MOBILE DEVICE FORENSIC TOOLS: A HELP OR A HINDRANCE TO CONSTITUTIONAL CELLPHONE SEARCHES?

Taylor Applegate*

U.S. law enforcement agencies are increasingly relying on advanced mobile device forensic tools (MDFTs) when conducting digital searches of cellphones and other devices. MDFTs are powerful tools built and sold by third-party vendors, which allow law enforcement to (a) circumvent security features to access locked cellphones, (b) access data stored on the device, cloud-based backups, and online accounts, and (c) utilize enhanced cellphone data analytics, sorting, and querying capabilities. Although some 2,000 law enforcement agencies in almost every U.S. state are using MDFTs, there is little public transparency into the technology. This is particularly concerning considering police often use MDFTs in consent searches, even if the person subject to the search is unaware that the tool enables police to conduct a full download (“extraction”) of the data on their device for subsequent parsing. Even with a warrant, as the U.S. Supreme Court’s ruling in Riley intended to require absent an exigency, lower courts’ unpredictable application of the plain view doctrine in digital search cases can and indeed has permitted authorities to “rummage” through a mobile device until evidence of some crime is discovered. Even in the rare instances where courts have deemed cellphone warrants illegally overbroad, they have been quick to apply the good faith exception to the exclusionary rule, removing any incentive for police to narrow the scope of future affidavits. The broad, unchecked digital searches enabled by MDFTs are even more concerning today as many states criminalize abortions or restrict access to gender-affirming medical care, among other repressive laws.

This Note analyzes existing case law related to digital searches of hard drives and cellphones, to pinpoint the primary legal and policy problems with MDFT use: a lack of transparency, insufficiently informed consent searches, insufficiently scoped search warrants, and inadequate auditing and record-keeping. Further, this Note discusses an aspect overlooked in the current literature—that MDFTs, if used with the appropriate restrictions in place, could help limit rather than expand the scope of cellphone searches. Machine learning algorithms enable features that

* J.D. Candidate, Stanford Law School, 2024. This Note began as a project for Richard Salgado’s class on Modern Surveillance Law. To him I owe immense gratitude for providing feedback on initial drafts and inspiring me to delve into a fascinating field of law. Thanks also to Riana Pfefferkorn for entertaining countless questions related to this research and other projects, and to the staff of the Stanford Law & Policy Review for their generous feedback and careful editing.
can auto-detect certain images and text, allowing officers to view only material flagged within the scope of their search. Similarly, MDFTs can generate audit reports allowing greater transparency into and repeatability of searches, allowing courts and defense attorneys to verify that a cellphone search stayed within lawful scope. Finally, because using MDFTs in these beneficial ways won’t happen organically, the Note concludes by proposing enforcement of such requirements through a federal statute that would require (1) restricting consent searches, the plain view exception, and types of crimes for which MDFT-enabled searches are allowed; (2) more narrowly scoped search warrants; and (3) record-keeping and reporting requirements to increase transparency and accountability.

INTRODUCTION ........................................................................................................286
I. WHAT ARE MDFTS AND HOW DO THEY WORK?........................................288
   A. MDFTs Can Bypass Security Features to Access Most Devices ........289
   B. MDFTs Provide Access to a “Goldmine” of Data .................................290
   C. MDFTs Streamline Data Processing and Analytics ..........................291
II. MDFTS AND FOURTH AMENDMENT IMPLICATIONS ..................................291
   A. MDFT-Enabled Searches Authorized by Consent Are Often Not Adequately Informed or Voluntary, Considering the Volume and Quality of Data Obtainable via Extraction ........................................292
      1. Cellphones Are Minicomputers, GPS Trackers, Diaries, and More .................................................................293
      2. Suspects’ Consent Is (Often) Not Truly Voluntary .................293
      3. Suspects Are Not Adequately Informed About MDFTs and the Scope of the Search ............................................295
   B. Courts Are Divided on Sufficient Probable Cause and Particularity Standards in MDFT-Enabled Searches, but the Good Faith Exception Almost Always Applies .................................297
   C. Applying the Plain View Doctrine in MDFT-Enabled Cellphone Searches Can Give Law Enforcement Access to an Unreasonable Quantity (and Quality) of Data ........................................299
III. CRITIQUES: CONCERNS ABOUT THE UNCONSTRAINED USE OF MDFTS ........................................................................................................... 303
   A. Widespread Proliferation with Little-to-No Oversight or Transparency Has Precluded Democratic Debate About the Use of and Risks Associated with These Tools ........................................304
   B. MDFTs Undermine Mobile Device Security and the Public’s Reasonable Expectation of Privacy in Their Devices, with Disparate Impacts ......................................................................................... 306
IV. PROONENTS’ POSITIONS: A POWERFUL TOOL, IF WIELDED RESPONSIBLY .......................................................... 307
A. MDFTs Promise to Facilitate More Particularized Phone Searches

B. MDFTs Are a Powerful Enabler for Criminal Investigations and Public Safety Efforts

C. MDFTs Can Record Extraction and Search Steps to Improve Auditing

V. RECOMMENDATIONS

A. Establish Threshold Requirements for MDFT-Enabled Cellphone Searches: Limiting Consent Searches, Plain View Doctrine, and Use in Minor Offenses

B. Ex Ante Restrictions: Scoping Search Warrants

C. Improving Transparency and Accountability: Reporting and Recording Requirements

CONCLUSION

INTRODUCTION

On a balmy December day in 2015, a couple armed with .223-caliber assault rifles and semiautomatic handguns terrorized a social services center in San Bernardino, California.1 They killed fourteen people and wounded twenty-one more in an attack that shook the nation.2 As authorities began searching for clues into the couple’s motives, focus soon shifted to a major hurdle in the investigation—the FBI’s inability to unlock one of the suspect’s iPhones.3 When the FBI sought Apple’s assistance unlocking the device, the company refused, arguing that creating a “backdoor” for the government would pose a serious vulnerability to every iPhone in the world.4 The decryption debate led to a showdown in court. But on the eve of the hearing to determine whether Apple would be forced to comply,5 the FBI quietly dropped the case, claiming an

