Received 4/7/2021 10:24:24 AM Supreme Court Middle District

IN THE SUPREME COURT OF PENNSYLVANIA
MIDDLE DISTRICT

No. 6 MAP 2021

COMMONWEALTH OF PENNSYLVANIA,
Appellee,

v.

ERIC LAVADIUS GREEN
Appellant.

Brief *Amicus Curiae* of Upturn, Inc. in Support of Appellant

Appeal from the order of the Superior Court of Pennsylvania entered February 12, 2019 at No. 242 MDA 2018

Jim Davy, I.D. No. 321631
ALL RISE TRIAL & APPELLATE
P.O. Box 15216
Philadelphia, PA 19125
609-273-5008
jimdavy@allriselaw.org

Counsel for Amicus Curiae

DATE FILED: April 7, 2021

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Constitutional Provisions

Other Authorities

STATEMENT OF INTEREST OF *AMICUS CURIAE*

Upturn, Inc. ("Upturn") is a nonprofit organization based in Washington, D.C. that works in partnership with many of the nation's leading civil rights and public interest organizations to advance equity and justice in the design, governance, and use of technology. One of Upturn's priorities is to ensure that technology does not exacerbate or entrench mass incarceration and racial inequity in the criminal legal system. Upturn has two key interests in this case: the case involves how law enforcement use mobile device forensic tools to search cellphones, and how laws will safeguard Pennsylvanians from general digital searches.

Amicus has unique expertise on these matters. On October 21, 2020 Upturn published *Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones*.[1] This report is the most comprehensive examination of law enforcement's use of mobile device forensic tools to date. Mobile device forensic tools, such as the Cellebrite tool used in this case, are a powerful technology that allow law enforcement to extract and programmatically search a full copy of data from a cellphone.

Mass Extraction documents the widespread adoption of mobile device forensic tools by law enforcement in the United States. Based on more than 110

[1] Logan Koepke, Emma Weil, Urmila Janardan, Tinuola Dada, Harlan Yu, *Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones*, Upturn, October 21, 2020, *available at* https://www.upturn.org/reports/2020/mass-extraction/.

public records requests, more than 12,000 pages of documents, and more than two years of research, the report documents the widespread proliferation and use of this technology by state and local law enforcement agencies.[2] More than 2,000 agencies have purchased these tools, in all 50 states and the District of Columbia.[3] State and local law enforcement agencies have performed hundreds of thousands of cellphone extractions since 2015, often without a warrant.[4] Few departments have detailed policies governing when and how officers can use this technology.[5] Most either have boilerplate policies that accomplish little, or have no policies in place at all.[6] The report also documents the existing technical capabilities of today's mobile device forensic tools,[7] finding that the tools provide sweeping access to personal information on a phone.[8]

This Brief aims to aid the Court in its understanding of how mobile device forensic tools work, how law enforcement typically use these tools, and how mobile device forensic tools could be used to narrow the search of a cellphone. This Brief

[2] Every document Amicus received from state and local law enforcement agencies in response to these public records requests is publicly available. Those documents are accessible here: https://www.documentcloud.org/app?q=project%3Adevice-search-200411%20&page=1.

[3] *Mass Extraction* (2020), 31-39.

[4] *Id.*, 40-48.

[5] *Id.*, 48-57.

[6] *Id.*

[7] *Id.*, 10-31.

[8] In order to assess the technical capabilities of current mobile device forensic tools, *Amicus* examined technical manuals, software release notes, marketing materials, webinars, and digital forensics blog posts and forums. *Amicus* also consulted with one of the few public defenders in the U.S. with these forensic tools (and forensic staff) in-house.

explains how cellphone search warrants issued across the country — such as the search warrant in this case — are far broader in scope than is constitutionally permissible, but mobile device forensic tools and appropriate legal rules and safeguards can help narrow cellphone searches.[9]

[9] *Amicus* certifies, pursuant to Pa. R.A.P. 531(b)(2), that no person or entity, other than amicus, their members, or their counsel, made a monetary contribution to the preparation or submission of this brief, nor authored this brief in whole or in part.

ARGUMENT

Every day, law enforcement agencies across the country search hundreds to thousands of cellphones. To search these phones, law enforcement frequently rely upon mobile device forensic tools (MDFTs). An MDFT is a computer program and its hardware (*e.g.*, cables and external storage) that can copy and analyze data from a cellphone or other mobile device. MDFTs can be incredibly invasive. As one expert puts it, with the amount of sensitive information stored on smartphones today, MDFTs provide law enforcement a "window into the soul."[10]

MDFTs used by law enforcement have three key features. First, the tools allow law enforcement to access and extract information from cellphones. Second, the tools organize extracted data in an easily navigable and digestible format for law enforcement to more efficiently explore and analyze the data. Third, the tools help law enforcement circumvent most security features in order to copy data. By physically connecting a cellphone to a forensic tool, law enforcement can extract, analyze, and present data that's stored on the phone.

