No. 19-10842

IN THE UNITED STATES COURT OF APPEALS
FOR THE FIFTH CIRCUIT

UNITED STATES OF AMERICA,
Plaintiff-Appellee,

v.

BRIAN MATTHEW MORTON,
Defendant-Appellant.

On Direct Appeal from the United States District Court
for the Northern District of Texas
Forth Worth Division

BRIEF OF *AMICUS CURIAE* UPTURN, INC. IN SUPPORT OF DEFENDANT-APPELLANT

Charles "Chad" Baruch
Texas Bar No. 01864300
chad@jtlaw.com
Johnston Tobey Baruch PC
12377 Merit Drive, Suite 880
Dallas, Texas 75251
Telephone: (214) 741-6260 (phone)
Facsimile: (214) 714-6248 (fax)

Counsel for Amicus Curiae

CERTIFICATE OF INTERESTED PERSONS

United States v. Morton, No. 19-10842

The undersigned counsel of record certifies that the following listed persons and entities as described in the fourth sentence of Rule 28.2.1 have an interest in the outcome of this case. These representations are made in order that the judges of this court may evaluate potential disqualification or recusal.

District Judge

The Honorable Reed C. O'Connor

Magistrate Judge

The Honorable Jeffrey L. Cureton

Plaintiff-Appellee

United States of America

Counsel for Plaintiff-Appellee

Prerak Shah
Aisha Saleem
Leigha Simonton
Amber Grand

Defendant-Appellant

Brian Matthew Morton

Counsel for Defendant-Appellant

Jason D. Hawkins
Kevin Joel Page
Brandon Beck
Aisha Dennis

Amicus Curiae on this Motion

Upturn, Inc.

Counsel for *Amicus Curiae* on this Motion

Charles Baruch

Amicus Curiae Upturn is a non-profit entity that does not have a parent corporation. No publicly held corporation owns more than 10% or more of any stake or stock in *Amicus Curiae*.

Dated: July 13, 2021

/s/Charles "Chad" Baruch
Texas Bar No. 01864300
chad@jtlaw.com
Johnston Tobey Baruch PC
12377 Merit Drive, Suite 880
Dallas, Texas 75251
Telephone: (214) 741-6260
Facsimile: (214) 741-6248

Counsel for Amicus Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

OTHER AUTHORITIES

STATEMENT OF INTEREST OF *AMICUS CURIAE*[1]

Upturn, Inc. 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 Americans from general digital searches.

Upturn has unique expertise on these matters. Last year, Upturn published *Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones*. This report is the most comprehensive examination of law enforcement's use of mobile device forensic tools to date. Mobile device forensic tools are a powerful technology that allow law enforcement to extract and search a full copy of data from a cellphone.

Based on more than 110 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 U.S. law

[1] *Amicus* confirms that all parties have consented to the filing of this brief, that no party or counsel for any party authored this brief in whole or in part, and that no person other than *Amicus* or their counsel made any monetary contribution intended to fund the preparation or submission of this brief.

enforcement agencies.[2] Among the report's findings, more than 2,000 agencies have purchased these tools in all 50 states and the District of Columbia. State and local law enforcement agencies have performed hundreds of thousands of cellphone extractions since 2015, often without a warrant. Few departments have detailed policies governing when and how officers can use this technology. The report also documents the existing technical capabilities of today's mobile device forensic tools, finding that the tools provide sweeping access to personal information on a phone.[3]

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 can be used in ways that are compatible with the panel's ruling. This brief also argues that cellphone search warrants issued across the country — such as the search warrants in this case — are far broader in scope than is constitutionally permissible.

INTRODUCTION AND SUMMARY OF THE ARGUMENT

Every day, law enforcement agencies across the country search hundreds to thousands of cellphones. To search these phones, law enforcement frequently rely

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

[3] In order to assess the technical capabilities of current mobile device forensic tools, *Amicus* extensively reviewed and 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.

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."[4]

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 to 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 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 extractions using MDFTs. Law enforcement use these tools not only to investigate cases involving serious harm, but also for offenses like graffiti, shoplifting,

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

marijuana possession, prostitution, vandalism, car crashes, parole violations, untaxed cigarettes, petty theft, and public intoxication.

