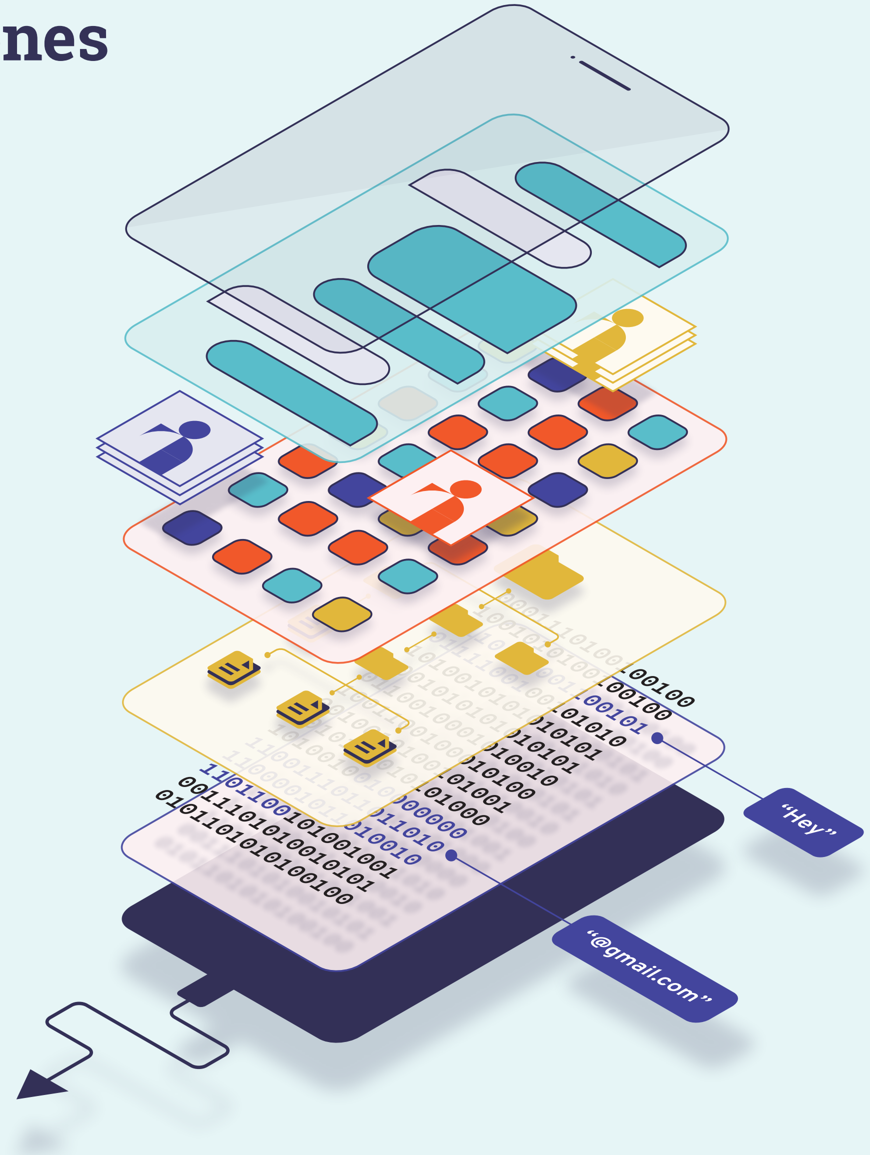
Upturn
Toward Justice
in Technology

October 2020

Mass Extraction:

The Widespread Power of U.S. Law Enforcement to Search Mobile Phones



Logan Koepke
Emma Weil
Urmila Janardan
Tinuola Dada
Harlan Yu

Mass Extraction:

The Widespread Power of U.S. Law Enforcement to Search Mobile Phones

October 2020

Logan Koepke
Emma Weil
Urmila Janardan
Tinuola Dada
Harlan Yu

About Upturn

Upturn is a 501(c)(3) nonprofit organization that advances equity and justice in the design, governance, and use of digital technology. For more information, see https://www.upturn.org.

Upturn
Toward Justice
in Technology

Contents

Executive Summary

Every day, law enforcement agencies across the country search thousands of cellphones, typically incident to arrest. To search phones, law enforcement agencies use mobile device forensic tools (MDFTs), a powerful technology that allows police to extract a full copy of data from a cellphone — all emails, texts, photos, location, app data, and more — which can then be programmatically searched. As one expert puts it, with the amount of sensitive information stored on smartphones today, the tools provide a "window into the soul."

This report documents the widespread adoption of MDFTs by law enforcement in the United States. Based on 110 public records requests to state and local law enforcement agencies across the country, our research documents more than 2,000 agencies that have purchased these tools, in all 50 states and the District of Columbia. We found that state and local law enforcement agencies have performed hundreds of thousands of cellphone extractions since 2015, often without a warrant. To our knowledge, this is the first time that such records have been widely disclosed.

Every American is at risk of having their phone forensically searched by law enforcement.

Law enforcement use these tools to investigate not only cases involving major harm, but also for graffiti, shoplifting, marijuana possession, prostitution, vandalism, car crashes, parole violations, petty theft, public intoxication, and the full gamut of drug-related offenses. Given how routine these searches are today, together with racist policing policies and practices, it's more than likely that these technologies disparately affect and are used against communities of color.

The emergence of these tools represents a dangerous expansion in law enforcement's investigatory powers. In 2011, only 35% of Americans owned a smartphone. Today, it's at least 81% of Americans. Moreover, many Americans — especially people of color and people with lower incomes — rely solely on their cellphones to connect to the internet. For law enforcement, "[m]obile phones remain the most frequently used and most important digital source for investigation."

We believe that MDFTs are simply too powerful in the hands of law enforcement and should not be used. But recognizing that MDFTs are already in widespread use across the country, we offer a set of preliminary recommendations that we believe can, in the short-term, help reduce the use of MDFTs. These include:

- banning the use of consent searches of mobile devices,
- abolishing the plain view exception for digital searches,
- requiring easy-to-understand audit logs,
- enacting robust data deletion and sealing requirements, and
- requiring clear public logging of law enforcement use.

Of course, these recommendations are only the first steps in a broader effort to minimize the scope of policing, and to confront and reckon with the role of police in the United States. This report seeks to not only better inform the public regarding law enforcement access to mobile phone data, but also to recenter the conversation on how law enforcement's use of these tools entrenches police power and exacerbates racial inequities in policing.

1. Introduction

"We just want to check your phone to see if you were there."

You know you weren't at the 7-Eleven — you hadn't been there in two weeks. You don't want the cops to search your phone, but you feel immense pressure. "If you don't give us your consent, we'll just go to a judge to get a search warrant — do you really want to make us handle this the hard way?" You relent, knowing that they aren't going to find anything. You quickly sign a form, and the police officers take your phone.

What happens next, in a backroom of the police department, is secretive. Within a few hours, the police have traced almost everywhere you've been, looked at all of your text messages, videos, and photos, searched through your Google search history, and have built a highly detailed profile of who you are. This report seeks to illuminate what happens in those police backrooms.[1]

Every day, law enforcement agencies across the country search thousands of cellphones, typically incident to arrest. Often, these searches are done against people's wills or without meaningful consent. To search phones, law enforcement agencies use **mobile device forensic tools (MDFTs)**, a powerful technology that allows police to extract a full copy of data from a cellphone — all emails, texts, photos, locations, app data, and more — which can then be programmatically searched.[2] By physically connecting a cellphone to a forensic tool, law enforcement can extract,

[1] As of the publication of this report, we are suing the NYPD for records concerning the department's use of mobile device forensic technology. Upturn is represented on a pro bono basis by Shearman & Sterling, LLP and the Surveillance Technology Oversight Project (S.T.O.P.). The NYPD argues that they "should not be required to actively harm its investigative capabilities in responding to [Upturn's] FOIL Request," that "seeking information that, if disclosed, would harm those vendors' continued business activity," and that "confirming that the potential scope of Upturn's demand would overwhelm NYPD's FOIL response capacity." *See* NYPD Memorandum of Law in Support of its Verified Answer and Objections in Points of Law, September 4, 2020, Index No. 162380/2019 Doc. 21.

[2] We borrow the umbrella term "mobile device forensic tools," from the National Institute of Standards and Technology. Others have used different terms, such as "mobile phone extraction tools," "mobile device acquisition tools," "mobile phone hacking tools," and "mobile phone cracking tools." We use "mobile device forensic tools" as we believe it's the most accurate terminology. *See* NIST, *Mobile Security and Forensics*, available at https://csrc.nist.gov/Projects/Mobile-Security-and-Forensics/Mobile-Forensics. ("When mobile devices are involved in a crime or other incident, forensic specialists require tools that allow the proper retrieval and speedy examination of information present on the device. A number of existing commercial off-the-shelf (COTS) and open-source products provide forensics specialists with such capabilities.")

analyze, and present data that's stored on the phone.[3] As one expert puts it, with the amount of sensitive information stored on smartphones today, MDFTs provide a "window into the soul."[4]

Law enforcement agencies of all sizes across the United States have already purchased tens of millions of dollars worth of mobile device forensic tools. The mobile device forensic tools that law enforcement use have three key features. First, the tools empower law enforcement to access and extract vast amounts of information from cellphones. Second, the tools organize extracted data in an easily navigable and digestible format for law enforcement to more efficiently analyze and explore the data. Third, the tools help law enforcement circumvent most security features in order to copy data.

The proliferation and development of mobile device forensic tools in large part mirrors the adoption of smartphones across the United States. In 2011, only 35% of Americans owned a smartphone.[5] Today, it's at least 81% of Americans.[6] Moreover, many Americans — especially people of color and people with lower incomes — rely solely on their cellphones to connect to the internet.[7] For law enforcement, "[m]obile phones remain the most frequently used and most important digital source for investigation."[8] In many ways, mobile device forensic tools have helped to vastly expand police power in ways that are rarely apparent to communities.

In 2014, the Supreme Court decided *Riley v. California*, holding that the warrantless search of a cellphone incident to an arrest was unconstitutional.[9] As a result, today law enforcement need a warrant to search a cellphone.[10] Since this landmark decision, the public debate surrounding

[3] There are a surprisingly large range of tools that can serve these purposes: some work to get easily accessible data on all popular phones, and some are tailored to specific systems or phones; some can be purchased and used as much as police want, and others cost per-use or can only be used so many times.

[4] 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/.

[5] Pew Research Center, "Mobile Fact Sheet," June 12, 2019, available at https://www.pewresearch.org/internet/fact-sheet/mobile/.

[6] *Id.* (Noting 96% own a cellphone of some kind.)

[7] Camille Ryan, U.S. Department of Commerce, Economics and Statistics Administration, U.S. Census Bureau, "Computer and Internet Use in the United States: 2016," American Community Survey Reports, August 2018; Jamie M. Lewis, *Handheld Device Ownership: Reducing the Digital Divide?*, March 2017, https://www.census.gov/library/working-papers/2017/demo/SEHSD-WP2017-04.html.

[8] Cellebrite Annual Industry Trend Survey 2019: Law Enforcement, at 3.

[9] Riley v. California, 573 U.S. 373 (2014). In this case, police searched two individuals' cellphones after they had been arrested: David Riley in August 2009 for driving with expired registration tags, and Brima Wurie in September 2007 for allegedly making a drug sale. In both cases, police officers at first manually examined the phones at the police station — scrolling through contact lists, and looking through videos and pictures. Police did not obtain a warrant to search either phone. *See* People v. Riley, D059840 (Cal. Ct. App. Feb. 8, 2013) https://casetext.com/case/people-v-riley-263; United States v. Wurie, 728 F.3d 1 (1st Cir. 2013) https://casetext.com/case/united-states-v-wurie-4.

[10] Riley v. California, 573 US 373 (2014).

evidence on mobile phones has largely focused on the rare cases when law enforcement can't access the contents of a phone, due to encryption. For example, after the high-profile San Bernardino shooting in 2015[11] and, more recently, after a deadly shooting at Naval Air Station Pensacola.[12]

However, substantial public attention to these rare, high-profile cases in which law enforcement *cannot* access the contents of a phone overshadows a more significant change: the rise in law enforcement's ability to search the thousands of phones that they can access in a wide range of cases, and the power this gives to the police when it has routine and easy access to people's most sensitive data.

Throughout 2019 and 2020, Upturn filed more than 110 public records requests with state and local law enforcement agencies to determine which agencies have access to mobile device forensic tools, and how they use them. Some have suggested that technologies "to extract data from mobile phones . . . are things that few state and local police departments can afford,"[13] or that this technology is "cost prohibitive, however, for all but a handful of local law enforcement agencies."[14]

But our research tells a different story. Our records show that at least 2,000 agencies have purchased a range of products and services offered by mobile device forensic tool vendors. Law enforcement agencies in all 50 states and the District of Columbia have these tools. Each of the largest 50 police departments have purchased or have easy access to mobile device forensic tools. Dozens of district attorneys' and sheriff's offices have also purchased them. Many have done so through a variety of federal grant programs. Even if a department hasn't purchased the technology itself, most, if not all, have easy access thanks to partnerships, kiosk programs, and sharing agreements with larger law enforcement agencies, including the FBI.

[11] The Department of Justice sought to compel (and a federal court ordered) Apple to provide technical assistance in unlocking an iPhone used by the gunman. *In The Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300*, Order Compelling Apple, Inc. to Assist Agents in Search, February 16, 2016, *available at* https://assets.documentcloud.org/documents/2714001/SB-Shooter-Order-Compelling-Apple-Asst-iPhone.pdf.

[12] Attorney General William Barr publicly called on Apple to help unlock two phones used by the gunman. See Katie Benner, "Barr Asks Apple to Unlock Pensacola Killer's Phones, Setting Up Clash," The New York Times, Jan. 13, 2020, *available at* https://www.nytimes.com/2020/01/13/us/politics/pensacola-shooting-iphones.html. The Department of Justice also recently held a symposium regarding access to evidence on digital devices, entitled "Lawless Spaces: Warrant-Proof Encryption and Its Impact on Child Exploitation Cases." *See* https://www.justice.gov/olp/lawless-spaces-warrant-proof-encryption-and-its-impact-child-exploitation-cases.

[13] William, Carter, Jennifer Daskal, *Low Hanging Fruit: Evidence-Based Solutions to the Digital Evidence Challenge*, Center for Strategic & International Studies, July 2018, 12.

[14] New York County District Attorney Cyrus R. Vance, Jr., Written Testimony for the United States Senate Committee on the Judiciary on Smartphone Encryption and Public Safety, "Smartphone Encryption and Public Safety," Washington, D.C. December 10, 2019, https://www.judiciary.senate.gov/imo/media/doc/Vance%20Testimony.pdf.

Despite the widespread proliferation of these tools, there is almost no public accounting of how often or in what kinds of cases law enforcement use these tools. The under-the-radar adoption of these tools also means that there has been little public debate about the risks of these tools and how they shift power to the police.

The records we obtained through our public records requests demonstrate that law enforcement use mobile device forensic tools as an all-purpose investigative tool for a wide array of cases. Law enforcement use these tools to investigate not only cases involving major harm, but also for graffiti, shoplifting, marijuana possession, prostitution, vandalism, car crashes, parole violations, petty theft, public intoxication, and the full gamut of drug-related offenses. Few departments have detailed policies governing how and when officers can use this technology. Most either have boilerplate policies that accomplish little, or have no policies in place at all.

This report proceeds as follows. In Section 2, we describe the precise technical capabilities of mobile device forensic tools. With that technical background, in Section 3, we then trace the widespread proliferation of mobile device forensic tools throughout local law enforcement agencies nationwide. Next, in Section 4, we show how agencies routinely use these tools, even for the most mundane cases. In Section 5, we explain the unconstrained nature of these uses, especially as most agencies have no specific policies in place. Finally, we offer policy recommendations for state and local policymakers in Section 6.

This report seeks to not only better inform the public regarding law enforcement access to mobile phone data, but also to recenter the conversation on how law enforcement's use of these tools entrenches police power and exacerbates racial inequities in policing.

2. Technical Capabilities of Mobile Device Forensic Tools

We begin with a basic primer on how mobile device forensic tools (MDFTs) work and explain their capabilities with respect to **data extraction**, **data analysis**, and **security circumvention**.[15] Our technical analysis surfaces three key points:

- **MDFTs are designed to copy all of the data commonly found on a cellphone.** Mobile device forensic tools are designed to extract the maximum amount of information possible. This includes data like your contacts, photos, videos, saved passwords, GPS records, phone usage records, and even "deleted" data.
- **MDFTs make it easy for law enforcement to analyze and search data copied from phones.** A range of features help law enforcement quickly sift through gigabytes of data — a task that would otherwise require significantly more labor. This includes mapping where someone has been through GPS data, searching specific keywords, and searching images using image classification tools.
- **While security features like device encryption have received significant public attention, MDFTs can circumvent most security features in order to copy data.** Challenges to access can often be surmounted, because of the wide range of phones with security vulnerabilities or design flaws. Even in instances where full forensic access is difficult due to security features, mobile device forensic tools can often still extract meaningful data from phones.

MDFTs provide sweeping access to personal information on a phone, enabling "an extent of surveillance that in earlier times would have been prohibitively expensive."[16] In many circumstances, this access can be disproportionately invasive compared to the scope of evidence being sought and poses an alarming challenge to existing Fourth Amendment protections. **Our findings suggest that today's mobile device forensic tools can extract data from most phones and represent a dangerous expansion in law enforcement's investigatory powers.**

[15] Little public research has explored the precise technical capabilities of mobile device forensic tools that allow law enforcement to search thousands of phones in a wide range of everyday cases. To the extent there has been a public debate on mobile device forensic tools, it has centered on the rare cases when law enforcement cannot access the contents of a phone, due to encryption.

[16] United States v. Garcia, 474 F.3d 994, 998 (7th Cir. 2007).

A Primer

Mobile device forensics is typically a two-step process: data extraction, then analysis. MDFTs help law enforcement accomplish both.[17] An MDFT is a computer program and its supplemental equipment (*e.g.*, cables, external storage) that can copy and analyze data from a cellphone or other mobile device.[18] The 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 Cellebrite, Grayshift, MSAB, Magnet Forensics, and AccessData.

The investigator initiates the extraction process by plugging the phone into the computer or tablet. With Cellebrite software (which is similar to other tools), once the tool recognizes the phone,[19] 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, as shown in Figures 2.1 and 2.2.[20] Often, in order to extract data, tools may bypass a phone's security features by taking advantage of security flaws or built-in diagnostic or development tools.

In essence, to extract data from a device, some methods work with the phone's built-in features, while others work around them. Circumventing the phone's built-in features usually entails more data access, but any extraction method can be invasive because of how much data people store on their phones.[21]

[17] In order to assess the technical capabilities of current mobile device forensic tools, we reviewed technical manuals, examined software release notes, marketing materials, webinars, and digital forensics blog posts and forums. We also visited the office of one of the few public defenders in the US with these forensic tools (and forensic staff) in-house.

[18] We borrow the umbrella term "mobile device forensic tools," from the National Institute of Standards and Technology. *See* NIST, *Mobile Security and Forensics*, *available at* https://csrc.nist.gov/Projects/Mobile-Security-and-Forensics/Mobile-Forensics. ("When mobile devices are involved in a crime or other incident, forensic specialists require tools that allow the proper retrieval and speedy examination of information present on the device. A number of existing commercial off-the-shelf (COTS) and open-source products provide forensics specialists with such capabilities.")

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

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

[21] We make these distinctions to give a sense of how the tools work and to explain how searches can technically be limited in scope based on the physical state of data when it is copied.

Figure 2.1

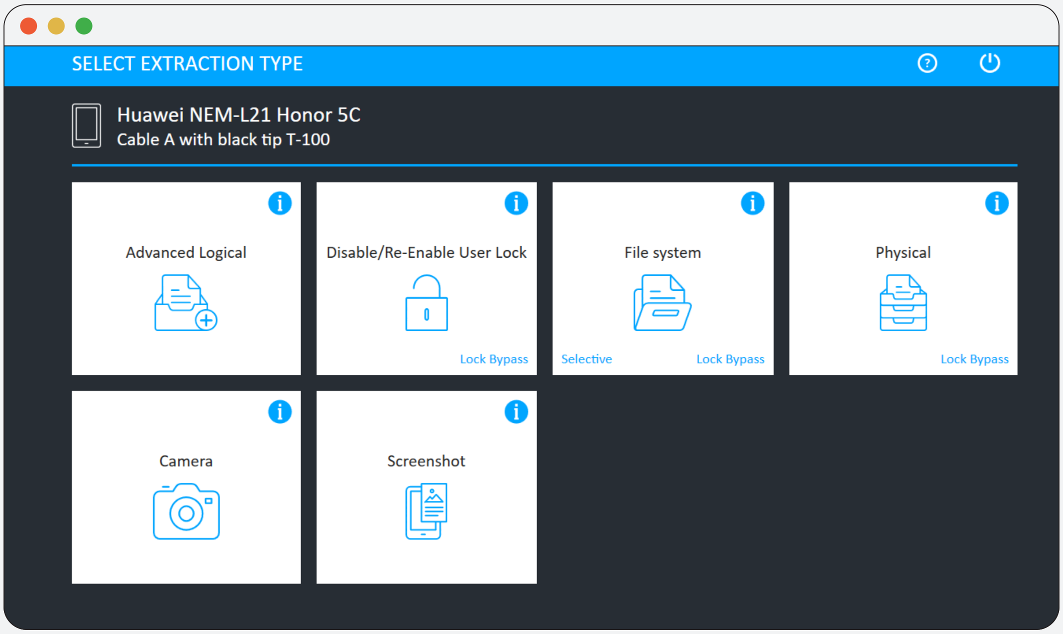


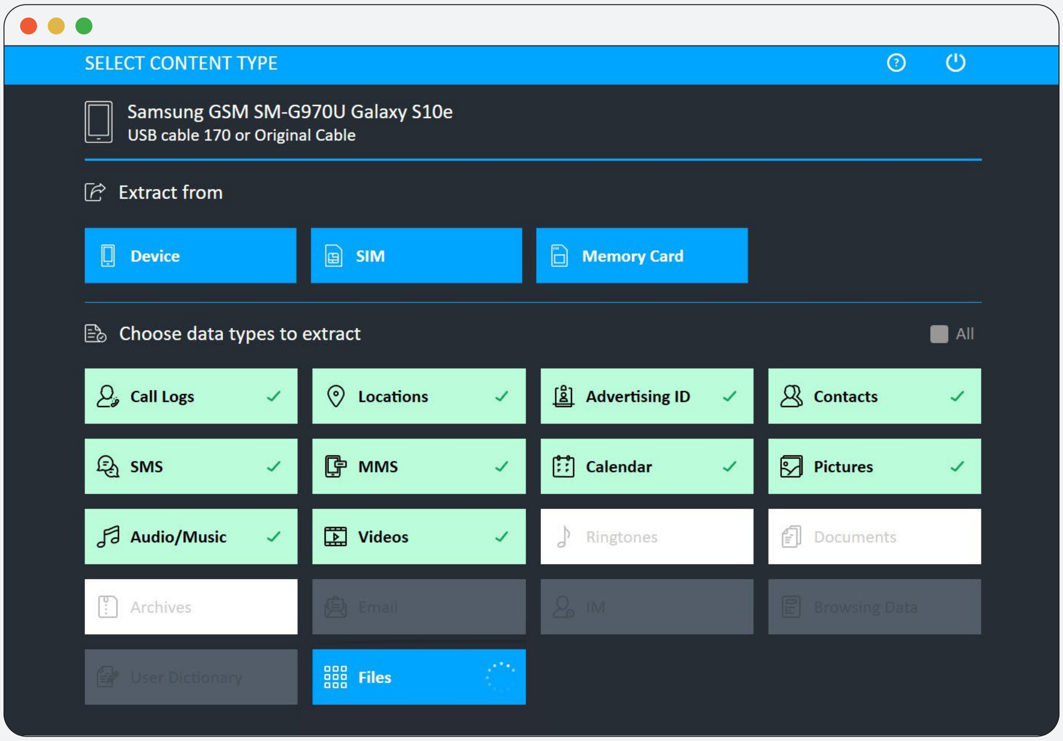
Figure 2.1 *shows one of the initial user interface screens of Cellebrite Universal Forensic Extraction Device (UFED). The "Select Extraction Type" screen offers various options for type of extraction and device unlocking.*[22]

After extraction, law enforcement use MDFTs to efficiently analyze the data — after all, the ability to copy gigabytes of phone data is not worth much if it can't be effectively searched. 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. They can also search for key terms across the entire phone, just like you might use Google to search the web. This means police can take data extracted from different apps on the phone and view them together as a chronological series of events. It also means they can pull all pictures from the phone to view in one place, regardless of how they are organized on the phone.[23]

[22] Paul Lorentz and Heather Mahalik, Cellebrite Blog, "Android Data Acquisition Simplified," July 20, 2020, *available at* https://www.cellebrite.com/en/blog/android-acquisition-simplified/.

[23] When you take a photo with your phone's camera app, it's stored in a different folder than photos taken using other apps, like Instagram or Whatsapp. With just 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.

Figure 2.2



SELECT CONTENT TYPE

Samsung GSM SM-G970U Galaxy S10e
USB cable 170 or Original Cable

Extract from

Choose data types to extract ☐ All

- Call Logs ✓
- Locations ✓
- Advertising ID ✓
- Contacts ✓
- SMS ✓
- MMS ✓
- Calendar ✓
- Pictures ✓
- Audio/Music ✓
- Videos ✓
- Ringtones
- Documents
- Archives
- Email
- IM
- Browsing Data
- User Dictionary
- Files

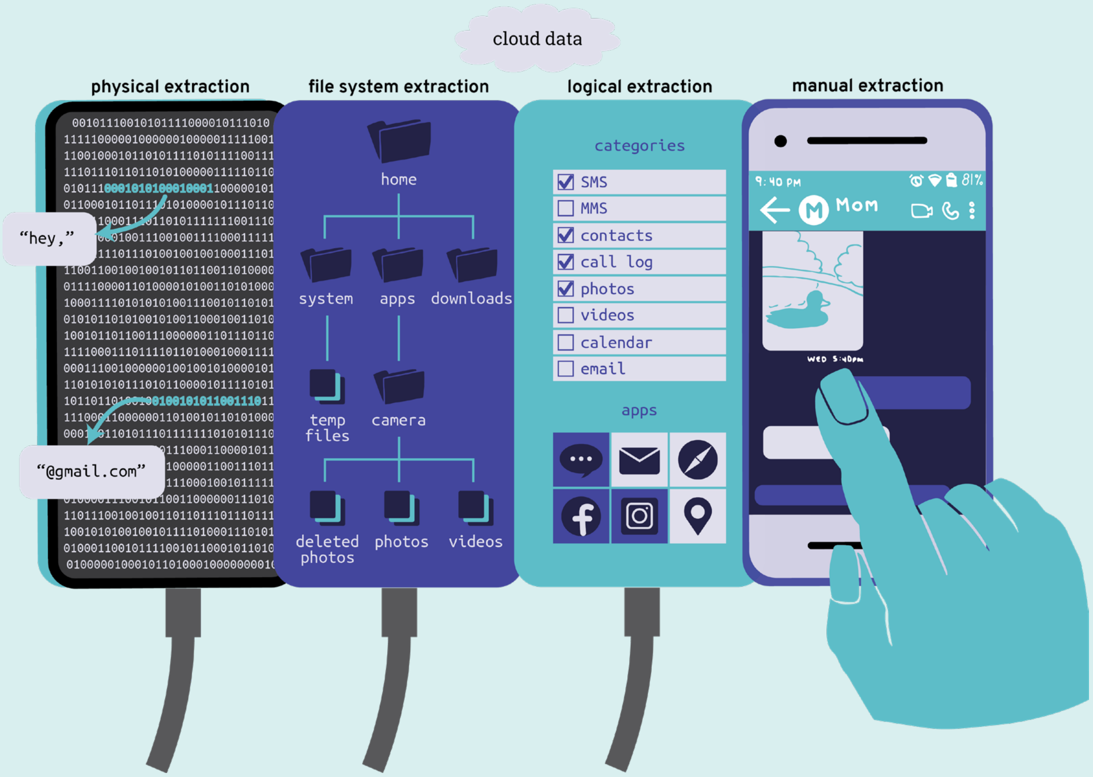
Figure 2.2 shows the "Select Content Type" screen of the Cellebrite UFED user interface, where the user can select the categories of data they want to extract from the phone's internal storage, SIM card, and/or memory card. There is a convenient option to select "All" categories.[24]

Device Extraction

Modern cellphones are a convenient combination of many tools: they're phones, cameras, notebooks, diaries, navigation devices, web browsers, and more. Smartphones centralize patterns of life on a single device with seemingly endless storage. MDFTs allow law enforcement to access all of this data and more, whether or not people knowingly store that information on their phones.