Law enforcement agencies of all sizes across the United States have purchased tens of millions of dollars' worth of MDFTs. Since 2015, state and local law enforcement agencies have performed hundreds of thousands of cellphone

[10] C.M. "Mike" Adams, "Digital Forensics: Window Into the Soul," *Forensic*, June 10, 2019, *available at* https://www.forensicmag.com/518341-Digital-Forensics-Window-Into-the-Soul/.

extractions using MDFTs. Law enforcement use these tools not only to investigate cases involving serious harm, but also for offenses like graffiti, shoplifting, marijuana possession, prostitution, vandalism, car crashes, parole violations, untaxed cigarettes, petty theft, and public intoxication.[11]

As the Supreme Court observed in *Riley*, given the storage capacity of modern cellphones and the different kinds of data stored on a phone, "the sum of an individual's private life can be reconstructed." *See Riley v. California*, 573 U.S. 373, 394 (2014). Critically, this concern — that the quantity and quality of data on a phone is so sensitive it can effectively reconstruct one's life — does not even consider the additional power of tools or methods used to conduct a search.

But there are critical differences between a manual search of a cellphone and a forensic search of a cellphone using an MDFT.

First, a search using an MDFT is more invasive than a manual search because it extracts substantially more data. MDFTs give an investigator access to not only quantitatively much more data than could be manually seized and inspected, but also entire categories of data that are not often accessible from the phone's user interface. For example, manual searches cannot easily surface certain data, like geolocation data, deleted data, application metadata (such as when a user last opened a specific application), or internet search history, but MDFTs can. Second, MDFTs are vastly

[11] *Mass Extraction* (2020), at 42.

more efficient than manual searches, substantially changing the feasibility of searches. While an investigator could manually search through each photo to look for someone, or scroll through messages to look for a specific conversation, MDFTs can automate the search process and filter out unwanted information. These differences enable "an extent of surveillance that in earlier times would have been prohibitively expensive." *See United States v. Garcia*, 474 F.3d 994, 998 (7th. Cir. 2007).

In *Amicus*' view, the proliferation of these tools represents a dangerous expansion in law enforcement's investigatory powers. Forensic searches of cellphones were not common practice a decade ago — but *Amicus*' research clearly demonstrates that today, every American is at risk of having their entire private life reconstructed by law enforcement, based on a forensic search of their cellphone.

Additionally, search warrants for digital evidence tend to be so broad that they permit law enforcement to search the entire contents of a cellphone. Even with language that seems to narrow their scope, such as authorizing only the search of evidence relating to an offense or listing of all the data to be seized, these search warrants often permit an unrestricted search of a cellphone.

Importantly, today's mobile device forensic tools could be used to narrow the search of a cellphone. But a technical possibility means little without the force of the law. Absent intervention by this Court, mobile device forensic tools will facilitate indiscriminate searches of cellphones that fundamentally sit at odds with the protections of the Fourth Amendment and Article I, Section 8 of the Pennsylvania Constitution.

I. How mobile device forensic tools enable law enforcement to search cellphones.

Mobile device forensics is typically a two-step process: data extraction, then analysis. MDFTs help law enforcement accomplish both. MDFT software can run on a regular desktop computer, or on a dedicated device like a tablet or a "kiosk" computer. These tools are sold by a range of companies, including, but not limited to, AccessData, Cellebrite, Grayshift, Magnet Forensics, MSAB, and OpenText. Based on *Amicus*' research, Cellebrite is the most common vendor for local and state law enforcement agencies.

The investigator initiates the extraction process by plugging the phone into the computer or tablet. With Cellebrite software (which is similar to other tools),[12] once the tool recognizes the phone, it will prompt the investigator to choose the kind of extraction to be performed and, sometimes, the categories and time range of data to be extracted.[13] Often, in order to extract data, tools may bypass a phone's security

[12] Typically, the tools either detect what kind of phone has been connected, or otherwise allow law enforcement to look up the kind of phone by its brand or model number. Some rarer phones running Android, Windows, or other operating systems may not be supported, but the vast majority of phones used in the United States are.

[13] Display of the categories and time range of data is highly fact-specific, depending on phone make, model, operating system, settings, and the extraction type. This feature is sometimes, but not always, available.

features by taking advantage of security flaws or built-in diagnostic or development tools.

