IN THE SUPREME COURT OF THE STATE OF CONNECTICUT

S.C. 20600

STATE OF CONNECTICUT,

v.

ONAJE SMITH

Amicus Curiae Brief of Upturn Inc., in Support of Defendant-Appellant

---

Jim Davy
PA I.D. No. 321631
All Rise Trial & Appellate
P.O. Box 15216
Philadelphia, PA 19125

Marisol Orihuela, Juris No. 439460
Jerome N. Frank Legal Services Org.
P.O. Box 209090
New Haven, CT 06520

Counsel for Amicus Curiae

DATE FILED: April 26, 2022

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

OTHER AUTHORITIES

STATEMENT OF INTEREST OF AMICUS CURIAE[1]

Upturn is a nonprofit organization based in Washington, D.C. that works with many leading civil rights 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 recently 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. 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 law 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 meaningful policies governing use of 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]

---

[1] No portion of this brief was written by counsel for a party to this appeal. Neither any party to this appeal, nor its counsel, contributed to the cost of the preparation or submission of this brief. No person or entity, other than the amicus and its members, contributed to the cost of the preparation or submission of this brief.

[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] 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 staff in-house.

This Brief aims to aid the Court in its understanding of how mobile device forensic tools work and how mobile device forensic tools can be used to narrow a cellphone search. This Brief also argues that the Court should use its supervisory authority to craft rules for the issuance and execution of cellphone search warrants.

ARGUMENT

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

Every day, law enforcement agencies across the country search hundreds to thousands of cellphones. To search these phones, law enforcement relies upon mobile device forensic tools (MDFTs). An MDFT is a computer program and its hardware that can copy and analyze data from a cellphone. MDFTs enable law enforcement to both extract and analyze data. MDFT software can run on a regular desktop computer, on a dedicated device like a tablet, or on a "kiosk" computer. These tools are sold by a range of companies, including AccessData, Cellebrite, Grayshift, Magnet Forensics, MSAB, and OpenText.[4]

[4] This Court deserves more context on Grayshift's amicus brief. During Upturn's research on MDFTs, Upturn sued the New York Police Department ("NYPD") under New York's Freedom of Information Law. At NYPD's request, Grayshift filed a letter in that case asking the NYPD to "include it in their opposition to Upturn's petition." *See Upturn, Inc. v. N.Y.C. Police Dep't*, Index No. 162380/2019 N.Y. Sup. Ct. NYSCEF DOC. No. 28. https://iapps.courts.state.ny.us/nyscef/ViewDocument?docIndex=dguHgSLyBI6BIQuqX0Marw==. That letter, which was filed for the purpose of preventing Upturn from learning how law enforcement like the NYPD uses GrayKey, asserted that "the broad contours of how [GrayKey] works are not known outside of Grayshift," "Grayshift does not publicly comment on or otherwise publicly discuss Gray[K]ey *[sic]*," and "Grayshift stands to suffer irreparable commercial harm if *even seemingly innocuous commercial or technical information is released*" (emphasis added). Further, GrayKey is only available to law enforcement agencies — even if defense attorneys in Connecticut had the resources to do so, they would be unable to purchase this tool, even if just to understand how it works. This Court should treat Grayshift's claims appropriately. *See Upturn, Inc. v. N.Y.C. Police Dep't,* 2021 N.Y. Slip Op. 31129 (N.Y. Sup. Ct. 2021).

Investigators initiate the extraction process by plugging a phone into the computer or tablet. Cellebrite software, which is like other tools,[5] will then 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 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 or videotape their exploration of a phone's content.

"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).[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) oversees their delivery and organization.

"File system extraction" is like 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 dishes that are not on the menu, which is possible at some restaurants, but not others.

---

[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.

[6] Pre-extraction 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.

[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.").

"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 must 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 (fully prepared menu items, ingredients, things in the trash) directly as it exists in the kitchen without mediation from the waitstaff.