As the Supreme Court observed in *Riley v. California*, 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." *Riley v. California*, 573 U.S. 373, 394 (2014). Critically, this concern — that the quantity and quality of data on a cellphone is so sensitive that it can effectively reconstruct one's life — does not consider the additional analytical power of MDFTs beyond a manual search.

There are key 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 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).

The proliferation of these tools represents a dangerous expansion of law enforcement's investigatory powers. Today, every American is at risk of having their entire private life reconstructed by law enforcement, based on a forensic search of their cellphone.

In the Government's view, once law enforcement officials obtain a search warrant for a cellphone, they are always authorized to conduct the most exhaustive and invasive search possible with an MDFT. To make this argument, the Government relies on two claims: one technical, one legal. Technically, the Government argues that MDFTs are incapable of searching by category of information, and are only capable of extracting all cellphone data, not simply data from certain applications. (Gov't Pet. Reh'g at 14–15). Legally, the Government argues that, beyond requiring a search warrant to search a phone, *Riley* affords law enforcement an unrestricted search. (Gov't Pet. Reh'g at 10–12). But both claims are incorrect.

First, MDFTs are capable of narrower searches. True, MDFTs are purposefully designed to allow law enforcement to extract as much data as possible

from a cellphone so as to not miss anything. But MDFTs also have a range of features — such as pre- and post-extraction filtering and categorization — that make it possible to narrow the content to be searched on a cellphone.

Second, regarding the Government's legal argument, the panel's holding does not conflict with *Riley*. The Court in *Riley* clearly articulated how "a cell phone search would typically expose to the government far more than the most exhaustive search of a house." *Riley*, 573 U.S. at 396. As a result, special care is required to ensure that cellphone search warrants are as narrow as possible. The panel's holding did just that.

Without an intervention to narrow digital searches, mobile device forensic tools will continue to facilitate indiscriminate searches of cellphones that fundamentally deny the protections of the Fourth Amendment. This case presents an opportunity for this Court to intervene and stop such indiscriminate searches, much as the panel did.

ARGUMENT

I. HOW MOBILE DEVICE FORENSIC TOOLS ENABLE LAW ENFORCEMENT TO SEARCH CELLPHONES

Mobile-device forensics typically is 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 AccessData, Cellebrite, Grayshift, Magnet Forensics, MSAB, and OpenText. Based on Upturn's research, Cellebrite tools are commonly found among local and state 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),[5] 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 extract.[6] Often, to extract data, tools may bypass a phone's security 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 found on the phone.

"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

[5] 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.

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

user, using the device's application programming interface (API).[7] By way of analogy, 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.

"File system extraction" empowers 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 non-advertised 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.

[7] 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.").

After extraction, law enforcement uses MDFT software programs to efficiently analyze the data. MDFTs preserve information like filename and file location, but can also aggregate every file found into a searchable and filterable pool. So, law enforcement can sort data by the time and date of its creation, by location, by file or media type, or by source application.[8] This means officials can take data extracted from different apps on a phone and view them together as a chronological series of events. It also means they can view all pictures or videos from the phone to view in one place, as a grid of thumbnails, regardless of how they are organized or named on the phone.[9] MDFTs also can search for key terms across the entire phone, just like you might use Google to search the web, and display information about the results and where they're organized within the phone's file system.

II. MOBILE DEVICE FORENSIC TOOLS CAN HELP NARROW THE SEARCH OF CELLPHONE DATA

Core to the Government's argument that law enforcement must always be authorized to conduct the most exhaustive and invasive search possible with MDFTs are several technical claims regarding cellphones and MDFTs.

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

[9] 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.

First, the Government claims that:

> the forensic tools that the government uses to best ensure the integrity and completeness of data obtained from cell-phones during the execution of warrants do not enable searching their contents by "place" or application … [the tools] extract all cell-phone data (not simply data from certain applications) in its raw format, producing what is colloquially called a "cell-phone dump." (Gov't Pet. Reh'g at 14).

Second, the Government claims that law enforcement could not "know in advance what 'places' are in [a] target's phone and what types of data types are in each 'place' so that it could provide separate probable cause to search each of these 'places.'" (Gov't Pet. Reh'g at 12).