There are a few distinct methods for copying data from phones:

"Manual extraction" refers to when an investigator views a phone's contents like a normal user of the phone. Typically, investigators will take photographs or screenshots of the screen, email data to themselves from the phone, or videotape their exploration of a phone's contents, to prove that data was actually found on the phone.[14]

"Logical extraction" automates what can be done through manual extraction. In other words, it automatically extracts data that's presented on the phone to the user, using the device's application programming interface (API).[15] A logical extraction is like ordering food from a restaurant: what you can get is limited to menu items, and the waitstaff (the API) is in charge of their delivery and organization.

[14] This process can create issues with forensic integrity, as a later forensic extraction would show records of these manual interactions. Forensic integrity refers to the assurance that a separate party didn't interfere with or modify the data on the phone. For instance, a photo's metadata contains the last time it was accessed by the user, such that records of a police officer manually scrolling through and opening photos on a phone could show up when software is assembling a timeline of records from an extraction.

[15] 18F, "What are APIs? – Anecdotes and Metaphors," *available at* https://18f.github.io/API-All-the-X/pages/what_are_APIs-anecdotes_and_metaphors/ ("APIs are like the world's best retriever. You say, 'Fido - go fetch me X' and he brings you back X.").

“File system extraction" refers to an extraction that allows investigators to get data not usually available to the user. A file system extraction is similar to a logical extraction, but also copies other data, such as files or information in internal databases, that a phone doesn't typically display to users. Continuing the restaurant analogy, this is akin to asking the chef for specific secret dishes outside of the menu, which is possible at some restaurants, but not others.

“Physical extraction” refers to an extraction that copies data as it’s physically stored on the phone’s hardware — in other words, copying data bit-by-bit, instead of as distinct files. Data from a physical extraction has to be restructured into files for anyone to make sense of it. A physical extraction is like going to a restaurant and sneaking into the kitchen to take the food directly, as it exists in the kitchen (menu items that are waiting to be brought out, the ingredients used to prepare them, and even what's in the trash) without mediation from the waitstaff.

After extraction, law enforcement use MDFTs to efficiently analyze the data. MDFTs preserve information like filename and file location, but also aggregate every file found into a searchable and filterable pool. For example, law enforcement can sort data by the time and date of its creation, by location, by file or media type, or by source application.[16] This means law enforcement can take data extracted from

[16] This is possible because all files contain metadata including their date of creation, and dates of most recent access and modification.

different apps on the phone and view it together in list format as a chronological series of events. It also means they can pull all pictures or videos from the phone to view in one place, as a grid of thumbnails, regardless of how they are actually organized or named on the phone.[17] MDFTs can also search for key terms across the entire phone, just as one might use Google to search the web, and display information about the results and where on the phone they're from. Beyond searching and filtering files using their own metadata, MDFTs, like those from Cellebrite, contain artificial intelligence tools that categorize text and images based on what content they seem to contain, like "drugs" or "nudity."

Because MDFTs can extract more and different types of data, and analyze it more efficiently, they are significantly different from manually searching a cellphone.

II. Without intervention, mobile device forensic tools will facilitate indiscriminate searches of cellphones. But narrower searches of devices are possible.

MDFTs are purposefully designed to allow law enforcement to extract as much data as possible from a cellphone. Without intervention, *Amicus* believes that

[17] When you take a photo with your cellphone's camera application, the photo is stored in a different folder than photos taken using other applications, like Instagram or WhatsApp. With direct access to the phone's file system, someone may have to manually navigate in and out of levels of folders to find all of the images on a phone. But because images have predictable file extensions, MDFTs like Cellebrite's UFED can automate the process of looking for image files on the phone and aggregate them in one place.

MDFTs will continue to facilitate indiscriminate searches of cellphones and violate individuals' constitutional rights. But MDFTs also offer a variety of technical capabilities that can help to narrow digital searches.

During extraction, before any data is actually copied from the phone, MDFTs can be set to copy only data that was created within a certain date range. For example, law enforcement could limit an extraction to only the hour before a car crash occurred. During a logical or file system extraction, investigators can also select the specific categories of data they want to copy, such as SMS text files, app data, contacts, locations, call logs, web and search history, photos, or videos. For example, law enforcement could limit a logical extraction to only text messages sent and received between March 1 and March 15 if they were investigating written threats made during that time frame. These limits can be set before data is even discovered by the MDFT, and can narrow what data is persistently copied from the cellphone onto the investigator's system. Importantly, such pre-extraction filtering further limits what data is accessible to the investigator to examine. Limiting the data accessible to law enforcement on the front-end could also mitigate some concerns regarding the application of the plain view doctrine to digital searches.