[24] Paul Lorentz and Heather Mahalik, Cellebrite Blog, "Android Data Acquisition Simplified," July 20, 2020, *available at* https://www.cellebrite.com/en/blog/android-acquisition-simplified/.

EXTRACTION METHODS



There are a few distinct methods for copying data from phones.[25]

Manual Extraction

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. This process can compromise data integrity, as it may leave new artifacts of use on the phone.[26]

[25] The mobile device forensics industry has its own labels for these methods, but often uses them imprecisely, or for marketing purposes.

[26] This can create issues with forensic integrity, as a later forensic extraction would show records of these interactions. Forensic integrity refers to the assurance that police or other parties 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.

Logical Extraction

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).[27] 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.[28]

File System Extraction

File system extraction is similar to logical extraction, but it copies even more data — such as files or other data (like 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

Physical extraction 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. This data 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.

[27] 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.")

[28] A logical extraction tends to be the quickest method of extracting mobile phone data, because it does not copy every single piece of data on the phone, and can easily be limited in scope to certain apps or types of files (for example, only texts, calls, and contacts). Although logical extractions are usually faster, file system or physical extractions are often more desirable, because those methods can retrieve richer data, like app usage logs, and can often discover deleted data.

Smartphone photography is a prime illustration of how invasive MDFTs can be. No longer limited by physical prints, people casually accumulate thousands of photos on their phones. In 2017, an estimated 85% of all pictures taken were captured on smartphones, and the number of pictures taken each year worldwide has doubled from 660 billion in 2013 to 1.2 trillion in 2017.[29] MDFTs also extract the embedded metadata from each image file, such as the GPS coordinates of where a photo was taken, and the time and date it was taken.[30] Not only do people carry with them orders of magnitude more photos than they would without a smartphone, but they may also unwittingly carry with them a geographic record of their movements.

MDFTs extract gigabytes of data that are both casually accumulated and unexpectedly revealing. Their core utility is to extract call logs, contacts, text conversations, and photos. However, there is much more stored on phones than these obvious categories. Data from online accounts, third-party apps, "deleted" data, and even people's precise interactions with the device itself all leave behind artifacts, which MDFTs can find. Through this "gold mine of information,"[31] "the sum of an individual's private life can be reconstructed."[32]

Application Data

Virtually every app on a smartphone stores user information, from mobile web browsing history to health tracker data, mobile wallet payments, dating app conversations, and more. MDFTs can copy data for the most popular apps, and are constantly updated to support a wide range of apps. For example, Cellebrite's tools can extract and interpret data from at least 181 apps on Android's operating system, and at least 148 apps on Apple iPhones. These apps span from Google apps like Google Maps, Gmail, and Google Photos, to dating apps like Tinder, Grindr, and OkCupid, to Nike+ Run Club, to social media apps like Facebook, Instagram, Twitter, and Snapchat,

[29] Felix Richter, "Smartphones Cause Photography Boom," August 31, 2017, Statista, https://www.statista.com/chart/10913/number-of-photos-taken-worldwide/.

[30] Exchangeable Image File Format (EXIF) data is embedded into files, documenting, among other things, the date and time the picture was taken, camera settings like shutter speed, type of camera used, and the GPS coordinates of where a picture was taken. See "Pic2Map Photo Location Viewer" *available at* https://www.pic2map.com/. *See also* "Exif Tool" available at https://exiftool.org/.

[31] Thomas Germain, "How a Photo's Hidden 'Exif' Data Exposes Your Personal Information," Dec. 6, 2019, Consumer Reports, *available at* https://www.consumerreports.org/privacy/what-can-you-tell-from-photo-exif-data/.

[32] Riley v. California, 573 U.S. 373, 394 (2014).

web browsers like Chrome and Firefox, and even encrypted messenger apps like Signal and Telegram.[33] Because user-installed apps from third parties usually store data in predictable ways, it can be very easy for MDFTs to copy and parse data from them.[34]

Account-Based Cloud Data

Not all of the app data on phones are stored on the phone itself. Many apps are account-based, meaning the data in the account is synced to the cloud so that it can be accessed remotely. This means that data created elsewhere on the account may end up existing on the phone, data from the phone may be backed up remotely, and remote data may be viewable from the phone. MDFTs account for each of these possibilities, and many vendors even offer specific features or products to extract cloud backups and other remote account information. For example, Cellebrite offers a UFED Cloud product specifically for these purposes.[35]

One way that MDFTs access account-based information is by copying the account credentials that the phone stores in order to remain logged in, essentially pretending to be the user's phone. This gives investigators access to any cloud data that the user has access to from their phone, like social media data, emails, or backups of photos and other data. For the most part, this data is not encrypted. For example, an MDFT may be able to pull a remote backup of the phone from Apple's iCloud service by copying information it finds in the phone's password management system.[36] And because many services allow users to download all of their data (*e.g.*, Google's Takeout), MDFTs can access even more sources of data, some of which are shown in Figure 2.3. Figures 2.4 to 2.6 show the process of retrieving account-based cloud data in Magnet's AXIOM software.

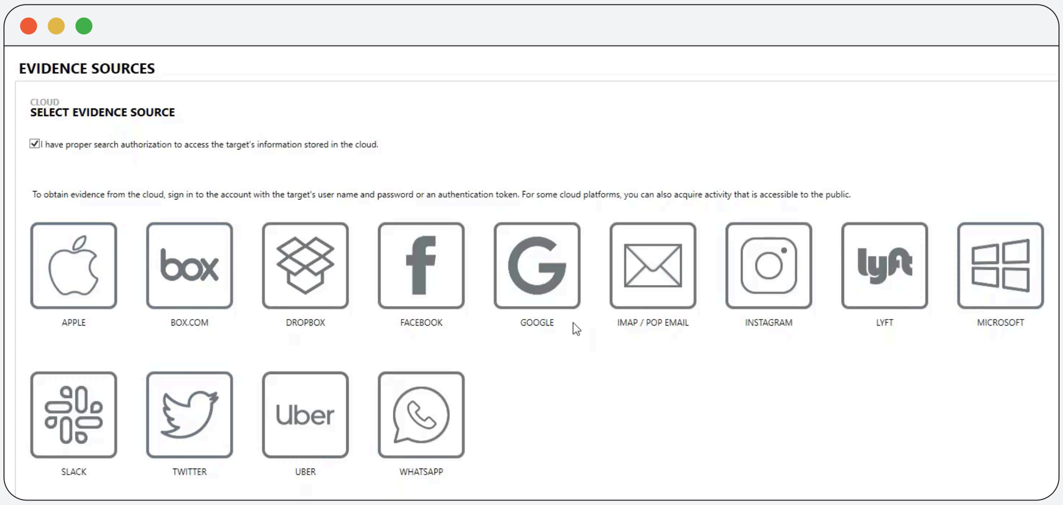
[33] Cellebrite, "Cellebrite Physical Analyzer, Cellebrite Logical Analyzer, UFED Cloud and Cellebrite Reader v7.35," Release Notes, June 2020, *available at* https://cf-media.cellebrite.com/wp-content/uploads/2020/06/ReleaseNotes_UFEDPA_735_web.pdf. Data from apps that aren't supported by an MDFT vendor may nevertheless still be extracted, but likely will not be parsed out. As a result, it would still be possible to examine this data, but it would take more time and skill.

[34] Through all of these applications, mobile device forensic tools can access fairly precise location information, in-app communications, and in-app photos. Searches on the web from a browser app are also easily accessible — revealing personal interests, hobbies, fears and worries, and even medical conditions. See, e.g., Proper searching in Physical Analyzer can help you identify location data of interest," Cellebrite, *available at* https://www.youtube.com/watch?v=0byyzAO4akE; Jason Bays, Umit Karabiyik, "Forensic Analysis of Third Party Location Applications in Android and iOS," *available at* https://arxiv.org/pdf/1907.00074.pdf; Barak Goldberg, "How Health App Data Improves Location Accuracy and Activity Identification for Investigations," October 24, 2019, *available at* https://www.cellebrite.com/en/blog/how-health-app-data-improves-location-accuracy-and-activity-identification-for-investigations/; Heather Mahalik, "How to View Chat Conversations in Cellebrite Physical Analyzer," June 1, 2020, *available at* https://www.cellebrite.com/en/ask-the-expert/how-to-view-chat-conversations-in-cellebrite-physical-analyzer/; Ryan Philips, "Infant death case heading back to grand jury," May 8, 2019, Starkville Daily News, *available at* https://www.starkvilledailynews.com/infant-death-case-heading-back-to-grand-jury/article_cf99b-cb0-71cc-11e9-963a-eb5dc5052c92.html. (Internet search histories, from law enforcement's point of view, give investigators a supposed map to your intent, mental state, or motives. In this case, Latice Fisher's internet search results gave law enforcement a "motive" — if she wanted to be pregnant, why was she looking up medication abortion?).

[35] Cellebrite UFED Cloud, https://www.cellebrite.com/en/ufed-cloud.

[36] This can also be accomplished via a warrant to the holding company itself, *e.g.*, Apple. This method is legally dubious and would require a second warrant in most instances, but MDFTs are also built for internal corporate investigations where employers have more control over their employee's accounts.

Figure 2.3



EVIDENCE SOURCES

CLOUD

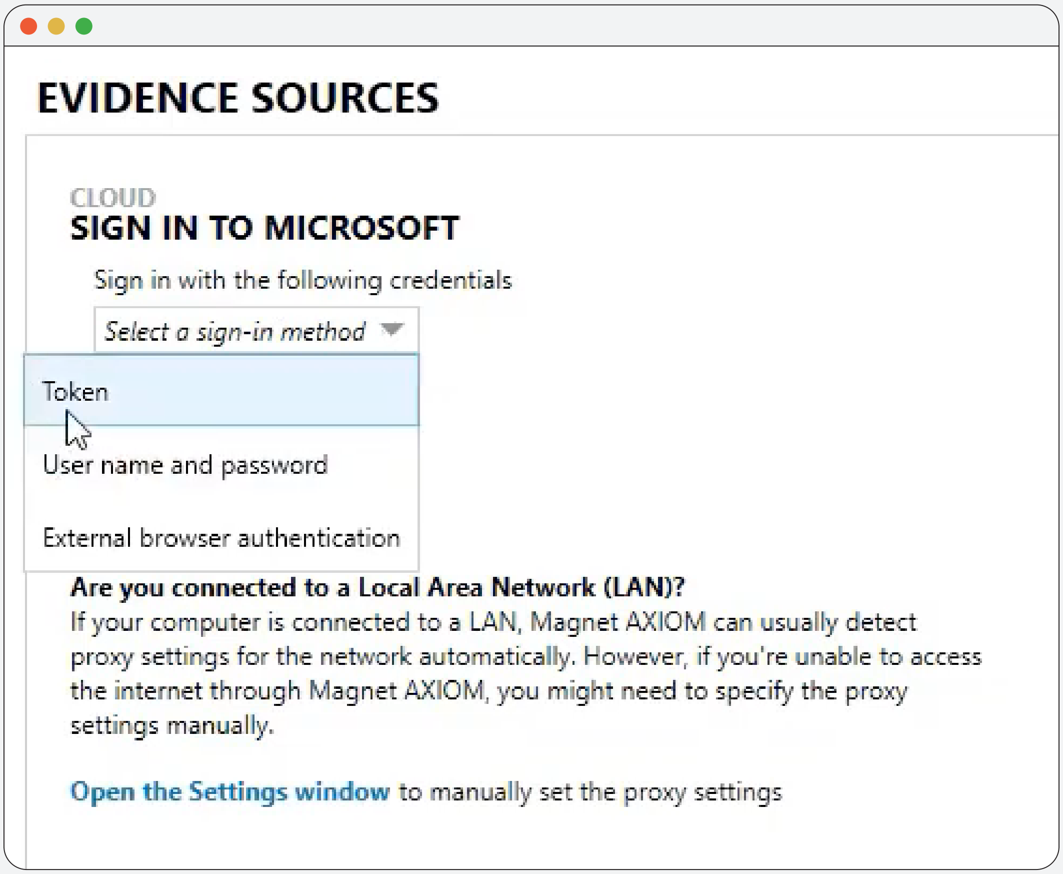
SELECT EVIDENCE SOURCE

☑ I have proper search authorization to access the target's information stored in the cloud.

To obtain evidence from the cloud, sign in to the account with the target's user name and password or an authentication token. For some cloud platforms, you can also acquire activity that is accessible to the public.

***Figure 2.3** shows the user interface of Magnet AXIOM, displaying options to extract remote data from various internet-based accounts.*[37]

Figure 2.4



EVIDENCE SOURCES

CLOUD

SIGN IN TO MICROSOFT

Sign in with the following credentials

Are you connected to a Local Area Network (LAN)?

If your computer is connected to a LAN, Magnet AXIOM can usually detect proxy settings for the network automatically. However, if you're unable to access the internet through Magnet AXIOM, you might need to specify the proxy settings manually.

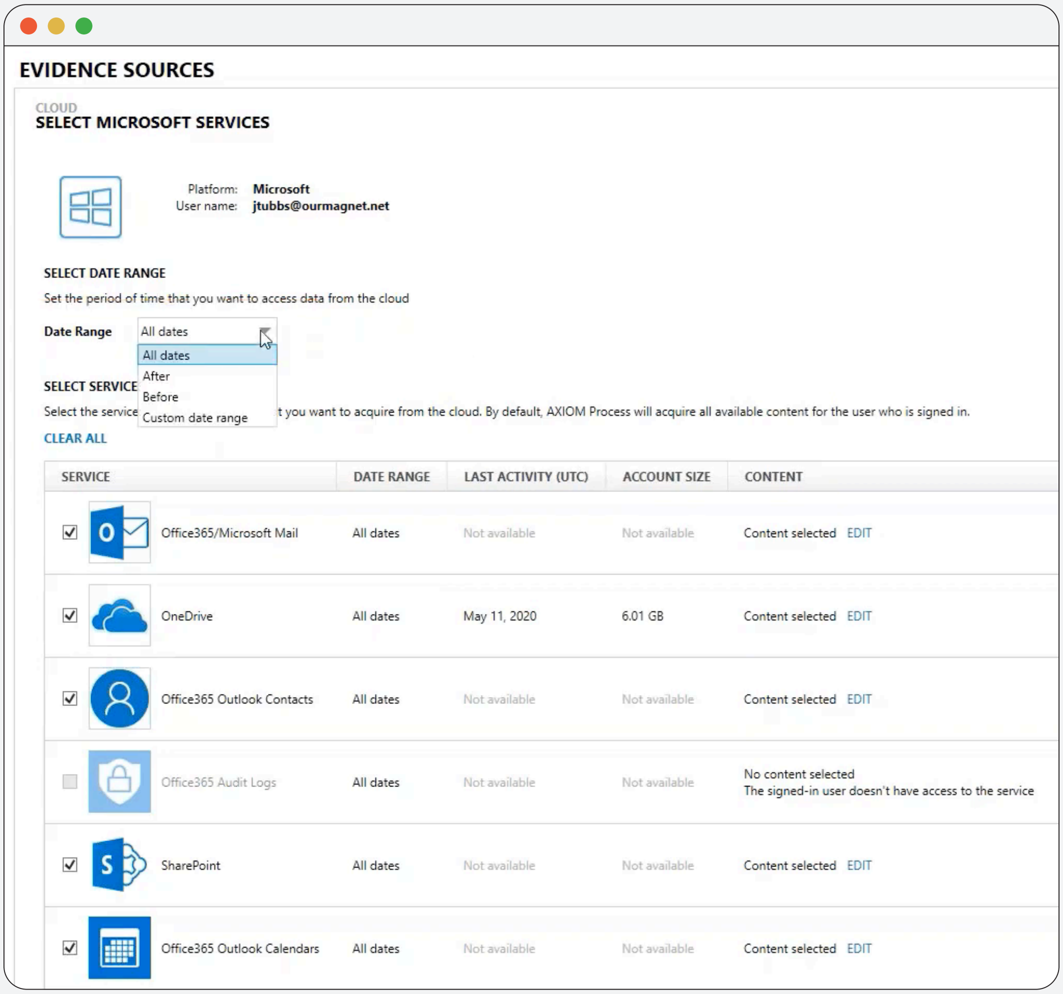
Open the Settings window to manually set the proxy settings

***Figure 2.4** shows how Magnet AXIOM allows investigators to use extracted authentication tokens to sign into the device owner's Microsoft account*[38]

[37] Magnet Forensics, "Cloud Forensics For Law Enforcement: A Search Warrant is Great But Not Always Needed For Cloud Data," May 19, 2020, *available at* https://www.youtube.com/watch?v=q8pqZ8N4zd8.

[38] Magnet Forensics, "Cloud Forensics For Law Enforcement: A Search Warrant is Great But Not Always Needed For Cloud Data," May 19, 2020, *available at* https://www.youtube.com/watch?v=q8pqZ8N4zd8.

Figure 2.5



EVIDENCE SOURCES

CLOUD

SELECT MICROSOFT SERVICES

Platform: Microsoft
User name: jtubbs@ourmagnet.net

SELECT DATE RANGE

Set the period of time that you want to access data from the cloud

Date Range: All dates

SELECT SERVICE

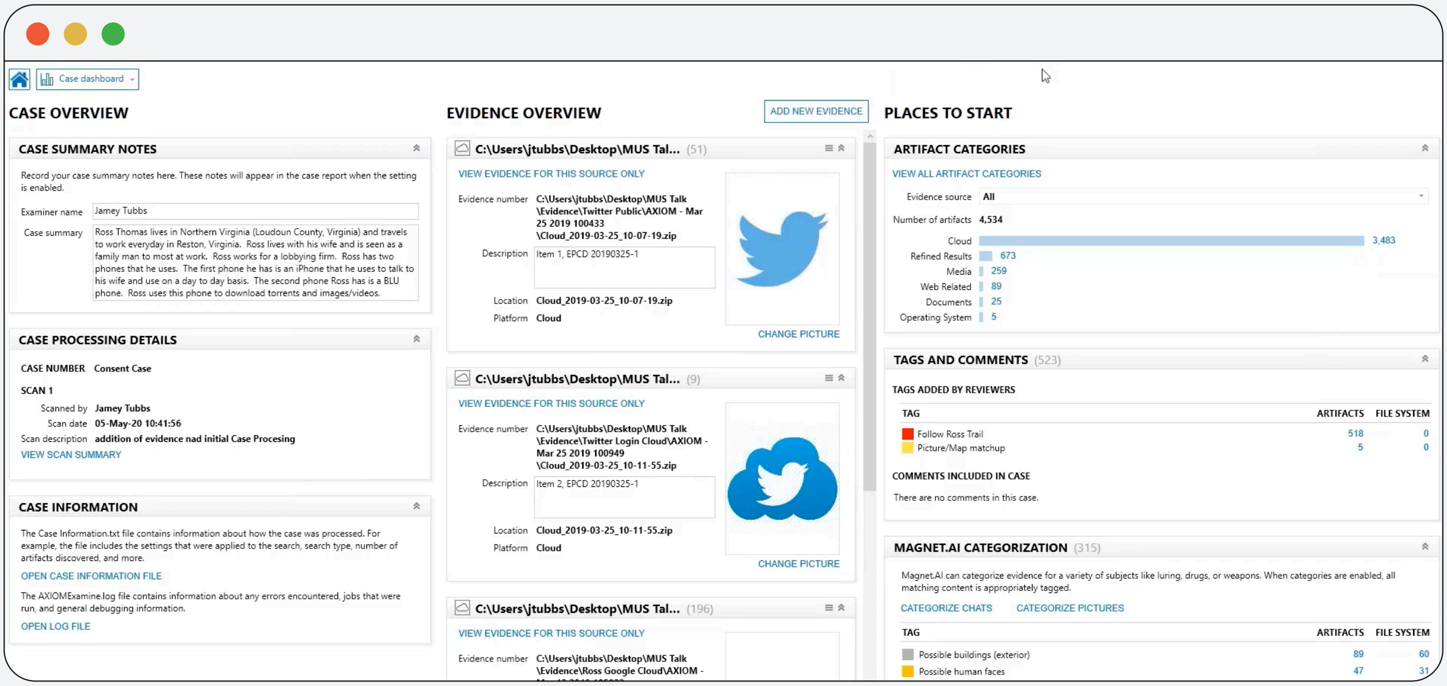
Select the service t you want to acquire from the cloud. By default, AXIOM Process will acquire all available content for the user who is signed in.

	SERVICE	DATE RANGE	LAST ACTIVITY (UTC)	ACCOUNT SIZE	CONTENT
☑	Office365/Microsoft Mail	All dates	Not available	Not available	Content selected EDIT
☑	OneDrive	All dates	May 11, 2020	6.01 GB	Content selected EDIT
☑	Office365 Outlook Contacts	All dates	Not available	Not available	Content selected EDIT
□	Office365 Audit Logs	All dates	Not available	Not available	No content selected The signed-in user doesn't have access to the service
☑	SharePoint	All dates	Not available	Not available	Content selected EDIT
☑	Office365 Outlook Calendars	All dates	Not available	Not available	Content selected EDIT

***Figure 2.5** shows the Microsoft services that Magnet AXIOM can extract remotely, like Microsoft OneDrive or Office365.*[39]

[39] Magnet Forensics, "Cloud Forensics For Law Enforcement: A Search Warrant is Great But Not Always Needed For Cloud Data," May 19, 2020, *available at* https://www.youtube.com/watch?v=q8pqZ8N4zd8.

Figure 2.6



CASE OVERVIEW

CASE SUMMARY NOTES

Record your case summary notes here. These notes will appear in the case report when the setting is enabled.

Examiner name: Jamey Tubbs

Case summary: Ross Thomas lives in Northern Virginia (Loudoun County, Virginia) and travels to work everyday in Reston, Virginia. Ross lives with his wife and is seen as a family man to most at work. Ross works for a lobbying firm. Ross has two phones that he uses. The first phone he has is an iPhone that he uses to talk to his wife and use on a day to day basis. The second phone Ross has is a BLU phone. Ross uses this phone to download torrents and images/videos.

CASE PROCESSING DETAILS

CASE NUMBER Consent Case

SCAN 1

Scanned by: Jamey Tubbs
Scan date: 05-May-20 10:41:56
Scan description: addition of evidence nad initial Case Procesing

CASE INFORMATION

The Case Information.txt file contains information about how the case was processed. For example, the file includes the settings that were applied to the search, search type, number of artifacts discovered, and more.

The AXIOMExamine.log file contains information about any errors encountered, jobs that were run, and general debugging information.

EVIDENCE OVERVIEW

C:\Users\jtubbs\Desktop\MUS Tal... (51)

Evidence number: C:\Users\jtubbs\Desktop\MUS Talk \Evidence\Twitter Public\AXIOM - Mar 25 2019 100433 \Cloud_2019-03-25_10-07-19.zip
Description: Item 1, EPCD 20190325-1
Location: Cloud_2019-03-25_10-07-19.zip
Platform: Cloud

C:\Users\jtubbs\Desktop\MUS Tal... (9)

Evidence number: C:\Users\jtubbs\Desktop\MUS Talk \Evidence\Twitter Login Cloud\AXIOM - Mar 25 2019 100949 \Cloud_2019-03-25_10-11-55.zip
Description: Item 2, EPCD 20190325-1
Location: Cloud_2019-03-25_10-11-55.zip
Platform: Cloud

C:\Users\jtubbs\Desktop\MUS Tal... (196)

Evidence number: C:\Users\jtubbs\Desktop\MUS Talk \Evidence\Ross Google Cloud\AXIOM -

PLACES TO START

ARTIFACT CATEGORIES

Evidence source: All
Number of artifacts: 4,534

Cloud	3,483
Refined Results	673
Media	259
Web Related	89
Documents	25
Operating System	5

TAGS AND COMMENTS (523)

TAGS ADDED BY REVIEWERS

TAG	ARTIFACTS	FILE SYSTEM
🟥 Follow Ross Trail	518	0
🟨 Picture/Map matchup	5	0

COMMENTS INCLUDED IN CASE

There are no comments in this case.

MAGNET.AI CATEGORIZATION (315)

Magnet.AI can categorize evidence for a variety of subjects like luring, drugs, or weapons. When categories are enabled, all matching content is appropriately tagged.

TAG	ARTIFACTS	FILE SYSTEM
⬜ Possible buildings (exterior)	89	60
🟧 Possible human faces	47	31

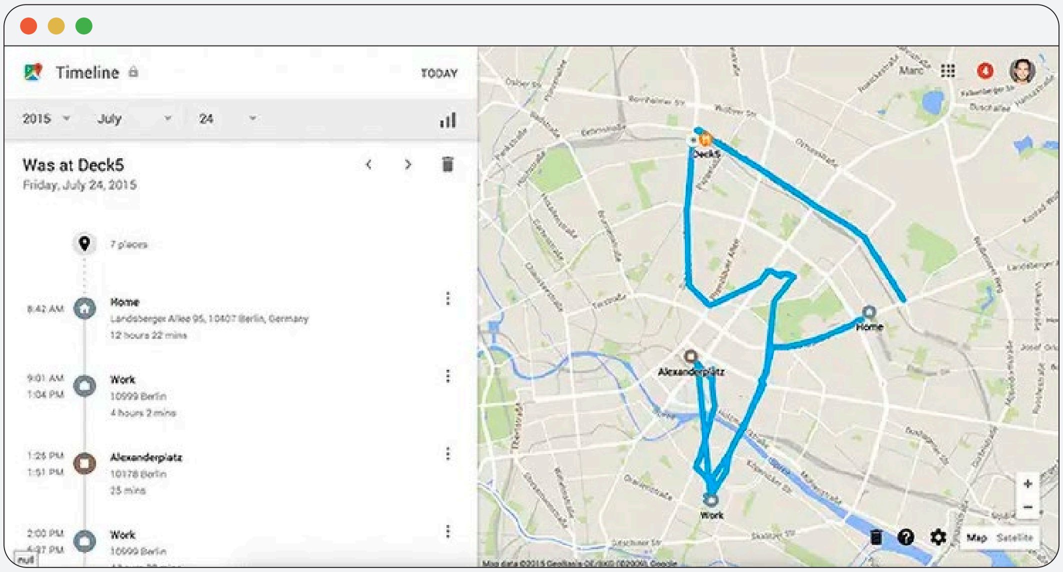
Figure 2.6 *shows the dashboard interface of Magnet AXIOM, showing access to Google and Twitter account data, along with other available data called "artifacts." There are also options to search by image content ("Magnet.AI Categorization") as well as "Keyword Matches" and "Passwords and Tokens."*[40]

One major source of information is Google's Location History. Any user with their location history turned on in their Google account will have records of their location stored online in their Google account. These location records are precise and can span years, and many users do not realize this data is being stored. In fact, Google stores this information even when the user is not doing anything that uses the phone's location. If law enforcement has physical access to a phone, they can use an MDFT to log into the user's Google account and extract this location history, which can be displayed as a timeline or map, shown in Figure 2.7.