3. Although the shooters had destroyed their personal phones and hard drives, police recovered Mr. Farook’s work iPhone 5 intact. The phone was locked with a four-digit pin and was set to wipe all its data after ten failed passcode attempts. Referred to as “bricking,” this is a common security feature for modern smartphones that prevents authorities from using “brute force” to unlock the phone by guessing passcode combinations. Ellen Nakashima, Apple Vows to Resist FBI Demand to Crack iPhone Linked to San Bernardino Attacks, WASH. POST (Feb. 7, 2016, 1:50 PM EST), https://perma.cc/LP6V-RP2J.
4. See Tim Cook, A Message to Our Customers: The Need for Encryption, APPLE (Feb. 16, 2016), https://perma.cc/HQ3D-SSUU (emphasizing that any tool to undermine encryption could be used repeatedly—a master key able to open millions of locks).
unnamed “outside party” had helped unlock the phone.\textsuperscript{6}

The media’s attention on investigations like the San Bernardino shooting, in which law enforcement cannot decrypt a device, obscure the many cases in which they can.\textsuperscript{7} Despite concerns about criminals “going dark,”\textsuperscript{8} law enforcement authorities possess a range of tools to circumvent encryption. They can go after the data rather than the device,\textsuperscript{9} or take a self-help approach.\textsuperscript{10} But law enforcement’s most immediate option for breaking into a locked phone is by

\begin{quote}
\begin{footnotesize}
QYZM. Although the All Writs Act had been used to order Apple’s assistance with decryption in at least seventy cases prior to the San Bernardino investigation, this was the first time the Act was being used to compel a company to create new software rather than provide technology it already possessed. Legal scholars noted this marked an “unprecedented” stretch of an antiquated law—one that is likely to spark an epic fight pitting privacy against national security.” Id.

6. Alina Selyukh, Apple-FBI: The Theories and Mysteries of the San Bernardino iPhone, NPR (Apr. 16, 2016, 8:00 AM ET), https://perma.cc/S3GW-GYMR. Though the identity of the FBI’s mysterious assister remained “classified,” theories ranged from Cellebrite to private hackers-for-hire. Five years later, reports revealed Australian security research firm Azimuth had assisted the FBI at the cost of $900,000. Ellen Nakashima & Reed Albergotti, The FBI Wanted to Unlock the San Bernardino Shooter’s iPhone. It Turned to a Little-Known Australian Firm., WASH. POST (Apr. 14, 2021, 8:00 AM EDT), https://perma.cc/CW8M-9QWP.

7. Other high-visibility locked-device cases include the government’s request for a court order compelling Apple to bypass the passcode of a phone seized from a Brooklyn drug dealer. In re Apple, Inc., 149 F. Supp. 3d 341 (E.D.N.Y. 2016); see also Jack Nicas & Katie Benner, F.B.I. Asks Apple to Help Unlock Two iPhones, N.Y. TIMES (Jan. 7, 2020), https://perma.cc/4KDY-ANRV (detailing how the FBI sought Apple’s assistance unlocking the phone of the Saudi Royal Air Force Lieutenant who shot and killed three sailors at Pensacola Naval Air Station); Samantha Raphelson, Texas Gunman’s Locked Cellphone Renewed Debate over Encryption, NPR (Nov. 9, 2017, 2:34 PM ET), https://perma.cc/4CWX-VEGN.

8. See, e.g., The Lawful Access Challenge, FBI, https://perma.cc/ZKF8-HRSM (archived May 21, 2024). The FBI has long complained that “[b]ecause of warrant-proof encryption, the government often cannot obtain the electronic evidence necessary to investigate and prosecute threats to public and national safety, even with a warrant or court order.” However, the FBI lost some credibility after it reported inflated statistics about the problem posed by encrypted cellphones, claiming investigators were locked out of nearly 7,800 devices when the correct number was probably between 1,000 and 2,000. Devlin Barrett, FBI Repeatedly Overstated Encryption Threat Figures to Congress, Public, WASH. POST (May 22, 2018, 7:11 PM EDT), https://perma.cc/MJE2-97VK.


10. The FBI’s Operational Technology Division (OTD) is an in-house hacking R&D unit that designs malware and network investigative techniques (NITs) for use in investigations. See, e.g., MICHAEL CHERTOFF, ERIC JARDINE & CENTRE FOR INT’L GOVERNANCE, POLICING THE DARK WEB: LEGAL CHALLENGES IN THE 2015 PLAYPEN CASE (2021), https://perma.cc/T7L6-8UB (describing the FBI’s use of an NIT to takedown a dark web child sexual abuse material site called Playpen, and associated legal considerations). The FBI has also run complex undercover operations to gain access to otherwise encrypted communication networks. See, e.g., Press Release, U.S. Att’y’s Off. for the S. Dist. of Cal., FBI’s Encrypted Phone Platform Infiltrated Hundreds of Criminal Syndicates; Result is Massive Worldwide Takedown (June 8, 2021), https://perma.cc/T27S-MFYK (detailing how the FBI conducted over 500 arrests by operating its own encrypted device company, called “ANOM,” to sell devices and infiltrate criminal groups worldwide).
\end{footnotesize}
\end{quote}
using a mobile device forensic tool (MDFT), purchased from a third-party vendor, which allows them to bypass security and “extract”—download—a trove of data from the device.\(^\text{11}\)

Despite their ubiquity, there is little reporting about or public awareness of MDFTs and the capabilities they provide. The lack of public transparency means that MDFT use is largely unrestricted and unaccountable. Without sufficient checks, MDFTs risk allowing authorities to rummage through the vast quantities of private information on a cellphone and its cloud backup, posing an obvious threat to Fourth Amendment protections against unreasonable searches and seizures. On the flip side, if used with appropriate policies and checks in place, MDFT filtering and classification features can help limit the scope of a search.

Ensuring MDFTs are used to minimize rather than multiply the scope of digital searches requires federal-level policy reforms including (1) restricting consent searches, the plain view exception, and types of crimes for which MDFT-enabled searches are allowed; (2) more narrowly scoped search warrants; and (3) record-keeping and reporting requirements to increase transparency and accountability.

I. WHAT ARE MDFTS AND HOW DO THEY WORK?

An MDFT is a device and accompanying software that can copy (“extract”), organize, and analyze data from a cellphone or other mobile device.\(^\text{12}\) U.S.