After extraction and during data analysis, MDFTs provide further opportunities to narrow law enforcement's search. MDFTs typically allow investigators to navigate through the extracted data according to its original location or category on the phone, or by media type.[18] For example, Cellebrite software separates the various categories of data — such as "SMS Messages," "Pictures," "Device Locations," or "Contacts," and data from individual apps — and allows investigators to peruse each category separately. For example, if an investigator selected the "Pictures" category, the software would populate with image files found in the extraction. Similarly, if they selected the "Facebook Messenger" category, the software would populate with chat messages and images found in the Facebook Messenger app. Importantly, media files can be displayed as thumbnails in a grid, so an investigator can quickly scan through all of the images without having to individually open any of the files.

In addition, investigators can use search or filter tools to narrow their searches. Searches look for the keyword (*e.g.,* "Jane Doe," "2025551234," or "janedoe@hotmail.com") across all data categories — in the filename, content, or metadata of all the files on the phone. Filters can include metadata attributes about a file, such as the file type, file size, and the date and time the file was created, last accessed, and last modified. Search and filter tools can also narrow the data displayed to only communications involving a particular phone number or contact

[18] Sometimes locations of data are indicative of the category of data, but in other cases, MDFTs can simply look at file extensions to group files into categories, especially for media files. For example, files with the ".jpg" extension in a "/home/media/camera" folder can predictably be put into a "Camera Photos" category by MDFTs. Additionally, all files found in any folder on the device with ".jpg" extensions can be put into a "Pictures" category, as ".jpg" is a file extension that normally tells a computer to interpret the file as a picture.

over a certain period of time. Tools also include more complex analytical features, like those that allow law enforcement to view data with attached GPS information (like photos taken with the phone's camera) on a map, and search for files with GPS metadata near a point of interest.

The filters can also use predictive analytics to assess whether certain data is "related" to certain predefined content categories like "drugs," "weapons," or "nudity."[19] These predictive filters have become a common feature in MDFTs in recent years. They rely on a technique called machine learning (a kind of artificial intelligence, or AI) that enables software to perform specialized pattern matching. For example, the MDFT software may include a predictive model for "currency," which was built by training the model with many different example images of currency, so that it learns to recognize the features of currency. The model can later try to predict whether a new image matches the features of currency, and can report its confidence in its prediction.[20] The investigator can set "confidence thresholds" (*e.g.*, 75% confidence, or 95% confidence) to tune the breadth of results that the

[19] There are also child sexual abuse material (CSAM)-specific tools for determining whether that content is on a phone. CSAM can be found through specially-trained AI models built into MDFTs. They can also be found in a more standardized way, which is through the use of hashing. CSAM can be identified by doing a checksum (hash) on the file, and seeing if that matches the checksum of any known CSAM. But images can be altered such that they hash to different values and no longer match.

[20] For example, a model may see an image of dollar bills on a cellphone, and say it is 99% certain that the image contains currency. Or, the model may see an image of a drivers' license (which is similar to currency because it is also a rectangular shape with text and a human face on it) and say it is 50% certain that the image contains currency.

software should surface. A predictive text model for “drugs” could surface all of the text messages and emails that relate to drugs, even if those communications do not actually use the word “drugs.”

However, even though predictive searches are powerful for automating discovery, they may have varying levels of accuracy, depending on how the models were trained and how the software developer defined each category. Such searches can simultaneously fail to surface relevant content while also bringing much unrelated data into view.

In sum, the combination of pre-extraction filters, post-extraction filters, and post-extraction categorization makes it possible to narrow the content to be searched on a cellphone. This means that an investigator does not need to access or review every file on a device to determine whether it is relevant to the warrant.

Despite these technical capabilities, law enforcement frequently assert that they must be able to access and search *all data* on a device, because individuals may have misleadingly renamed or purposefully hidden files on their device. For example, the affidavit of probable cause attached to the search warrant in this case notes that:

> a suspect may try to conceal criminal evidence, and he might store criminal evidence in random order or with deceptive file names or deceptive file extensions. This requires searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crime.

In other words, this warrant purports that investigators cannot be restricted in their search because potential digital evidence can exist anywhere on a device, and suspects can and will conceal evidence within a computer's storage. Language similar to this pervades many of the cellphone search warrants we've seen.

While this argument may seem intuitive, it is unpersuasive in the context of MDFT cellphone searches because it misunderstands how MDFTs operate.

MDFTs can surface all images stored on a cellphone, regardless of file names, file extensions, or where they are stored. MDFTs do pay attention to how files are organized on the phone in order to conduct logical searches of the devices (*i.e.*, in order to copy "text messages" from a cellphone through a logical extraction, the MDFT uses the device's protocol for making a copy of text messages, which depends on the fact that it stores the texts in a specific folder and/or with specific file names). However, MDFTs can still index and filter files based on their content, agnostic of their filenames or locations. This means that an image file hidden in an unexpected folder and renamed with a misleading file extension can still be discovered, re-interpreted, and displayed. MDFTs can even perform "carving," where they search the data for recognizable pieces of files,[21] allowing them to decode

[21] "Carving" is possible because most files contain headers or other distinct sequences of data within the file that imply the file extension, called signatures. For example, all ".jpg" files start with the sequence "FF D8 FF" and end with the sequence "FF D9." This means MDFTs can simply scan the raw version of the phone's storage until it finds the header, copy until it sees the trailer,

and interpret files even when the file extensions have been changed or the files have been concealed (*e.g.*, image files embedded in documents). The fact that a small number of users may be more technically sophisticated and *could* conceal such information cannot, in and of itself, justify a default rule for broad searches of *most* cellphones.

Regardless of whether a phone must be accessed in its entirety in order to access any files, there is no reason that the full copy of the phone must be stored as evidence. Because of the powerful filtering tools built into most MDFTs, data responsive to the warrant can be quickly identified and saved, and the non-responsive data (which in all likelihood is most of the data, considering the immense storage capacity of modern smartphones) can be permanently deleted.[22]

In sum, at each stage of the forensic process, from extraction to analysis, MDFTs provide the tools to narrow and limit forensic searches of cellphones. The reason these narrower and more limited searches are not more common is not for

and display the contents as an image. *See* "User's guide: JPG Signature Format: Documentation & Recovery Example," Active@ File Recovery, https://www.file-recovery.com/jpg-signature-format.htm

[22] Cellphone searches are unlike traditional searches because law enforcement can extract all of the data on the device and subsequently search for case-relevant information. Maintaining information outside the scope of the warrant is akin to law enforcement maintaining the ability to indefinitely and limitlessly search a home. Furthermore, forensic analysis tools make it easy for law enforcement to reexamine the contents of a previously extracted phone — it's as simple as opening a file on a computer. Absent specific requirements that mandate notifying someone that their phone has been searched, it would be impossible for those under investigation to know of — let alone challenge — situations where law enforcement continues to search previously extracted data for new or unrelated investigations.

lack of technical capabilities, but instead, because of a lack of appropriate legal rules and safeguards.

III. Given how mobile device forensic tools work, search warrants like the one in this case essentially offer no limitation.

A "cell phone search would typically expose to the government far more than the most exhaustive search of a house." *See Riley* 573 U.S. at 396. Mobile device forensics tools, however, create further problems: they now enable law enforcement to conduct the most exhaustive search of a cellphone. The Supreme Court and other courts have long recognized across varying contexts that search warrants must be limited to avoid trampling civil rights. Despite this, cellphone search warrants issued across the country, like the one in this case, are often far broader in scope than is constitutionally permissible. Courts must take special care to ensure that warrants to search cellphones are as narrow as possible.

As part of *Amicus*' public records research, *Amicus* obtained hundreds of search warrants that law enforcement obtained to search cellphones using MDFTs. Many of these warrants authorized a search of "any and all data" on a cellphone.[23] Others authorized a search of a laundry list of data, often offering a bulleted list of effectively every piece of data one could plausibly find on a cellphone.[24] Other

[23] *See, e.g.*, Search Warrant 39163, obtained by the Euless Police Department (2018), *available at* https://assets.documentcloud.org/documents/20580218/sw_39163.pdf.
[24] *See e.g.*, Search Warrant 40701, obtained by the Fort Worth Police Department (2019), *available at* https://assets.documentcloud.org/documents/20580219/sw_40701.pdf.

search warrants authorized a "full extensive download/and or search of the [phone] to include all compartments, and items within the electronic devices that may contain contraband or evidence of the crime, and the data stored within said devices."[25] Still others authorized a search of a cellphone for "evidence related to this [narcotics offense] and other criminal offenses."[26] And for many, regardless of the words used, the nexus between a phone's data and the alleged offense is tenuous at best.[27]

Although these search warrants vary in their particular language, each one has the same result: they all authorize an unlimited, unrestricted search of a cellphone.