Third, the Government claims that "[a] warrant that authorizes a search of only 'text messages' or only 'photographs' is … incompatible with the way authorities conduct forensic analyses of cell-phones and with the way cellphones store data." (Gov't Pet. Reh'g at 15).

Each of these claims is inaccurate.

MDFT software has built-in pre- and post-extraction filtering and categorization features, all of which can be used to narrow the search of cellphone data. MDFTs can categorize data in different ways, including by source application, file type, or date at different points in the extraction and analysis process.[10]

[10] MDFTs can categorize and filter data stored on cellphones because cellphone data is stored predictably. At a high level, in order for a cellphone to function, the phone must know where it stores data and how to interpret that data's format in order to display it. All data, in its raw form, is binary. However, file extensions and file signatures (specific identifiable sequences that indicate

The simplest MDFT feature used to separate data into categories is the logical extraction interface. Cellebrite's software, at the beginning of a logical extraction, prompts the user to select the general categories of data to extract from the phone. This takes place before data is copied from the phone. These categories are easy to understand, and include "call logs," "photos," "contacts," and "SMS text messages." Data then is copied from the cellphone according to whether it fits one of the selected categories, based on its file type and/or location in the file system of the phone, or through use of the phone's own Application Programming Interface (API).[11] For example, law enforcement could limit an extraction to only the hour before a car crash occurred, or limit a logical extraction to only text messages sent and received between March 1 and March 15 if they were investigating threats made during that time.

Cellebrite tools also offer a "selective file system" extraction, as opposed to a "full file system" extraction. This feature allows investigators to see which specific applications are present on the phone before extracting data (similar to a logical extraction). The selective file system extraction "enable[s] you to select key artifacts

---

file type, *e.g.* all .jpg image files begin with the hexadecimal "FF D8 FF" and end with "FF D9") tell the phone how to display data, whether it is an image or text. This means an MDFT can easily separate images from contacts and from SMS texts, which all have different file types.

[11] "What Happens When You Press that Button? Explaining Cellebrite UFED Data Extraction Processes," Cellebrite, available at https://smarterforensics.com/wp-content/uploads/2014/06/Explaining-Cellebrite-UFED-Data-Extraction-Processes-final.pdf.

that you are authorized to extract from these devices."[12] Users can search to see whether certain apps are on the phone and then select them for extraction. For example, investigators could search for terms like "Facebook," "Snapchat," "calendar," or "voice memos," or scroll through the list of available apps.[13]

In short, multiple pre-extraction features exist to identify cellphone data by category and to narrow the search.

Post-extraction features can do similarly. After data is copied off the device and loaded into the investigator's computer, MDFT analysis software reassembles data into categories, regardless of the extraction type. MDFT software can sort extracted data according to its original location or category on the phone, or by media type.[14] For example, Cellebrite software separates the various categories of data — such as "SMS Messages," "Pictures," "Device Locations," or "Contacts," and data

[12] Cellebrite, *Cellebrite UFED Selective File System Extractions Now Available for iOS Devices*, YouTube (Jun. 21, 2021), https://www.youtube.com/watch?v=7DRL8R5kw94.

[13] Cellphone operating systems have relatively predictable file systems, so that applications know where to find their own data. Modern phones do not generally allow users to directly interact with the file system, and implement application sandboxing, which means a given application can only access files and directories that it manages. This means an MDFT can simply look at the directories for the Calendar application, and be relatively sure that it contains all the user's calendar data. *See, e.g.,* Laurent Sacharoff, *The Fourth Amendment Inventory as a Check on Digital Searches*, 105 Iowa L. Rev. 1643, 1660-1662 (2020) (describing how "users no longer determine where an app stores its files, because users have no direct access to the file directory. As a result, files are stored in predictable places.").

[14] 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.

from individual apps — and allows investigators to view each category separately. 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. 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. Search and filter tools can also narrow the data displayed to only communications involving a particular phone number or contact over a certain period of time.

Finally, even if investigators are only able to get a physical extraction of the raw data (a "cellphone dump"), common tools exist for interpreting it. The most prevalent is Cellebrite's Physical Analyzer, which according to Cellebrite, is able to "reassemble device and application data into readable formats with SQLite Wizard, Python scripting, App Genie and Hex highlighting."[15] This means that even raw data can be reassembled back into a file system structure that gives information about files' original locations, which is then used to categorize the files (in the same way that a logical extraction categorizes data based on location).

[15] "Cellebrite Physical Analyzer: The Industry Standard for Digital Data Examination," Cellebrite, https://www.cellebrite.com/en/physical-analyzer/.

Nevertheless, law enforcement frequently assert that they must be able to access and search *all data* on a cellphone because it's either impossible to know where evidence may be stored, or because individuals may have misleadingly renamed or purposefully hidden files on their device. Courts have largely accepted these assertions.

For example, the Sixth Circuit has held that broad cellphone search warrants can be reasonable because "officers could not have known where th[e] information [sought] was located in the phone or in what format" and "because criminals can—and often do—hide, mislabel, or manipulate files to conceal criminal activity [such that] a broad, expansive search of the [computer] may be required." (quotation marks and citation omitted) *See United States v. Bass*, 785 F.3d 1043, 1049-50 (6th Cir. 2015).

Similarly, the Seventh Circuit has held that even if a cellphone search warrant "permit[s] the police to look at every file on [a] phone and decide which files satisfy the description," that does not make the warrant too general because "[c]riminals don't advertise where they keep evidence." *See United States v. Bishop,* 910 F.3d 335, 336 (7th Cir. 2018). And this Court held in *Triplett* that law enforcement were authorized to look through every document to determine whether it was responsive to the warrant, because law enforcement could not have known in advance what

information would be on the computer or "where" it would be. *See United States v. Triplett*, 684 F.3d 500 (5th Cir. 2012).

In sum, investigators argue that they cannot be restricted in their search because potential evidence can exist anywhere on a device, and suspects can and will conceal evidence within a computer's storage. But this argument 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,[16] allowing them to decode

[16] "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 display the contents as an image. *See* "User's guide: JPG Signature Format: Documentation &

and interpret files even when the file extensions have been changed or the files have been concealed (*e.g.*, image files embedded in documents).

These advanced capabilities already help to address the rare occasions where a more technically sophisticated user attempts to conceal digital data. At any rate, these rare occasions should not justify a default rule for broad searches of most cellphones. *See* Laurent Sacharoff, *The Fourth Amendment Inventory as a Check on Digital Searches*, 105 Iowa L. Rev. 1643, 1658 (2020) (observing how "[c]ourts have allowed the very rare prospect of the computer mastermind to drive the entire doctrine, rather than taking the most typical user as the prototype.").

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 can be permanently deleted.

Given the many ways to narrow a search of a cellphone, the Government's claim that a search limited to specific categories of data is "incompatible" with cellphone forensics is simply incorrect. The combination of pre- and post- extraction

Recovery Example," Active@ File Recovery, https://www.file-recovery.com/jpg-signature-format.htm.

filters and categorization makes it possible to narrow the content to be searched on a cellphone.

III. THE GOVERNMENT'S POSITION WOULD EFFECTIVELY RENDER *RILEY* MEANINGLESS

Every day, state and local law enforcement arrest people for a variety of alleged criminal offenses. Often, after these arrests, law enforcement obtain search warrants to perform a forensic extraction of an accused person's cellphone to find evidence of alleged criminal activity. As *Amicus'* research demonstrated for the first time, state and local law enforcement agencies have performed potentially hundreds of thousands of cellphone extractions in the years since the Supreme Court decided *Riley* in 2014.

In other words, on a scale previously not well understood, law enforcement agencies of all sizes use MDFTs — often in the most invasive ways possible — to forensically extract and search cellphones, which "with all they contain and all they may reveal … hold for many Americans the privacies of life." *Riley,* 573 U.S. at 403 (internal quotation marks and citation omitted).

Further, in many cases where law enforcement arrest someone and seek to extract data from their cellphone — such as drug possession, public intoxication, shoplifting, vandalism, petty theft, or graffiti — the nexus between a cellphone's data and the alleged criminal offense is tenuous at best. In records Upturn obtained

in which law enforcement logged their use of MDFTs, many offenses bore little to no relationship to a cellphone. In fact, for many of the alleged offenses logged in these records, it's difficult to understand why such an invasive investigative technique would be necessary, other than mere speculation that evidence *could* be on the phone.

All of this occurs despite the Supreme Court's admonition in *Riley* that "a cell phone search would typically *expose to the government far more than the most exhaustive search of a house*: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form — unless the phone is." *Riley*, 573 U.S. at 396–97 (2014) (emphasis added).

The Government argues that there's no problem to see here. But its position — that law enforcement cannot be "limited" in their searches of cellphones in ways the panel ruling articulated — would render *Riley* meaningless. Taken to its logical conclusion, this argument would mean that even in cases where the nexus between a person's cellphone and the alleged criminal offense is tenuous, law enforcement should be empowered to use an MDFT to conduct the most invasive, exhaustive possible search and rummage through the extracted cellphone data for evidence. If adopted, this reading would transform *Riley* from a case that clearly details why

cellphones may even deserve more protection than the home, into a case that authorizes digital general warrants.

According to the Government's reading of *Riley*, once law enforcement obtains a cellphone search warrant to search for evidence of a crime, law enforcement can search the entire cellphone for that evidence, not just certain features or categories of data within the cellphone. (Gov't Pet. Reh'g at 10).

But the Government's reading of *Riley* conflicts with what the Supreme Court itself said in *Riley*:

> The United States asserts that a search of *all data stored* on a cell phone is 'materially indistinguishable' from searches of [personal items carried by an arrestee]. This is like saying a ride on a horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together.

Riley, 573 U.S. at 393 (emphasis added).

Notably, the Court in *Riley* went on to explain that the sources of potentially pertinent information on cellphones "are virtually unlimited." *Id.* at 399. Accordingly, the Court rejected the Government's proposal in *Riley* to apply the *Gant* standard to cellphones because doing so would give "police officers unbridled discretion to rummage at will among a person's private effects." *Id.* It cannot be the case that to preserve *Riley*, law enforcement must be afforded the same kind of unbridled discretion that the Court rejected in *Riley*.

IV. 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 when they are used to execute broadly worded warrants: 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 constitutional rights. Despite this, cellphone search warrants issued across the country, like those 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 Upturn's public records research, it received 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.[17] Others authorized a search of a laundry list of data, often offering a bulleted list of effectively every piece of data one could find on a cellphone.[18] Other search warrants

[17] *See, e.g.,* Search Warrant 39163, obtained by the Euless Police Department (2018), available at https://assets.documentcloud.org/documents/20580218/sw_39163.pdf.
[18] *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.

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."[19] Still others authorized a search of a cellphone for "evidence related to this [narcotics offense] and other criminal offenses."[20]

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.

The search warrant in this case resembles a laundry list-style search warrant. Here, the affidavit for the search warrant notes:

> It is the belief of affiant that suspected party was in possession of and is concealing in [the cellphones] . . . [e]vidence of the offense of Possession of [ecstasy], possession of marijuana, possession of marijuana *and other criminal activity*; to wit telephone numbers, address books; call logs, contacts, recently called numbers, recently received calls; recently missed calls; text messages (both SMS messages and MMS messages); photographs, digital images, or multimedia files in furtherance of narcotics trafficking or possession. (ROA.269) (emphasis added).

The affidavit further states that:

> The search [of the cellphone] includes the examination of stored materials, media, documents, and data, *including but not limited* to: address books; recently called numbers; recently received numbers; digital images; and text messages ... *The search may also include other areas of the cellular telephone in which said suspected party may store*

[19] *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.
[20] *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.

> *data evidence which is the object of the search requested herein*. (ROA.271-72) (emphasis added).

The panel found that "[t]he affidavits seek approval to search Morton's contacts, call logs, text messages, and photographs for evidence of his drug possession crimes." *United States v. Morton*, 984 F.3d 421, 425 (5th Cir. 2021). But the affidavits sought much more than that. They sought cellphone data "including but not limited to" contacts, call logs, text messages, and photographs for Morton's alleged drug possession "and other criminal activity." (ROA.269–72).

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? If law enforcement allege they may need to examine all data (as relevant evidence could be anywhere or could be hidden), and if law enforcement use an MDFT that can extract all data from a cellphone, such a 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 on January 15, 2021." Law enforcement 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 that 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 lists some kinds of data of interest, such as texts, contacts, and photos, but also 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. 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 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, app 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.

Warrants such as those at issue in this case leave substantial discretion to the officer executing the warrant. *See United States v. Allen,* 625 F.3d 830, 835 (5th Cir. 2010) (observing that to avoid fatal generality, the place and items to be seized must "be described with sufficient particularity so as to leave nothing to the discretion of the officer executing the warrant."); *see also 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 those at issue in this case authorize a search "of all computer records without … limitation" and as a result do "not meet the Fourth Amendment's particularly requirement." *See United States v. Burgess*, 576 F.3d 1078, 1091 (10th Cir. 2009).

Such ambiguous search warrants, like those here, combined with the exhaustive technical capabilities of MDFTs, allow law enforcement to rummage through extracted cellphone data in an unrestrained search for evidence of criminal activity. Accordingly, it should be "constitutionally intolerable for search warrants

simply to list generic categories of data typically found on such devices as items subject to seizure." *See Burns v. United States*, 235 A.3d 758, 775 (D.C. 2020). Instead, cellphone search warrants "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." *Id*. at 773.

CONCLUSION

Technology continues to expand law enforcement's investigatory powers. In this case, the Government argues that the law should too. "Obviously, the police will not have probable cause to search through and seize such an expansive array of data every time they search a cell phone." *See United States v. Oglesby*, No. 4:18-CR-0626, 2019 WL 1877228, at *7 (S.D. Tex. Apr. 26, 2019). But, according to the Government, when executing a cellphone search warrant, law enforcement should always be afforded unfettered access and discretion to search the entire contents of a cellphone using a mobile device forensic tool. That is a remarkable position.

More remarkable, this argument paints a disturbingly accurate picture of today's reality. Combined with search 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. It happens hundreds of

thousands of times a year, often in cases where the nexus between a cellphone's data and the alleged offense is tenuous at best.

Importantly, today's mobile device forensic tools could be used to narrow the search of a cellphone just as the panel contemplated. But a technical possibility means little without the force of the law. Without 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.

Dated: July 13, 2021

/s/Charles "Chad" Baruch
Texas Bar No. 01864300
chad@jtlaw.com
Johnston Tobey Baruch PC
12377 Merit Drive, Suite 880
Dallas, Texas 75251
Telephone: (214) 741-6260
Facsimile: (214) 741-6248

Counsel for Amicus Curiae

CERTIFICATE OF COMPLIANCE

1. This brief complies with the type-volume limitation of Fed. R. App. P. 29(a)(5) because it contains 6,343 words, excluding the parts of the brief exempted by Rule 32(f).
2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type-style requirements of Fed. R. App. P. 32(a)(6) because it has been prepared in a proportionally spaced typeface using Microsoft Word in 14-point Times New Roman.

Dated: July 13, 2021

/s/Charles "Chad" Baruch
Texas Bar No. 01864300
chad@jtlaw.com
Johnston Tobey Baruch PC
12377 Merit Drive, Suite 880
Dallas, Texas 75251
Telephone: (214) 741-6260
Facsimile: (214) 741-6248

Counsel for Amicus Curiae

CERTIFICATE OF SERVICE

I certify that on this 13th day of July, 2021, the foregoing Motion of Upturn, Inc. for Leave to File *Amicus Curiae* Brief in Support of Defendant-Appellant was filed electronically through the Court's CM/ECF system. Notice of this filing will be sent by e-mail to all parties by operation of the Court's electronic filing system.

Dated: July 13, 2021

/s/Charles "Chad" Baruch
Texas Bar No. 01864300
chad@jtlaw.com
Johnston Tobey Baruch PC
12377 Merit Drive, Suite 880
Dallas, Texas 75251
Telephone: (214) 741-6260
Facsimile: (214) 741-6248

Counsel for Amicus Curiae