[40] Magnet Forensics, "Cloud Forensics For Law Enforcement: A Search Warrant is Great But Not Always Needed For Cloud Data," May 19, 2020, *available at* https://www.youtube.com/watch?v=q8pqZ8N4zd8.

[41] Marc Knoll, trendblog.net, "Can't remember last night? Google's Location History can tell where you were," November 28, 2016, *available at* https://trendblog.net/cant-remember-last-night-google-location-history-can-help-you/.

Figure 2.7



Timeline

TODAY

2015 July 24

Was at Deck5
Friday, July 24, 2015

7 places

8:42 AM Home
Landsberger Allee 95, 10407 Berlin, Germany
12 hours 22 mins

9:01 AM
1:04 PM Work
10999 Berlin
4 hours 2 mins

1:26 PM
1:51 PM Alexanderplatz
10178 Berlin
25 mins

2:00 PM
4:37 PM Work
10999 Berlin

Figure 2.7 shows a user's Google location history as a timeline and also on a map. The timeline can show how long a user stayed at a particular location.[41]

"Deleted" Data

Mobile device forensic tools can sometimes access "deleted" data from phones.[42] Often, deleting a file on a phone isn't permanent, and the file can be recovered — similar to how most computers have a "recycling bin" for getting rid of files. Deleting a file from the phone itself often doesn't delete it from a user's cloud backup, or the variety of other places it may have been redundantly stored at some point. Even "permanently deleted" files can sometimes be recovered with the

[42] There is a difference between deleting a file from the phone's operating system and physically clearing the bits from the device's hardware. Traditionally, when an electronic device permanently deletes a file, this means that the operating system declares the space where the file was stored as "free" to be overwritten, and removes the file from the file system. However, newer storage hardware must clear an entire block of space before writing to any part of that block, and many devices routinely clear space immediately after a file is deleted from the device interface in order to quicken this process. Another factor is that encryption can prevent permanently deleted files from being recovered. That means, for some newer models of phones, "deleted data" is more likely to actually be cleared.

For example, since iPhones encrypt each file on the phone individually with its own key, files deleted from the device are essentially impossible to recover because they are encrypted and the key is deleted. So even if the data itself remains, it's completely unintelligible. On the other hand, non-permanent deletion is very common in digital devices because users often accidentally delete files and want to retrieve them. An example is when you drag a file over to your computer's recycling bin — the space where it is physically stored is not actually marked as "free" to be overwritten, and the file sticks around until it's either permanently deleted or restored. Also, cloud-based storage may keep track of deleted files, such that they are permanently deleted from the device but remain tracked elsewhere. iCloud keeps track of deleted files for 30 days and can recover them at the request of the user, unless they are also permanently deleted from iCloud. This means that if a user syncs files on their phone to their iCloud account, and then deletes the files from their phone, the files can likely be recovered by looking for them in iCloud as opposed to on the device's storage.

right tools, because data isn't always physically wiped from storage when it's deleted — it's just marked as "free space" until it's overwritten by other data. However, access to deleted data depends on a range of factors, including phone hardware,[43] encryption design,[44] and extraction method.[45]

Other Data on a Phone

Phones also record vast amounts of data about how people interact with their devices — data that's considered a "digital forensics goldmine."[46] For example, MDFTs can recover logs showing when applications were installed, used, and deleted, as well as how often someone used an application. Other data includes when a device was locked or unlocked, when a message was viewed, when a Bluetooth device was connected, words added to a user's dictionary, notification contents, as well as past "spotlight searches" on iPhones, a search function that combines on-device and web results. Phones can even store screenshots of apps as they're brought out of focus so users can see all of the apps they have open.[47] These "behind the scenes" data are stored to improve the phone's performance, but they leave incredibly detailed artifacts that MDFTs can later analyze.[48]

[43] For example, some storage devices must physically clear entire blocks of data before they can write to any part of it, meaning data is more likely to be wiped within a short period of time. *See* "What is trim and active garbage collection?," Crucial Blog, *available at* https://www.crucial.com/articles/about-ssd/what-is-trim. ("Flash memory, which is what SSDs are made of, cannot overwrite existing data the way a hard disk drive can. Instead, solid state drives need to erase the now invalid data. The problem is that a larger unit of the memory, a block, must be erased before a smaller unit, a page, can be written.")

[44] Similarly, in cases where the phone encrypts each file individually (like on iOS), deleting a file that's not backed up in the cloud also gets rid of the corresponding key. So although deleted data might stick around on the hardware, it is likely encrypted and without any key to decrypt it — therefore useless. *See* Oleg Alfonin, "The iPhone Data Recovery Myth: What You Can and Cannot Recover," July 10, 2020, Elcomsoft Blog, *available at* https://blog.elcomsoft.com/2020/07/the-iphone-data-recovery-myth-what-you-can-and-cannot-recover/. ("In the iPhone, almost every user file is stored encrypted. The file system employs file-based encryption with separate, unique encryption keys for every file. Once a file is deleted, the encryption key is [also] destroyed, making it impossible to "undelete" or recover that file.")

[45] To attempt to recover permanently deleted data directly from the device, law enforcement must perform a physical extraction, which copies the data bit-by-bit as it's stored on the phone.

[46] Mati Goldberg, "How a Suspect's Pattern-of-life Analysis is Enhanced with KnowledgeC Data," Cellebrite, June 13, 2019, *available at* https://www.cellebrite.com/en/blog/how-a-suspects-pattern-of-life-analysis-is-enhanced-with-knowledgec-data/.

[47] Cellebrite, "UFED, UFED Physical Analyzer, UFED Logical Analyzer, & Cellebrite Reader v7.28," Release Notes, January 2020, *available at* https://cf-media.cellebrite.com/wp-content/uploads/2020/01/ReleaseNotes_PA-7.28_A4.pdf. ("[W]hen a user swipes up on the screen while using an application in an iOS device, or presses the home button, or if they receive a call while using an application, the active application is sent to the background. A 'snapshot' of the current screen is taken in order to provide a smooth visual transition while changing screens. UFED Physical Analyzer can now recover all these snapshots under images data files. You can also filter by this file format."), at 4.

[48] *Id.*

Figure 2.8

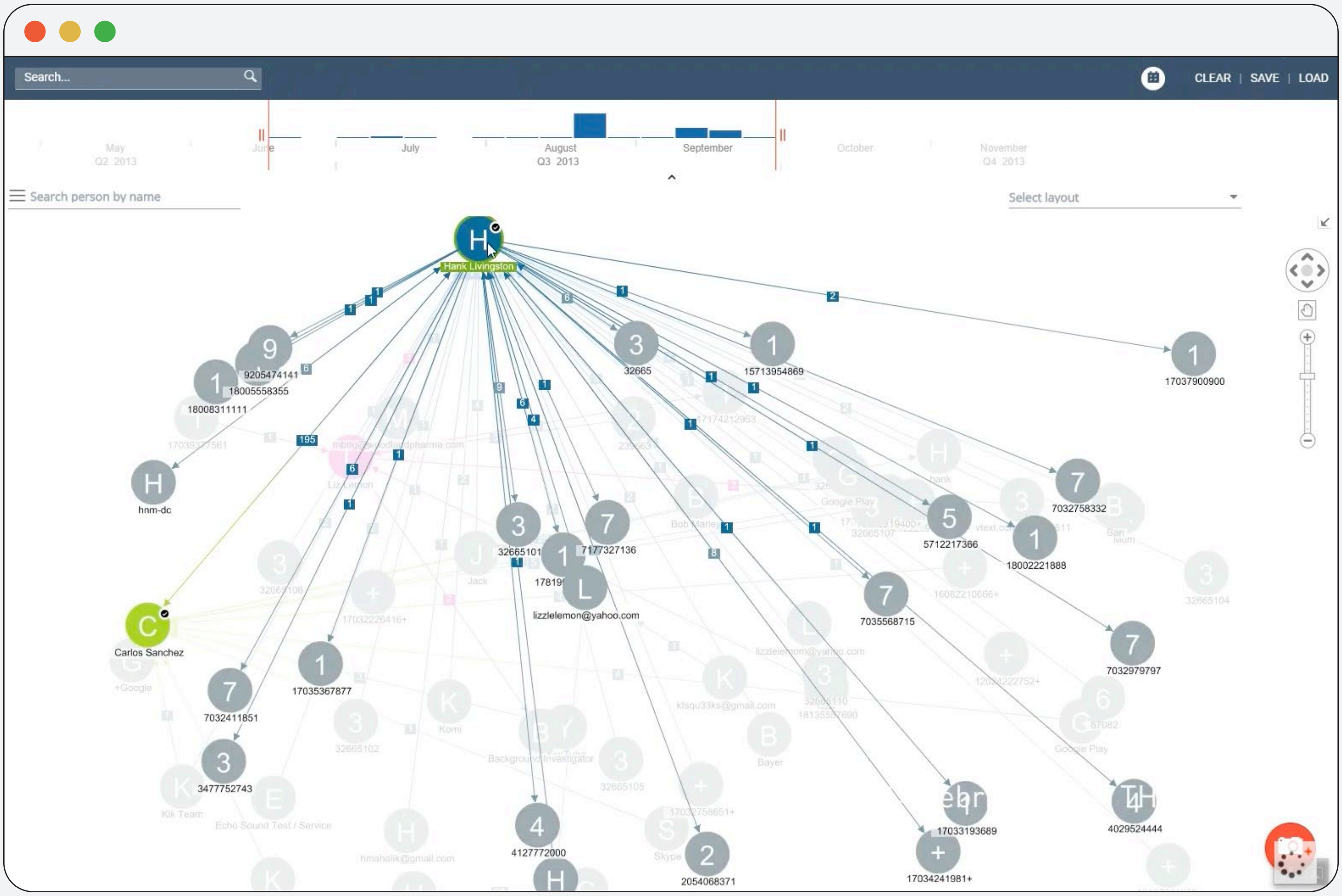


Figure 2.8 shows a screenshot of Cellebrite Analytics, now called Cellebrite Pathfinder, which infers a social graph based on communication events. This graph shows the participants of communications extracted from the phone, as well as a histogram of communication volume over time.[49]

Ultimately, MDFTs offer law enforcement a powerful window into almost all data stored on — or accessible from — a cellphone, as well as substantial amounts of data that users cannot see. These tools are invasive, especially for people who depend on their phone for internet access because they do not have a computer or broadband.

[49] Heather Mahalik, Cellebrite Blog, "When Data Overwhelms You, Cellebrite Pathfinder Empowers You With Actionable Insights," March 19, 2020, *available at* https://www.cellebrite.com/en/ask-the-expert/when-data-overwhelms-you-analytics-empowers-you-with-actionable-insights/.

Device Analysis

Once data is extracted, MDFTs accelerate data analysis with powerful visualization tools. For example, law enforcement can view full text conversations as a chat instead of individual messages in a database; trace a user's actions on a map or chronological timeline using "patterns of life" metadata; sort data by file type regardless of its location on the phone (*e.g.*, all of the images on the phone, whether they came from the camera app or an email attachment); or create network graphs, like in Figure 2.8, to infer social relationships using contact data.

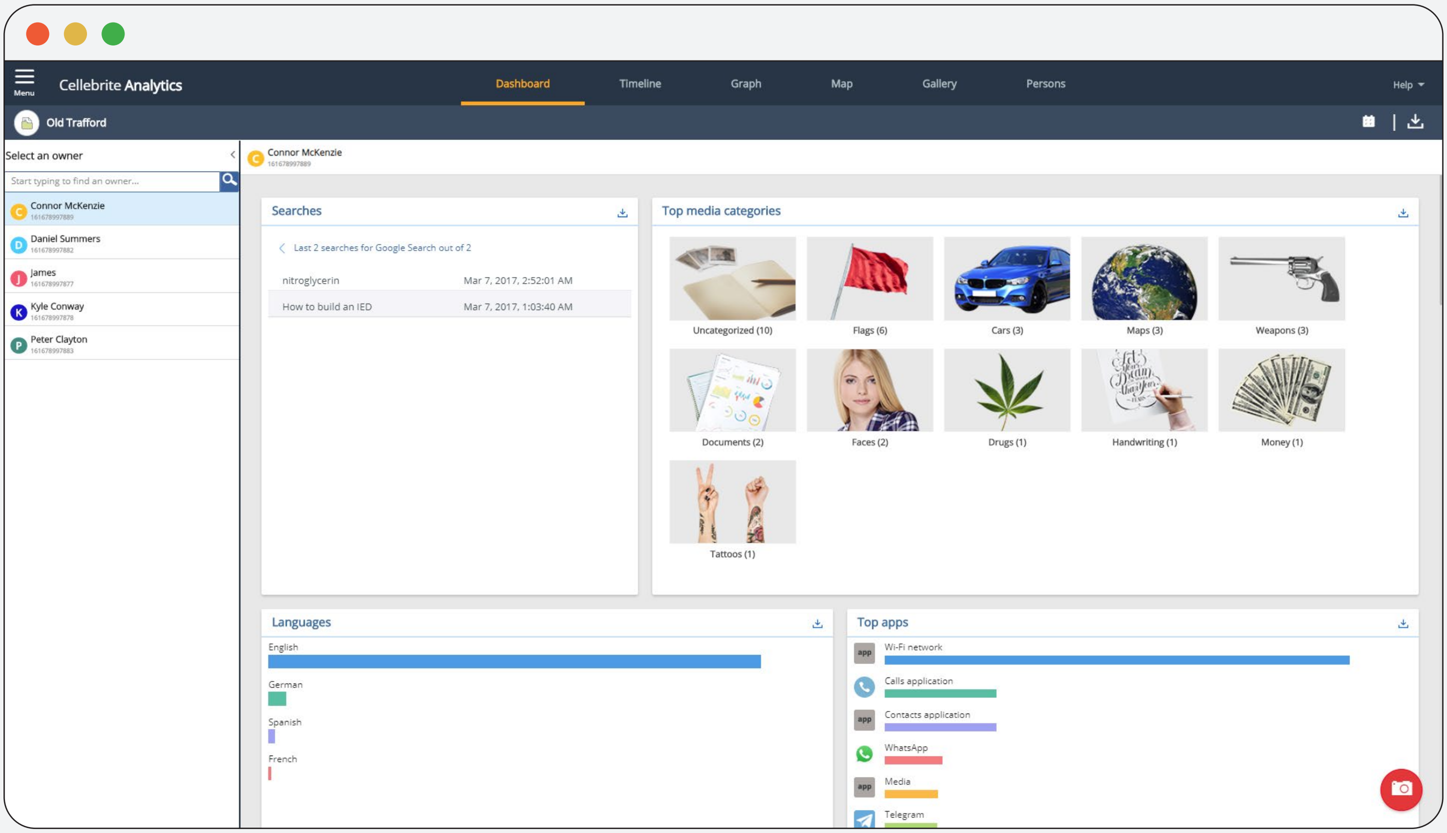
Search features also help law enforcement quickly navigate extracted data. These features include basic keyword searches, as well as more advanced techniques. Some mobile device forensic tools now use machine learning-based text and image classification to categorize file contents, including individual frames in a video.[50] For instance, as shown in Figure 2.9, Cellebrite offers a "search by face" function, whereby law enforcement can compare an image of a face to all other images of faces found on the phone. Cellebrite also allows law enforcement to define new image categories by feeding its software a small set of example images to search for (for example, searching for hotel rooms by giving the software a set of five images of hotel rooms that were taken from Google images). As another example, Magnet Forensics' AXIOM can employ text classification models in attempts to detect "sexual conversations,"[51] or to filter conversations by topics ranging from family, drugs, money, and police.[52] Tools also allow law enforcement to search for a specific address on a map and view all "location related" events surrounding a point of interest.

[50] Christa Miller, "Industry Roundup: Image Recognition And Categorization," Forensic Focus, July 8, 2019, *available at* https://www.forensicfocus.com/articles/industry-roundup-image-recognition-and-categorization/. ("Thanks to developments in machine learning and artificial intelligence, a number of vendor products have been able to incorporate rapid recognition or categorization tools into their software.")

[51] Magnet Forensics, "Taking Magnet.AI Up a Notch in AXIOM 2.0," April 25, 2018, *available at* https://www.magnetforensics.com/blog/taking-magnet-ai-up-a-notch-in-axiom-2-0/. ("With the launch of AXIOM 2.0, the Magnet.AI module now identifies images that may contain depictions of child sexual abuse, nudity, weapons, and drugs. We've also expanded our text classification model to detect potential sexual conversations in addition to child luring (both in the English language).")

[52] Cellebrite, "Cellebrite Pathfinder 8.2: Cutting edge textual analysis takes the edge off searching through conversations," February 20, 2020, *available at* https://www.cellebrite.com/en/productupdates/analytics-desktop-8-2-cutting-edge-textual-analysis-takes-the-edge-off-searching-through-conversations/. ("Cellebrite Pathfinder v8.2 introduces cutting edge textual analysis. Building on Text Analytics and NLP (Natural Language Processing), Topic Identification allows investigators to focus on the interesting communications with utmost ease and speed.")

Figure 2.9



Connor McKenzie 161678997889
Daniel Summers 161678997882
James 161678997877
Kyle Conway 161678997878
Peter Clayton 161678997883

Connor McKenzie 161678997889

Last 2 searches for Google Search out of 2

nitroglycerin	Mar 7, 2017, 2:52:01 AM
How to build an IED	Mar 7, 2017, 1:03:40 AM

Figure 2.9 *sshows Cellebrite Pathfinder, which allows investigators to perform an image-based search using pre-generated filters, like "Flags," "Faces," "Drugs," "Weapons," or "Tattoos." The software also has features, shown at the top, such as "Timeline" (for viewing events on the phone chronologically), "Graph" (to make a social network graph of contacts and communications), "Map" (to display all phone events and media with location data on a map), "Gallery" (to view all media like photos and videos in one place regardless of source), and "Persons" (to view profiles of discrete users on the phone).*[53]

MDFTs can also apply these visualization features to data from multiple phones or other data sources together, to find links across the devices, like common contacts, call or text records, or account information. They can even look for common geolocation or purchase data between phones, to show that the phones were at some point near each other, say, to buy things at the same place and time. What might otherwise take weeks to do manually can be done automatically.

[53] Cellebrite, "Cellebrite Pathfinder," *available at* https://www.cellebrite.com/en/pathfinder/.

Security Circumvention

Phone manufacturers like Apple, Samsung, Google, and others have built sophisticated security features designed to protect user information in case, for example, a phone is lost or stolen. Manufacturers design these features to balance[54] user convenience with security and privacy.[55] This balancing act can lead to design flaws, software bugs, or other vulnerabilities that law enforcement can then exploit.

MDFTs can often circumvent the security features built into phones in order to extract user data. In response, phone manufacturers continuously patch known security vulnerabilities and develop even more advanced security features, seeking to thwart unwelcome access, including by MDFTs. This "cat-and-mouse game" has evolved over years and continues to this day. MDFTs use numerous tactics to gain access to users' data on phones, such as guessing a password, exploiting a vulnerability or developer tool, or even installing spyware. With rare exception, MDFTs can nearly always access and extract some, if not all, data from phones.

MDFTs Can Extract Data From Nearly All Popular Phones

Many of the phones that law enforcement seize can be extracted with off-the-shelf tools. Departments often purchase tools from multiple vendors to increase the likelihood that any given phone can be extracted. Large MDFT vendors, like Cellebrite and Magnet Forensics, support extraction for thousands of phones. For example, in March 2016, Cellebrite supported logical extractions for 8,393 devices, and physical extractions for 4,254 devices. Since then, out of the five major phone manufacturers, Cellebrite added the most physical extraction support for Samsung (346 devices). Crucially, Cellebrite has also added lock-bypass support (*e.g.*, by exploiting a vulnerability to force the phone to skip the passcode-checking step when it turns on) for about 1,500 devices since March 2016. However, as of 2017, 28% of smartphone users did not even have screen lock enabled on their phones.[56]

[54] IBM's study found that many people would still be willing to trade security for convenience if it would save them even a few seconds. Young adults are particularly likely to demand a more convenient experience, with nearly half of those under the age of 35 saying they would use a less secure method if it would save them between 1 and 10 seconds. See "Beyond Passwords," *The Atlantic*, *available at* https://www.theatlantic.com/sponsored/ibm-2018/beyond-passwords/1859/.

[55] Manufacturers deploy these security features for a variety of reasons. For example, Apple has argued that "information needs to be protected from hackers and criminals who want to access it, steal it, and use it without our knowledge or permission," and also because it believes privacy is a fundamental human right. See Apple, "Introduction to Apple platform security" *available at* https://support.apple.com/guide/security/introduction-seccd5016d31/web.

[56] Aaron Smith, "Americans, Passwords, and Mobile Security," January 26, 2017, Pew Research, https://www.pewresearch.org/internet/2017/01/26/2-password-management-and-mobile-security/.

MDFT vendors add support for new devices and software at a rapid pace, especially for popular devices. For example, about 45% of U.S. smartphone users have iPhones.[57] iOS 13 was released on September 19, 2019,[58] and Cellebrite announced support for Apple devices running iOS 13 less than three weeks later.[59]

Although iPhones encrypt data by default, there are many phones that still do not support encryption, or have easily surpassed encryption schemes, like lower-end Android phones.[60] Other common targets are phone chipsets or developer tools, which tend to be consistent across brands, meaning a single exploit or method can be successfully reused for a large number of devices. For example, independent researchers recently released the "checkm8" exploit, which takes advantage of a permanent[61] vulnerability in all but the newest iPhone chipsets, providing an opportunity for MDFTs to extract data without knowing the passcode.[62]

MDFTs Can Often Bypass Security Measures

Sometimes, MDFTs cannot immediately extract data from a phone due to encryption and other security features. In those cases, MDFTs often turn to another strategy: repeatedly trying random passwords until guessing the correct one, which then allows the MDFT to decrypt the phone's contents. MDFTs can also look for unencrypted data on a phone when its password is difficult to guess.

For many phones, the decryption key is generated from the password, so the strength of the protection that encryption provides is directly related to the length and complexity of the user's password. Shorter or common passcodes are easier to guess. In April 2018, Professor Matthew Green estimated that brute-forcing a passcode on an iPhone would take no more than 13 minutes

[57] S. O'Dea, "Share of smartphone users that use an Apple iPhone in the United States from 2014 to 2021," February 27, 2020, Statista, https://www.statista.com/statistics/236550/percentage-of-us-population-that-own-a-iphone-smartphone/.

[58] "iOS 13," 9TO5Mac, https://9to5mac.com/guides/ios-13/.

[59] Cellebrite, "UFED Ultimate and UFED InField v7.24 Release Notes," October 2019, https://cf-media.cellebrite.com/wp-content/uploads/2019/10/ReleaseNotes_UFED_v7.24.pdf.

[60] For example, some do not have hardware-enforced security features, making it easy for mobile device forensic tools to get past locks to copy data. Some Android phones have decryption keys that are simply generated from the phrase "default_password" instead of the user's password. Others have lock screens that are only visual, and don't prevent data transfer with MDFTs. Some even have leaked signed firmware that allows tools to use the manufacturer's proprietary decrypting data reading tools, with no password needed. See Oleg Alfonin, "Demystifying Android Physical Acquisition," May 29, 2018, Elcomsoft Blog, *available at* https://blog.elcomsoft.com/2018/05/demystifying-android-physical-acquisition/.

[61] The bug is in read-only (as opposed to writeable) memory, such that there are physically enforced protections against patching it.

[62] Dan Goodin, "Developer of Checkm8 explains why iDevice jailbreak exploit is a game changer," Ars Technica, September 28, 2019, *available at* https://arstechnica.com/information-technology/2019/09/developer-of-checkm8-explains-why-idevice-jailbreak-exploit-is-a-game-changer/.

for a 4-digit passcode, 22 hours for 6 digits, and 92 days for 8 digits. The default length prompted by iOS is 6 digits.[63] For an advanced off-the-shelf tool like GrayKey or Cellebrite Premium, this can mean guessing passcodes in under a day.

However, since the release of the iPhone XS, XR, and XS Max in 2018, which are no longer vulnerable to the major hardware flaw in previous iPhones, the rate of password guessing is much more limited, making them more difficult to access. Nonetheless, the September 2020 Cellebrite Advanced Services information sheet says that they can "determine locks and perform a full file system extraction of all iPhone devices from iPhone 4S to the latest iPhone 11 / 11 Pro / Max running the latest iOS versions up to the latest 13.4.1."[64]

Separately, without even needing to guess the password, MDFTs can take advantage of the fact that, in order to balance convenience and security, phones don't actually encrypt all data on a device.[65] Most people still want to receive calls and texts and hear alarms after their phone restarts but before they've unlocked it. Accordingly, certain data is unencrypted upon startup, including some account information that is needed to receive notifications. For example, Cellebrite's UFED Premium claims it can extract data even on locked iPhones.[66] The data that appears "before first unlock" (BFU) even includes parts of Apple's password manager.[67] Once the iPhone is unlocked after being powered on — "after first unlock" (AFU) — even more unencrypted data becomes available. Vendors like Oxygen Forensics and Grayshift advertise their ability to find and extract these unencrypted data. Figure 2.10 shows all the artifacts exacted from

[63] Matthew Green (matthew_d_green), "Guide to iOS estimated passcode cracking times (assumes random decimal passcode + an exploit that breaks SEP throttling): 4 digits: ~13min worst (~6.5avg) 6 digits: ~22.2hrs worst (~11.1avg) 8 digits: ~92.5days worst (~46avg) 10 digits: ~9259days worst (~4629avg)," 10:17am, Apr 16, 2018, https://twitter.com/matthew_d_green/status/985885001542782978.

[64] Cellebrite, "Cellebrite Advanced Services," September 2020, https://cf-media.cellebrite.com/wp-content/uploads/2020/09/SolutionOverview_CAS_2020.pdf.