A search warrant that authorizes a search of "any and all data" on a cellphone, by its own terms, places no limits or restrictions on law enforcement's search, and would allow them to inspect everything on a cellphone. Courts have held such warrants invalid as they have no limiting principle. *See State v. Henderson*, 854 N.W.2d 616 (Neb. 2014). "Laundry list"-style warrants do much the same: even though these warrants do not use "any and all" language, they simply list out each category of digital data that would exist on a cellphone. Courts have also invalidated such warrants. *See United States v. Walker,* No. 13-64-RGA, 2015 WL 3485647, at

[25] *See e.g.*, Search Warrant 4B-18-0377, obtained by the Colorado State Patrol (2018), *available at* https://assets.documentcloud.org/documents/20580220/4b180377.pdf.

[26] *See e.g.*, Search Warrant 39648, obtained by the Fort Worth Police Department (2018), *available at* https://assets.documentcloud.org/documents/20394695/sw_39468.pdf.

[27] For many of the cases in which law enforcement turn to MDFTs, it's often difficult to assess why such an invasive technique would be necessary at all. Almost universally, the search warrants Amicus obtained for drug-related offenses rely on conclusory statements that drug dealers use cellphones to conduct their business.

*4 (D. Del. May 29, 2015). The words are different, but the result is the same: the warrant authorizes a search of the entire contents of a cellphone.

Warrants that authorize a search of a cellphone for evidence related to a criminal offense, like the search warrant at issue in this case, may not appear at first blush to pose similar problems. But given how MDFTs work and how law enforcement can use them, these warrants are similarly constitutionally defective.

The opinion below in this case found that "[a]though the warrant permitted the initial seizure of the phone as a whole, it limited the subsequent search and seizure of information on the phone to "evidence relating to the possession and/or distribution of child pornography." *See Commonwealth v. Green*, 204 A.3d 469, 482 (Pa. Super. Ct. 2019). Putting aside whether or not the warrant in this case was actually limited in that way,[28] what limitations and restrictions does this warrant actually place on law enforcement's search of the cellphone? What kinds of information on the phone are off-limits to be searched? If law enforcement allege they may need to examine all data (as relevant evidence can exist anywhere or could be hidden), and if law enforcement use an MDFT that can extract all data from a

[28] The warrant appears to have defined "contraband digital files" as: "child pornographic files (pictures or movies) and *any other digital evidence* relating to the possession and / or dissemination of child pornography, contained on the electronic storage media [such as a cellphone] seized as a result of this search warrant." (emphasis added).

cellphone, in practice, such a vaguely worded warrant authorizes law enforcement to rummage through reams of personal, but unrelated, data.

To illustrate, consider the difference between two hypothetical scenarios.

In Case A, a search warrant authorizes law enforcement to search a cellphone for "evidence of criminal threats that occurred over text message between January 1 to January 15, 2021." Law enforcement also possess an MDFT that empowers them to extract and analyze every piece of data on a cellphone. In this case, two different investigators *separately* perform the extraction and analysis using an MDFT. Given the warrant's clear restrictions on the type of data and the timeframe, it's highly likely the two investigators will perform the same kind of search and return with similar evidence.

In Case B, a search warrant authorizes law enforcement to search a cellphone for "evidence relating to possession of marijuana and / or distribution of marijuana." The affidavit states that evidence can exist anywhere on a digital device (and can even be hidden) — as a result, law enforcement may need to examine all stored data. The affidavit also states that, based on training and expertise, the affiant knows that "individuals engaged in the sale of narcotics use their cellphone to arrange and conduct their business." Law enforcement also possess an MDFT that empowers them to extract and analyze every piece of data on a cellphone. If two different investigators *separately* perform the extraction and analysis using an MDFT, in all likelihood, the two investigators in Case B will not perform the same search and will return with wildly different evidence, unlike in Case A. While one investigator may take reasonable steps in their search, another might not, largely depending on how they exercise their unfettered discretion and where each investigator thinks they could find evidence related to the possession and distribution of marijuana. One may explore internet search history, calendar entries, text messages, deleted text messages, and geolocation data amassed from apps downloaded onto the phone. Another might limit their search just to text messages and photos. One may return with evidence for entirely unrelated offenses, for which they had no preexisting suspicion, and which the search warrant did not cover.