---

\(^{11}\) This Note will limit its focus to MDFTs that require physical access to a device, because the limited reporting available suggests those are the most common tools currently in use. However, the same issues posed by MDFTs are present, if not exacerbated by, remote forensic capabilities. Dubbed widely as “spyware,” remote tools can be installed without physical access to a device, and some are even “zero-click,” meaning they can infect a device without a user clicking on anything, such as a malicious link. See, e.g., Dana Priest, Craig Timberg & Souad Mekhennet, Private Israeli Spyware Used to Hack Cellphones of Journalists, Activists Worldwide, WASH. POST (July 18, 2021, 8:15 PM), https://perma.cc/NAB4-DA7S (detailing at length the most infamous of these tools, Pegasus, produced by the Israeli company NSO Group). Another issue beyond the scope of this Note is that repressive foreign regimes are using remote forensic tools to monitor dissidents, journalists, and activists. These tools have facilitated human rights violations, including the murder of Jamal Khashoggi, and chilled free speech in countries around the globe. And between late 2021 to mid 2022, reports emerged that the FBI had purchased a license for NSO’s Pegasus spyware, though it stopped short of deploying it in criminal investigations. Mark Mazzetti & Ronen Bergman, Internal Documents Show How Close the F.B.I. Came to Deploying Spyware, N.Y. TIMES (updated Nov. 15, 2022), https://perma.cc/24VH-QEV5 (quoting from an FBI legal brief that “[j]ust because the FBI ultimately decided not to deploy the tool in support of criminal investigations does not mean it would not test, evaluate and potentially deploy other similar tools for gaining access to encrypted communications used by criminals”). For more on this important topic, see Steven Feldstein, Governments Are Using Spyware on Citizens. Can They Be Stopped?, CARNEGIE ENDOWMENT FOR INT’L PEACE (July 21, 2021), https://perma.cc/4SUU-NDCF.

authorities ranging from the federal government agencies to local law enforcement are increasingly purchasing and using MDFTs to extract and programatically search a full copy of data from a device. While various companies offer different capabilities, most MDFTs offer three primary advantages to law enforcement: (a) circumvention of security features to access locked devices, (b) access to data stored on the device, cloud-based backups, and online accounts, and (c) enhanced cellphone data analytics and querying.

A. MDFTs Can Bypass Security Features to Access Most Devices

A perpetual cat-and-mouse game persists between device manufacturers who rush to patch security vulnerabilities, and companies that build and sell MDFTs to exploit those vulnerabilities. Entities that sell digital forensic tools like MDFTs or other “hacking” capabilities have the offensive advantage, leaving device manufacturers scrambling to detect and repair vulnerabilities. For example, to prevent brute force attacks—using computer power to rapidly generate and guess a passcode—Apple introduced escalating timeouts after a certain number of failed passcode attempts. Eventually, after enough failed attempts, the phone will erase itself.

But MDFT vendors adapted to the new security feature quickly. For most (but not all) smartphones, MDFTs can access a locked device by injecting it with a software “agent” that deactivates the security features that cause the phone to “brick” after a certain number of failed passcode attempts—either delaying additional guesses or wiping all data entirely. Once the security mechanism is


14. Jason Healey, Understanding the Offense’s Systemwide Advantage in Cyberspace, LAWFARE (Dec. 22, 2021, 8:01 AM), https://perma.cc/T9VG-KQB8 (discussing the myriad causes for the offensive cyber advantage, including the conventional wisdom that while, “the attacker must find but one of possibly multiple vulnerabilities in order to succeed; the security specialist must develop countermeasures for all”).

15. Avery Hartmans, There’s a Scary iPhone Feature That Erases All Your Data After Too Many Password Attempts—Here’s Why You Should Turn It on Anyway, BUSINESS INSIDER (Dec. 16, 2018, 12:10 PM PST), https://perma.cc/J36E-T4VZ.

16. Id.

17. Olivia Solon, iPhone Spyware Lets Police Log Suspects’ Passcodes When Cracking Doesn’t Work, NBC (May 18, 2020, 12:34 PM PDT), https://perma.cc/HT3R-ZSBS. Even when a tool cannot crack a password, some MDFTs like Oxygen Forensic Detective’s toolkit, can uncover a wealth of before first unlock (BFU) data including keychain records and files from chat applications, Apple Notes, Apple Wallet, Contacts, and Gmail. Vladimir Katalov, BFU Extraction: Forensic Analysis of Locked and Disabled iPhones, ELCOMSOFT BLOG
deactivated, the MDFT software is free to guess an endless number of passcodes as rapidly as possible—taking just minutes to guess a four-digit passcode. If those methods fail, law enforcement could alternatively install passcode-recording spyware onto the device. For instance, Grayshift’s Hide UI spyware will record and store a user’s passcode in a text file on the phone, which can be extracted the next time law enforcement plugs the phone into the GrayKey MDFT.

B. MDFTs Provide Access to a “Goldmine” of Data

The quantity and quality of information on a modern cellphone allows anyone with access to reconstruct “[t]he sum of an individual’s private life.” MDFTs can provide access to the entirety of a phone’s contents, including contacts, photos, videos, saved passwords, GPS records, phone usage records, and even “deleted” data. MDFTs can also give access to web browsers, online accounts, and third-party applications. Industry leader Cellebrite has advertised that its tools can extract and analyze at least 181 Android apps and 148 iPhone apps.

MDFTs allow police to obtain information that would not be readily accessible during a manual search. This includes data the user has “deleted” from the phone but that remains on the phone’s local storage or backed up in the cloud. Some tools can also provide “behind the scenes” device usage information—a “digital intelligence goldmine” that can reveal detailed insights


18. Lorenzo Franceschi-Bicchierai, Stop Using 6-Digit iPhone Passcodes, VICE (Apr. 16, 2018), https://perma.cc/7JSA-YD24. According to estimates, a tool sold by Grayshift can guess a six-digit pin in under twenty-four hours and a four-digit pin in mere minutes. By comparison, it would take Grayshift an average of twelve years to guess a passcode made of ten random digits. Id.

19. Id.


21. Koepke et al., supra note 13. As critics are quick to point out, MDFTs don’t only invade the device user’s privacy, but can also reveal private, intimate information about a massive swath of people that the user communicates with using the device. Search, Seize, and Extract: Challenging Law Enforcement Use of Mobile Device Forensic Tools and Technologies in Criminal Cases, NAT’L ASS’N OF CRIM. DEF. LAWYERS (Aug. 31, 2022), https://perma.cc/K72A-N6EA.

22. Koepke et al., supra note 13. Cellebrite, for instance, can extract data from apps including Google Maps, Gmail, Tinder, Grindr, OkCupid, Nike+ Run Club, Facebook, Instagram, Twitter, Snapchat, Chrome, Firefox, and “even encrypted messenger apps like Signal and Telegram.” Id.

23. Id. Many devices do not physically delete a file but rather mark it as “free space” until it is overwritten by other data. MDFTs can sometime access these files. And even when a file is permanently deleted from a device, MDFTs may be able to access the data from a cloud-based backup. iCloud, for instance, keeps deleted files for 30 days and can recover them at the user’s request. Id.
into the user’s patterns of life. For example, Cellebrite advertises a tool that parses information from Apple iOS’ knowledgeC database, providing access to a device’s event log of processes including when an application was installed, opened, and used. It can also show Spotlight searches, screen status, and when a device was locked, unlocked, or plugged in. Moreover, some MDFTs can even reach data beyond the local device itself. By extracting authentication tokens from a device, some of these tools can access a user’s remote backups stored on the cloud. This technique can also provide authorities with access to external cloud-based accounts, including Microsoft, Facebook, Google, Lyft, and Dropbox, among others.

C. MDFTs Streamline Data Processing and Analytics

In addition to extracting a vast swath of data, MDFTs compile and organize information across applications and processes into a single, searchable database. MDFTs allow authorities to perform keyword and image searches across the various applications and storage locations on a device. They can also generate easily digestible graphics, including a network map showing communication with contacts, a chronological timeline of user activity, or a map of a person’s location history. By automizing the data analysis process, MDFTs slash the human hours required by manual device searches.

II. MDFTs and Fourth Amendment Implications

Courts have long struggled to translate Fourth Amendment doctrines—born and developed in the physical world—into the digital context. MDFTs further complicate Fourth Amendment application for at least three reasons. First, MDFTs allow law enforcement to make full extractions of a cellphone with the owner’s or user’s consent, even though very few people understand that the search will extend well beyond clicking through a few texts or images. Second, if search warrants are insufficiently scoped, law enforcement can use an MDFT to conduct an unreasonably broad search—and even if that warrant is later insufficiently scoped, law enforcement can use an MDFT to conduct an unreasonably broad search—and even if that warrant is later insufficiently scoped, law enforcement can use an MDFT to conduct an unreasonably broad search—and even if that warrant is later

25. Id.
26. Id. Spotlight is the desktop search feature on Apple’s macOS and iOS operating systems. A record of these searches can reveal what internal files or programs the user was searching for at a given time. Screen status, meanwhile, can indicate whether the screen was backlit, unlit, or dark, giving insight into whether a user was actively looking at a device at a given time.
28. Koepke et al., supra note 13. If a user has Google location history enabled, police can use a MDFT to pull saved passwords, log in to the Google account, and extract the user’s repository of precise location data.
29. Id.
deemed invalid, courts readily apply the good faith exception to allow the ill-gotten cellphone evidence into trial. Lastly, the plain view doctrine can have especially alarming implications in an MDFT-enabled cellphone search because if officers are authorized to peruse all of the data extracted from a device, odds increase that they might “inadvertently” stumble upon evidence of a crime. Courts are grappling with these issues in disparate ways, increasing the need for federal legislation that regulates when and how law enforcement can use MDFTs to search cellphones while setting threshold requirements for cellphone search warrants.30

A. MDFT-Enabled Searches Authorized by Consent Are Often Not Adequately Informed or Voluntary, Considering the Volume and Quality of Data Obtainable via Extraction

Police are required to have a warrant to search a cellphone unless an exigency exists, or they obtain the user’s consent.31 Consent searches for cellphones are surprisingly common compared to searches authorized by a warrant, even accounting for the majority of searches in some jurisdictions.32 Consent searches must be based on voluntary consent, considering the totality of the circumstances.33 In that analysis, “two competing concerns must be accommodated in determining the meaning of a ‘voluntary’ consent—the legitimate need for such searches and the equally important requirement of assuring the absence of coercion.”34 The totality of the circumstances test will thus consider whether the interaction had any elements of coercion,35 as well as the consenters’ age, gender, race, and level of education.36 Finally, the Supreme Court has held that consent searches are permissible under the Fourth Amendment regardless of whether or not the person knows they may refuse

30. See infra Part V.
32. For example, fewer than half of the 1,583 cellphone extractions conducted by the Harris County (TX) Sheriff’s Office between August 2015 to July 2019 were subject to a search warrant. 53% were consent searches, or searches of phones denoted as “abandoned/deceased.” Koepke et al., supra note 13.
35. Drayton, 536 U.S. at 204 (finding consent voluntary where the police and consenters’ interaction appeared cooperative, there “was nothing coercive [or] confrontational” about the encounter, and there was “no application of force, no intimidating movement, no overwhelming show of force, no brandishing of weapons, no blocking of exits, no threat, no command, not even an authoritative tone of voice”).
36. See United States v. Mendenhall, 446 U.S. 544, 558 (1980) (observing that these factors are relevant, but not decisive, in evaluating the voluntariness of a suspect’s consent). Additionally, in searches of shared property, “great significance [is] given to widely shared social expectations” when assessing whether a suspect’s consent was voluntary. Georgia v. Randolph, 547 U.S. 103, 111 (2006).
Consent-based MDFT-enabled cellphone searches generate unique concerns relative to consent searches in the physical domain (i.e., bags, vehicles, homes, or other real property) for several reasons, including: (1) the distinctive quality and quantity of data on a cellphone; (2) the high rates of consent to unlock a phone despite expectations of just the opposite, suggesting consent to an MDFT search is not truly voluntary; (3) and ill-informed knowledge about MDFTs’ capabilities.

1. Cellphones Are Minicomputers, GPS Trackers, Diaries, and More

As the Court emphasized in Riley, “[t]he term ‘cell phone’ is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as telephones. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.” Given the volume and diversity of content they contain, cellphone searches can be uniquely invasive whether done manually or using an MDFT.

Cellphones have “immense storage capacity” and “collect[] in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record.” These quantitative and qualitative characteristics make cellphone searches distinct from a search of one’s physical person, bag, or real property—all of which have a finite scope. And MDFTs take this invasion a step further than the manual cellphone searches considered in Riley. An MDFT’s extraction, processing, and analytic capabilities provide officers with a “window into the soul”—an infinite world of data, ready for parsing, capable of revealing intimate information and insight into a user’s pattern of life.

2. Suspects’ Consent Is (Often) Not Truly Voluntary

Consent searches in any context present complex questions of implicit coercion, power, and voluntariness. The legality of a consent search depends on whether a “reasonable person would understand that [they are] free to refuse,” and may not be coerced, implicitly, or explicitly. Yet the notion that people can refuse police requests has an “air of unreality.” This is especially the case for

37. Schneckloth, 412 U.S. at 218 (noting that “[w]hile knowledge of a right to refuse consent is a factor to be taken into account, the State need not prove that the one giving permission to search knew that he had a right to withhold his consent”).
39. See id. at 375, 394.
42. Id. at 208 (Souter, J., dissenting).
African Americans and people of color, whose collective experience suggests any noncompliance with police requests could result in serious bodily harm.\textsuperscript{43} Refusing consent is harder than it appears. Findings from a lab study comparing expected and actual cellphone search consent rates suggest that decision-makers—judges and juries—weighing the voluntariness of consent tend to “underestimate the pressure people feel to comply with intrusive [police] requests.”\textsuperscript{44} In the study, a group of 209 “Experiencers” were asked to unlock their password-protected smartphones and give them to an experimenter while they waited in a room. A separate group of 194 “Forecasters” were asked whether a reasonable person in the above situation would comply. More than 97% of “Experiencers” handed over their phone to be searched when requested, even though only 14.1% of Forecasters said that a reasonable person would do so. While refusing to consent to a cellphone search is “harder, and rarer, than we realize,” the study found a “systematic bias whereby neutral third parties view consent as more voluntary, and refusal easier, than actors experience it to be.”\textsuperscript{45} Consent to any type of search may be less voluntary than it seems to onlookers—whether police, judges, or juries.\textsuperscript{46}

Another study examining the tactics law enforcement uses to gain consent for cellphone searches found that detectives employed nearly identical techniques as those used to obtain criminal confessions during an interrogation.\textsuperscript{47} Detectives build rapport and use “contemporary interrogation techniques” including “minimization techniques,” which work to alleviate the suspect’s anxiety and appeal to the suspect’s self-interest.\textsuperscript{48} For instance, one detective asked a suspect, nonchalantly, “[c]an I look at [your phone]? That way I can put in the report that I looked and there was nothing in it.”\textsuperscript{49} Other times, officers emphasize that only “guilty” people refuse a cellphone search. Detectives may also try to assuage a suspect’s apprehensions by assuring them the cellphone search will be isolated—limited to certain parts of the phone or types of data. These assurances, paired with promises of quick turnaround times (e.g., “you’ll have your phone back in an hour”), can mislead suspects who are unaware that

\begin{itemize}
\item \textsuperscript{43} Marcy Strauss, Reconstructing Consent, 92 J. CRIM. L. & CRIMINOLOGY 211, 242-43 (2001) (noting that “at least for some persons of color, any police request for consent to search will be viewed as an unequivocal demand to search”).
\item \textsuperscript{45} Id. at 2019.
\item \textsuperscript{46} Id. at 1967 (finding that “third parties judging the voluntariness of consent are likely to underestimate the pressure people feel to comply with intrusive requests”).
\item \textsuperscript{47} Stacy Dewald, “So, You Can Let Me Look at Your Phone?”: Detectives Obtaining Consent to Search Cell Phones, 5 J. CRIM. JUST. & L. 1, 5-6 (2022).
\item \textsuperscript{48} Id. at 4-5, 7-10 (describing minimization techniques including “appealing to the suspect’s self-interest, appealing to the suspect’s conscience, offering rationalization, offering moral justifications, emphasizing the benefits of cooperation, and minimizing the seriousness of the offense”).
\item \textsuperscript{49} Id. at 8.
\end{itemize}
the phone will be taken to another room and plugged into an MDFT device, likely for a complete extraction.\textsuperscript{50} These techniques come together in convincing ways. Take, for instance, a real-world situation where the detective is investigating allegations that the suspect, a 20-year-old college student, took nude photos of the victim without her consent:

\textit{Detective Kristin}: I can look at your phone to exonerate you, otherwise I think you’re lying. I will jailbreak your phone. I will send it in and then look at it that way.

\textit{Suspect}: How long will that take?

\textit{Detective Kristin}: It will take a long time, I’ll take my time, you’re not helping. Does your phone open with a fingerprint?

\textit{Suspect}: Yes.

\textit{Detective Kristin}: Put it in airplane mode for me. The faster way is for you to consent and you’ll get your phone back in a day or two. You could give me written consent.

\textit{Suspect}: I don’t feel comfortable.

\textit{Detective Kristin}: Guilty people don’t feel comfortable.\textsuperscript{51}

With a bit more cajoling, including the threat of expulsion from college, Detective Kristin ultimately prevails in getting the suspect to sign a consent form to have his phone searched.\textsuperscript{52} Suspects are goaded into believing they are consenting to a quick manual search either to find exculpating evidence, or to avoid worse outcomes or the threatened inevitability of a search warrant down the line.\textsuperscript{53} Just as police deceive suspects during interrogation,\textsuperscript{54} so too are they intentionally misleading suspects to gain consent for a cellphone search. Considering the inherent difficulties with refusing law enforcement requests (or demands), paired with interrogation-style tactics, many consent-based cellphone searches may rest on a legal fiction of consent.

3. Suspects Are Not Adequately Informed About MDFTs and the Scope of the Search

The scope of information accessible using an MDFT is especially problematic considering most people who consent to a search may not realize that (a) an MDFT will be used, (b) what capabilities these tools offer, or (c) the potential for their extracted phone data to be retained for future purposes. Often, when people give consent for law enforcement to look at part of their phone, it

\textsuperscript{50} See id. at 8-10.
\textsuperscript{51} Id. at 9.
\textsuperscript{52} Id. at 9-12.
\textsuperscript{53} Id. at 8.
\textsuperscript{54} Police are allowed to lie to suspects during interrogation, see Frazier v. Cupp, 394 U.S. 731 (1969), but many legal scholars have called for reforms to this rule, and some states are passing laws to bar this technique when questioning children or adolescents. See, e.g., Saul Kassin, \textit{Law Enforcement Experts on Why Police Shouldn’t Be Allowed to Lie to Suspects}, \textit{Time} (Dec. 16, 2022, 7:00 AM EST), https://perma.cc/6SU7-HXHV.
is to show the officers exculpatory information. Little do they know that their consent can be stretched much further, even to justify a complete extraction of their cellphone.

Given there is close-to-zero public awareness about MDFTs, people who consent to a search are likely imagining a manual search rather than a detailed forensic extraction. The Fifth Circuit, however, reached the opposite conclusion, finding that most people would understand that signing a consent form for a “complete” cellphone search refers “not just to a physical examination of the phone, but further contemplates an inspection of the phone’s ‘complete’ contents.” The dissent disagreed, arguing that such an assumption would require an average person to “make the inferential leap that ‘property’ refers to [one’s] digital content, including text messages, photos, Google Maps locations, bank account statements, and even your highest score on Candy Crush.” The suspect’s verbal consent to “look through” his phone, backed by a generic, outdated form hardly reflects informed consent or an awareness that the Cellebrite MDFT used in the case had powerful extraction and processing capabilities. The suspect could neither see the physical extraction of his device—the iPhone plugged into the Cellebrite box—because he was kept in a different room, and he had no way of knowing that the officers would use it to retain a copy of the iPhone’s contents for forensic review at a later point. After all, if they truly understood law enforcement’s MDFT-enabled capabilities, no reasonable person would ever voluntarily consent to a sweeping, digital forensic search of their phone—particularly when that person knew their phone contained evidence of a crime.

Further, while people are entitled to restrict the areas they consent to be searched, efforts to specify partial consent to a limited search can be muddied when an MDFT is used. Take the case of George Burch, for instance. Burch was a suspect in a series of vehicle-related crimes. When Burch offered an alibi that he was at a bar on the night in question and texting a woman, the officer requested to see the text messages. Burch consented, but only to allowing the officer to read his texts—which Burch knew would be exculpatory as support for

55. United States v. Gallegos-Espinal, 970 F.3d 586, 592-94 (5th Cir. 2020) (deeming a search of a cellphone data three days after its extraction as constitutionally permissible because the user had signed a broad, generic consent form).

56. Id. at 593-95 (Graves, J., dissenting) (elaborating that the consent form was insufficient because it failed to explain that the cellphone data could be extracted for later review).

57. Id.

58. Id. (concluding that “[t]he general consent form was insufficient to alert Gallegos-Espinal that the government was going to extract and retain the iPhone data for later examination, especially when Gallegos-Espinal was told the phone searches were only needed to determine if he could take custody of his younger siblings”).


60. Id.
MOBILE DEVICE FORENSIC TOOLS

his alibi. The officer then explained he preferred to download the information because it was easier than taking photos and scanning them in. Burch again agreed and signed a generic consent form to search his phone. Two months later, when Burch became a suspect in an unrelated murder, detectives discovered the extracted phone data saved in the police database, searched it, and found additional evidence contributing to Burch’s eventual conviction. What began as Burch’s limited verbal consent for an officer to look only at his text messages snowballed into a full forensic extraction of his device, which was saved in the police department’s long-term storage and used by a separate law enforcement agency to dig for evidence related to a separate, unrelated crime.

B. Courts Are Divided on Sufficient Probable Cause and Particularity Standards in MDFT-Enabled Searches, but the Good Faith Exception Almost Always Applies

While a warrant may resolve issues of questionable consent, cellphone search warrants come with a host of their own issues. The Fourth Amendment requires a warrant be based on (a) probable cause and (b) ”particularly describ[e] . . . the persons or things to be seized.” When taken together, these requirements mean that search warrants must list the items to be searched or seized and create a sufficient nexus between those items and the officer’s probable cause statement.

Courts have taken widely varied approaches when assessing cellphone search warrants. Some have found that warrants giving officers authority to search for “any and all information” and “any and all data” are overly broad. While “[t]here is no ‘one size fits all’ solution for ensuring particularity in cell phone search warrants . . . [they] must be specific enough so that the officers will only search for the items that are related to the probable cause that justifies the search in the first place.”

Id. at 316-17.

Id. at 317.

Id.

The court suggested the investigators acted in good faith reliance by searching the phone extraction because “[n]othing in the consent form, the narrative, or anything else in the file, indicated that Burch limited the scope of the data he consented to have downloaded from his phone.” Burch’s internet history showed sixty-four viewings of news stories about the woman’s murder and revealed an email address linked to a Google account. Investigators obtained a warrant for data from Google, which provided location information tying Burch to the murder. Id.

Probable cause exists when “there is a fair probability that contraband or evidence of a crime will be found in a particular place.” Illinois v. Gates, 462 U.S. 213, 214 (1983).

See, e.g., Richardson v. State, 481 Md. 423, 441 (2022).

Id. at 462. Also note that, although the court found the warrant impermissibly overbroad, and thus invalid, it nonetheless admitted the contested evidence under the good faith exception. Id. This is an overwhelming trend in cases where digital search warrants are deemed invalid.
However, this seems to be the minority approach. In 2021, Pennsylvania’s highest court upheld a warrant for the search and seizure of all electronic devices in a suspect’s home after investigators traced child sexual abuse material (CSAM) files shared on BitTorrent back to his IP address.\textsuperscript{69} Although the police’s probable cause was limited to the belief that CSAM images would be found on devices using the suspect’s IP address, the warrant was far broader by allowing a search for any evidence relating to the possession and/or distribution of CSAM. Though the distinction is nuanced, such a broad warrant fails to cabin officer discretion because “[o]ne officer could read the warrant as authorizing a broad search of every single file on the computer and phone—every spreadsheet, every executable, every deleted text message, every Apple pay record, all of the exercise data on the app tracking [the suspect’s] steps.”\textsuperscript{70} Without a closer tie to the probable cause established—that there were likely CSAM images on the devices—officers could read such a broad warrant as authorizing a search for anything that could provide evidence related to CSAM possession (purchasing histories, communications, diaries, personal notes, etc.). The majority used a physical analogy—a police officer searching the suspect’s home for printed copies of CSAM could open a drawer to check inside—but, as the dissent points out, the officer could not read through the pages of a diary that happened to be inside that drawer, which is exactly what the warrant would have permitted.\textsuperscript{71} A separate dissenting opinion pointed out that the warrant was overbroad because it authorized a search of all devices in the apartment—had others lived there, their phones would have been subject to the same sweeping search.\textsuperscript{72}

Despite those issues, federal courts have been similarly lenient with cellphone warrants. The Fourth Circuit, for instance, upheld a warrant as sufficiently particular \textit{despite} it lacking details about the types and location of files sought or the relationship between the files and the crime under investigation.\textsuperscript{73} Here too, however, not all judges agreed. The dissenting judge found that the warrant limiting the search to information “associated with” the crime under investigation was insufficiently particular because the affiant had

\footnotesize{\textsuperscript{69}. Commonwealth v. Green, 265 A.3d 541, 555 (Pa. 2021). The IP address traced back to a modem, and since there was no way to know which specific device in the property connected to the modem and shared the CSAM, a warrant allowing search of all devices was not unreasonable. Despite allowing search of all devices, the warrant’s scope was sufficiently narrow because it was limited to “evidence relating to the possession and/or distribution of child pornography.” \textit{Id.} at 552.

\textsuperscript{70}. \textit{Id.} at 560 (Donohue, J., dissenting).

\textsuperscript{71}. \textit{Id.} at 557 n.3.

\textsuperscript{72}. \textit{Id.} at 568 (Wecht, J., dissenting) (hypothesizing that, had a three-person family been living in the apartment, “nothing would prohibit the officers from scouring the wife’s personal calendar. If they are looking for audio files, they can read every page of the daughter’s personal diary. If they are seeking only documents, they nonetheless can pore over countless personal, confidential messages passed between the girl and her friends or love interests”).

\textsuperscript{73}. United States v. Cobb, 970 F.3d 319, 326-29 (4th Cir. 2020) (noting the long-recognized principle that “[a] warrant need not—and in most cases, cannot—scrupulously list and delineate each and every item to be seized”).}
more information available that could have more precisely defined the bounds of the search. Despite decreasing unanimity in decisions upholding broad warrants, courts still tend to deem them as passing muster.

Even where they have found cellphone warrants deficient, courts have generously applied the good faith exception to admit evidence. For instance, in United States v. Morton, the Fifth Circuit held that CSAM found on a cellphone seized during a traffic stop should have been admitted under the good faith exception even though the original panel concluded the officers’ search of photographs went beyond the warrant’s scope to search for drug-related evidence. The only facts in the affidavit supporting probable cause for the phone search were that the defendant possessed a “user-quantity of drugs,” possessed a cellphone, and that the officer’s training and experience informed him that people use their phones to communicate. As the concurrence highlights, if those three facts are sufficient, then any time an officer finds contraband on a person or in a vehicle, they have probable cause to search the entire contents of a nearby cellphone.

Relying on the good faith exception to admit evidence before turning to the Fourth Amendment question is precisely the “inflexible practice” the Supreme Court warned against in Leon. By repeatedly applying the good faith exception to invalid search warrants, or dodging the question altogether, courts “condone[] the government’s extensive and intrusive search of cellphones and its failure to provide any explanation of how those particular phones relate to the charged crime.” Allowing officers to take refuge in the good faith exception incentivizes continued “bare bones” affidavits and “insulates officers from having to connect the dots between their general knowledge and experience . . . and the basis for that specific search warrant.”

C. Applying the Plain View Doctrine in MDFT-Enabled Cellphone Searches Can Give Law Enforcement Access to an Unreasonable Quantity (and

74. Id. at 336-40 (Floyd, J., dissenting).
75. Courts apply the “good faith exception” when officers acted in reasonable reliance on a search warrant that was later found to be invalid. In such a situation, the exclusionary rule does not apply. United States v. Leon, 468 U.S. 897, 918-22 (1984) (explaining that if the purpose of the exclusionary rule is to deter police misconduct, there is no value in excluding evidence where an officer acted in “good faith” and within the scope of a warrant).
76. See, e.g., United States v. Morton, 46 F.4th 331, 334 (5th Cir. 2022).
77. Id.
78. Id. at 340-41 (Higginson, J., concurring). Finding that contraband possession paired with phone possession is sufficient probable cause to search that phone conflicts with the Court’s reasoning in Riley, rendering a cellphone search warrant a mere paperwork requirement. Rather, the concurrence suggests implementing use restrictions for data that is inadvertently discovered during a digital search. See Kerr, infra note 158.
80. Leon, 468 U.S. at 924.
81. Morton, 46 F.4th at 342-43 (Graves, J., dissenting).
82. Id.
Quality) of Data

Courts are similarly divided over whether to apply the plain view doctrine to cellphone and other digital searches. The plain view doctrine allows officers 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. For example, if an officer is searching a home for firearms used in a robbery and encounters illegal drugs sitting on the kitchen countertop, the officer can seize those drugs under the plain view doctrine.\(^{83}\) The officer would also be allowed, ostensibly, to look inside any container or drawer that could be concealing firearms. On the other hand, if the officer were to open a container too small to fit a gun, but found drugs inside, those drugs would not be seizable because the officer was not looking in a place where they were legally permitted to look.

The plain view doctrine does not map well into the MDFT-enabled cellphone search context. In the complete extraction of a cellphone, pursuant either to a broad warrant or consent, an officer will likely be able to view, sort, and search all of the data on the phone, whether or not it is necessarily responsive or connected to the probable cause in the case. To illustrate:

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.\(^{84}\)

A more sympathetic case version of that hypothetical is if officers seeking evidence of tax fraud were to come across text messages with that person’s seventeen-year-old daughter, helping her obtain abortion pills or coordinate travel to access an abortion out-of-state.\(^{85}\) That parent could be charged not only with tax fraud but also with providing or aiding and abetting an abortion.\(^{86}\) The same could happen to a parent who is arranging gender-affirming care for their child in a state where doing so is banned.\(^{87}\)

\(^{83}\) Emily Berman, Digital Searches, the Fourth Amendment, and the Magistrates’ Revolt, 68 EMORY L.J. 49, 59 (2018).
\(^{84}\) Id.
\(^{85}\) This isn’t a purely hypothetical situation. In July 2023, a Nebraska woman plead guilty to helping her daughter access abortion pills to end her pregnancy. Nebraska Mom Pleads Guilty to Giving Daughter Pills for an Abortion and Helping Bury the Fetus, AP NEWS (July 7, 2023, 4:29 PM PST), https://perma.cc/SJ47-59FV. Though police in that case used a search warrant to obtain key incriminating evidence—Facebook messages between the mother and daughter—the same results come stem from a “plain view” discovery of texts, emails, or social media exchanges following a cellphone extraction. Id.
\(^{86}\) See id.
\(^{87}\) Bans on Best Practice Medical Care for Transgender Youth, MOVEMENT ADVANCEMENT PROJECT, https://perma.cc/PVQ2-G5J2 (archived May 21, 2024). As of March 2024, twenty-three states had attempted to restrict or ban gender-affirming health care for...
Courts have struggled to stretch a doctrine born in the physical world to fit the digital domain. In United States v. Carey, one of the first cases exploring the issue, the Tenth Circuit ruled that the plain view doctrine does not extend to closed files on a hard drive. There the court ruled inadmissible CSAM images discovered during a drug trafficking investigation because, by opening numerous JPEGs under the presumption they would contain CSAM, the detective went beyond the scope of the original warrant, which authorized the search of “documentary” drug-related evidence. In doing so, the court rejected the government’s argument that the detective could lawfully “seize” the CSAM because it was in “plain view” and discovered inadvertently. Although opening the initial JPEG may have been inadvertent, the detective “abandoned” his search for drug-related evidence and instead commenced a separate search for CSAM—the equivalent of opening closed cabinets in a house.

Other courts have been more generous to law enforcement. For instance, in United States v. Mann, the Seventh Circuit held that a detective’s discovery of CSAM during a voyeurism investigation did not exceed the scope of a warrant for “images of women in locker rooms or other private areas.” This scenario is distinct from that in Carey, where the detective’s opening of image files fell outside the warrant’s scope because the warrant was limited to “names, telephone numbers, ledgers, receipts, addresses, and other documentary evidence” related to drug trafficking. The warrant in Mann, in contrast, authorized a search for images of women that would be relevant to the voyeurism charges under investigation—a file type that made it inevitable for an officer conducting a thorough search to inadvertently stumble upon the defendant’s extensive CSAM collection.

The plain view doctrine has also been applied in digital search cases with less nuance. As recently as 2020, the Fourth Circuit held that the plain view doctrine applied to CSAM found during a search for evidence related to a murder investigation, reasoning the warrant impliedly authorized agents to open every

transgender minors, with five states making it a felony to provide such care. Although a federal district judge preliminary enjoined the law in December 2023, Idaho’s HB 71 made it a felony for medical providers to provide gender-affirming care to minors, threatening up to a decade in prison. Families Block Idaho Law Banning Health Care for Transgender Youth, ACLU (Dec. 27, 2023, 10:00 AM), https://perma.cc/G232-WTNE.

88. United States v. Carey, 172 F.3d 1268, 1273 (10th Cir. 1999).
89. Id.
90. Id. at 1273-74.
91. Id.
92. See, e.g., United States v. Cobb, 970 F.3d 319, 332 (4th Cir. 2020).
93. United States v. Mann, 592 F.3d 779, 781 (7th Cir. 2010). The court did, however, find that the detective knew or should have known the four images flagged by forensic toolkit (FTK) software as child pornography were likely to contain such. By opening those files without obtaining a second warrant specifically for CSAM, the officer exceeded the scope of the search warrant. Suppressing those four images, however, would not have impacted the trial outcome because the government had a host of evidence against Mann. Id. at 784-85.
94. Carey, 172 F.3d at 1272-73.
95. Mann, 592 F.3d at 783-84.
file on the computer to determine if it fell within the warrant’s scope. Under this logic, officers were authorized to take a “cursory” look at an entire computer—looking dangerously like a general warrant.

While these cases suggest factors to consider when assessing the constitutionality of digital search warrants, generally, much of the logic applied to computer hard drives is stretched when applied to cellphones. Unlike physical searches—say of a filing cabinet—hard drives contain a greater quantity and variety of files that are likely intermingled, requiring law enforcement to sort various types of documents and then only search the ones specified in a warrant. Although cellphones may contain a lower quantity of data, due to storage limitations, they may nonetheless provide more robust and more intermingled data than the organized file folder structure of a hard drive. For example, because a user typically carries a phone with them everywhere, it can serve as the functional equivalent of a GPS tracker, pulling and storing location data from any number of applications—from Google Maps to Starbucks to weather apps. The parallels are even further stretched when considering data extracted using MDFTs because their advanced processing, querying, and analytical functions give investigators the ability to search and reconstruct data aggregated across applications and file types. Although a cellphone may have limited storage, MDFT extractions that pull authentication credentials can serve as a gateway to accessing cloud-based applications with troves of data.

Nonetheless, we can gather some basic principles from existing case law to apply to the MDFT context. Carey highlights a key requirement for the plain view doctrine—that an officer is looking where they are legally authorized to look when they inadvertently discover evidence. While MDFTs’ sorting and analytic functions can help create filtered searches of aggregate data extracted from a phone, investigators may still encounter incriminating information while conducting their search. As is discussed at length in Part V, if investigators stumble into contraband outside the scope of their original search warrant, they ought to pause and obtain a second warrant before continuing to search the extracted data.

Many gaps remain in applying digital search precedents to MDFT-enabled

---

96. Cobb, 970 F.3d at 332.
97. Id.
98. See, e.g., Carey, 172 F.3d at 1275.
100. Carey, 172 F.3d at 1273 (stating the CSAM JPEGs “were in closed files and thus not in plain view”). Importantly, 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.” Coolidge v. New Hampshire, 406 U.S. 443, 466 (1971).
101. This depends on how warrants are written and how the investigator uses the MDFT. Requiring police to use MDFT image and text classification and filtering functions could reduce rather than increase the chance of inadvertently discovering contraband. See infra Part V.
102. See United States v. Wong, 334 F.3d 831, 838 (9th Cir. 2003).
cellphone extractions. Because it is not often clear in advance where or in what file type investigators might find responsive criminal evidence, cellphone search warrants tend to permit unlimited searches. For example, language in approved warrants commonly authorizes the search of “any and all data” on a cellphone, or “laundry list”-style warrants that list all possible categories of data on a phone. Even if the warrant is limited to evidence related to the crime under investigation, it often fails to specify which of the many types of files, applications, or processes the agent may search on the device. And the broader the warrant, the easier it is for investigators to fall back on the plain view doctrine by claiming they were legally permitted to look in the place where the inadvertent discovery was made. For this reason, some legal scholars have argued that magistrate judges ought to require the government to waive reliance on the plain view doctrine when applying for digital search warrants. