

In addition to probable cause and particularity, reasonableness is an independent requirement under the Fourth Amendment and Article I, section 12 (*see Winston v Lee*, 470 US 753, 767 [1985] ["the Fourth Amendment's command that searches be 'reasonable' requires that when the State seeks to intrude upon an area in which our society recognizes a significantly heightened privacy interest, a more substantial justification is required to make the search 'reasonable.'"]; *United States v Koyomejian*, 970 F2d 536, 550 [9th Cir 1992] [Kozinski, J., concurring]

["[R]easonableness is an independent requirement of the Fourth Amendment, over and above the Warrant Clause requirements of probable cause and particularity."]; *United States v Torres*, 751 F2d 875, 883 [7th Cir. 1984] ["[A] search could be unreasonable, though conducted pursuant to an otherwise valid warrant, by intruding on personal privacy to an extent disproportionate to the likely benefits from obtaining fuller compliance with the law."]; *People v Nieves*, 36 NY2d 396, 402 [1975] [referring to reasonableness as a warrant's "ultimate mandate"]).

In order to assess whether a search is constitutionally reasonable, the Court must first assess the degree of intrusiveness of the proposed search. In determining how intrusive the search of a cell phone is, it is telling that the Supreme Court of the United States observed that searches of cell phones generally reveal more private information than the search of a home (*Riley*, 573 US at 396–397). Today, the intrusion surpasses even the most thorough search of the body, as the rise of medical, workout, and other health-related apps has led to the collection and storage of voluminous physiological data on cell phones (*See Taylor v State*, 260 A3d 602, 613, 614 [Del. 2021] (recognizing that the "scope and intimacy of the information" at issue in a cell phone search necessitates "greater protections than other forms of property"). Cell phones now commonly contain a person's heart rate, skin

conditions, weight, menstrual cycle, and more.[9] This information, combined with our most intimate thoughts, musings, and location, provides a complete picture of our minds and bodies. An intrusion into our digital anatomy thus must be justified with a public need of utmost importance (*cf. Winston v Lee*, 470 US 753, 759 [1985] ["A compelled surgical intrusion into an individual's body for evidence . . . implicates expectations of privacy and security of such magnitude that the intrusion may be 'unreasonable' even if likely to produce evidence of a crime."]).

In the modern era, a search of *all* files and data on a cell phone is one of the most intrusive searches that can be conducted. The affidavit in this case describes a brief incident unconnected to any phone use. It does not come close to justifying an intrusion of such magnitude.

[9] *See e.g.*, *Best Free Heart Rate Monitor Apps for Android and iOS (2025 Edition)*, Impulse, https://heartwellness.app/knowledge/heart-rate-monitor-app [last accessed June 24, 2026]; Shannon Wongvibulsin et al., *Current state of dermatology mobile applications with artificial intelligence features*, JAMA Dermatology 160.6, 646-650 [June 2024]; Rahul Verma, *10 Best Weight Tracker Apps for Android & iOS (2026)*, Tech Dator [Apr. 21, 2026], https://techdator.net/best-weight-tracker-apps/ [last accessed June 24, 2026]; Emile Radyte, *The 5 Best Period Tracking Apps to Try in 2026*, Samphire [Oct. 17, 2025], https://www.samphireneuro.com/en-us/blog/best-period-tracking-apps?srsltid=AfmBOopTGqWqLq_rtdZnkMVcdtd0SzVqaF1znt6RjcwbJVyTj8lbBIY1 [last accessed June 24, 2026]; Jason Koebler, *Internet of Shit: AI Poop Analysis App Offered to Sell Me Database of Its Users' Poops*, 404 Media [May 14, 2026], https://www.404media.co/ai-poop-analysis-app-offered-to-sell-me-access-to-its-users-poops/ [last accessed June 24, 2026].

III. FORENSIC TOOLS FACILITATE TARGETED SEARCHES SO THAT OFFICERS NEED NOT SEARCH THROUGH ALL DATA FROM A CELL PHONE.

Respondent contends that, to the extent the warrant authorized a search of all of the data on the cell phone, it authorized a "threshold scan" that was "necessary to isolate the materials that are responsive to the [warrant]" (Resp. Br. 32). While it is not entirely clear what Respondent means by "scan," Respondent appears to suggest that, after law enforcement has extracted or copied all the data from a cell phone, officers must manually search through everything "to identify the specific categories of evidence enumerated in and authorized by the warrant" (*Id.* at 40). However, such a search of all data is not necessary. Law enforcement conducts cell phone searches using forensic tools that are specifically designed to seize all data and automatically sort the data into categories such as messages, audio, images, videos, web history, etc.[10] The tools permit examiners to select relevant categories of data and further filter the data within those categories to target evidence for which there is probable cause.[11] With these tools, law enforcement need not review or "scan" all of the device's data.

---

[10] The facts in this section are based on Amici's knowledge and experience with forensic tools, as well as the online sources cited.

[11] *See e.g. State v Smith*, 344 Conn 229, 278 A3d 481, 501 n 14 [2022] ("Cellebrite software was used to extract data from the defendant's cell phone and categorized it into separate 'container file[s]' by placing, for example, text messages into a text messages folder and

Forensic tools facilitate searches in two phases: extraction and analysis. In the extraction phase, forensic tools make an exact copy of the data on the device. The purpose of the extraction is to preserve the data in its original form and avoid altering or damaging the data on the device itself.[12]

Different types of extractions copy different amounts and types of data. A *full file system extraction* copies all files in the device's memory, and includes files hidden from users themselves. A *logical extraction* copies a more limited set of data and typically includes only those files that a user would be able to view on their device.[13] Some forensic tools allow for *category extractions* to copy even more limited sets of data—for example, the tools could extract only communication data, multimedia files, and location information from the device.[14]

After the extraction is complete, forensic tools allow examiners to analyze the extracted data. The tools automatically sort the extracted data into different categories so that examiners can limit their search to those categories of data

---

call logs into a call logs folder."); Logan Koepke et al., *Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones* 24, Upturn [Oct. 21, 2020], https://www.upturn.org/static/reports/2020/mass-extraction/files/Upturn%20-%20Mass%20Extraction.pdf [last accessed June 24, 2026].

[12] *See* n 11 Logan Koepke et al. at 13–16, *supra*; *see generally* Cellebrite Digital Intelligence Glossary, https://cellebrite.com/en/glossary/ [last accessed June 24, 2026].

[13] *See* n 11 at 15, *supra*.

[14] *See e.g. What Lies Beneath: An Investigator's Guide to Magnet Graykey Category Extractions*, Magnet Forensics [May 15, 2023], https://www.magnetforensics.com/blog/an-investigators-guide-to-magnet-graykey-category-extractions/ [last accessed June 24, 2026].

specified in the warrant. *See Smith*, 278 A3d at 501 n 14. As shown below, an examiner could limit their search to images, messages, or web history:

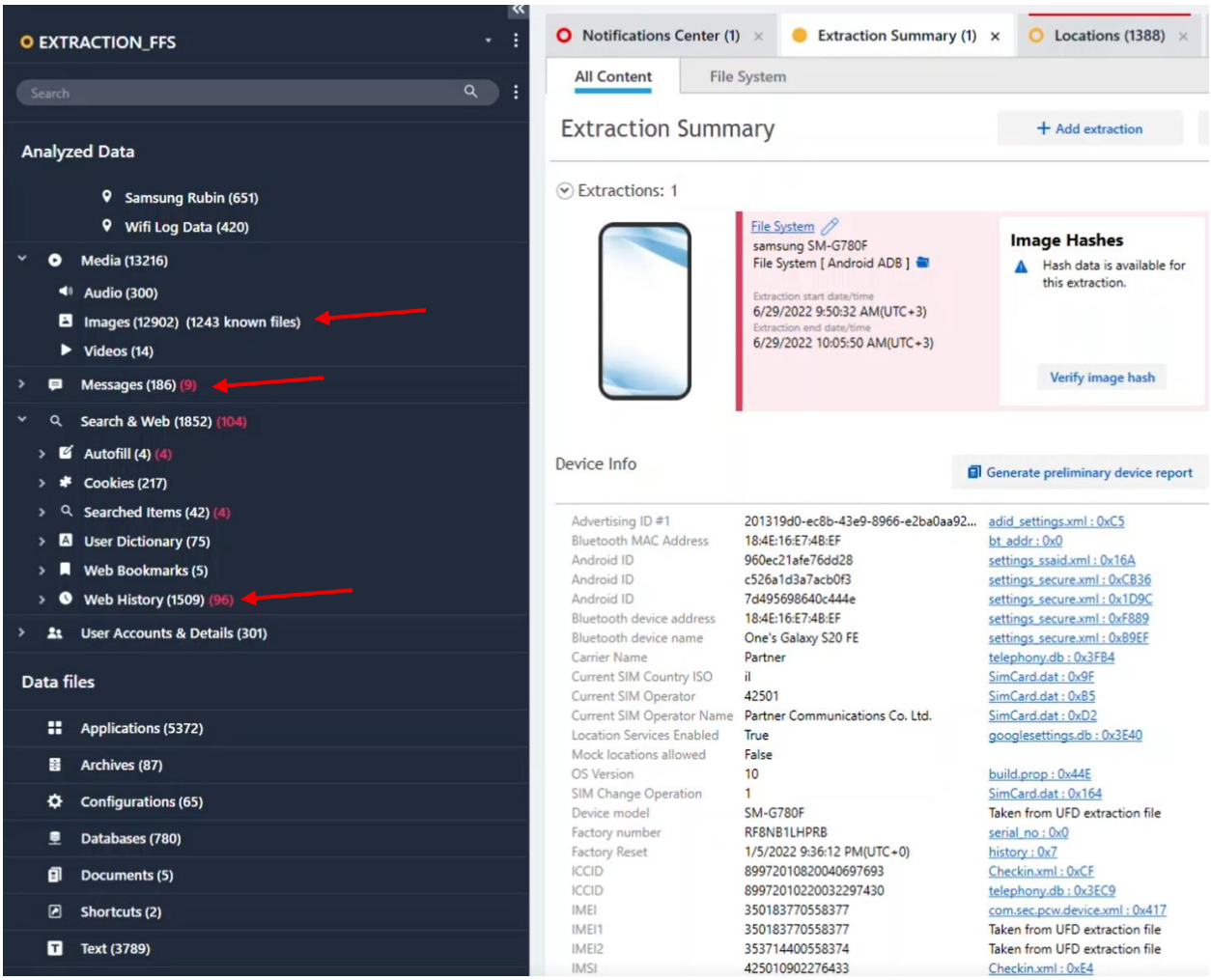

Image 1: Cellebrite's extraction summary[15]

[15] Heather Mahalik, *2 Ways to Get Cellebrite Reader and Share Findings with the Investigative Team*, Video at 0:11, Cellebrite [Mar. 7, 2023], https://cellebrite.com/en/series/tip-tuesday/2-ways-to-get-cellebrite-reader-to-share-findings-with-the-investigative-team/ [last accessed June 24, 2026].

Furthermore, the tools contain myriad ways of filtering the data beyond their automatic categorizations. For example, the tools permit examiners to select a particular time period and review data only in that range. The timeline feature in Cellebrite Physical Analyzer, one of the main forensic tools, is shown below. In this example, the examiner limited their search to the web history category, and then further filtered the data to show only web history from October 1 through October 31, 2021.

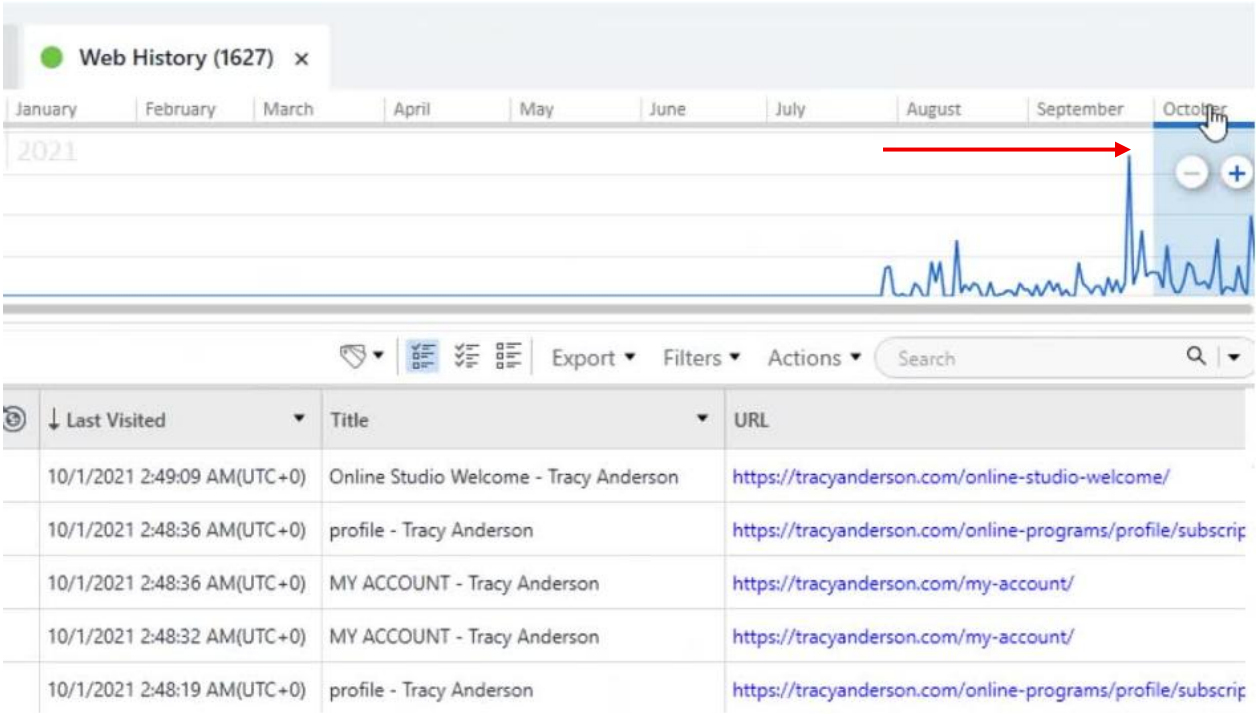

Image2: Cellebrite's timeline feature[16]

[16] Cellebrite, *Timeline Graph inside of Physical Analyzer* at 0:11, Facebook [Nov. 15, 2021], https://www.facebook.com/reel/231504808915170 [last accessed June 24, 2026].

Forensic tools also permit examiners to limit image searches, restricting analysis exclusively to images from certain spans of time, or for particular illicit files.[17] For example, in investigations for child sexual abuse material ("CSAM"), forensic tools can isolate CSAM by comparing image and video files in the extraction to existing collections of known CSAM. This is accomplished using sources like Project VIC, which identify CSAM, process the CSAM using a hash function, which outputs a string of characters unique to that individual file, and then compiles those strings of characters ("hash values") for forensic tools to use.[18] The tools compare those hash values compiled by Project VIC to the hash values of image and video files from the device extraction in order to isolate known CSAM.

[17] *See e.g.* Heather Mahalik, *Images and Export Options in Cellebrite Physical Analyzer*, Video at 0:51, Cellebrite [Feb. 8, 2022], https://cellebrite.com/en/series/tip-tuesday/images-and-export-options-in-cellebrite-physical-analyzer/ [last accessed June 24, 2026].
[18] *See generally Get Project Vic Hashes*, Project VIC, https://www.projectvic.org/get-hashes [last accessed June 24, 2026].

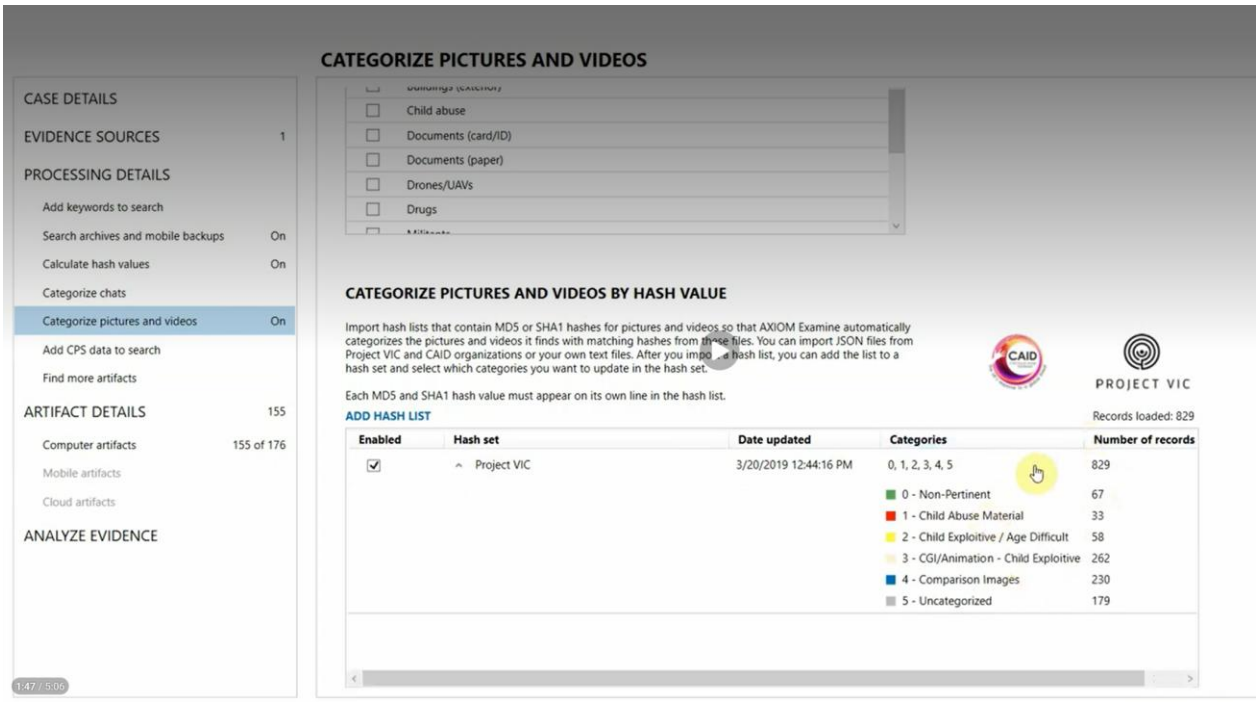

Image 1: Using Project VIC in Magnet Axiom to identify CSAM[19]

Forensic tools also permit examiners to restrict their search to files containing particular keywords. For example, an examiner searching for a document referencing an employee named Jody could limit the scope of their search not only to documents, but to documents that contain the words "employee" and "jody," as shown in the example below.

[19] Resource Center, *Overhauling Media Categorization in Magnet AXIOM 3.0 with New Project VIC/CAID Features*, Video at 1:46, Magnet Forensics, https://www.magnetforensics.com/resources/overhauling-media-categorization-in-magnet-axiom-3-0-with-new-project-vic-caid-features/ [last accessed June 24, 2026].

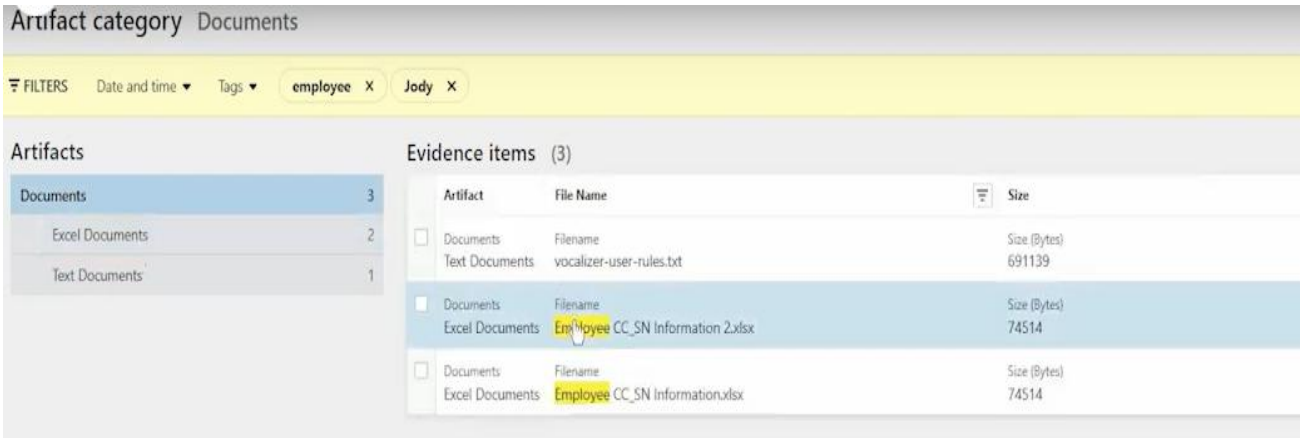

Image 4: Magnet Review's Keyword Search[20]

The affidavit in this case asserts that keyword searches are insufficient to capture information from non-text data, and that "there often are many communications that are responsive and relevant to an investigation that do not contain any keyword that law enforcement personnel are likely to know in advance to search for." (Appendix 55). But forensic tools are constantly adapting to meet the needs of modern investigators. Cellebrite uses optical character recognition on photos, so that a keyword search would turn up any photos that contained the word in them. Regardless, any technical limitations of the tools do not obviate the need to comport with constitutional requirements.

As the examples above show, forensic tools permit examiners to limit digital searches to the relevant categories of information, and to further filter within those

[20] Resource Center, *Exploring the New User Interface Features in Review 5.0*, Video at 3:31, Magnet Forensics, https://www.magnetforensics.com/resources/exploring-the-new-user-interface-features-in-review-5-0/ [last accessed June 24, 2026].

categories to target relevant data and decrease the amount of nonresponsive data that examiners search. To be sure, these mechanisms are not perfect. Just as an individual officer searching an apartment might not see *every* piece of relevant evidence, a forensic tool might not perfectly filter for *every* relevant file. But examiners must still conduct their searches and seizures in a way that comports with constitutional requirements, and modern forensic tools can help with that. To the extent officers are unsatisfied with tools' capabilities, they may adopt other tools or rely more heavily on other investigative practices. But they are not permitted to conduct a search whose scope is broader than the probable cause on which it was based, or whose parameters are insufficiently particularized.

The warrant in this case first authorizes an extraction of all electronically stored information on Mr. Morris's device. (Appendix 57–58). The authorization for an extraction of the full device is not at issue in this case. What is at issue is the warrant's subsequent authorization to "search . . . all files and data" extracted from the device. (*Id.*). That search of all extracted data allowed law enforcement to ignore the forensic tool's categorizations and filters. Instead of limiting the search to data of certain types and from certain time periods, the warrant instead authorizes law enforcement to search *everything*. Respondent's reference to this search as a "scan" does not change its unrestricted character—it still leaves an impermissibly broad class of data (*all* of it) subject to review and analysis.

Modern forensic tools can narrow the scope of the search by allowing examiners to select particular categories of data to search and then further filter for items within those categories for which there is probable cause. The availability of these tools makes searching all data on a cell phone all the more unreasonable.

CONCLUSION

For the foregoing reasons, this Court should hold that, in the absence of probable cause to believe that each and every file on a phone is evidence of the crime under investigation, warrants cannot constitutionally authorize a search of all data on a cell phone.

Dated: June 25, 2026
New York, NY

Respectfully submitted,

/s/ Laura Moraff

(Counsel listed on following page)

Laura Moraff
Brett Max Kaufman
Nathan Freed Wessler
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Tel.: (212) 549-2500
lauramoraff@aclu.org

Daniel R. Lambright
NEW YORK CIVIL LIBERTIES UNION FOUNDATION
125 Broad St., 19th Floor
New York, NY 10004
Tel.: (202) 607-3300
dlambright@nyclu.org

Jeramie Scott
Thomas McBrien
ELECTRONIC PRIVACY INFORMATION CENTER
1519 New Hampshire Ave. NW
Washington, DC 20036
Tel.: (202) 483-1140
scott@epic.org

Jerome D. Greco
THE LEGAL AID SOCIETY
49 Thomas Street
New York, NY 10013
Tel.: (212) 298-3075
jgreco@legal-aid.org

Counsel for Amici Curiae

CERTIFICATE OF COMPLIANCE

Pursuant to Part 500.1(j)(1) and Part 500.13(c)(1) of the Rules of Practice of the Court of Appeals, State of New York, the undersigned attorney for Amici curiae hereby certifies that this Brief was prepared on a computer; that Times New Roman, a 14-point proportionally spaced typeface, was used; that the body of the brief is double-spaced, with 12-point single spaced footnotes; and that, according to the Microsoft Word Processing System used, the total number of words in the brief, inclusive of point headings and footnotes and exclusive of pages containing the Table of Contents, the Table of Authorities, Disclosure Statement, Proof of Service, and Certificate of Compliance is 6,305.

Dated: June 26, 2026
New York, NY

Respectfully submitted,

/s/ Laura Moraff