While warrants such as the one in this case do identify the item to be seized by their relation to designated crimes, the description of the items leaves *substantial* discretion to the officer executing the warrant. *See United States v. Williams*, 592 F.3d 511, 519 (4th Cir. 2010) (noting the "particularity requirement is fulfilled when the warrant identifies the items to be seized by their relation to designated crimes and when the description of the items leaves nothing to the discretion of the officer executing the warrant"). Here, there is no clear limit on the date or time frame of the evidence sought. Nor is there a limit on the kind of digital data that can be searched, or how that data may be related to specific criminal activity. In other words, search warrants for cellphones like the one in this case authorize a search "in terms so ambiguous as to allow the executing officers to pick and choose among an individual's possessions to find which items to seize." *See Commonwealth v. Orie*, 88 A.3d 983, 1002 (Pa. Super. Ct. 2014).

Such ambiguous search warrants, combined with the exhaustive technical capabilities of MDFTs, allow law enforcement to rummage through the extracted cellphone data in an unrestrained search for evidence of criminal activity. While the specific language of the search warrant does not, on its face, appear to be as broad as a warrant authorizing a search of "any and all data" or a laundry list of data, it accomplishes the same in practice.

These varying types of warrants result in similarly broad and discretionary searches, in part because of an unconstitutional lack of particularity. Federal courts have understood the Fourth Amendment's particularity requirement to be unique for digital searches. *See United States v. Galpin,* 720 F.3d 436, 446 (2d Cir. 2013) ("Where, as here, the property to be searched is a computer hard drive, the particularity requirement assumes even greater importance."); *see also United States v. Burgess,* 576 F.3d 1078, 1091 (10th Cir. 2009) ("If the warrant is read to allow a search of all computer records without description or limitation it would not meet the Fourth Amendment's particularity requirement").

Article 1, Section 8 of the Pennsylvania Constitution has a more stringent particularity requirement than the Fourth Amendment. Notably, search warrants must describe the items to be seized "as nearly as may be" and be "as particular as is reasonably possible." *See Commonwealth v. Orie,* 88 A.3d 983, 1002 (Pa. 2014) (quoting *Commonwealth v. Rivera,* 816 A.2d 282, 290 (Pa. 2003)) ("The clear meaning of the language is that a warrant must describe the items as specifically as is reasonably possible").

In *Orie,* the Court addressed overbroad warrants in the context of electronic devices. There, the Court invalidated a warrant which authorized seizure of a flash drive and "any contents contained therein, including all documents, images, recordings, spreadsheets or any other data stored in digital format." *Orie*, 88 A.3d at 1008. The warrant in this case amounts to the same authorization as the warrant deemed unconstitutional in *Orie* because it allows law enforcement to search the entire contents of the phone in order to determine what qualifies as evidence of the offense in question.

Courts have also interpreted the Fourth Amendment as requiring probable cause to search each category of content in cell phone searches. *See United States v. Morton*, 984 F.3d 421, 426 (5th Cir. 2021) (holding that separate probable cause is required to search each of the categories of information found on the cellphone and "[a]bsent unusual circumstances, probable cause is required to search each category of content); *see also Burns v. United States*, 235 A.3d 758, 773 (D.C. 2020) (observing that "[i]t is not enough for police to … establish probable cause to believe the phone contains some evidence of a crime").

Courts have also held that cellphone searches for evidence related to an offense are not adequately particular. *See State v. Savath*, 298 Or. App. 495 (2019) (finding that a search of the defendant's cellphone for "all evidence" of possession of controlled substances offenses was invalid because those offenses did not involve contraband located on the cellphone); *see also State v. Bock*, 310 Or. App. 329 (2021) (finding the command authorizing a search for all evidence of the various offenses that police were investigating on the defendant's cellphone invalid because a warrant authorizing a search for all "evidence of a particular crime" is not sufficiently specific to pass constitutional muster.)

Although Pennsylvania courts have not ruled on this specific issue, this Court has maintained in other cases and contexts that probable cause must exist for each item to be searched. *See Commonwealth v. Grossman,* 555 A.2d 896 (Pa. 1989) ("Any unreasonable discrepancy between the items for which there was probable cause and the description in the warrant requires suppression. An unreasonable discrepancy reveals that the description was not as specific as was reasonably possible.")

In some instances, search warrants for cellphones may be overbroad simply because probable cause to search the cellphone does not exist. This Court addressed similar search warrants in *Commonwealth v. Johnson*, 240 A.3d 575 (Pa. 2020). In *Johnson*, this Court held that "where law enforcement seeks to search a person's cell phone based on the person's mere proximity to illegal contraband, some link sufficient to connect the two must be provided in the affidavit of probable cause." *Id.* at 587. While this Brief does not discuss the issue of probable cause with respect to this specific case, the issues identified by this Court in *Johnson* are pervasive throughout search warrants authorized across the country. Indeed, many warrants adopt the logic that this Court in *Johnson* expressly rejected — that "simply because there was probable cause to arrest [an individual for certain offenses] . . . there was necessarily probable cause to search his cell phone for evidence of those same offenses." *Id.* Though law enforcement cannot rely upon the general ubiquity of cellphones in daily life as a substitute of particularized information that a specific device contains evidence of a crime or contraband, often, law enforcement do just that. A clearer nexus between the cellphone and the conduct under investigation is necessary.