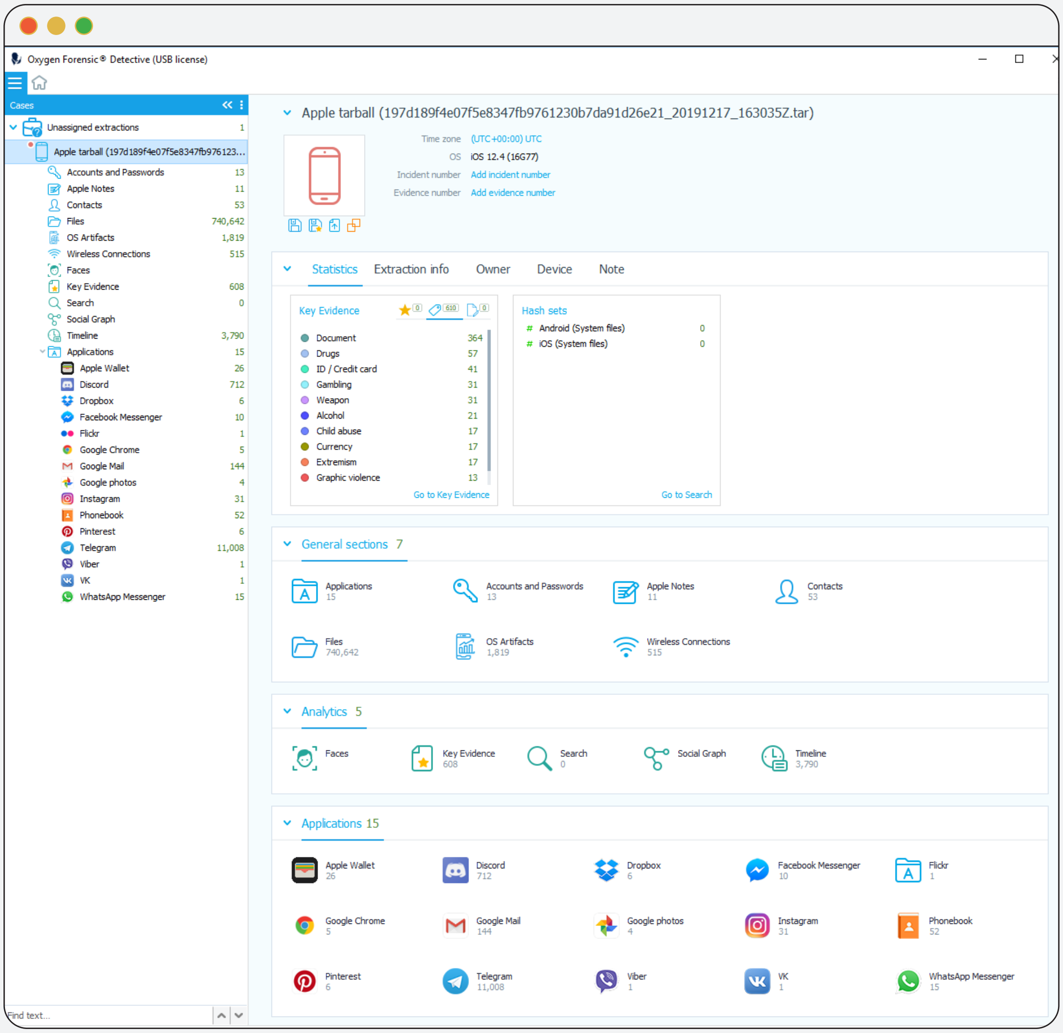
[65] The exception to this is Android's Secure Startup, which, when enabled by the user, prevents the phone from fully booting until the user password is entered and keeps all data encrypted. This means users can't receive notifications or alarms without entering their password, which most people would not casually opt into doing for its inconvenience. However, vendors like Cellebrite have advertised their ability to circumvent this for some phones with Secure Startup enabled. See Joanna Shemesh, "Cellebrite Advanced Services Solves the Toughest Encryption Problems for Apple and Android Devices," September 24, 2019, *available at* https://www.cellebrite.com/en/blog/cellebrite-advanced-services-solves-the-toughest-encryption-problems-for-apple-and-android-devices/. ("Take, for example, Secure Startup, which is an encryption mode. Two years ago, we were the first in the world to offer support for that feature. To this day, no other vendor has managed to support it.")

[66] Cellebrite, "Premium access to all end-high iOS and Android Devices," May 2020, *available at* https://cf-media.cellebrite.com/wp-content/uploads/2020/05/ProductOverview_CellebritePremium_A4_web.pdf.

[67] This data includes account information like usernames, which can provide leads to law enforcement for other sources of evidence.

a BFU extraction by Oxygen Forensic Detective.[68] There are thousands of files available, and as one software reviewer highlights: "Yes, all this data is from BFU extraction. Pay attention to the 'Image Categorization' – this [is] the new built-in feature . . . that allows [you] to detect, analyze, and categorize images from twelve different categories, such as weapon, drugs, child abuse, extremism and more."[69]

Figure 2.10



Oxygen Forensic® Detective (USB license)

Cases

Unassigned extractions	1
Apple tarball (197d189f4e07f5e8347fb976123...	
Accounts and Passwords	13
Apple Notes	11
Contacts	53
Files	740,642
OS Artifacts	1,819
Wireless Connections	515
Faces	
Key Evidence	608
Search	0
Social Graph	
Timeline	3,790
Applications	15
Apple Wallet	26
Discord	712
Dropbox	6
Facebook Messenger	10
Flickr	1
Google Chrome	5
Google Mail	144
Google photos	4
Instagram	31
Phonebook	52
Pinterest	6
Telegram	11,008
Viber	1
VK	1
WhatsApp Messenger	15

Find text...

Apple tarball (197d189f4e07f5e8347fb9761230b7da91d26e21_20191217_163035Z.tar)

Time zone (UTC+00:00) UTC
OS iOS 12.4 (16G77)
Incident number Add incident number
Evidence number Add evidence number

Key Evidence ★ 0 610 0

Document	364
Drugs	57
ID / Credit card	41
Gambling	31
Weapon	31
Alcohol	21
Child abuse	17
Currency	17
Extremism	17
Graphic violence	13

Go to Key Evidence

Hash sets

# Android (System files)	0
# iOS (System files)	0

Go to Search

General sections 7

Applications	15
Accounts and Passwords	13
Apple Notes	11
Contacts	53
Files	740,642
OS Artifacts	1,819
Wireless Connections	515

Analytics 5

Faces	
Key Evidence	608
Search	0
Social Graph	
Timeline	3,790

Applications 15

Apple Wallet	26
Discord	712
Dropbox	6
Facebook Messenger	10
Flickr	1
Google Chrome	5
Google Mail	144
Google photos	4
Instagram	31
Phonebook	52
Pinterest	6
Telegram	11,008
Viber	1
VK	1
WhatsApp Messenger	15

***Figure 2.10** shows the result of a "Before First Unlock" extraction by Oxygen Forensics Detective on an Apple iPhone running iOS 12.4. The software detects thousands of files, including 11,000 Telegram files, 712 Discord files, 11 Apple Notes files, 53 Contacts files, 144 files from Google Mail, 26 files from Apple Wallet, and 13 files marked as "Accounts and Passwords."*[70]

[68] Vladimir Katalov, "BFU Extraction: Forensic Analysis of Locked and Disabled iPhones," December 20th, 2019, Elcomsoft Blog, https://blog.elcomsoft.com/2019/12/bfu-extraction-forensic-analysis-of-locked-and-disabled-iphones/.

[69] *Id.*

[70] Vladimir Katalov, Elcomsoft Blog, "BFU Extraction: Forensic Analysis of Locked and Disabled iPhones," December 20, 2019, *available at* https://blog.elcomsoft.com/2019/12/bfu-extraction-forensic-analysis-of-locked-and-disabled-iphones/.

When password guessing fails, and BFU or AFU extractions are not workable, MDFTs provide yet other tactics to gain access. For example, Grayshift offers a tool called HideUI, which is essentially spyware that law enforcement installs on a phone in order to record future password entries to eventually access the phone.[71]

Of course, there are even more basic approaches. Law enforcement often seek “consent” to search a person’s phone, but that consent is often not as voluntary as one may assume. People being arrested likely do not understand how much information they are giving away when they consent to a search, even when they presume that information will be exculpatory — yet consent searches happen frequently. We highlight the problems with consent searches in Sections 4 and 6 below.

When All Else Fails, Vendors Offer “Advanced Services”

Although we’ve previously described how the majority of phones can be partially or completely searched, there are some phones that might take specialized effort. For example, one investigator describes being able to get extractions from 25 of 33 (76%) of phones in his cases using just Cellebrite UFED and GrayKey in his lab.[72] To cover the remaining portion of phones, Cellebrite offers “Advanced Services,” which, according to their website, can unlock iOS devices including iPhone 11, 11 Pro/Max, and Android devices including newer Samsung phones.[73]

According to our public records research, the base cost of unlocking and extracting data from a phone using Advanced Services is $1,950, though they can be cheaper in bulk. In 2018, the Seattle PD purchased 20 “actions” for $33,000,[74] and email records show them using Cellebrite to unlock various iPhones within days or weeks.[75] For example, Seattle PD sent Cellebrite an

[71] Olivia Solon, “iPhone spyware lets police log suspects’ passcodes when cracking doesn’t work,” NBC News, May 18, 2020, *available at* https://www.nbcnews.com/tech/security/iphone-spyware-lets-cops-log-suspects-passcodes-when-cracking-doesn-n1209296.

[72] “Possible Alternatives to Cellebrite,” November 29, 2018, Reddit “/r/computerforensics,” *available at* http://web.archive.org/web/20200625164840/https://www.reddit.com/r/computerforensics/comments/a1j43j/possible_alternatives_to_cellebrite/.

[73] Cellebrite, “Cellebrite Advanced Services: Comprehensive Services to Access Inaccessible Data,” May 2020, *available at* http://web.archive.org/web/20200626143910/https://cf-media.cellebrite.com/wp-content/uploads/2020/05/Cellebrite_Services_CAS_A4_2020_web.pdf

[74] See Seattle Police Department Purchase & Supply Request, https://beta.documentcloud.org/documents/20394507-installment_101.

[75] *See* Seattle Police Department, Cellebrite Advanced Services emails, https://beta.documentcloud.org/documents/20394508-installment_51.

iPhone X with an unknown 6-digit passcode in August 2018: Cellebrite received it on August 24, began processing on August 28, finished processing on September 12, and shipped it back the same day. Today, Cellebrite Premium allows law enforcement to bring these advanced unlocking capabilities in-house for $75,000 to $150,000, based on the frequency of use.[76]

3. Widespread Law Enforcement Adoption Across the United States

To date, most public reporting on law enforcement use of mobile device forensic tools has focused on law enforcement authorities with the most resources, like the Federal Bureau of Investigation, U.S. Immigration and Customs Enforcement,[77] the Drug Enforcement Administration,[78] and Customs and Border Protection,[79] or on state law enforcement agencies.[80] Much less is publicly known about the availability of these tools to the thousands of local law enforcement agencies across the United States.[81] To find out, we filed more than 110 public records requests to law enforcement agencies across the country, and searched a variety of databases on government spending and grantmaking.[82]

[76] Cellebrite, "Premium access to all iOS and high-end Android devices," *available at* https://cf-media.cellebrite.com/wp-content/uploads/2020/07/ProductOverview_CellebritePremium.pdf.

[77] Thomas Brewster, "Immigration Cops Just Spent A Record $1 Million On The World's Most Advanced iPhone Hacking Tech," Forbes, May 8, 2019, *available at* https://www.forbes.com/sites/thomasbrewster/2019/05/08/immigration-just-spent-a-record-1-million-on-the-worlds-most-advanced-iphone-hacking-tech/#7d8860a85a0a.

[78] Joseph Cox, "The DEA Says It Wants That New iPhone Unlocking Tool 'GrayKey,'" Vice, March 28, 2018, *available at* https://www.vice.com/en_us/article/mbxba4/graykey-grayshift-dea-iphone-hack.

[79] See, e.g., U.S. Customs and Border Protection Purchase Orders, Federal Procurement Data System, https://www.fpds.gov/ezsearch/fpdsportal?indexName=awardfull&templateName=1.5.1&s=FPDS.GOV&q=grayshift+customs+and+border&x=0&y=0.

[80] Joseph Cox, "US State Police Have Spent Millions on Israeli Phone Cracking Tech," Vice, December 21, 2016, *available at* https://www.vice.com/en_us/article/aekqkj/us-state-police-have-spent-millions-on-israeli-phone-cracking-tech-cellebritea.

[81] Some information is known about the largest local law enforcement agencies. *See* George Joseph, "Cellphone Spy Tools Have Flooded Local Police Departments," February 8, 2017, CityLab, *available at* https://www.bloomberg.com/news/articles/2017-02-08/cellphone-surveillance-gear-floods-u-s-cities.

[82] For more details on our methodology and our data, see Appendix A and Appendix B. Appendix C is a table that provides total amounts each agency has spent on MDFTs since 2015 based on agency responses to our public records requests. These figures represent lower bounds on the amounts actually spent, since records responses may be incomplete.

Mobile device forensic tools can cost thousands of dollars for law enforcement agencies. Some have argued that these tools are "cost prohibitive . . . for all but a handful of local law enforcement agencies,"[83] or "are things that few state and local police departments can afford."[84] The Manhattan District Attorney's Office has claimed:

> *Faced with growing backlogs of encrypted devices, some law enforcement agencies have begun working with private-sector partners to attempt to develop workarounds to obtain contents from otherwise "warrant-proof" Apple and Android phones. This office, with our relatively considerable resources, is one of the few local agencies that can afford to pursue this kind of solution. Other offices lack such resources, which creates an unequal system in which access to justice depends on a particular jurisdiction's financial capacity.*[85]

Our research indicates that this is not the case. **Rather, we found widespread adoption of mobile device forensic tools by law enforcement in all fifty states and the District of Columbia. In all, we documented more than 2,000 agencies across the United States that have purchased a range of products and services offered by mobile device forensic tool vendors.[86] Every American is at risk of having their phone forensically searched by law enforcement.**

Almost every kind of law enforcement actor is represented in the data we collected: Local police departments, sheriffs, district attorneys, forensic labs, prisons, housing authorities, public schools, statewide agencies, and more.

Many agencies purchase MDFTs from multiple vendors, including Cellebrite, Magnet Forensics, Grayshift, MSAB, AccessData, and Oxygen Forensics.[87] A single GrayKey unit — which is

[83] Written Testimony of New York County District Attorney Cyrus R. Vance, Jr. Before the United States Senate Committee on the Judiciary, "Smartphone Encryption and Public Safety," Washington, D.C., December 10, 2019 https://www.judiciary.senate.gov/imo/media/doc/Vance%20Testimony.pdf.

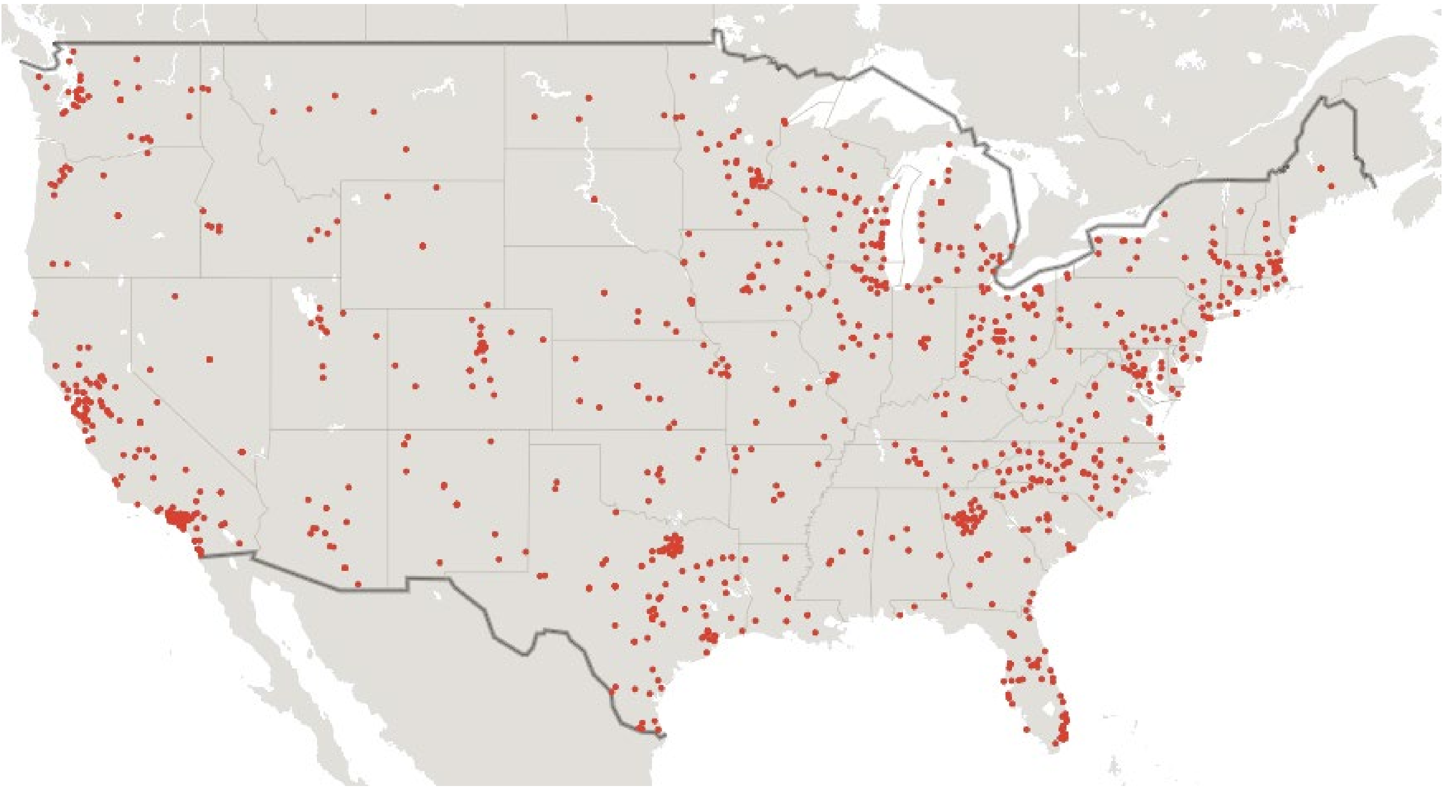
[84] William, Carter, Jennifer Daskal, *Low Hanging Fruit: Evidence-Based Solutions to the Digital Evidence Challenge*, Center for Strategic & International Studies, July 2018, 12.

[85] Third Report of the Manhattan District Attorney's Office on Smartphone encryption and Public Safety, November 2017, at 8, https://www.manhattanda.org/wp-content/themes/dany/files/2017%20Report%20of%20the%20Manhattan%20District%20Attorney%27s%20Office%20on%20Smartphone%20Encryption.pdf.

[86] This number represents a floor — many agencies do not upload their information to GovSpend, and we have documented multiple instances of such agencies purchasing MDFTs.

[87] This aligns with a recommendation from a National Institute of Standards and Technologies report, which notes that "it is advisable to have multiple tools available . . . to switch to another if difficulties occur with the initial tool." *See*, Rick Ayers, Sam Brothers, Wayne Jansen, *Guidelines on Mobile Device Forensics*, NIST Special Publication 800-101, Revision 1, National Institute of Standards and Technology, May 2014, 41, *available at* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf.

Map 1

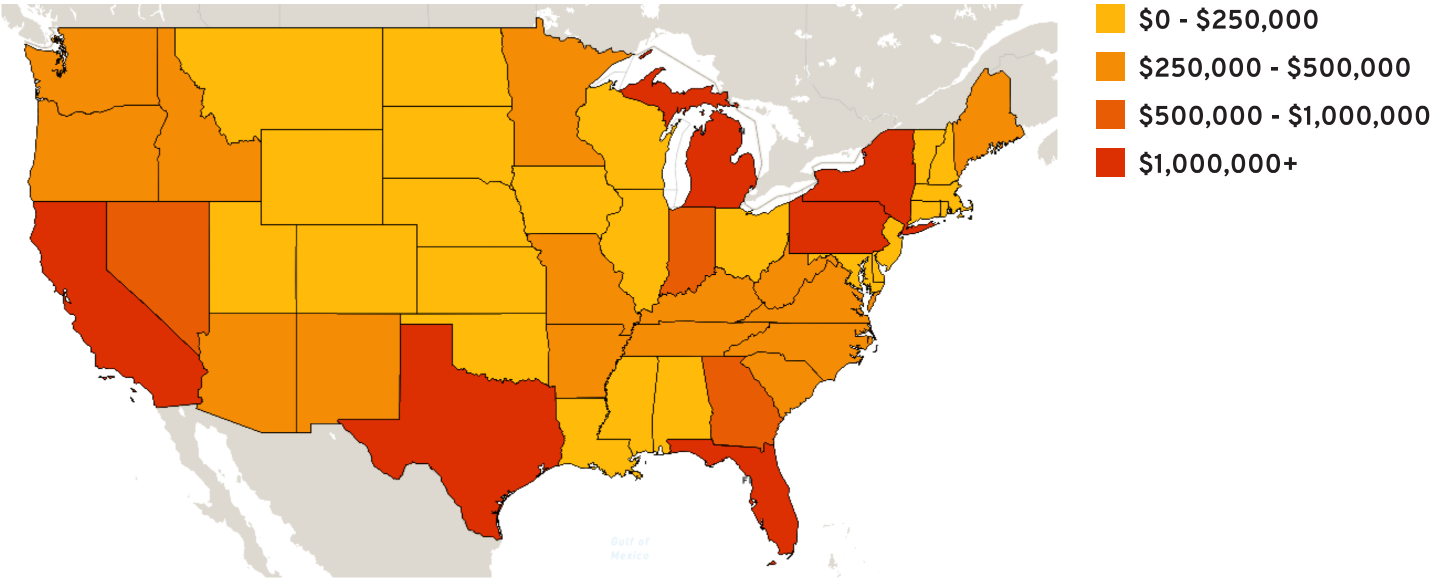


Map 1 *shows the proliferation of MDFTs across agencies in the United States. Each dot represents an agency that has purchased at least one MDFT based on our records. We believe many more agencies in the U.S. have purchased MDFTs than the ones we were able to identify.*

considered the most advanced iPhone extraction device — costs between $15,000 and $30,000.[88] Cellebrite products vary in cost, but a UFED product costs about $10,000, with a $3,000 to $4,000 annual license fee. The level of spending documented below would allow a law enforcement agency to buy dozens of licenses for different kinds of MDFTs each year, such that they could extract data from numerous phones every day.

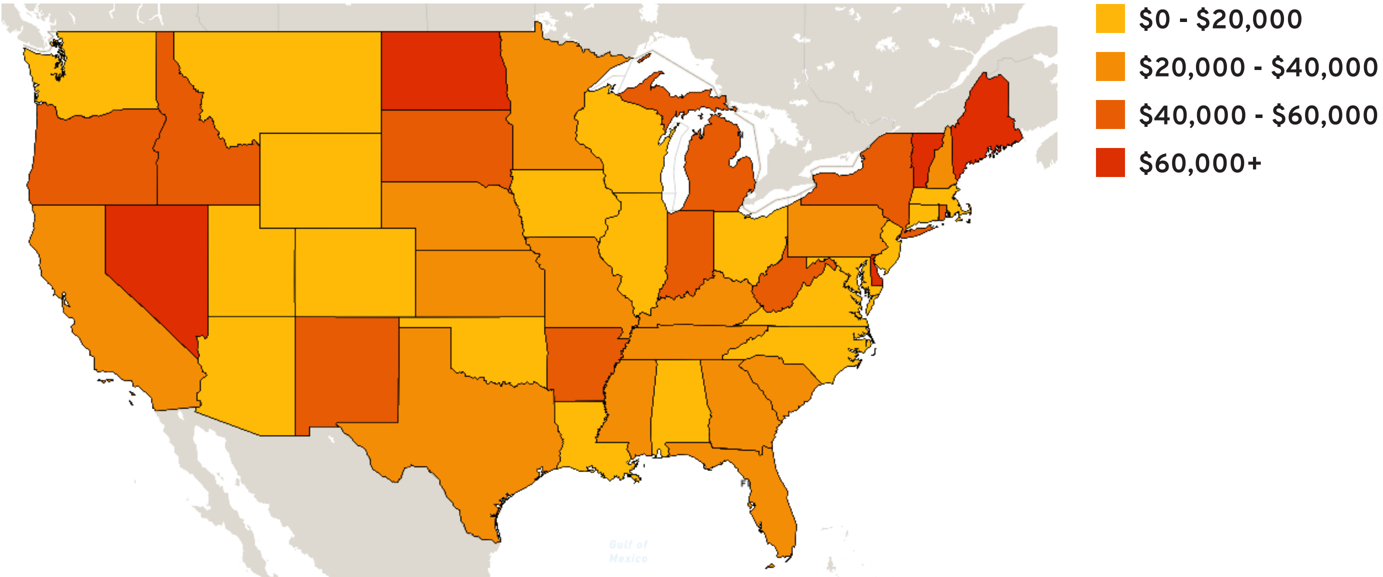
[88] The $15,000 unit is an “online” version, which permits 300 uses. The $30,000 “offline” version permits unlimited use.

Map 2.1



***Map 2.1** shows the total amount of money spent on MDFTs in each state since 2015. Total amounts come from our records requests and from financial transparency websites that states offer. Given this, the total amounts we calculated are likely underestimates.*

Map 2.2



***Map 2.2** shows the total amount of money spent on MDFTs in each state per 1,000 sworn officers.*

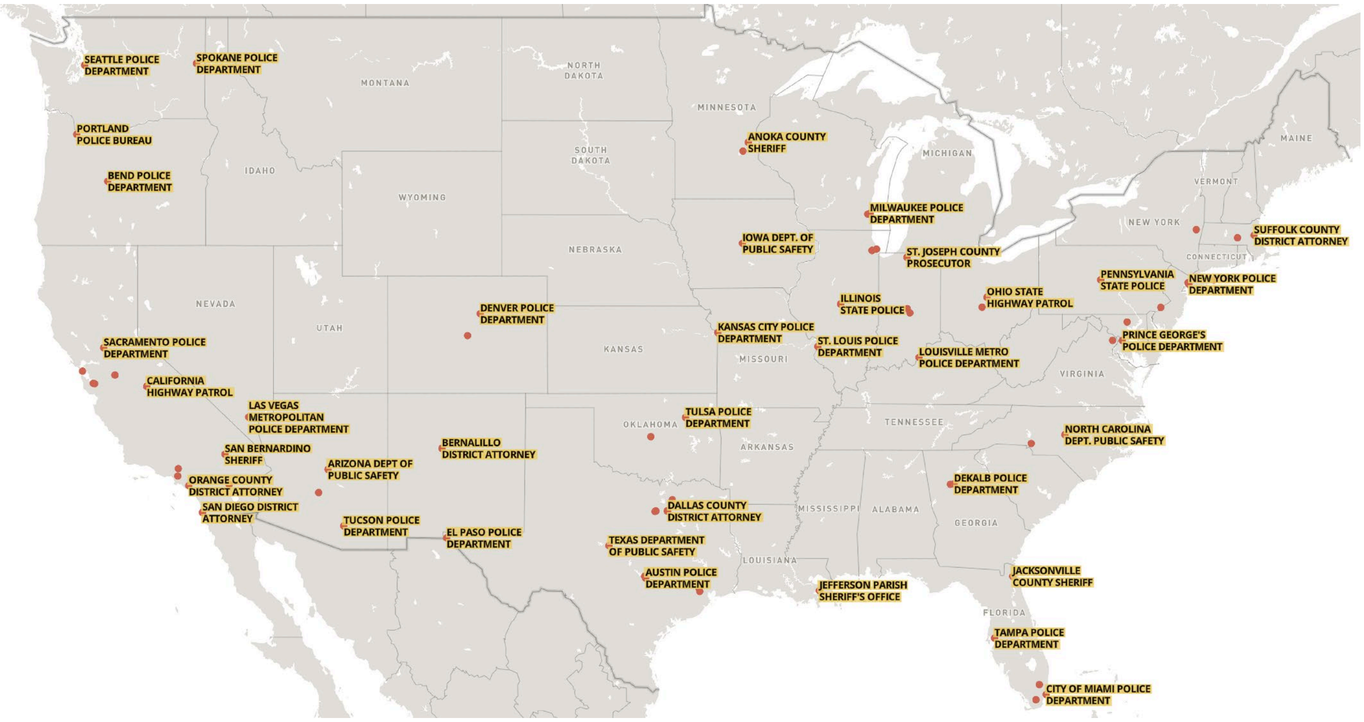
Almost Every Major Law Enforcement Agency Has These Tools

From documents we've obtained, it is clear that the vast majority of large U.S. law enforcement agencies have purchased or used a range of MDFTs. They include:

- Every one of the 50 largest local police departments,
- State law enforcement agencies in all 50 states,
- At least 25 of the 50 largest sheriff's offices and,
- At least 16 out of the 25 largest district or prosecuting attorneys' offices.

These departments have spent hundreds of thousands of dollars on these tools. For example, the Las Vegas Metropolitan Police Department has spent at least $640,000 on MDFTs, the Miami-Dade Police Department has spent at least $330,000, the San Diego Police Department has spent

Map 3


SEATTLE POLICE DEPARTMENT
SPOKANE POLICE DEPARTMENT
MONTANA
NORTH DAKOTA
MINNESOTA
PORTLAND POLICE BUREAU
ANOKA COUNTY SHERIFF
MAINE
SOUTH DAKOTA
MICHIGAN
BEND POLICE DEPARTMENT
IDAHO
WYOMING
VERMONT
MILWAUKEE POLICE DEPARTMENT
NEW YORK
SUFFOLK COUNTY DISTRICT ATTORNEY
IOWA DEPT. OF PUBLIC SAFETY
NEBRASKA
ST. JOSEPH COUNTY PROSECUTOR
CONNECTICUT
PENNSYLVANIA STATE POLICE
NEW YORK POLICE DEPARTMENT
NEVADA
ILLINOIS STATE POLICE
OHIO STATE HIGHWAY PATROL
DENVER POLICE DEPARTMENT
UTAH
KANSAS CITY POLICE DEPARTMENT
PRINCE GEORGE'S POLICE DEPARTMENT
SACRAMENTO POLICE DEPARTMENT
KANSAS
ST. LOUIS POLICE DEPARTMENT
MISSOURI
LOUISVILLE METRO POLICE DEPARTMENT
VIRGINIA
CALIFORNIA HIGHWAY PATROL
LAS VEGAS METROPOLITAN POLICE DEPARTMENT
TULSA POLICE DEPARTMENT
OKLAHOMA
TENNESSEE
NORTH CAROLINA DEPT. PUBLIC SAFETY
SAN BERNARDINO SHERIFF
BERNALILLO DISTRICT ATTORNEY
ARKANSAS
ARIZONA DEPT OF PUBLIC SAFETY
ORANGE COUNTY DISTRICT ATTORNEY
DEKALB POLICE DEPARTMENT
SAN DIEGO DISTRICT ATTORNEY
DALLAS COUNTY DISTRICT ATTORNEY
MISSISSIPPI
ALABAMA
GEORGIA
TUCSON POLICE DEPARTMENT
EL PASO POLICE DEPARTMENT
TEXAS DEPARTMENT OF PUBLIC SAFETY
LOUISIANA
AUSTIN POLICE DEPARTMENT
JEFFERSON PARISH SHERIFF'S OFFICE
JACKSONVILLE COUNTY SHERIFF
FLORIDA
TAMPA POLICE DEPARTMENT
CITY OF MIAMI POLICE DEPARTMENT

Map 3 **displays the total amount of money that law enforcement agencies that responded to our public records requests have spent on MDFTs since 2015. Some agency amounts are "unknown" if their response indicated they purchased MDFTs, but did not share with us specific purchase orders or invoices. Appendix C contains the full data underlying this map.**

at least $230,000, the Charlotte-Mecklenburg Police Department has spent at least $160,000, the Tucson Police Department has spent at least $125,000, and the Columbus Police Department has spent at least $114,000. Between 2018 and 2019, the Georgia Bureau of Investigation spent over $610,000 on MDFTs. Since 2018, state agencies in Michigan have spent more than $1.1 million, and the Indiana State Police have spent at least $510,000 on MDFTs since 2015.

Similarly, sheriff's offices and district attorneys' offices have also spent hundreds of thousands on MDFTs: the Broward County (FL) Sheriff's Office spent at least $560,000, the San Bernardino (CA) Sheriff's Office has spent at least $270,000, the Santa Clara (CA) District Attorney's Office has spent at least $250,000, and the Harris County (TX) Sheriff's Office has spent at least $175,000.

Many Smaller Agencies Can Afford Them

It may be unsurprising that many of the largest law enforcement agencies in the United States have the resources to acquire these tools. **But our research clearly shows that MDFTs are prevalent even among smaller law enforcement agencies.** Many are willing to spend a surprisingly large amount of money to acquire these capabilities.

A range of police departments that serve cities of fewer than 100,000 residents have spent tens of thousands of dollars. For example, the Buckeye (AZ) Police Department has spent at least $80,000, the Alpharetta (GA) Police Department has spent at least $66,000, the Bend (OR) Police Department has spent at least $62,000, and the Asheville (NC) Police Department has spent at least $49,000.[89]

Similarly, GovSpend and city data indicate that a range of cities have purchased MDFTs.[90] For example, the City of Shaker Heights (OH) spent at least $136,134, the City of Mansfield (OH) has spent at least $75,000, the City of Superior (WI) has spent at least $61,259, and the City of Walla Walla (WA) has spent at least $59,000. Each of these cities have populations of 25,000 to 50,000.[91] A range of smaller cities, counties, and towns, like the city of Papillion (NE),[92] the

[89] Population estimates derived from Annual Estimates of the Resident Population for Incorporated Places of 50,000 or More, Ranked by July 1, 2019 Population: April 1, 2010 to July 1, 2019, based off of 2018 data. Bend, Oregon: 97,620; Buckeye, Arizona: 74,339; Asheville, North Carolina: 92,630; Alpharetta, Georgia: 66,257.

[90] For these particular cities, it is not listed that a law enforcement agency purchased mobile device forensic technology. We believe this is an appropriate and fair inference, nevertheless, given all of our data.

[91] Population estimates derived from Annual Estimates of the Resident Population for Incorporated Places: April 1, 2010 to July 1, 2019, based on 2018 data. Mansfield has an estimated population of 46,538, Superior has an estimated population of 26,064, Shaker has an estimated population of 27,215, and Walla Walla has an estimated population of 32,893.

[92] City of Papillion, Nebraska, City Council Minute Records, October 15, 2019, *available at* https://www.papillion.org/AgendaCenter/ViewFile/Minutes/_10152019-205.

town of Whitestown (IN),[93] Jackson Township (NJ),[94] the city of Richland (WA),[95] Glynn County (GA),[96] and the city of Lompoc (CA),[97] have all purchased Grayshift's GrayKey. Budget documents indicate places like the city of Allen (TX)[98] and the city of Pearland (TX) are planning to purchase GrayKey soon.[99]

These examples underscore how accessible and affordable these tools can be, even for agencies with smaller budgets.

Federal Grants Drive Acquisition

A wide variety of federal grants help law enforcement agencies of all sizes acquire MDFTs. In fact, law enforcement agencies "regar[d] assistance from both federal and state governments as critical to success in digital evidence processing," especially for smaller agencies, "given [their] more limited potential budgets compared with large agencies."[100] But even larger departments and agencies have estimated that "95 percent of our [mobile device forensic] equipment" comes from outside funding.[101]

Grants from the Edward Byrne Memorial Justice Assistance Grant (JAG) Program have helped a variety of agencies in particular acquire Cellebrite products — such as police in Salt Lake City

[93] Town of Whitestown, Indiana, Check Register History, Town Council Claims for February 2020, *available at* https://whitestown.in.gov/vertical/sites/%7BB8BE8AC3-9DE8-4247-BCB0-1173F48CC7C3%7D/uploads/February_2020_Disbursements.pdf.

[94] Jackson Township, New Jersey, Board of Trustees Meeting, Record of Proceedings, February 11, 2020, *available at* http://www.jacksontwp.com/Downloads/Feb%2011%2020%20Mtg.pdf.

[95] City of Richland, Washington, City Council Regular Meeting, December 18, 2018, *available at* https://richlandwa.civicclerk.com/Web/UserControls/DocPreview.aspx?p=1&aoid=2310.

[96] Glynn County, Georgia, County Board of Commissioners, Agenda for Regular Meeting, October 1, 2020, *available at* https://www.glynncounty.org/DocumentCenter/View/68006/100120.

[97] City of Lompoc, California, Regular Meeting of the Lompoc City Council, December 4, 2018, https://www.cityoflompoc.com/Home/ShowDocument?id=7151.

[98] City of Allen, Texas, Proposed Annual Budget, Fiscal Year 2020-2021, 181, *available at* https://www.cityofallen.org/DocumentCenter/View/5398/Proposed-Budget-Document.

[99] City of Pearland, Texas, FY21 Proposed Budget "Resilience in Uncertainty," Special Revenue Funds, Page 12, *available at* https://www.pearlandtx.gov/home/showdocument?id=28457.

[100] Sean E. Goodison, Robert C. Davis, and Brian A. Jackson, Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence, 2015, 16 *available at* https://www.rand.org/content/dam/rand/pubs/research_reports/RR800/RR890/RAND_RR890.pdf.

[101] *Id.*

(UT), Burlington (NC), Sumter (SC), and the Marathon County (WI) Sheriff's Department. As of this year, the Miami-Dade Police Department is looking to use $283,000 of JAG grant money to buy Cellebrite tools.[102]

The Internet Crimes Against Children (ICAC) task force, a program run by the Department of Justice's (DOJ) Office of Juvenile Justice and Delinquency Prevention, is a particularly large source of funding for local acquisition of MDFTs. For example, the Arizona Department of Public Safety purchased two GrayKey units with the funds, the Phoenix Police Department used the funds to "complete a project to supply, across the State of Arizona, Cellebrite mobile forensic products,"[103] and police departments from Las Vegas, to Dallas, to DeKalb County (GA) used ICAC money to purchase a variety of MDFTs.

Similarly, the DOJ's Paul Coverdell Forensic Science Improvement Grants Program has provided significant local funding. For example, the Bronx County (NY) District Attorney used the grant money to purchase Cellebrite products.[104] The Charleston (SC) Police Department was funded to purchase two new Cellebrite UFEDs because their digital evidence unit "witnessed a dramatic increase in mobile device submissions."[105] The Alameda County (CA) Sheriff used funds to purchase two GrayKey units,[106] as did forensic science laboratories in Kansas.[107]

[102] *See*, Miami-Dade Board of County Commissioners, Office of the Commission Auditor, Public Safety and Rehabilitation Committee Meeting, June 9, 2020, *available at* https://www.miamidade.gov/auditor/library/2020-06-09-psr-meeting.pdf; Memorandum from the Mayor to the Board of County Commissioners, "Request for Additional Expenditure Authority to Contract SS9737-1/23-1, Cellebrite Forensic System, Service and Maintenance," July 8, 2020, *available at* http://www.miamidade.gov/govaction/legistarfiles/MinMatters/Y2020/201021min.pdf.

[103] Department of Justice, Office of Juvenile Justice and Delinquency Prevention, "FY 2012 Internet Crimes Against Children Task Force Continuation Program," Award Number: 2012-MC-FX-K008, Awardee: Phoenix police Department, *available at* https://ojjdp.ojp.gov/funding/awards/2012-mc-fx-k008.

[104] Department of Justice, National Institute of Justice, "Bronx Coverdell Digital Forensic Science Laboratory," Award Number: 2019-CD-BX-0075, Awardee: Office of the Bronx County District Attorney, *available at* https://nij.ojp.gov/funding/awards/2019-cd-bx-0075.

[105] Department of Justice, National Institute of Justice, "City of Charleston Police Department's Forensic Services Division-Maintaining Quality Digital Examinations," Award Number: 2017-CD-BX-0060, Awardee: City of Charleston, *available at* https://nij.ojp.gov/funding/awards/2017-cd-bx-0060.

[106] Memorandum, Alameda County Sheriff's Office, "Accept the 2018 Paul Coverdell Forensic Science Improvement Grant, July 9, 2019, *available at* http://www.acgov.org/board/bos_calendar/documents/DocsAgendaReg_07_09_19/PUBLIC%20PROTECTION/Regular%20Calendar/Sheriff_281959.pdf.

[107] Department of Justice, National Institute of Justice, "Kansas Federal NIJ FY 19 Paul Coverdell Forensic Science Improvement Grants Program," Award Number: 2019-CD-BX-0028, Awardee: Executive Office of the State of Kansas. https://nij.ojp.gov/funding/awards/2019-cd-bx-0028.

Agencies Share Their Tools With One Another

Even if a law enforcement agency has not purchased MDFTs themselves, many — if not all — have fairly easy access. One option is to form partnerships with other, larger departments. For example, many larger local law enforcement agencies conduct extractions at the request of smaller nearby agencies.[108] Another option is to turn to state-wide agencies — ranging from the offices of Attorneys General, to state departments of forensics or crime labs — that accept requests to perform examinations of digital devices from local agencies.[109]

Yet another common option is to visit labs run by the Federal Bureau of Investigation (FBI). The FBI maintains 17 Regional Computer Forensic Laboratories with broad capabilities to assist local law enforcement.[110] There are at least 84 locations where "cellphone investigative kiosks" (CPIKs) are available, which allow law enforcement "to extract data from a cellphone, put it into a report, and burn the report to a CD or DVD in as little as 30 minutes."[111]

From publicly available data, law enforcement used the cellphone investigative kiosks and virtual cellphone investigative kiosks at least 31,000 times between fiscal years 2013 and 2016.[112]

[108] *See, e.g.*, Ft. Worth Police Department, Request Log Redacted, https://beta.documentcloud.org/documents/20390983-2018-request-log-redacted1; also see Boone County Sheriff's Department, "Law Enforcement Portal," available at http://bcsdcybercrimes.com/leportal.html.

[109] *See, e.g.*, Virginia Department of Forensic Sciences, "Frequently Asked Questions," https://www.dfs.virginia.gov/faq/; Ohio Attorney General, "Unlocking digital evidence: BCI's Cyber Crimes Unit helps law enforcement access, preserve valuable data," On the Job: Criminal Justice update, September 28, 2017, https://www.ohioattorneygeneral.gov/Media/Newsletters/Criminal-Justice-Update/Fall-2017/Unlocking-digital-evidence-BCI%E2%80%99s-Cyber-Crimes-Uni.

[110] The Service Areas are: Chicago, Greater Houston, Heart of America, Intermountain West, Kentucky, New England, New Jersey, New Mexico, North Texas, Northwest, Orange County, Philadelphia, Rocky Mountain, San Diego, Silicon Valley, Tennessee Valley, and Western New York.

[111] Regional Computer Forensics Laboratory, Service Offerings, https://www.rcfl.gov/services.

[112] See U.S. Department of Justice, Regional Computer Forensics Laboratory Annual Report For Fiscal Year 2015, at 13; also see, U.S. Department of Justice, Regional Computer Forensics Laboratory Annual Report For Fiscal Year 2016, at 13. The FY 2017 and FY 2018 reports unfortunately do not report CPIK or VCPK usage numbers.

4. A Pervasive Tool for Even the Most Common Offenses

Our public records requests asked law enforcement agencies for logs of use that identified, among other things, how often and in what kinds of cases law enforcement used MDFTs.[113] The records we've obtained can at best tell an incomplete story, as we did not receive records of use from every department we sent records requests to. Only 44 agencies disclosed usage records, and their form varied greatly.[114]

But here is the story they do tell: **Law enforcement use mobile device forensic tools tens of thousands of times, as an all-purpose investigative tool, for an astonishingly broad array of offenses, often without a warrant. And their use is growing.**

These records challenge two prominent, connected narratives surrounding the use of this technology. The first narrative focuses on the rare instances in which law enforcement cannot access the contents of a phone in a high-profile case. The records we obtained document frequent, seemingly routine, everyday instances in which law enforcement do gain access. The second, connected narrative is that these tools are only (or in large part only) used in cases involving serious harm. They are certainly used in those cases — and in some jurisdictions the majority of MDFT use is for cases of serious harm. But such a framing not only misses the dominant uses of these tools, but also completely ignores racially biased policing policies and practices.

[113] In particular, our request sought "records reflecting the department's *aggregate* use of MDFTs. For example, monthly reports that reflect the total number of MDFT cases for each month, broken down by type of crime, and number and type of phones, and number and type of other devices." *See* Appendix B.

[114] Some departments, like the Arizona Department of Public Safety, provided us with presentations documenting yearly numbers of cellphone extractions. Others, like the Seattle Police Department, provided us hundreds of cellphone extraction request forms. Some, like the San Francisco, Atlanta, and Fort Worth Police Departments provided spreadsheets that logged a range of information — like the kind of offense, the make and model of the phone, the relevant legal authority with specific search warrant numbers, and whether or not the extraction was successful. Some were handwritten. Some were Excel spreadsheets. Much of the documentation we received is haphazard, or otherwise incomplete. For example, in the Gwinnett County District Attorney's Office response to our records request, they noted that "[o]nly one employee maintains a log of his use of MDFTs."

Tens of Thousands of Device Extractions Each Year

The records of use we've assembled from 44 law enforcement agencies represent at least 50,000 extractions of cellphones between 2015 and 2019.[115] To our knowledge, this is the first time that such records have been widely disclosed.[116]

Importantly, *this number represents a severe undercount* of the actual number of cellphone extractions performed by state and local law enforcement since 2015 for many reasons. First, this number only captures usage by 44 agencies, while we know that at least 2,000 agencies have these tools, out of more than 18,000 agencies nationwide. Second, some departments that did disclose usage logs did not start tracking their use of MDFTs until recently. Third, many departments that responded indicated that while they possess MDFTs, they do not track or collect how often they use them. Finally, many of the largest local police departments — such as New York City, Chicago, Washington DC, Baltimore, and Boston — have either denied or did not respond to our requests.

Combining all the information we've gathered,[117] it's safe to say that state and local law enforcement agencies collectively have performed hundreds of thousands of cellphone extractions since 2015.

[115] As we sent many of our public records requests in early 2019, many agencies responded with records up to that chronological point. For example, if we sent a public records request in February 2019, we would receive records documenting use of MDFTs up to February 2019, even if a department responded in March 2020.

[116] We found one prior public records project that asked for "utilization logs," but only two departments responded to those requests. Neither of the responses provided details about the underlying offenses. https://www.muckrock.com/search/?page=1&per_page=25&q=Mobile+Phone+Forensics+Tools.

[117] *See*, *e.g.*, U.S. Department of Justice, Regional Computer Forensics Laboratory Annual Report For Fiscal Year 2015, at 13; also see, U.S. Department of Justice, Regional Computer Forensics Laboratory Annual Report For Fiscal Year 2016, at 13; Essex County Prosecutor's Office, Forensic Analysis and Cyber Tech Services Unit, http://www.njecpo.org/?page_id=2550 ("In 2018, the FACTS Unit conducted over 1,000 cellphone extractions and analysis."); George Woolston, "Inside the special law enforcement unit that brings down child predators," Echo-Pilot, August 7, 2020, *available at* https://www.echo-pilot.com/news/20200807/inside-special-law-enforcement-unit-that-brings-down-child-predators (noting that Burlington County Prosecutor's Office High-Tech Crimes Unit "do somewhere in the neighborhood of 500 phones a year."); Curtis Waltman, "Police are getting a lot of use out of cellphone extraction tech," Muckrock, June 5, 2017, *available at* https://www.muckrock.com/news/archives/2017/jun/05/tulsa-tucson-cellebrite/. For comparison's sake, Customs and Border Protection officers conducted several thousand "advanced" searches of electronic devices from FY2012-FY2018. Of course, this data doesn't disaggregate between "electronic devices." *See* Statement of Undisputed Material Facts, *Alasaad v. McAleenan*, No. 17-cv-11730-DJC, at 10. Dkt. 90-2.

Graffiti, Shoplifting, Drugs, and Other Minor Cases

The records we've obtained demonstrate that some law enforcement agencies use MDFTs as an all-purpose investigative tool for a broad array of offenses.

Some law enforcement agencies frequently point to the need to investigate serious offenses like homicide, child exploitation, and sexual violence to justify their use of these tools. And it is certainly true that in some instances, the most common offenses logged in records of use are things like murder or child sexual abuse material — instances where substantial harm has allegedly occurred.

But the records we've obtained also tell a different story: that law enforcement also use these tools to investigate cases involving graffiti, shoplifting, marijuana possession, prostitution, vandalism, car crashes, parole violations, petty theft, public intoxication, and the full gamut of drug-related offenses.

Many logged offenses appear to have little to no relationship to a mobile device, nor are the offenses digital in nature. In fact, for many of these alleged offenses, it's difficult to understand why such an invasive investigative technique would be necessary, other than mere speculation that evidence could be found on the phone.

To better understand law enforcement's use of these tools, we began seeking out search warrants that law enforcement obtained to search phones. As part of a search warrant, law enforcement submit affidavits — written statements of alleged facts from an agent's point of view — to a judicial authority. The affidavit must establish probable cause for a search, in this case, of a mobile phone.[118] By examining warrant affidavits, we can begin to understand the routine use of these tools.

These records are imperfect, as search warrant affidavits only provide a law enforcement officer's perspective on an alleged incident. Nevertheless, these documents can help paint a picture of what allegedly went on prior to law enforcement's seizure of a phone, and why there is supposedly probable cause to search the phone. A sample of some these incidents include:

[118] The probable cause standard means there's a reasonable basis to believe a crime may have been committed and that the target of suspicion committed the crime, or that evidence of the crime is present and in the place to be searched. It's a low standard to begin with. See Illinois v. Gates, 462 U. S. 213, 232, 243-244, n. 13 (1983)(probable cause "is not readily, or even usefully, reduced to a neat set of legal rules" and "requires only a probability or substantial chance of criminal activity, not an actual showing of such activity.") *See also* Kaley v. United States, 571 U. S. 320, 338. (2014) ("Probable cause, we have often told litigants, is not a high bar.")

- After an undercover purchase of $220 worth of marijuana, officers sought to search two phones for evidence of narcotics sales and “other criminal offenses.”[119]
- An off-duty officer witnessed what they thought was shoplifting at a Dick’s Sporting Goods Store and said the individuals had left in a Honda Accord. Another officer initiated a vehicle pursuit. Five individuals were arrested and four phones seized. After speaking to the five individuals, officers learned they “had been communicating, via cellphone, throughout the night and were allegedly going to sell the stolen clothing to ‘their regulars.’” Officers sought to search the phones for “plans and correspondence regarding these thefts and the organized crime,” and “[t]he identity of ‘their regulars.’”[120]
- Officers witnessed “suspicious behavior” in a Whole Foods grocery store parking lot that they believed to be a “controlled substance exchange” between occupants in a Lexus and a Buick. After the Lexus drove by the unmarked police car, one of the officers “reported the smell the odor [sic] of Marijuana coming through his open window seemingly from the Lexus.” The officers stopped the Lexus because they “did not have a front license plate which is an equipment violation.” Upon searching the car, officers found a small amount of what appeared to be cocaine and marijuana and a black scale. Officers sought to search a subject’s phone for “further evidence of the nature of the suspected controlled substance exchange,” and for evidence “on the knowledge of possession and/or sales of the controlled substances found . . . in [the] vehicle.”[121]
- Officers were dispatched to a dispute at a McDonald’s. After arriving, they learned that the dispute appeared to be over $70 that was owed. Apparently, the person who was owed money was “forcing” the person who owed money “to remove his clothing and forcefully removed it as some sort of collateral.” One individual was arrested for charges of simple robbery. Four phones were ultimately seized and officers sought to search them “to further this investigation.”[122]
- A plain clothes DEA Task Force Officer was “making consensual contacts” with individuals at the Dallas/Fort Worth International Airport. After asking a traveler “if he had any large sums of US Currency with him,” the officer received consent to search his backpack, and found a large sum of U.S. currency. At this point the subject said he “had used this backpack to store marijuana inside of it before.” Officers then saw a WhatsApp message displayed on the subject’s phone that said “This flower is so good by far one of my fav strands ever.” Officers sought to search the phone for evidence of narcotics sales and money laundering.[123]

[119] *See* Tarrant County Search Warrant SW38982, https://beta.documentcloud.org/documents/20394694-sw_38982.

[120] *See* Tarrant County Search Warrant SW40465, https://beta.documentcloud.org/documents/20394702-sw_40465.

[121] *See* Anoka County Search Warrant 18-108859, https://beta.documentcloud.org/documents/20394762-18-108859.

[122] *See* Anoka County Search Warrant 17015643, https://beta.documentcloud.org/documents/20394763-17015643.

[123] *See* Tarrant County Search Warrant SW39468, https://beta.documentcloud.org/documents/20394695-sw_39468.

- A patrol car stopped a vehicle for a “left lane violation.” “Due to nervousness observed and inconsistent stories, a free air sniff was conducted by a . . . K9 with a positive alert to narcotics.” A search of the car revealed several shrink-wrapped bags of suspected marijuana and marijuana wax. Officers seized eight phones from the car’s occupants, and sought to find “evidence of drug transactions, which would provide further evidence with intent to distribute.”[124]
- An officer stopped a “white minivan . . . for speeding and traveling in the left lane when prohibited.” The driver was “nervous upon contact.” After denying a consent search of the car, a K9 sniff of the car led to the discovery of marijuana. A search of the car revealed several bags of suspected marijuana. After seizing two phones from the car, officers sought to search the phones for “evidence of drug transactions that will provide further evidence with intent to distribute.”[125]
- In a particularly egregious case, officers shot and killed a man after he “ran from the driver’s side of the vehicle” during a traffic stop. Police ultimately discovered a small orange prescription pill container next to the victim. Tests of the pills revealed they were a mix of acetaminophen and fentanyl. After a subsequent search of the victim’s vehicle, officers discovered a phone. Officers sought to search the phone for evidence related to “counterfeit Oxycodone,” “evidence relating to . . . motives for fleeing from the police,” and evidence “relating to the stolen Smith & Wesson SD9 Handgun.”[126]
- During an eviction with an “uncooperative” individual, officers shot the individual 15 times after he apparently reached under a blanket for what officers saw as a rifle. Officers seized several cellphones and sought to search them for “any information which would reveal [the individual’s] mindset and motivation at the time of the shooting.”[127]
- Officers were looking for a juvenile who allegedly violated the terms of his electronic home monitoring. Officers eventually located the individual and, after a “short foot pursuit . . . he threw several items to the ground,” including a phone. Officers located the phone and sought to search it for evidence of escape in the second degree.[128]

[124] *See* Colorado State Patrol Search Warrant ST170049-4A170155, https://beta.documentcloud.org/documents/20394714-st1700494a170155-search-warrant.

[125] *See* Colorado State Patrol Search Warrant ST170210-17-SW-380, https://beta.documentcloud.org/documents/20394713-st170210-redacted.

[126] *See* King County Search Warrant 19-272, https://beta.documentcloud.org/documents/20394722-affidavit-19-272.

[127] *See* Spokane Search Warrant 2018-10032539, https://beta.documentcloud.org/documents/20394723-warrant-5_-closed_2018-10032539.

[128] *See* King County Search Warrant 19-527, https://beta.documentcloud.org/documents/20394724-affidavit-19-5271.

Some departments use MDFTs by and large to investigate drug-related offenses. For example, the vast majority of logged cellphone extractions by the Colorado State Patrol and Baltimore County Police Department are for drug-related offenses. Logs from the Dallas Police Department indicated that drug-related offenses were the second most common offense in which MDFTs were used, behind murder.

For other law enforcement agencies, drug-related offenses are often in the top three or five most common offenses listed in logs we obtained. For example, 20% of phones the Suffolk County (NY) Police Department forensically examined in 2018 were narcotics cases. A log of outside agency cellphone extraction requests to the Santa Clara County (CA) District Attorney's Office appears to show that drug-related offenses are in the top three most common offenses listed. The same is true of the San Bernardino (CA) Sheriff's Office. And while drug-related offenses didn't constitute many cellphone extractions by the Fort Worth Police Department before 2017, they ballooned in 2018 and 2019 to be the third most common offense.

The prominence of drug-related offenses in cellphone extraction logs is especially worrisome given the extreme racial disparities in drug arrests,[129] the disproportionate severity of drug sentences, and the role drug arrests play in deportations.[130] Although none of the extraction logs we received maintained data on race or ethnicity, given this disparity, it's highly likely that these cellphone extractions disproportionately affect Black and Latinx people.

[129] Human Rights Watch, ACLU, *Every 25 Seconds: The Human Toll of Criminalizing Drug Use in the United States*, October 2016; also see, Joseph E Kennedy, Isaac Unah, Kasi Wahlers, *Sharks and Minnows in the War on Drugs: A Study of Quantity*, Race and Drug Type in Drug Arrests, 52 U.C. Davis L. Rev. 729, 746 (2018)("Overall, marijuana dominates all other types of drugs in terms of arrests. Blacks and Hispanics are arrested disproportionately in terms of their share of the overall population. The racial disparities involved are not as great as those present among arrests for hard drugs. Whites dominate heroin and meth/amphetamine arrests, but those drugs account for relatively few hard drug arrests overall. Blacks, in contrast, dominate crack cocaine arrests and are disproportionately represented in powder cocaine arrests. One racial disparity in drug arrests overall may, then, be at least partially driven by what drugs we arrest people for, with Black overrepresentation driven by crack cocaine arrests and White underrepresentation driven by the relatively low levels of heroin and meth/amphetamine arrests."); also see Ojmarrh Mitchell, Michael S. Caudy, *Examining Racial Disparities in Drug Arrests*, 32 Justice Quarterly 288, (2013) ("For example, holding all other variables constant, at ages 17, 22, and 27 African-Americans' odds of drug arrest are approximately 13, 83, and 235% greater than whites, respectively.")

[130] Drug Policy Alliance, *The Drug War and Mass Deportation*, February 2016.

[131] *See, e.g.*, Tarrant County Search Warrant SW41310 https://beta.documentcloud.org/documents/20394768-sw_41301; Colorado State Patrol Search Warrant ST170210-17-SW-379, https://beta.documentcloud.org/documents/20394713-st170210-redacted. ("individuals engaged in narcotic sales send/receive text messages regarding narcotic sales, make/receive phone calls regarding narcotic sales and take photographs/video of themselves possessing narcotics," and that data the phone that will likely either "contain evidence of drug transactions that will provide further evidence with intent to distribute.")

Almost universally, the search warrants we obtained for drug-related offenses rely on the logic that boils down to a claim that drug dealers use cellphones.[131] An affidavit from a Fort Worth (TX) officer provides a prototypical example:

> *it is a common practice for individuals involved in the drug trade, to store, keep or conceal contact names, phone numbers, addresses, address books, and contact list of associates, inside cellular telephones, along with logs of incoming and outgoing calls, text messages, e-mails, direct connect data, SIM cards, voice mail messages, logs of accessing and downloading information from the internet, photographs, moving video, audio files, dates, appointments, and other information on personal calendars, Global position system (GPS) data, and telephone memory cards.*[132]

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. Of course, there are some allegations where the connection between the data on a phone and the alleged conduct make it easier for law enforcement to establish probable cause. But there are plenty of cases where the nexus between a phone's contents and data and the alleged offense is tenuous at best.[133] The use of an MDFT in these cases seems like a drastic investigative overreach.

Officers Often Rely on Consent, Not Warrants

In 2014, the Supreme Court held in Riley that in order to search a cellphone, police must get a warrant. However, "consent searches" have long been understood to be an exception to the Fourth Amendment's warrant requirement. Our records show that, for some agencies, law enforcement regularly rely on a person's consent as the legal basis to search cellphones.

Of the 1,583 cellphone extractions that the Harris County (TX) Sheriff's Office performed from August 2015 to July 2019, only 47% of phones were extracted subject to a search warrant — the other 53% were consent searches, or searches of phones that were "abandoned/deceased." Of the 437 cellphones that the Denver Police Department extracted from March 2018 to early April 2019,

[132] See Tarrant County Search Warrant SW40869, https://beta.documentcloud.org/documents/20394764-sw_40869.

[133] For example, a recent DC Court of Appeals decision centered on a first-degree murder investigation. There, law enforcement's original search warrant for the suspect's cellphone allowed the police to search for "[a]ll records and "any evidence" related to the alleged offense, and law enforcement used a Cellebrite machine to extract all data off the phone. But, as the Court of Appeals held, while law enforcement had probable cause to search a phone for text messages between two individuals on one specific day, and the relevant GPS data from the phone on two specific days, "beyond those discrete items, the affidavits stated no facts that even arguably provided a reason to believe that any other information or data on the phones had any nexus to the investigation of [the victim's] death." See Eugene Burns v. United States, District of Columbia Court of Appeals 17-CF-1347, Dec. 2019.

nearly half were searched pursuant to a search warrant. Approximately one third of the phones the Seattle Police Department sought to extract data from were consent searches.

Of the 497 cellphone extractions that the Anoka County (MN) Sheriff's Office performed from early 2017 to May 2019, 38% were consent searches of some kind. For the Atlanta Police Department, of the at least 985 cellphone extractions performed from 2017 to early April 2019, about 10% were pursuant to a consent to search form. And for the Broward County (FL) Sheriff's Office, at least 18% of extractions were based on consent.

Given the broad prevalence of consent searches in other criminal legal contexts,[134] it is perhaps unsurprising that consent searches play a decent role in the searches of mobile phones. We address the problems with consent searches for mobile phones in particular in Section 6.

A Routine and Growing Practice

The records we've obtained clearly indicate that law enforcement agencies are using MDFTs for an ever-expanding array of offenses. **Given that racial disparities in arrest rates are one of the defining aspects of the American criminal legal system, it's likely that cellphone extractions already mirror these disparities.**[135]

In documents we obtained, law enforcement readily admit that these tools are regularly used and internally understood as a standard investigatory tool: "[R]equests for cellphone analysis has become the standard for phones involved in all types of criminal investigation;"[136] "it is used on a daily basis;"[137] "[our department] relies heavily on Cellebrite . . . tools."[138] In a recent D.C. court

[134] Ric Simmons, *Not "Voluntary" but Still Reasonable: A New Paradigm for Understanding the Consent Searches Doctrine*, 80 Ind. L. J. 773 (2005) ("Over 90% of warrantless police searches are accomplished through the use of the consent exception to the Fourth Amendment.")

[135] Megan Stevenson, Sandra G. Mayson, *The Scale of Misdemeanor Justice*, 98 B.U. L. Rev. 731, 769-770 (2018) (Finding that Black people are arrested at higher rates compared to their similarly situated white counterparts for a large number of misdemeanors offenses, a decades long, consistent disparity. In particular finding "that black people are arrested at more than twice the rate of white people for nine of twelve likely-misdemeanor offenses: vagrancy, prostitution, gambling, drug possession, simple assault, theft, disorderly conduct, vandalism, and 'other offenses.'")

[136] Dallas Police Department Purchase Authorization Request, December 3, 2019, https://beta.documentcloud.org/documents/20390026-d004755-021319_r.

[137] Illinois State Police Procurement Justification Form in June 2016, https://beta.documentcloud.org/documents/20391543-cellebrite-an17-0107_marked_redacted.

[138] San Diego Police Department, "Critical Data Extraction Tool Upgrades," April 30, 2018, Memorandum, https://beta.documentcloud.org/documents/20392573-sole-source-cellebrite-mod-3778-052118.

opinion, the court noted that "search warrant requests seeking access to cellphone data have become a common feature of law enforcement investigations."[139]

Statistics on use, where available, help demonstrate that law enforcement use of these tools is growing. For example, the Las Vegas Metropolitan Police Department examined 260% more cellphones in fiscal years 2018-2019 compared to 2015-2016 (from 222 in FY15-16 to 800 in FY18-19). Louisville's Metropolitan Police Department examined 236% more phones between 2017 and 2018 (from 88 phones to 296). Arizona's Department of Public Safety use grew 50% from 2015 to 2018 (from 796 phones in 2015 to 1,198 phones in 2018). Honolulu's Police Department used MDFTs 568% more in 2018 than 2015 (from 25 in 2016 to 167 in 2018). And Dallas' Police Department noted a 25% increase in cellphone extractions from 2018 to 2019.[140]

5. Few Constraints and Little Oversight

Despite how invasive MDFTs are, few departments have detailed internal policies that clearly restrict how or when they are used. In our public records requests, we asked each department for any policies or guidelines that would control MDFT use.[141]

Many departments have no policies at all — despite using these tools for years. Nearly half of the departments that responded to our records requests (40 out of 81) indicated they had no policies in place. Even when policies exist, they are often remarkably vague, for instance, by giving general guidance to officers to obtain a search warrant. Among the policies we did receive, we rarely saw any detailed guidance on concerns related to digital searches, such as the scope and particularity of searches, and the retention and use of extracted data. Unsurprisingly, agencies almost always acquire these tools with no public oversight. From our research, we found scant evidence of any community discussion or debate regarding the adoption of these tools.

[139] Eugene Burns v. United States, District of Columbia Court of Appeals 17-CF-1347, Dec. 2019, 4.

[140] To be certain, some departments' usage of MDFTs fluctuates somewhat between years — like the Fort Worth Police Department, St. Louis Metropolitan Police Department, San Francisco Police Department, or Harris County Sheriff's Office. Generally speaking, however, these departments were already regularly using the tools several hundred times per year as of 2015 or 2016.

[141] Our request noted that these policies and guidelines included, but were not limited to the following "training materials regarding their operation, restrictions on when they may be used, limitations on retention and use of collected data, security measures taken to protect stored and in-transit data, guidance on when a warrant or other legal process must be obtained, and guidance on when the existence and use of MDFTs may be revealed to the public, criminal defendants, or judges." *See* Appendix B.

Many Agencies Have No Specific Policies in Place

Many agencies simply have no policies in place to govern how MDFTs are used. Among the 81 law enforcement agencies that responded to our public records requests, at least 40 of them indicated that they did not have any policies.

Of the 41 policies we received, only nine are detailed enough to provide meaningful guidance to officers. Combined, this means that nearly 90% of the departments that responded to our records requests give their officers wide discretion to use MDFTs and the phone data they collect.

Even very large agencies like the Los Angeles Police Department (LAPD) had no specific policies in place for MDFTs, even though the LAPD has spent hundreds of thousands of dollars on these tools and has used them thousands of times. Other major departments that have no policies include the Houston (TX) Police Department and the Nassau County (NY) Police Department.[142] State law enforcement agencies and county sheriff's offices are similarly lacking.[143]

Many of the country's largest and most prominent district attorneys' offices also use these tools without specific policies, including offices in Manhattan (NY), Cook County (IL), Tarrant County (TX), Philadelphia (PA), Suffolk County (MA), and Dallas County (TX). In their responses to our public records requests, some offices simply noted that they follow applicable case law governing the use of MDFTs. For example, the Manhattan District Attorney's Office responded that their office "strictly follows and adheres to all applicable federal and state constitutional laws, New York criminal procedure laws, and search and seizure case law in the utilization of this [technology] on a case by case basis."[144]

[142] In addition, many mid-size and smaller police departments, like the Portland (OR) Police Bureau, Sacramento (CA) Police Department, the Bend (WA) Police Department, and the West Allis (WI) Police Department also have no specific policies in place. The Tulsa (OK) Police Department similarly had no policy in place, but indicated they "follow best practices," without indicating what those best practices are or who had designated them.

[143] Of the 13 state law enforcement agencies that responded to our request, five indicated they had no relevant policies — the Arizona Department of Public Safety, the California Highway Patrol, the Indiana State Police, the Pennsylvania State Police, and the Washington State Patrol. Days before publication, the New York State Police sent responsive records to our request but did not include any policies in their response. Of the ten sheriff's offices that responded, four indicated they had no policies. The Broward County Sheriff Office noted that their office was in the process of drafting policies "as part of the department's restructuring."

[144] *See* New York County District Attorney FOIL Response, https://beta.documentcloud.org/documents/20394637-upturn-foil_da-response2.

The policies we did receive varied substantially in length and detail. Some were nearly 40 pages long; others were barely a paragraph. Some were clearly in the process of being developed; others were boilerplate policies that were too broad to be meaningful. Of course, detailed policies won't by themselves ensure that people's rights will be respected. But without them, mobile device searches will expand the power of the police in an even less constrained way. We highlight a few acute problems below.

Overbroad Searches and the Lack of Particularity

The Fourth Amendment to the United States Constitution requires warrants to describe with particularity the places to be searched and the things to be seized.[145] This "particularity requirement" was designed to protect against "general warrants," such that law enforcement could not indiscriminately rummage through a person's property. In addition, the warrant application must identify the specific offense for which law enforcement has established probable cause. To be certain, almost every department policy acknowledges the need to have a sound legal basis to search a phone, whether it's a search warrant, verbal or written consent, or some other basis, like abandonment or exigent circumstances. But few departments provide much more clarity or direction beyond this general acknowledgement.

Some departments vaguely allude to the need for particularized searches. For example, the Las Vegas Metropolitan Police Department's Digital Forensics Lab policy notes that "searches that constitute a 'fishing expedition' . . . will not be conducted," but does not add any more detail.[146] Similarly, the Kansas City Police Department's policy mentions that an examiner "conducting the data extraction will adhere to the details and limitations regarding allowable data extraction and retention as specified in the warrant" — but does not further elaborate on what those limitations can or should be.[147]

In fact, some policies, like the Illinois State Police's, encourage broad search warrants, noting that "[a]ll computer hardware and software should be included [in search warrant applications], keeping in mind the entire system is necessary to replicate the suspect's use of it and to enable forensic examination of the system."[148]

[145] U.S. Const. amend. IV. ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and *particularly describing the place to be searched, and the persons or things to be seized*.")

[146] *See* Las Vegas Metropolitan Police Department, Digital Investigations Bureau, https://beta.documentcloud.org/documents/20392915-logan-koepke-190403-20-lvmpd-digital-investigations-bureau-policies.

[147] *See* Kansas City Missouri Police Department Examination of Electronic Data Storage Devices, https://beta.documentcloud.org/documents/20392850-4316_001.

[148] *See* Illinois State Police, Collecting and Packaging Computer and Digital/Multimedia Forensic Evidence, https://beta.documentcloud.org/documents/20391527-ops-202-dir.

Other policies ask officers to seek broad search authority from the courts, and only to narrow their search when making internal requests to forensic examiners. For example, the Indianapolis Metropolitan Police Department directs officers requesting forensic analysis to describe "the evidence you expect to recover from the exam. Be specific as to what information the examiner should search for, such as 'Evidence of Dealing Narcotics' . . . [d]on't list types of data (e.g. call log, text, email, etc. . . .) as *your search warrant should cover all data*."[149] Similarly, the Jacksonville Sheriff's Office policy notes that failing to provide "details of the investigation and what detailed information the detection seeks from a forensic analysis . . . will greatly increase the processing and analysis time."[150] In other words, to the extent that law enforcement policies do speak to narrow forensic searches, they do so with reference to productivity and efficiency, not legal authority or constitutional protections.

Relatedly, few policies provide guidance on what examiners should do if they encounter potential evidence of another crime that is not detailed in the initial search warrant. Using a search warrant to look for digital evidence of one potential crime, only to then search for digital evidence of a completely separate crime, raises serious constitutional questions. This practice and limitation is crucial, because without it, law enforcement could go on a "fishing expedition" in search of evidence of any crime, far beyond the original justification for a search. We observed only two policies that provided any guidance on this point.[151]

The risk of overbroad searches is especially worrying given the fact that it's nearly impossible for those outside of law enforcement — such as a defense lawyer — to repeat the steps that a forensic examiner took and to audit the scope of a search.[152] A handful of agency policies do require examiners to document how a search was conducted, but the level of documentation required is still unlikely to allow a defense lawyer to meaningfully audit a search.

[149] *See* Indianapolis Metropolitan Police Department, Request Form for Mobile Device Forensics, https://beta.documentcloud.org/documents/20391585-mobile_forensics_request_form_02-20-2019. (emphasis added)

[150] *See* Jacksonville Sheriff's Office, Computer Forensic Investigations, Order 392, https://beta.documentcloud.org/documents/20392554-redacted_upm_392_computer_forensic_investigations_.

[151] For example, the Santa Clara District Attorney's Office advises that if an "[e]xaminer discovers evidence of another crime(s) that is outside the scope of the submitted search warrant, the Examiner may continue the examination for items named in the warrant. The Examiner should contact the submitting agency and/or the prosecutor handling the case for guidance before conducting any searches for evidence not named in the original warrant." *See* Santa Clara District Attorney's Office, Santa Clara County Crime Laboratory Computer Forensic Standard Operating Procedures, https://beta.documentcloud.org/documents/20394644-2019-08-19-pra-resp-email-att-standard-operating-procedures-rev-26-112820181. As another example, the San Diego Police Department says that if "an examiner discovers evidence of another crime(s) that is outside the scope of the submitted legal authority, the examiner will notify the assigned prosecutor and/or submitting investigator of the discovery and nature of any evidence of other crime(s) outside the scope of the original search warrant." *See* San Diego Police Department, Forensic Technology Unit Manual, https://beta.documentcloud.org/documents/20392583-forensic-technology-unit-manual-082218-current.

[152] Repeatability refers to obtaining the same results when using the same method on identical test items in the same laboratory by the same operator using the same equipment within short intervals of time. Reproducibility refers to obtaining the same results being obtained when using the same method on identical test items in different laboratories with different operators utilizing different equipment.

One policy from the Massachusetts State Police states that "[f]ull documentation of all procedures performed and software used should be recorded for every examination and added to the case file."[153] The Tucson Police Department's Forensic Electronic Media Unit's Quality Manual notes that "[n]otes should be taken contemporaneous to the examination or as close as possible."[154] And the Texas Department of Public Safety's Computer Information Technology and Electronic Crimes Unit Standard Operating Procedure requires the unit to establish a "peer review process where 20% of all forensic analysis completed will be reviewed,"[155] but they did not provide an example.

There are longstanding legal debates over how to properly govern digital searches: Legal scholars and courts have wrestled with the problems of overbroad digital searches for decades.[156] These arguments are incredibly important, and we surface only some of them in Section 6. Suffice it to say that it's especially striking, given the prominence of these legal debates, that law enforcement agencies have largely allowed officers and forensic examiners to search mobile phones without detailed policies and with few constraints.

[153] *See* Massachusetts State Police Forensic Services Group Digital Evidence and Media Section, Technical Manual, https://beta.documentcloud.org/documents/20393038-4708_001.

[154] *See* Tucson Police Department, Forensic Electronic Media Unit Quality Manual, https://beta.documentcloud.org/documents/20390047-femu-qa-manual-final-rev-27.

[155] This peer review process is supposed to evaluate and document the following: Whether proper evidence intake procedures were followed (legal authority, chain of custody, and handling of evidence); Whether appropriate forensic acquisition methods were followed (write protection, CMOS date/time captured, sterilization procedures, and validating DDE integrity); Whether appropriate forensic examination procedures were followed; Whether appropriate information was identified in the Digital Forensics Report and CID Case Management Report; Whether dissemination procedures were completed properly; Upon review of post-examination evidence, whether archival procedures were properly followed. See Texas Department of Public Safety, Computer Information Technology & Electronic Crimes (CITEC) Unit Standard Operating Procedures, January 2019, https://beta.documentcloud.org/documents/20393187-citec-sop.

[156] *See, e.g.*, Paul Ohm, *Massive Hard Drives, General Warrants, and the Power of Magistrate Judges*, 97 VA. L. Rev In Brief 1 (2011); James Saylor, *Computers As Castles: Preventing the Plain View Doctrine From Becoming a Vehicle for Overbroad Digital Searches*, 79. Ford. L. Rev. 2809 (2011); Eric Yeager, *Looking for Trouble: An Exploration of How to Regulate Digital Searches*, 66 Vand. L. Rev. 685 (2013); Andrew D. Huynh, *What Comes after Get a Warrant: Balancing Particularity and Practicality in Mobile Search Warrants Post-Riley*, 101 Cornell L. Rev. 187 (2015); Adam Gershowitz, *The Post-Riley Search Warrant: Search Protocols and Particularity in Cell Phone Searches*, 69 Vand. L. Rev. 585 (2016); Michael Mestitz, *Unpacking Digital Containers: Extending Riley's Reasoning to Digital Files and Subfolders*, 69 Stan. L. Rev. 321 (2017); Sara J. Dennis, *Regulating Search Warrant Execution Procedure for Stored Electronic Communications*, 86 Ford. L. Rev. 2993 (2018); Laura Donohue, *Customs, Immigration, and Rights: Constitutional Limits on Electronic Border Searches*, 128 Yale L. J. Forum 961 (2019).

Police Databases and Unrelated Investigations

After law enforcement extracts data from a phone and prepares a forensic report, what happens to the underlying data and how might it be used later? Few policies we received mention any limits on how long extracted data may be retained, or how that data may be used beyond the scope of an immediate investigation.

Absent specific prohibitions, law enforcement could copy data from someone's phone — say, their contact list — and add that information into a far-reaching police surveillance database. For instance, it's easy to imagine law enforcement seeing data extracted from mobile phones as providing valuable "leads" for "gang databases," given the low bar for individuals and their information to be added to such databases. "Gang databases" are notorious, in part, for the loose standards and criteria upon which law enforcement rely to enter people into the databases. Factors can include things like "pictures of the individual displaying perceived gang signals on social media,"[157] "association with known gang members,"[158] "frequenting gang areas,"[159] and other indicators fabricated by law enforcement.[160] This discretion has led to extreme racial disparities in gang databases.[161] Critically, these designations can have profound effects on peoples' lives: it can "immediately make people ineligible for jobs and housing, subject to increased bail and enhanced charges, and more likely to get deported."[162] For law enforcement who operate gang databases, data extracted from a phone, like contacts, photos and videos, messages, location history, and more, would be of immediate interest.

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 policies or laws that require notifying someone that their phone has been searched,[163] it would

[157] City of Chicago Office of Inspector General, *Review of the Chicago Police Department's "Gang Database,"* April 11, 2019, *available at* https://igchicago.org/wp-content/uploads/2019/04/OIG-CPD-Gang-Database-Review.pdf.

[158] Josmar Trujillo, Alex Vitale, *Gang Takedowns in the De Blasio Era: The Dangers of 'Precision Policing,'* The Policing and Social Justice Project at Brooklyn College, December 2019, *available at* https://static1.squarespace.com/static/5de981188ae1bf14a94410f5/t/5df14904887d561d6cc9455e/1576093963895/2019+New+York+City+Gang+Policing+Report+-+FINAL%29.pdf.

[159] California State Auditor, The CalGang Criminal Intelligence System, Report 2015-130, August 2016, *available at* https://www.auditor.ca.gov/pdfs/reports/2015-130.pdf.

[160] Stefano Bloch, "Are You in a Gang Database?" New York Times, February 3, 2020, *available at* https://www.nytimes.com/2020/02/03/opinion/los-angeles-gang-database.html.

[161] Keegan Stephan, *Conspiracy: Contemporary Gang Policing and Prosecutions*, 40 Cardozo L. Rev. 991 http://cardozolawreview.com/wp-content/uploads/2019/01/Stephan.40.2.9..pdf

[162] *Id.*, 1018-1019.

[163] For example, the New Mexico Electronic Communications Privacy Act requires notifications to the subject of an investigation contemporaneously with the execution of a warrant.

be impossible for those under investigation to know of — let alone challenge — situations where law enforcement continues to rifle through previously extracted data for new or unrelated investigations.

There are a small handful of state laws that do prescribe evidence retention periods specifically for digital evidence obtained from cellphones. For example, New Mexico's recently enacted Electronic Communications Privacy Act requires that "any information obtained through the execution of the warrant that is unrelated to the objective of the warrant be destroyed within thirty days after the information is seized and be not subject to further review, use or disclosure."[164] However, such laws are far from the norm, and most Americans are currently not protected by these types of data deletion or sealing requirements.

Expanding Searches From a Phone Into the Cloud

Digital forensics practitioners consider cloud data to be "a virtual goldmine of potential evidence."[165] A recent report from Cellebrite indicated that "one in every two cases requires access to cloud-based data."[166] As previously discussed in Section 2, major vendors like Cellebrite now sell tools that specifically help law enforcement parlay access to data stored on a phone into further access to data held in the cloud. These tools could, for instance, allow law enforcement to siphon and collect all data from an iCloud account, or all emails from a Gmail account. Or they could allow the police to impersonate the individual. These "cloud analyzer" tools, which are relatively new, represent an immense expansion of law enforcement investigatory powers.

Yet no agency turned over any policies that specifically control the use of cloud data extraction tools.

In theory, unless cloud-based data is specifically detailed in a search warrant for a mobile device, law enforcement should not be able to extract data from the cloud. Cloud extraction poses further challenges: collecting data after execution of a search should require a wiretap order. Search warrants allow for police to get data as of the time of the search warrant's issuance. But if data keeps coming in, this future collection should be treated like a wiretap.

[164] *See* https://nmlegis.gov/Sessions/19%20Regular/final/SB0199.pdf. Similarly, California's Electronic Communications Privacy Act allows judges to, at their discretion, "require that any information obtained through the execution of the warrant or order that is unrelated to the objective of the warrant be destroyed as soon as feasible after the termination of the current investigation and any related investigations or proceedings." *See* https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201520160SB178.

[165] Ben Rossi, "CSI in the cloud: how cloud data is accelerating forensic investigations," Information Age, May 12, 2015, *available at* https://www.information-age.com/csi-cloud-how-cloud-data-accelerating-forensic-investigations-123459485/.

[166] Cellebrite, 2020 Digital Intelligence Industry Benchmark Report: The top trends redefining Law Enforcement, *available at* https://www.cellebrite.com/en/insights/industry-report/.

The National Institute of Standards and Technology's Guidelines on Mobile Device Forensics advises law enforcement that "[r]etrieval and analysis of cloud based data should follow agency specific guidelines on cloud forensics."[167] But our research did not find any local agency policy that provided guidance on or control over cloud data extraction.

Rare Public Oversight

The adoption of mobile device forensic tools is almost always a secretive, obscured process.[168] Community engagement on the tools, like other surveillance technologies, is the very rare exception — and in some cases, dissenting voices are deliberately excluded from public discussion.[169] Where it does occur, it is substantially hindered by law enforcement secrecy. Even where existing governance structures ought to facilitate public debate regarding law enforcement use of these tools, these processes are skewed towards law enforcement.

[167] Rick Ayers, Sam Brothers, Wayne Jansen, *Guidelines on Mobile Device Forensics*, NIST Special Publication 800-101, Revision 1, National Institute of Standards and Technology, May 2014, 47, *available at* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf.

[168] To find evidence of community engagement and debate, we searched for news articles, opinion pieces, and editorials featured in local newspapers, and trawled through agendas of city councils and county commissions. For the most part, we were unable to locate much news coverage. To the extent we could find coverage, most local reporting we could identify simply reported the fact that a local law enforcement agency had already acquired a new mobile device forensic tool. Headlines like "Police can now access your iPhone without your help," "Local law enforcement using mysterious new tool to unlock cellphones," and "Charlottesville police buy equipment to crack locked iPhones" were common. Most news articles that address concerns with the technology only do so when reporting on objections raised by a third-party, like an ACLU lawsuit, or when journalists are prevented from accessing information. For example, in San Diego, NBC 7 recently published a story with the headline "Spy Games? Civil Rights Advocate Calls out San Diego PD's Covert Use of iPhone Spyware." See Brooks Jarosz, "Police can now access your iPhone without your help," KTVU Fox 2, July 19, 2018, *available at* https://www.ktvu.com/news/police-can-now-access-your-iphone-without-your-help; Jim Otte, "Local law enforcement using mysterious new tool to unlock cellphones," WHIO TV 7, November 22, 2018, *available at* https://www.whio.com/news/local/local-law-enforcement-using-mysterious-new-tool-unlock-cell-phones/W9zAfzQXrFsJmOJjO04TJK/; Bryan McKenzie, "City police purchase equipment to crack locked iPhones," The Daily Progress, November 2, 2018, *available at* https://www.dailyprogress.com/news/local/city-police-purchase-equipment-to-crack-locked-iphones/article_1299d766-df01-11e8-bb6e-8fafe6b93387.html; Ryan Poe, "The 901: This is why people don't trust Memphis police," Memphis Commercial Appeal, January 22, 2020, *available at* https://www.commercialappeal.com/story/news/local/the-901/2020/01/22/memphis-police-use-cellebrite-tool-but-wont-answer-questions-901/4533550002/; Dorian Hargorve, Mari Payton, Tom Jones, "Spy Games? Civil Rights Advocate Calls out San Diego PD's Covert Use of iPhone Spyware," NBC 7, August 18, 2020, *available at* https://www.nbcsandiego.com/news/investigations/spy-games-civil-rights-advocate-calls-out-san-diego-police-departments-covert-use-of-iphone-spyware/2387761/. Similarly, most of what we could identify from city councils and county commissioners or board or county supervisors resembled pro forma approval of budgets and resolutions that included mobile device forensic tools.

[169] David Thomas, "City Council considers use of 'Textalyzer' technology," *Chicago Daily Law Bulletin*, January 12, 2018, https://www.chicagolawbulletin.com/archives/2018/01/12/city-council-reviews-textalyzer-tech-1-12-18.

There were a few notable exceptions, but public debate rarely translated into limits on law enforcement use of these tools. For example, the city council of Rochester, New York recently debated an ordinance to allow the Rochester Police Department to purchase a GrayKey.[170] During the city council meeting, the Chief of the Rochester Police Department claimed that the GrayKey would only be "used for solving the most violent crimes we have in Rochester, such as homicide or serious assaults." In response, one council member asked what the mechanism would be "to ensure that this [technology] is not used for things like a low-level drug offense?" The police chief indicated that "it has to be a certain level of criteria for a judge [to sign off] . . . so it can never be used for a traffic stop, for a marijuana violation." This claim is, at best, misleading.[171]

Every person who submitted comments to the city council urged the city council to vote no on the Rochester Police Department's request to purchase GrayKey. One person told the city council that "with the increasing concentration of highly personal information in electronic devices, information not historically available in any form under any type of seizure, tools like GrayKey constitute an unacceptable threat to Fourth Amendment protections."[172] Another person said that the tool should not be purchased "without explicit policies concerning its implementation, that would include the means to restrict which information is stored, shared, or which information is accessed." Yet another noted that "devices like this set a precedent for surveillance that more than often directly impacts marginalized communities, specifically black and brown communities." Ultimately, the city council voted unanimously to authorize the Rochester Police Department to purchase a GrayKey.[173]

Limited community engagement occurred in a handful of other jurisdictions. For example, Davis (CA) and Santa Clara County (CA) both enacted surveillance ordinances that are designed to "ensure residents, through local city councils are empowered to decide if and how surveillance technologies are used."[174] In both Davis and Santa Clara County, law enforcement had acquired

[170] Rochester City Council Meeting, May 12, 2020, *available at* https://www.youtube.com/watch?v=xvLGo4XAI_E.

[171] True, a judge must find probable cause exists to authorize a search warrant. Perhaps this is what the chief meant by "a certain level of criteria for a judge [to sign off]." But no law or policy restrictions prohibit a judge from issuing a search warrant to search a phone as a result of a traffic stop or marijuana violation.

[172] Rochester City Council Meeting, Public Comment, https://www.youtube.com/watch?v=LJDHh2GARio.

[173] City of Rochester, Ordinance No. 2020-146, May 13, 2020, *available at* https://www.cityofrochester.gov/WorkArea/DownloadAsset.aspx?id=21474844360; Gino Fanelli, "City Council greenlights GrayKey iPhone hacking tool for police," Rochester City Newspaper, May 12, 2020, *available at* https://www.rochestercitynewspaper.com/rochester/city-council-greenlights-graykey-iphone-hacking-tool-for-police/Content?oid=11779733.

[174] These ordinances are part of a broader Community Control Over Police Surveillance (CCOPS) effort, which usually requires law enforcement to develop a surveillance technology use policy and a surveillance impact report before they can acquire new surveillance technology. *See* ACLU, "Community Control Over Police Surveillance," https://www.aclu.org/issues/privacy-technology/surveillance-technologies/community-control-over-police-surveillance.

MDFTs before the surveillance ordinances took effect. Nevertheless, the city council and county board of supervisors, respectively, still had to approve surveillance use policies for the tools. In Davis, community members voiced opposition to the use of MDFTs.[175] During an October 2018 public hearing, one commenter noted that "I can only see [this technology] being used to harm marginalized people and to harm people that are fighting [law enforcement] abuse."[176] Others noted the importance of making statistics on police use of technologies like MDFTs publicly available. Throughout the MDFT surveillance use policy approval process in Santa Clara, there was only one public comment. In both instances, the surveillance use policies were unanimously approved.

Our review of the processes in Davis and Santa Clara indicate that while surveillance ordinances could theoretically play an important role in governing surveillance technologies like MDFTs, their impact has limitations in practice. One reason is that, despite a dedicated process for community oversight, law enforcement agencies were still not forthright with information. For example, the Santa Clara County District Attorney withheld the make and model of its MDFTs from its surveillance use policy to "promote officer safety and maximize the benefits to be derived from the use of data extraction/examination forensic tools and software."[177] Similarly, the Davis Police Department's annual surveillance report on its use of Cellebrite UFED provides little helpful information. The report mentions that the tool was "used to serve criminal search warrants on 33 devices for 13 felony investigations,"[178] but provides no more detail. Further, in response to a standard request for "information, including crime statistics, that help the City Council assess whether the surveillance technology has been effective at achieving its identified purposes," the Davis PD merely responded that "use of the device is still the most effective way to access electronic information on a cellphone."[179]

[175] City of Davis, City Council Meeting, Item 4.M, July 10, 2018 https://davis.granicus.com/player/clip/868?view_id=6.

[176] *Id*.

[177] County of Santa Clara, Office of the District Attorney Surveillance Use Policy, "Data Extraction/Examination Forensic Tools and Software," November 2018, at 1, FN 1, *available at* http://sccgov.iqm2.com/Citizens/FileOpen.aspx?-Type=4&ID=180351&MeetingID=9769.

[178] City of Davis, California, Memo to City Council, Surveillance Technology – 2019 Annual Surveillance Report, Cellebrite Universal Forensic Extraction Device, June 18, 2019, at 2, http://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/20190618/08D-Surveillance-Tech-PD-Cellebrite.pdf.

[179] *Id*., 8.

6. Policy Recommendations

We envision a society where systems of policing and incarceration are obsolete.[180] We therefore reject the necessity of both law enforcement and their investigatory tools. Based on our research, we believe that MDFTs are simply too powerful in the hands of law enforcement and should not be used.

Below, we offer a set of recommendations that we believe can bring us closer to this vision.[181] Recognizing that MDFTs are already in widespread use across the country, we offer a set of preliminary recommendations that we believe can, in the short-term, help reduce the use of MDFTs. At the margin, further increases in the already formidable tools and data available to law enforcement stand to amplify mass incarceration and worsen racial and other disparities. Therefore, we recommend policy steps that would reduce the tools and data available to law enforcement.

As we considered potential recommendations, we weighed whether or not each would likely reduce the scale of policing, whether it would reduce the tools and data available to law enforcement, and whether it would help challenge narratives that assume law enforcement will increase public safety.[182] We believe that the recommendations we make can limit the power of

[180] Mariame Kaba, "Yes, We Mean Literally Abolish the Police," New York Times, June 12, 2020, *available at* https://www.nytimes.com/2020/06/12/opinion/sunday/floyd-abolish-defund-police.html.

[181] There were a number of recommendations we considered that we ultimately did not include because they did not fit within this framework: 1) *Implementing an offense-based restriction to the use of MDFTs to the most serious cases of harm*. This recommendation could significantly limit the number of cases where MDFTs are used. However, offense-based restrictions on surveillance technology have proven to be porous over time. Consider the Wiretap Act. In 1968, "twenty-four categories of offenses listed in Title III had a clear relationship to national security or organized crime." Since Title III's passage, "Congress has amended 18 U.S.C. §2516—the section of Title III that enumerates wiretap-worthy offenses—thirty-one times." Where gambling offenses made up the predominate number of wiretaps in the 1970s, drug-related offenses have taken over, " making up roughly 50 to 80 percent of intercept orders and applications from 1987 to the present." See Jennifer S. Granick et al., *Mission Creep and Wiretap Act 'Super Warrants': A Cautionary Tale*, 52 Loy. L.A. L. Rev. 431, 446-447 (2019). Moreover, offense-based restrictions implicitly concede that there are a category of certain offenses that justify the role of the police and their investigatory powers which we do not support. 2) *Reciprocal funding for public defenders to have mobile device forensic tools from existing grants*. Although this could benefit low-income defendants, and although public defenders are severely under-resourced, this kind of recommendation would further legitimize the use of these tools and overall increase their prevalence. We also believe that such a recommendation could have the perverse effect of starting an "arms race" in attempts to purchase these tools. 3) *Law enforcement agencies should adopt robust internal use policies*. We do not believe that law enforcement can or should be responsible for enforcing their own accountability or transparency.

[182] We ask these questions based on the work of Critical Resistance. See Critical Resistance, "Reformist reforms vs. abolitionist steps in policing," http://criticalresistance.org/abolish-policing/.

the police, while not further entrenching the practices that remain. We also recognize that these recommendations are only the first steps in a broader strategy to minimize the scope of policing and reduce the options that police have to bring people into the criminal legal system.

Ban the Use of Consent Searches of Mobile Devices

Police consent searches in any context are troubling, but the power and information asymmetries of cellphone consent searches are egregious and unfixable. Accordingly, policymakers should ban the use of consent searches of cellphones. There are at least three reasons why.

The first reason is that the doctrine underlying "consent searches" is essentially a legal fiction.[183] Courts pretend that "consent searches" are voluntary, when they are effectively coerced. While the Supreme Court has held that the legality of a consent search depends on whether a "reasonable person would understand that he or she is free to refuse,"[184] the so-called "reasonable person" standard fails to account for the important racial differences in how individuals interact with law enforcement.[185] As one scholar noted, "many African Americans, and undoubtedly other people of color, know that refusing to accede to the authority of the police, and even seemingly polite requests—can have deadly consequences."[186] While the Supreme Court has held that consent cannot be "coerced, by explicit or implicit means,"[187] the notion that someone can actually feel free to walk away from an interaction with police has an "air of unreality" about it.[188] Given the extreme power asymmetries, it's a "simple truism that many people, if not most, will always feel coerced by police 'requests' to search."[189]

[183] Ric Simmons, *Not "Voluntary" but Still Reasonable: A New Paradigm for Understanding the Consent Searches Doctrine*, 80 Ind. L. J. 773, 775 (2005) ("Over 90% of warrantless police searches are accomplished through the use of the consent exception to the Fourth Amendment.")

[184] United States v. Drayton, 536 U.S. 194, 197 (2002).

[185] Tracey Maclin, *"Black and Blue Encounters" Some Preliminary Thoughts About Fourth Amendment Seizures: Should Race Matter?*, 26 Val. U. L. Rev. 243, 248 (1991). ("Instead of acknowledging the reality that exists on the street, the Court hides behind a legal fiction. The Court constructs Fourth Amendment principles assuming that there is an average, hypothetical person who interacts with the police officers. This notion . . . ignores the real world that police officers and black men live in.")

[186] Marcy Strauss, Reconstructing Consent, 92 J. Crim. L. & Criminology 211, 242-243 (2001). ("Given this sad history, it can be presumed that at least for some persons of color, any police request for consent to search will be viewed as an unequivocal demand to search that is disobeyed or challenged only at significant risk of bodily harm.") Indeed, as another scholar argued, the "consent search doctrine is the handmaiden of racial profiling." *See* George C. Thomas III, *Terrorism, Race and a New Approach to Consent Searches*, 73 Miss L. J. 525, 542 (2003).

[187] Schneckloth v. Bustamonte, 412 U.S. 218, 228 (1973).

[188] United States v. Drayton, 536 U.S. 194, 208 (2002)(Souter, J., dissenting).

[189] Marcy Strauss, *Reconstructing Consent*, 92 J.Crim. L. & Criminology 211, 221.(2001.)

A recent study designed "specifically to examine the psychology of consent searches" highlights the problems in relying on a so-called "reasonable person" to adjudicate consent searches.[190] Participants were brought into a lab and presented with "a highly invasive request: to allow an experimenter unsupervised access to their unlocked smartphone."[191] More than 97% of participants handed over their phone to be searched when requested to, even though only 14.1% of a separate group of observers said that a reasonable person would hand over their phone. The study reveals that there is a "systematic bias whereby *neutral third parties view consent as more voluntary, and refusal easier, than actors experience it to be*."[192] While there are plausible arguments that the lab-setting studies overestimate compliance rates in police searches, there are stronger arguments that they actually underestimate them.[193]

Second, someone consenting to a search of their phone likely doesn't even have a rough idea of what's really about to happen to their phone. The Fifth Circuit Court of Appeals recently held that a reasonable owner of a cellphone would functionally understand that a "complete" cellphone search "refers not just to a physical examination of the phone, but further contemplates an inspection of the phone's 'complete' content."[194] But, given the lack of public discussion of MDFTs, many people would likely be surprised by the power of the tools that law enforcement use to extract and analyze data from a phone. Further, most of the consent to search forms we obtained from law enforcement agencies don't clearly specify how they will search the phone, the tools they'll use, or the extent of the search.[195]

[190] Roseanna Sommers, Vanessa K. Bohns, *The Voluntariness of Voluntary Consent: Consent Searches and the Psychology of Compliance,* 128 Yale L. J. (2019).

[191] *Id*., 1980.

[192] *Id*., 2019.

[193] *Id*., 2007. ("First, police officers convey more authority than our experimenters likely did; our experimenters were college-aged peers dressed in street clothes, whereas police officers are government agents who wear badges and carry weap-ons. Second, in the policing context, citizens might feel that they are admitting guilt or acting suspiciously if they refuse a police officer's request. It is not clear that our participants would have felt it was self-incriminating to refuse the experimenter's request. Third, to the extent our participants were aware of the pol-icies regulating university research, they would have known that their participa-tion was completely voluntary and that they were free to quit at any time. Most people stopped by the police, by contrast, do not believe they can just walk away.")

[194] United States of America v. Cristofer Jose Gallegos-Espinal, (No. 19-20427) (5th. Cir. 2020), at 10.

[195] The Denver Police Department's consent form mentions that devices may be submitted "to the computer forensic laboratory for copying and examination." *See* https://beta.documentcloud.org/documents/20390003-consent-for-search-of-cell-phone-tablet. The Tampa Police Department's mentions that "this search may require the temporary utilization of software and/or hardware." *See* https://beta.documentcloud.org/documents/20393153-tpd-form-142-e-consent-to-search-electronic-media-devices-english. The Colorado State Patrol's consent form mentions that they can "submit the electronic device described below to a computer/electronic forensic examiner . . . who has specialized training necessary to conduct such an examination." *See* https://beta.documentcloud.org/documents/20391059-csp-343-consent-to-search-electronic-device. The Illinois State Police's consent to search form mentions that their search "may include the duplication/imaging and complete forensic analysis of any data contained within the internal, external, andlor removable storage media of this device." *See* https://beta.documentcloud.org/documents/20391550-img_0001.

Finally, law enforcement can do almost anything with data extracted from a cellphone after someone consents. At least one case appears to suggest that, so long as a consent form is written broadly enough, there's no limit on when law enforcement could re-examine a cellphone extraction.[196] The consent form at issue in that case and the consent forms we obtained are strikingly similar. One form from the Indianapolis Metropolitan Police Department says that "said search may take an extended period of time, however this time normally does not exceed sixty (60) days from the time of consent." The U.S. Border Patrol claims they can store data extracted from phones searched at the border for 75 years.[197]

Banning consent searches is not a new suggestion.[198] Nor is it a perfect solution, as it's easy for law enforcement to obtain a search warrant. But banning consent searches of cellphones can help limit police discretion, limit the coercive power of police, and minimize the amount of information that can be collected from people under investigation. State and local policymakers should ban consent searches of cellphones.

Abolish the Plain View Exception for Digital Searches

The plain view exception for digital searches should be eliminated. In a digital search, forensic analysis software can far too easily expose data unrelated to the immediate search, unrestricted by where the data physically resides on the phone. The idea that digital evidence can exist "in plain view" in the way that physical evidence can, when considering how software can display and sort over-seized data, is incoherent.

For physical searches, the plain view exception to the warrant standard allows law enforcement to seize evidence in plain view of any place they are lawfully permitted to be, if the incriminating character of the evidence is immediately apparent.[199] For example, if law enforcement were lawfully searching a house for stolen credit cards, but came across cocaine on the kitchen

[196] United States of America v. Cristofer Jose Gallegos-Espinal, (No. 19-20427) (5th. Cir. 2020).

[197] Department of Homeland Security, Privacy Impact Assessment, U.S. Border Patrol Digital Forensics Programs, DHS Reference No. DHS/CBP/PIA-053(a), July 30, 2020.

[198] For example, the New Jersey Supreme Court outlawed consent searches during traffic stops where no reasonable suspicion exists. The California Highway Patrol banned its use of consent searches as part of a broader class action lawsuit brought because of racial profiling. And in Rhode Island, by law, "[n]o operator or owner-passenger of a motor vehicle shall be requested to consent to a search by a law enforcement officer of his or her motor vehicle, that is stopped solely for a traffic violation, unless there exists reasonable suspicion or probable cause of criminal activity."

[199] Horton v. California, 496 U.S. 128, 130 (1990).

counter, the plain view exception would allow law enforcement to seize the drugs.[200] In other words, if law enforcement are authorized to search for one thing, but come across another thing that's clearly incriminating, the plain view exception allows them to seize that thing.

This exception may have made sense in the physical world, but it collapses in the digital world. When law enforcement extract all of the data from a cellphone, and then perform a search across all of that data, everything comes into "plain view." Traditionally, the plain view exception is limited by a range of physical factors, such as the size and opacity of closed containers. Only so much can become visible, lawfully, during a search of a physical environment, like the home.

Each of these limitations is upset by the digital environment. In digital searches, "[n]early everything can come into plain view and be subject to use in unrelated cases. The result seems perilously like the regime of general warrants that the Fourth Amendment was enacted to stop."[201] Because forensic software continues to provide law enforcement with ever more powerful search capabilities, the notion of data being "in plain view" is without limit.[202] A search for one kind of digital evidence will almost inevitably reveal troves of other digital evidence.[203] Searching for certain data or keywords, organizing data chronologically, or clicking on different types of extracted data fundamentally changes what's in "plain view" for the investigator.

The Supreme Court has held that the plain view exception "may not be used to extend a general exploratory search from one object to another until something incriminating at last emerges."[204] The trouble is, "[c]urrent law allows computer searches for evidence to look disturbingly like searches for all evidence."[205]

[200] Emily Berman, *Digital Searches, The Fourth Amendment, and the Magistrates' Revolt*, 68 Emory L. J. 49, 59 (2018). ("According to this doctrine, if the police have a warrant to search a home for firearms used in a robbery and see drugs sitting on a table upon entering the house, for example, those drugs may be seized as well. Imagine that officers seeking evidence of tax fraud come across email messages indicating that the suspect has enlisted a hitman to kill someone. Absent explicit restrictions, the suspect may now be charged not only with tax fraud, but also with attempted murder and solicitation. And while that example may not garner much sympathy for the suspect, who was,after all, soliciting murder, it represents a government intrusion into a private realm for which there was no probable cause and no warrant.")

[201] Orin Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 Tex. Tech L. Rev. 1 (2015) (symposium keynote), 11.

[202] Most software allows the user to sort by file type — for example, showing all images files in one group, regardless of where they were on the phone. Thus, even though files retain information on their location within the phone, they are not bound by this location when being searched for.

[203] Orin S. Kerr, S*earches and Seizures in a Digital World*, 119 Harv. L. Rev. 531 (2005).

[204] Coolidge v. New Hampshire, 406 U.S. 443, 466 (1971).

[205] Orin Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 Tex. Tech L. Rev. 1 (2015) (symposium keynote), 10-11

As it stands today, the basic equation for digital searches of cellphones is this: technologies like MDFTs empower law enforcement to seize everything and see everything, and the plain view exception effectively allows law enforcement to do anything during those searches. The result: protections guaranteed by the Fourth Amendment are made meaningless. The response from courts across the United States has been tepid, at best. Intervention is necessary.

It's worth considering the counterarguments. One frequent argument in support of the plain view exception for digital searches is that investigators cannot be restricted in their search because potential suspects can and will conceal evidence within a computer's storage.[206] As the argument goes, suspects may obfuscate the location of information by storing data in unanticipated places, with random file names and paths to mislead an investigator. As a result, digital evidence can exist anywhere on a device and investigators need the legal tools to find it.

While someone can fairly easily change where data is stored on a computer, it's significantly more difficult — and in many instances, technically impossible[207] — on cellphones. A cellphone's user interface is significantly more limiting than a desktop computer's, often restricting the ways that users can manipulate files. On a desktop, it's easy to move files around, change file names, or save files into folders or subfolders. Such capabilities are far more limited on a mobile device. Nevertheless, MDFTs allow police to search all of the data on the phone, as if most users have the technical expertise to hide data in arbitrary locations on their phone. With cellphones in particular, the argument that evidence could be hidden anywhere rings hollow.

Abolition of the plain view exception could take several forms. Congress could pass a law to bar the plain view exception for digital searches by amending Rule 41 of the Federal Rules of Criminal Procedure. State legislatures in states that have criminal procedure rules could take similar action. And judges could require, as a condition of issuing a search warrant, that law enforcement agents forswear reliance upon the plain view exception.

The Supreme Court has held that "a cellphone search would typically expose to the government far *more* than the most exhaustive search of a house."[208] As a result, it's time to address the existing loopholes in Fourth Amendment doctrine.

[206] Department of Justice, Computer Crimes and Intellectual Property Section, Criminal Division, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations Manual*, ("[c]riminals can mislabel or hide files and directories . . . attempt to delete files to evade detection, or take other steps designed to frustrate law enforcement searches for information. These steps may require agents and law enforcement or other analysts with appropriate expertise to conduct more extensive searches . . . or peruse every file briefly to determine whether it falls within the scope of the warrant.")

[207] iOS — Apple's mobile operating system for iPhones — does not allow a user to do any of this.

[208] Riley v. California, 573 U.S. 373, 396 (2014).

Require Easy-to-Understand Audit Logs

State and local policymakers should require that mobile device forensic tools used by law enforcement have clear recordkeeping functions, specifically, detailed audit logs and automatic screen recording. This would incentivize MDFT vendors to build this functionality. With such logs, judges and others could better understand the precise steps that law enforcement took when extracting and examining a phone, and public defenders would be better equipped to challenge those steps. Audit logs and screen recordings[209] would document a chronological record of all interactions that law enforcement had with the software, such as how they browsed through the data, any search queries they used, and what data they could have seen.[210]

There is an extreme power and resource imbalance between public defenders and law enforcement.[211] This disparity is only exacerbated by defenders' technological and resource disadvantage: Few public defenders have access to MDFTs. Instead, defenders are often forced to examine forensic reports that are thousands of pages long and "easily navigable only if you have a forensic company's proprietary software."[212] Further, defenders and judges often have no way of knowing whether law enforcement actually stayed within the bounds of a search warrant for a phone. For courts, simply taking law enforcement's word for it should be insufficient — lying under oath is endemic to the institution of American policing.[213] Audit logs would be especially helpful for defenders trying to suppress evidence that was obtained in a prohibited manner.

[209] One potential issue with screen recording is the presence of CSAM or other sensitive material.

[210] In order to function, software responds to specific events that the user triggers. This means that user activity can be logged at the point of it activating a response from the program.

[211] Research has demonstrated that fewer than 30 percent of county-based and 21 percent of state-based public defender offices have enough attorneys to adequately handle their caseloads. *See* Bureau of Justice Statistics, Lynn Langton and Donald Farole Jr., *County Based and Local Public Defender Offices, 2007* (2010), 8, https://www.bjs.gov/content/pub/pdf/clpdo07.pdf; Bureau of Justice Statistics, Lynn Langton and Donald Farole Jr., *State Public Defender Programs, 2007* (2010), 12, www.bjs.gov/content/pub/pdf/spdp07.pdf. *Also see* Justice Policy Institute, *System Overload: The costs of Under-Resourcing Public Defense, 2011*, available at http://www.justicepolicy.org/uploads/justicepolicy/documents/system_overload_final.pdf; American Bar Association, *Gideon's Broken Promise: America's Continuing Quest for Equal Justice* (2004); Bryan Furst, *A Fair Fight: Achieving Indigent Defense Resource Parity*, Brennan Center, September 9, 2019, *available at* https://www.brennancenter.org/sites/default/files/2019-09/Report_A%20Fair%20Fight.pdf.

[212] Kashmir Hill, "Imagine Being on Trial. With Exonerating Evidence Trapped on Your Phone." New York Times, November 22, 2019, *available at* https://www.nytimes.com/2019/11/22/business/law-enforcement-public-defender-technology-gap.html.

[213] *See*, e.g., Irving Younger, "The Perjury Routine," The Nation, May 8, 1967; Myron R. Orfield, *The Exclusionary Rule and Deterrence: An Empirical Study of Chicago Narcotics Officers*, 54 Chi. L. Rev. 1016 (1987); Commission to Investigate Allegations of Police Corruption and the Anti-Corruption Procedures of the Police Department, City of New York, Commission Report (1994) at 38; Stanley Fisher, *"Just the Facts, Ma'am": Lying and the Omission of Exculpatory Evidence in Police Reports*, 28 N. Eng. L. Rev. (1993); Joseph Goldstein, "'Testilying' by Police: A Stubborn Problem," The New York Times, March 18, 2018, *available at* https://www.nytimes.com/2018/03/18/nyregion/testilying-police-perjury-new-york.html; Peter Keane, "Why cops lie," San Francisco Chronicle, March 15, 2011; Michael Oliver Foley, *Police Perjury: A Factorial Survey*, (2000); Samuel Gross, et al., *Government Misconduct and Convicting the Innocent: The Role of Prosecutors, Police and Other Law Enforcement*, National Registry of Exoneration, September 1, 2020, *available at* https://www.law.umich.edu/special/exoneration/Documents/Government_Misconduct_and_Convicting_the_Innocent.pdf.

This recommendation even comports with principles articulated by law enforcement associations, like the Association of Chief Police Officers, which has said that "[a]n audit trail . . . of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result."[214]

Critically, audit logging is unlikely to be an effective tool for broad transparency and police accountability.[215] This tool will not improve police behavior. But on a case-by-case basis, this tool could give public defenders and judges a significantly clearer window into the nature and extent of cellphone searches.

Enact Robust Data Deletion and Sealing Requirements

State and local lawmakers should require law enforcement to delete any extracted cellphone data that is not related to the objective of the warrant within thirty days from the date the information is obtained.[216] In addition, for cases that result in a conviction, data that was deemed relevant should be sealed at the conclusion of the case. For other cases, where charges are dismissed or do not result in conviction, all data should be deleted, relevant or not. Data deemed relevant in one case should never be used for general intelligence purposes or used in unrelated cases.

As we explained in Section 5, in the absence of clear law or policy, law enforcement could use personal information like contact lists, photos, and location data to fuel police surveillance systems. This is true not only of the data of the person whose phone was searched, but also that of anyone they have been in contact with using their phone. Cellphone searches are unlike traditional seizures because law enforcement extracts all of the data on the device and subsequently searches 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.

[214] Association of Chief Police Officers, *APCO Good Practice Guide for Computer based Electronic Evidence*, March 2012, available at https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf. *Also see*: Rick Ayers, Sam Brothers, Wayne Jansen, *Guidelines on Mobile Device Forensics*, NIST Special Publication 800-101, Revision 1, National Institute of Standards and Technology, May 2014, *available at* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf. (noting that "[p]roper documentation is essential in providing individuals the ability to re-create the process from beginning to end."); Scientific Working Group on Digital Evidence, SWGDE Best Practices for Mobile Phone Forensics, Feb. 11, 2013, *available at* https://drive.google.com/open?id=18dwENQNzt-bEa0G9GLSUeDxZxeDEeUc-3 (noting that documentation should include "sufficient detail to enable another examiner, competent in the same area of expertise, to repeat the findings independently.").

[215] Based on lessons from body-worn cameras, there is little reason to believe that simply being recorded will alter the behavior of an investigator who can justify their actions after the fact. We are more concerned with defenders having the ability to successfully suppress evidence and to not be at a disadvantage in getting exonerating evidence.

[216] The only exception should be for exculpatory information.

Policies requiring this kind of data deletion or sealing already exist in New Mexico, Utah, and California.[217] Additionally, New York requires all arrest records for any person not convicted of a crime to be sealed.[218]

There is clear potential for abuse of this kind of policy if law enforcement unilaterally determines the relevancy of data to the warrant. Such abuse can partially be mitigated by requiring clear defense access to the extracted data so they can challenge law enforcement's inclusion or exclusion of information. Audit logs would also help.

Clear retention requirements could not only help hold law enforcement accountable to the scope of the warrant, but could also significantly limit the data that law enforcement could include in internal systems like intelligence databases, "gang databases," and predictive policing tools.[219]

Require Clear Public Logging of Law Enforcement Use

State and local policymakers should require public reporting and logging for how law enforcement use mobile device forensic tools. These records should be released at least monthly, as this would allow more immediate access to information by advocates, policymakers, and the public seeking to understand the capabilities of their police agency. Agencies should additionally release annual reports on overall department usage.

[217] New Mexico's Electronic Communications Privacy Act, Section 3.D.2 ("except when the information obtained is exculpatory with respect to the natural person targeted,require that any information obtained through the execution of the warrant that is unrelated to the objective of the warrant be destroyed within thirty days after the information is seized and be not subject to further review, use or disclosure.") *See* https://nmlegis.gov/Sessions/19%20Regular/final/SB0199.pdf; Utah's Electronic Information or Data Privacy Act, Section 1.B, 1.D ("electronic information or data [that is not the subject of the warrant] shall be destroyed in an unrecoverable manner by the law enforcement agency as soon as reasonably possible after the electronic information or data is collected.") *See* https://le.utah.gov/~2019/bills/static/HB0057.html; California's Electronic Communications Privacy Act, 1546.1(d)(2) ("The warrant shall require that any information obtained through the execution of the warrant that is unrelated to the objective of the warrant shall be sealed and not subject to further review, use, or disclosure without a court order."); 1546.1(e)(2) ("When issuing any warrant or order for electronic information, or upon the petition from the target or recipient of the warrant or order, a court may, at its discretion, do any or all of the following: . . . Require that any information obtained through the execution of the warrant or order that is unrelated to the objective of the warrant be destroyed as soon as feasible after the termination of the current investigation and any related investigations or proceedings.). *See* https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201520160SB178.

[218] *See* https://codes.findlaw.com/ny/criminal-procedure-law/cpl-sect-160-50.html.

[219] Rashida Richardson, Amba Kak, "It's Time for a Reckoning About This Foundational Piece of Police Technology," Slate, September 11, 2020, *available at* https://slate.com/technology/2020/09/its-time-for-a-reckoning-about-criminal-intelligence-databases.html.

These records should include aggregate information on how law enforcement is using MDFTs, including:

- How many phones were searched in a given time period.
- Whether those searches were by consent (though consent searches should be banned), or through a warrant.
- Warrant numbers associated with searches, when applicable.
- The type(s) of offenses being investigated.
- How often the tools led to successful data extractions.
- Explanations for any failed extractions.
- Which tools were used for extraction and analysis, and their version numbers.

Understanding how, when, and under what legal authority law enforcement use these powerful technologies can increase transparency and accountability.[220] Beyond mere transparency, these kinds of records are important as they can help advocates, researchers, policymakers, and the public effectively pursue policies that reduce the power and scope of law enforcement. More broadly, these kinds of records can help challenge law enforcement's narrative surrounding how, when, and why these tools are used.

While this kind of public reporting can be helpful, it will not inherently lead to a responsible or decreased use of MDFTs by law enforcement. Take wiretapping as an example. Federal law requires an annual reporting of the number of "applications for orders authorizing or approving the interception of wire, oral, or electronic communications."[221] But there is evidence of widespread underreporting of wiretaps.[222] Transparency reports published by wireless service providers like AT&T, Sprint, T-Mobile, and Verizon "state that they implemented three times as many wiretaps as the total number reported by the Administrative Office of the Courts."[223] This casts doubt on whether public reporting of MDFT usage will accurately represent their usage

[220] In fact, in a similar context, wiretapping, the Administrative Office of the United States Courts annually reports the number of federal and state "applications for orders authorizing or approving the interception of wire, oral, or electronic communications," including "the offense specified in the order." *See* 18 U.S.C. 2519(2)-(3).

[221] 18 U.S.C. 2519(1)-(3).

[222] Jennifer S. Granick, Patrick Toomey, Naomi Gilens, Daniel Yadron Jr., *Mission Creep and Wiretap Act 'Super Warrants': A Cautionary Tale*, 52 Loy. L.A. L. Rev. 431, 446. ("Despite the statute's reporting requirements, some scholars have raised concerns that the official number of wiretaps is inaccurately low.")

[223] *Id.*

by law enforcement. Worse, law enforcement could manipulate these records in order to justify increased funding. However, given that MDFT reporting should include warrant numbers and more detailed information than Title III reporting requires, there is less opportunity for the inaccuracies rampant in aggregate reporting.

Ultimately, this information will still be useful even if incomplete. Policymakers and advocates should remain cautious in using the information agencies report, and cross-reference with other sources of information, like warrants, public records, and reports from individuals and public defenders.

7. Conclusion

Our research shows that every American is at risk of having their phone forensically searched by law enforcement. Significantly more local law enforcement agencies have access to this technology than previously understood. These agencies use the tools far more than previously documented, and use them in a broad array of cases. They do so with few policies or legal constraints in place. Given how routine these searches are today, and given racist policing practices, it's more than likely that these technologies disparately affect and are used against communities of color. Put together, this report documents a dangerous expansion in law enforcement's investigatory power.

For too long, public debate and discussion regarding these tools has been abstracted to the rarest and most sensational cases in which law enforcement cannot gain access to cellphone data. We hope that this report will help recenter the conversation regarding law enforcement's use of mobile device forensic tools to the on-the-ground reality of cellphone searches today in the United States.

Acknowledgements

This work would not be possible without the tireless work of our colleagues and partners. We are grateful to them, and we take responsibility for any errors that remain here. Special thanks to Jerome Greco and The Legal Aid Society for allowing us to visit their Digital Forensics Unit, and for providing us with assistance since the beginning of this project. Also special thanks to Cameron Cantrell and Sarika Ram for their research as Summer Fellows at Upturn, and to Ming Hsu for his work on the maps in this report.

For their helpful input and feedback on this report, we'd like to thank several individuals: Khalil A. Cumberbatch, Senior Fellow, The Council on Criminal Justice; Jennifer Granick, Surveillance and Cybersecurity Counsel, ACLU Speech, Privacy, and Technology Project; Jerome Greco, Digital Forensics Supervising Attorney, Digital Forensics Unit/Criminal Defense Practice, The Legal Aid Society; Jennifer Lynch, Surveillance Litigation Director, Electronic Frontier Foundation; Jumana Musa, Fourth Amendment Center Director, National Association of Criminal Defense Lawyers; David Robinson, Visiting Scientist, AI Policy and Practice Initiative, Cornell's College of Computing and Information Science; Hannah Jane Sassaman, Policy Director, Movement Alliance Project; and Vincent Southerland, Executive Director Center on Race, Inequality, and the Law, New York University School of Law. We'd also like to thank Clare Garvie, Senior Associate at the Center on Privacy & Technology at Georgetown Law for early help in structuring our public records request project. All affiliations are for identification purposes only.

For *pro bono* representation of Upturn in our litigation under New York's Freedom of Information Law to compel the NYPD to produce documents related to its use of mobile device forensic tools, we'd also like to thank Albert Fox Cahn, the Executive Director of the Surveillance Technology Oversight Project and Shearman & Sterling, LLP.

Thanks to Objectively for assisting with the design of our report and to Spitfire Strategies for communications and press outreach.

Upturn is supported by the Ford Foundation, the Open Society Foundations, the John D. and Catherine T. MacArthur Foundation, Luminate, the Patrick J. McGovern Foundation, and Democracy Fund.

Appendix A: Methodology

In order to determine how many law enforcement agencies have purchased mobile device forensic tools, we sent more than 110 public records requests to a wide range of law enforcement agencies.

We began our public records survey in February 2019. We sent public records requests to a variety of law enforcement agencies: police departments, sheriff offices, district attorneys' and prosecuting offices, state law enforcement, and forensics labs across the country. We also sent records requests to Departments of Finances and Departments of Procurement, many of which keep records of purchases. We sent records requests to the country's 50 largest local police departments, as well as many of the largest state law enforcement agencies.[224] We also sent requests to smaller law enforcement agencies where previous public reporting indicated the purchase of MDFTs.

Many departments provided us some records in response to our requests — some provided full responses, some provided limited responses. As we expected, some departments denied our requests. For example, both the Baltimore and Cincinnati Police Departments denied our requests based on investigatory methods and technique exemption to public disclosure. Others quoted exorbitant fees to fulfill our records request, which we've declined to pay. For example, the Fairfax County (VA) Police Department quoted us $10,349, the Missouri State Highway Patrol quoted us $1,324, and the Jacksonville Sheriff's Office quoted us more than $700,000 to fulfill our requests. Other agencies simply have not responded in a determinative way.
Beyond public records requests to individual agencies, we supplemented our research in four other ways.

First, we explored existing, publicly available reporting or information, through services like MuckRock or other media reporting.

Second, we explored various open databases from city, county, and state governments, which document spending and vendor payments. Such databases often provide a transparent view into government purchasing as a whole, and contain specific purchasing information on MDFTs. In many instances, these databases helped us determine if a police department had purchased MDFTs, even if the department denied our records request. For example, although the Cincinnati

[224] U.S. Department of Justice, Bureau of Justice Statistics, "Census of State and Local Enforcement AGencies, 2008," July 2011, Appendix Tables 5, 8 *available at* https://www.bjs.gov/content/pub/pdf/csllea08.pdf.

Police Department denied our records request, a publicly available dataset indicates the police department paid more than $100,000 to vendors like Cellebrite, Grayshift, and MSAB. Similarly, although the Detroit Police Department quoted us over $1,000 to fulfill our request, the City of Detroit's Open Data Portal reveals that the Detroit Police Department paid at least $30,000 to Cellebrite.

Third, we searched databases that document federal grantmaking to local law enforcement agencies. Some data on federal grants helped us determine that a law enforcement agency purchasedMDFTs even if the agency denied our records request. For example, although the Bronx District Attorney's Office denied our request, the office is, among other things, funded through the Coverdell Forensics Science Improvement Grant to "to acquire the Cellebrite Advanced Universal Forensic Extraction Device software solution."

Finally, we used GovSpend, which is a database of government contracts and purchase orders. GovSpend aggregates purchase order data from local, state, and federal government agencies, to provide inter-agency transparency on costs. The database is also open to certain non-governmental parties, like news media organizations. We used GovSpend to better understand the scale of MDFT purchases across the country.

In all, we received more than 12,000 pages of documents in response to our records requests.

Appendix B: Public Records Request Template

[Date]
[Agency Address]

Re: [State Records Request Law] Request

To Whom it May Concern:

This is a request under the [State Records Request Law and citation], on behalf of Upturn, a 501(c)(3) nonprofit organization based in Washington D.C. Our mission is to promote equity and justice in the design, governance, and use of digital technology. This request seeks records relating to the [Agency's] use of mobile device forensic technologies, as well as the Department's policies and procedures governing such use.

Background

Due to the ubiquity of mobile devices, law enforcement sees the data stored on mobile devices, like cellphones, as key sources of evidence for investigations. However, mobile devices can contain large amounts of people's sensitive and private information, much of which may be irrelevant to a given investigation. As the Supreme Court recognized five years ago in *Riley v. California*, "[o]ne of the most notable distinguishing features of modern cellphones is their immense storage capacity." As such, forensic searches of mobile devices are often highly invasive, and we believe that such searches by law enforcement are increasingly common.

Mobile device forensic tools (MDFTs) are used by law enforcement to extract data from mobile devices. In some cases, if the data on the mobile device is encrypted, some MDFTs can help law enforcement circumvent a device's security features in order to access otherwise inaccessible data. These capabilities have been the subject of broad public debate, for example, in the aftermath of the high-profile San Bernardino shooting in 2015. Whether or not devices are encrypted, law enforcement's use of MDFTs is an issue of significant public interest.

Currently, there is a considerable lack of public information available regarding how local law enforcement agencies use MDFTs, and the policies and procedures that govern such use. The public is entitled to understand the Department's activities and capabilities with respect to MDFTs, and this request seeks to further the public's understanding.

Public Records Request

Upturn seeks records regarding the Department’s use of **mobile device forensic tools (MDFTs)**. This includes any software, hardware, process, or service that is capable of any of the following:

- extracting any data from a mobile device,
- recovering deleted files from a mobile device, or
- bypassing mobile device passwords, locks, or other security features.

Examples of MDFTs include, but are not limited to, products or services offered by vendors such as Cellebrite, Grayshift, Oxygen Forensics, BlackBag Technologies, Magnet Forensics, MSAB, AccessData, Paraben, Katana Forensics, BK Forensics, and Guidance Software/OpenText.

Upturn specifically requests the following records under the [applicable state law]:

1. Purchase Records and Agreements: Any and all records reflecting an agreement for purchase, acquisition, or license of MDFTs, or permission to use, test, or evaluate MDFTs since 2015.
2. Records of Use: Any and all records describing the Department’s use of MDFTs since 2015.
    a. In particular, we seek records reflecting the department’s aggregate use of MDFTs. For example, monthly reports that reflect the total number of MDFT cases for each month, broken down by type of crime, and number and type of phones, and number and type of other devices.
        i. Please specify any instances where the department used Cellebrite Advanced Services, or otherwise transferred possession of a device or its contents to a vendor for off-site processing, including Regional Computer Forensics Laboratories.
        ii. Please include any instances of forensic examination of a device (e.g. using JTAG or chip-off processes) that may not involve a vendor’s product.
3. Policies Governing Use: Any and all records regarding policies and guidelines governing the use of MDFTs, including but not limited to: training materials regarding their operation, restrictions on when they may be used, limitations on retention and use of collected data, security measures taken to protect stored and in-transit data, guidance on when a warrant or other legal process must be obtained, and guidance on when the existence and use of MDFTs may be revealed to the public, criminal defendants, or judges.

Information About the Request

Upturn appreciates [Agency's] attention to this request. According to [applicable state law], your agency must comply with a request [within X business days / timeframe]. Further, under [applicable state law] we request a fee waiver. As Upturn is a non-profit organization, and disclosure of requested records will promote public awareness and knowledge of governmental action, we are requesting that fees associated with this request be waived. If you determine that a fee waiver is not appropriate in this instance, and if the estimated cost associated with fulfilling this request exceeds $25, please contact me before proceeding to fulfill our request.

Please furnish all applicable records in electronic format to records@upturn.org. For records available only in a physical format, please send such records to:

Upturn
1015 15th St. N.W. Suite 600
Washington, D.C., 20005

Should you have any questions concerning this request, please contact Logan Koepke by telephone at (214) 801-4499 or via e-mail at logan@upturn.org.

Sincerely,

Logan Koepke
Emma Weil

Appendix C: Total Amounts Spent on MDFTs

Law Enforcement Agency	Amount Spent (at least)	Vendors
Anoka County Sheriff	$34,205	AccessData, BlackBag Technologies, Cellebrite, CRU, Guidance Software, Katana Forensics, Magnet Forensics, Micron Consumer Products Group, MSAB, Paraben Corporation
Arizona Department of Public Safety	$110,605	Grayshift, Cellebrite, BlackBag Technologies, Magnet Forensics, Tritech Forensics
Atlanta Police Department	Unknown	Unknown
Austin Police Department	$92,719	AccessData, BlackBag Technologies, Cellebrite, Grayshift, Guidance Software, Magnet Forensics
Baltimore County Police Department	Unknown	Unknown
Bend Police Department	$62,761	Cellebrite
Bernalillo District Attorney	$35,354	Cellebrite
Broward County Sheriff	$563,091	Cellebrite, Grayshift, Oxygen Forensics, Magnet Forensics, MSAB, BlackBag Technologies, AccessData, Katana Forensics, Guidance Software
California DOJ	$225,449	Cellebrite
California Highway Patrol	$25,289	BlackBag Technologies, Cellebrite, MSAB

Law Enforcement Agency	Amount Spent (at least)	Vendors
Charlotte-Mecklenburg Police Department	$181,557	BlackBag Technologies, Cellebrite, Grayshift, MSAB
Chicago Police Department	$31,830	Cellebrite
City of Miami Police Department	$66,558	Cellebrite
Collin County Sheriff	$90,724	Cellebrite, Magnet Forensics
Colorado State Patrol	$56,345	Cellebrite, Federal Law Enforcement Training CT
Columbus Police Department	$114,656	AccessData, Grayshift, Magnet Forensics, Oxygen Forensics, Cellebrite
Cook County District Attorney	$17,495	Cellebrite
Cook County Sheriff's Office	$37,342	Cellebrite
Dallas County District Attorney	$4,902	AccessData, BlackBag Technologies, Cellebrite, Katana Forensics
Dallas Police Department	$482,542	Cellebrite, GTS Technology Solutions, Cellebrite
DC Department of Forensic Sciences	$57,414	Cellebrite, MSAB
DC Metropolitan Police Department	$21,693	Cellebrite
DeKalb Police Department	$4,865	AccessData
Denver Police Department	$51,170	Cellebrite, Cellebrite
El Paso Police Department	Unknown	Unknown

Law Enforcement Agency	Amount Spent (at least)	Vendors
Fairfax County Police Department	Unknown	Unknown
Fort Worth Police Department	$120,921	AccessData, BlackBag Technologies, Cellebrite, Grayshift, MSAB, Oxygen Forensics, Magnet Forensics
Gwinnett County District Attorney	$66,388	H-11 Digital Forensics, Cellebrite, Oxygen Forensics, Magnet Forensics, Susteen, Cleverbridge, Passware
Harris County Sheriff	$176,854	BlackBag Technologies, Cellebrite, Katana Forensics, Magnet Forensics, MSAB
Hennepin County Sheriff	$59,661	Cellebrite, Grayshift
Honolulu Police Department	$60,212	Cellebrite
Houston Police Department	$210,255	AccessData, Cellebrite, Magnet Forensics, MSAB
Illinois State Police	$157,147	Cellebrite, Grayshift, Guidance Software, Magnet Forensics
Indiana State Police	$513,517	BlackBag Technologies, Cellebrite, Magnet Forensics, Grayshift, Katana Forensics, MSAB, OpenText, Oxygen Forensics
Indianapolis Metropolitan Police Department	$153,341	BlackBag Technologies, Cellebrite, Grayshift, Guidance Software, Katana Forensics, Magnet Forensics, MSAB
Iowa Department of Public Safety	$133,324	Cellebrite
Jacksonville County Sheriff	$22,728	Grayshift, Cellebrite

Law Enforcement Agency	Amount Spent (at least)	Vendors
Jefferson Parish Sheriff's Office	Unknown	Unknown
Kansas City Police Department	$81,688	Cellebrite
Las Vegas Metropolitan Police Department	$646,229	AccessData, BlackBag Technologies, Cellebrite, Guidance Software, Katana Forensics, Magnet Forensics, MSAB, EnCase Forensics
Los Angeles District Attorney	$55,795	Cellebrite, Grayshift
Los Angeles Police Department	$358,426	BlackBag Technologies, MSAB, Cellebrite, Guidance Software
Louisville Metro Police Department	$65,692	Cellebrite
Manhattan District Attorney	$638,676	Cellebrite
Massachusetts State Police	Unknown	Unknown
Miami Dade Police Department	$337,072	Cellebrite
Milwaukee Police Department	$7,400	Cellebrite
Modesto Police Department	$147,117	BlackBag Technologies, Grayshift, Cellebrite, AccessData
Nassau Police Department	$64,274	Cellebrite, MSAB, Oxygen Forensics

Law Enforcement Agency	Amount Spent (at least)	Vendors
New York County District Attorney	$495,315	Cellebrite, BlackBag Technologies, Final Data, Forensic Computers Inc, Grayshift, Magnet Forensics, MSAB, EnCase Forensics, AccessData, Teel
New York Police Department	$30,000	Grayshift
North Carolina Department of Public Safety	$122,621	AccessData, Cellebrite, Guidance Software, Katana Forensics, Magnet Forensics, MSAB, OpenText
Ohio State Highway Patrol	$75,088	BlackBag Technologies, Cellebrite, Grayshift, Magnet Forensics
Oklahoma City Police Department	$33,890	Cellebrite, Grayshift, Magnet Forensics, AccessData
Orange County District Attorney	$24,187	Cellebrite, Susteen
Pennsylvania State Police	$540,625	Cellebrite, Magnet Forensics, MSAB, Grayshift, Oxygen Forensics
Pennsylvania State Police	$623,929	Cellebrite, Magnet Forensics, MSAB, Grayshift, Oxygen Forensics
Philadelphia District Attorney	$64,506	AccessData, Cellebrite, Katana Forensics, Magnet Forensics
Phoenix Police Department	$117,460	Cellebrite
Portland Police Bureau	$261,119	AccessData, Cellebrite, Grayshift, Magnet Forensics, MSAB, Oxygen Forensics
Prince George's Police Department	$67,300	Cellebrite
Riverside County Sheriff	$180,535	Cellebrite

Law Enforcement Agency	Amount Spent (at least)	Vendors
Sacramento Police Department	$94,051	Cellebrite, Grayshift, EnCase Forensics
San Bernardino Sheriff	$270,380	BlackBag Technologies, Cellebrite, Guidance Software, Magnet Forensics, MSAB
San Diego District Attorney	$164,499	Cellebrite, Grayshift, Magnet Forensics, MSAB
San Diego Police Department	$232,999	Cellebrite, Grayshift, Magnet Forensics, MSAB, OMC2 LLC/Bantam Tools, Teel
San Francisco Police Department	$40,935	Cellebrite
San Jose Police Department	$296,363	BlackBag Technologies, Cellebrite, Grayshift, Guidance Software, Katana Forensics, Magnet Forensics, MSAB
Santa Clara District Attorney	$233,203	Grayshift, Cellebrite, MSAB, AccessData, Guidance Software
Seattle Police Department	$240,837	Cellebrite, MSAB, Magnet Forensics, Grayshift
Spokane Police Department	$255,369	Cellebrite
St. Joseph County Prosecutor	$14,626	AccessData, Cellebrite, Magnet Forensics
St. Louis Police Department	$26,652	AccessData, BlackBag Technologies, Cellebrite, MSAB, Oxygen Forensics
Suffolk County District Attorney	$31,195	Cellebrite

Law Enforcement Agency	Amount Spent (at least)	Vendors
Suffolk County Police Department	$34,671	BlackBag Technologies, Cellebrite, Grayshift, Guidance Software, Magnet Forensics, OpenText
Tampa Police Department	Unknown	Unknown
Tarrant County District Attorney	$9,986	AccessData, Magnet Forensics
Texas Department of Public Safety	$188,782	BlackBag Technologies, Grayshift, Cellebrite, Magnet Forensics, MSAB, EnCase Forensics, Oxygen Forensics
Travis County District Attorney	$171,980	Cellebrite, Grayshift, MSAB, Guidance Software, OpenText, EnCase Forensics, Teel, Magnet Forensics, BlackBag Technologies
Travis County Sheriff's Office	Unknown	Unknown
Tucson Police Department	$126,958	AccessData, Cellebrite, Grayshift, Magnet Forensics, MSAB, Sanderson Forensics
Tulsa Police Department	Unknown	Cellebrite, Susteen
Washington State Patrol	$52,343	Cellebrite, Magnet Forensics
West Allis Police Department	$10,397	Cellebrite

Upturn
Toward Justice
in Technology

✉ hello@upturn.org

@TeamUpturn

upturn.org