After extraction, MDFT software programs allows law enforcement 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. 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.[8] This means law enforcement 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 in one place, as a grid of thumbnails, regardless of how they are organized or named on the phone.[9] MDFTs can also search for key terms across the entire phone (just as 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 BE USED TO NARROW THE SEARCH. BUT A TECHNICAL POSSIBILITY MEANS LITTLE WITHOUT THE FORCE OF LAW.

[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.

At each stage of the mobile device forensic process there are opportunities to narrow the search. MDFTs can limit what information is *copied* from the phone or can limit what information will be *analyzed*. MDFT software has built-in pre- and post-extraction filtering and categorization features, all of which can help narrow the search of a cellphone.

The simplest MDFT feature that can be used to narrow the search is the logical extraction interface. Cellebrite software, at the beginning of a logical extraction, prompts users to select the general categories of data to extract from the phone. This takes place before any data is copied from the phone. These categories include "call logs," "photos," "contacts," and "SMS test messages." Data is then 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 using the phone's own API. For example, law enforcement could limit a logical extraction to only text messages between March 1 and March 15.[10] These limits can be set *before* data is extracted by the MDFT, narrowing the range of data copied from the cellphone. This is because cellphones store data predictably under the two major operating systems (iOS and Android), and because all files contain integral metadata, such as each file's date of creation. Cellebrite tools also offer a "selective file system" extraction, which allows investigators to see which specific applications are present on the phone before extracting data. This method allows law enforcement to search for terms like "Facebook" or "Snapchat," or scroll through the list of available apps and then select them for extraction.

[10] Investigators do not need to see phone data in advance to set a tool like Cellebrite UFED to only select photos from a certain date range. With these filters, a MDFT will simply automatically inspect each file it finds on the phone, without the investigator seeing it, determine wither it fits into the filter, and only then copy the file. Files that don't fit the filter will not be copied over, so the investigator does not have to risk seeing them.

After extraction and during analysis, MDFTs offer comprehensive filtering and searching tools. Once the data is on the computer or tablet running the MDFT software, it can be more thoroughly sorted. Data can be sorted by its original location on the phone (*e.g.,* WhatsApp messages), or simply by media type (*e.g.,* photos). For example, Cellebrite software separates the various categories of data — like "SMS Messages," "Pictures," "Device Locations," or "Contacts," and data from individual apps — and allows investigators to view each category separately. In addition, investigators can use keywords to search (*e.g.,* "Jane Doe," "2025221234," or "janedoe@hotmail.com") across all data categories, or limit data displayed to only communications involving a certain phone number or contact over a certain period. More complex analytical features include the ability to view data with attached GPS information (like photos taken with the phone's camera) on a map, and use predictive analytics to assess whether certain data (like texts or photos) is "related" to certain predefined categories like "drugs," "weapons," or "nudity."

Regardless of the specific method, MDFTs make it possible to narrow the search. This means that an investigator does not need to access or review every file on a device to determine if it is relevant.

III. THIS COURT SHOULD NOT BE LED ASTRAY BY CLAIMS THAT BECAUSE DIGITAL EVIDENCE ON CELLPHONES MIGHT BE DISGUISED OR MANIPULATED, LAW ENFORCEMENT MUST BE EMPOWERED TO SEARCH THE ENTIRE CELLPHONE.

Law enforcement claim that because digital data on cellphones may be disguised or manipulated, they will not know where evidence will be located. As a result, they argue that they must be able to seize and search everything on a cellphone. This argument falls apart upon basic inspection.

First, this argument ignores how most modern cellphones store information and what information is accessible to cellphone users. While courts have frequently likened cellphones to computers, modern cellphones operate differently from computers "because mobile operatizing systems are designed for ease of use and do not emphasize user-directed file organization." Andrew D. Huynh, *What Comes After Get a Warrant: Balancing Particularity and Practicality in Mobile Device Search Warrants Post-Riley*, 101 Cornell L. Rev. 187, 207-208 (2015). "As any iPhone or Android user can tell, users no longer determine where an app stores its files, because users have no direct access to the file directory." Laurent Sacharoff, *The Fourth Amendment Inventory as a Check on Digital Searches*, 105 Iowa L. Rev. 1643, 1660 (2020). This layer of abstraction over the cellphone's core functions (that computers do not exhibit to the same extent) means that cellphone users are generally not able to directly manipulate their cellphone data.