IV. Courts can and should insist on the production of audit logs when mobile device forensic tools are used to extract and analyze cellphone data.

The risk of overbroad searches of cellphones is especially worrying given that it's nearly impossible for actors outside of law enforcement — such as a defense lawyer — to understand the steps that a forensic examiner took and to challenge the execution of a search. Products and training can be expensive, and some MDFT vendors refuse to sell products to anyone outside of law enforcement. In *Amicus*' research, few law enforcement policies require examiners to document how a cellphone search was conducted. Worse, the level of documentation called for in these rare policies is unlikely to empower a third party to meaningfully audit a forensic search of a cellphone.

One way to address that risk is to require a digital audit log of a phone search. Digital audit logs could chronologically document a record of all interactions that law enforcement had with MDFT software, such as how they browsed through the data, any search queries they used, and what data they could have seen. With such logs, judges and others could better understand the precise steps that law enforcement took when extracting and examining a phone. In particular, these logs could equip judges to better assess the reasonableness of the search technique and ascertain if the search was sufficiently narrowly tailored to the warrant during *ex post* reasonableness review.

In *United States v. Christie*, 717 F.3d 1156 (10th Cir. 2013), then-Judge Gorsuch recognized the need for something like digital audit logs in this context:

> this *ex post* review comes with the benefit, too, of the adversarial process where evidence and experts from both sides can be entertained and examined. To undertake any meaningful assessment of the government's search techniques in this case (the how), we would need to understand what protocols the government used, what alternatives might have reasonably existed, and why the latter rather than the former

might have been more appropriate. *Id.* at 1167.

Although major MDFT vendors may not offer this capability today, they could easily build and incorporate it into their products. The feature could automatically capture and describe all of the actions an examiner took (*e.g.*, each click and what was clicked on, or what search terms were searched) as well as all the data that was shown on-screen to an examiner (*e.g.*, each image that an examiner could have seen). If courts were to insist upon the production of digital audit logs created by the MDFT upon the return of a search warrant, MDFT vendors would likely develop this feature.

CONCLUSION

Technology continues to expand law enforcement's investigatory powers. Nearly a decade ago, Justice Sotomayor noted that GPS tracking devices were "so amenable to misuse, especially in light of the Fourth Amendment's goal to curb arbitrary exercises of police power to and prevent 'a too permeating police surveillance.'" *See United States v. Jones*, 565 U.S. 400, 416-417 (Sotomayor, J., concurring) (quoting *United States v. Di Re*, 332 U.S. 581, 595 (1948)).

The same is true today of mobile device forensic tools. Combined with warrants that are so broadly and ambiguously worded as to be limitless, mobile device forensic tools facilitate exhaustive and indiscriminate searches of cellphones by law enforcement. At the same time, they can help to limit and narrow the execution of digital searches. But as *Amicus*' research shows, that is not how the tools are used today: these powerful tools are already in wide use by law enforcement. And given how routine forensic searches are today, these tools will likely worsen the racial disparities of the American criminal legal system.

Absent intervention by this Court, mobile device forensic tools will continue to facilitate indiscriminate searches of cellphones that fundamentally sit at odds with the protections of the Fourth Amendment and Article I, Section 8 of the Pennsylvania Constitution.

Respectfully submitted,

/s/ Jim Davy
Jim Davy, I.D. No. 321631
ALL RISE TRIAL & APPELLATE
P.O. Box 15216
Philadelphia, PA 19125
609-273-5008
jimdavy@allriselaw.org

Counsel for Amicus Curiae

CERTIFICATE OF COMPLIANCE WITH WORD LIMIT

I hereby certify pursuant to Pa.R.A.P. 531 that this brief does not exceed 7,000 words.

CERTIFICATE OF COMPLIANCE

I hereby certify that this filing complies with the provisions of the Public Access Policy of the Unified Judicial System of Pennsylvania: Case Records of the Appellate and Trial Courts that require filing confidential information and documents differently than non-confidential information and documents.

CERTIFICATE OF SERVICE

I hereby certify that on this 7th day of April, 2021, a true and correct copy of the foregoing Brief of *Amicus Curiae* was served on the Parties via PACFile.

/s/ *Jim Davy*
Jim Davy

Dated: April 7, 2021