Second, this argument ignores how MDFTs operate. MDFTs are agnostic toward file organization or file name. While a file's name or pathing may be useful for contextualizing data, MDFTs can simply traverse through all data on a phone and pick out data that has a particular data type, where file type is distinct from the name of a file (which most cellphone users do not control, anyway). As a result, even in the rare instance in which digital data may be disguised or manipulated, MDFTs can surface files based on their actual content, regardless of how a file is named or where it is located. This means that an image file hidden in an unexpected folder and renamed with a misleading file extension can still be discovered.

Third, this forces the exception to become the rule. Courts "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." *Id*., at 1658.

IV. CELLPHONE SEARCHES MERIT *SUI GENERIS* FOURTH AMENDMENT TREATMENT

A "cell phone search would typically expose the government to far more than the most exhaustive search of a house." *See Riley v. California*, 573 U.S. 373, 396 (2014). Combined with search warrants that are so broadly and ambiguously worded as to be limitless, MDFTs compound the issue: they facilitate exhaustive and indiscriminate searches of cellphones by law enforcement. *Amicus's* research demonstrates this happens hundreds of thousands of times per year, often in cases where the nexus between a cellphone's data and the alleged offense is tenuous. This arrangement is constitutionally untenable. More must be done, which is why cellphone searches merit *sui generis* treatment. *See* Cameron Cantrell, *A Dignitary Fourth Amendment Framework and Its Usefulness for Mobile Phone Searches*, 25 Va. J.L. & Tech 242 (2022). This Court should use its supervisory authority to craft specific guidance for the issuance and execution of cellphone search warrants. This guidance should clearly prescribe heightened particularity and overbreadth requirements for cellphone searches.

First, the Court's guidance should require that cellphone search warrants "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." *See Burns v. United States*, 235 A.3d 758, 773 (D.C. 2020). Rather than permitting

> law enforcement officers to operate through inferences, the Fourth Amendment demands a cellphone warrant specify the types of data to be seized with sufficient detail to distinguish material for which there is probable cause from information that should remain private. *See State v. Fairley* 457 P.3d 1150, 1154 (Wash. Ct. App. 2020).

To be sufficiently particular, "a warrant for a cell phone search presumptively must contain some temporal limit …. [and] should err on the side of narrowness." *See Commonwealth v.*

Snow, 486 Mass. 582, 594, 160 N.E.3d 277, 288 (2021). Further, the nexus between each category of information on a cellphone — such as texts, photographs, contacts, or emails — and the alleged criminal offense must be specific and clear. Cellphone search warrants to must be based on more than the fact that a defendant has a phone and the truism that people use phones to do seemingly everything. *See United States v. Opoku*, 556 F. Supp. 3d 633, 644 (S.D. Tex. 2021).

Second, the guidance should make clear that search warrants that authorize a search of "any and all cellphone data" or authorize a search of a laundry list of cellphone data are presumptively invalid. Catch-all provisions should be forbidden. The same is true of search warrants that authorize a search of a cellphone for "evidence related to this and other criminal offenses." Such warrants offer no limitations or restrictions on a search of a cellphone.

To illustrate, consider two hypotheticals. 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." 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." In Case A, it's highly likely that two different investigators will perform the same kind of search with an MDFT and return with similar evidence given the warrant's clear restrictions on the type of data and the timeframe. In Case B, one investigator might explore internet search history, calendar entries, text messages, dating app messages, and geolocation data amassed from apps downloaded onto the phone. Another might limit their search just to text messages and photos. Ultimately, it is unlikely they will perform the same search, or return with the same evidence. 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.

Third, the guidance should not extend the plain view exception to cellphone search warrants. The plain view exception "may not be used to extend a general exploratory search … until something incriminating at last emerges." *See Coolidge v. New Hampshire* 406 U.S. 443, 466 (1971). But in digital searches nearly anything can come into plain view. This "undercuts the plain view's pivotal assumption" — that any intrusion would be "minor" — and "effectively converts the plain view doctrine into a vehicle for the execution of a general warrant." *See State v. Bock*, 310 Or. App. 329, 339, 485 P.3d 931, 938 (2021).

Fourth, cellphone search warrants cannot rely on general statements that digital data may be disguised or manipulated to justify a search of the entire phone. If law enforcement has specific evidence to believe a more technically sophisticated user took steps to conceal digital data on a cellphone, they can seek a broader warrant based on that specific evidence.

Finally, the guidance should insist upon the production of digital audit logs created by the MDFT upon return of the warrant. Such logs would document the precise steps that law enforcement took when searching a phone to ensure compliance with the warrant. In particular, audit logs could equip judges to assess the reasonableness of a search technique and ascertain if the search was sufficiently tailored to the search warrant.

V. CONCLUSION

Every day across the country, hundreds to thousands of cellphone searches occur. Without guidance from this Court clearly establishing heightened requirements for cellphone search warrants, mobile device forensic tools will continue to facilitate indiscriminate searches of cellphones that sit at odds with the Fourth Amendment's protections.

Respectfully submitted,

/s/ Jim Davy
Jim Davy
PA I.D. No. 321631
All Rise Trial & Appellate
P.O. Box 15216
Philadelphia, PA 19125

/s/ Marisol Orihuela
Marisol Orihuela
Jerome N. Frank Legal Services Org.
All Rise Trial & Appellate
P.O. Box 209090
New Haven, CT 06520

Counsel for *Amicus Curiae* Upturn

April 26, 2022

CERTIFICATION

Pursuant to Practice Book § 62-7, on this 26th day of April, 2022, the undersigned hereby certifies that this document complies with all format provisions and further certifies that a copy of the foregoing was delivered in-hand, by first-class mail, postage pre-paid, or by fax or electronic delivery to:

Jennifer Smith
Assistant Public Defender
Office of the Chief Public Defender
Legal Services Unit
55 W. Main Street, Suite 430
Waterbury, CT 06702
Email: Jennifer.Smith@pds.ct.gov
Tel. (203) 574-0029

Ronald G. Weller
Senior Assistant State's Attorney
Office of the Chief State's Attorney
Appellate Bureau
300 Corporate Place
Rocky Hill, CT 06067
Email: Ronald.Weller@ct.gov, DCJ.OCSA.Appellate@ct.gov
Tel. (860) 258-5807

Thadius L. Bochain
Deputy Assistant State's Attorney
Office of the Chief State's Attorney
Appellate Bureau
300 Corporate Place
Rocky Hill, CT 06067
Thadius.Bochain@ct.gov, DCJ.OCSA.Appellate@ct.gov
Tel. (860) 258-5807

/s/ Marisol Orihuela
Marisol Orihuela

CERTIFICATION

The undersigned attorney hereby certifies, pursuant to Connecticut Rules of Appellate Procedure § 67-2, that:

(1) the electronically submitted brief has been delivered electronically to the last known e-mail addresses of each counsel of record for whom an email address has been provided; and

(2) the electronically submitted brief and the filed paper brief and appendix have been redacted or do not contain any names or other personal identifying information that is prohibited from disclosure by rule, statute, court order or case law; and

(3) a copy of the brief has been sent to each counsel of record and to any trial judge who rendered a decision that is the subject matter of the appeal, in compliance with § 62-7; and

(4) the brief being filed with the appellate clerk are true copies of the brief that was submitted electronically; and

(5) the brief complies with all provisions of this rule.

/s/ Marisol Orihuela
Marisol Orihuela

Counsel for Amicus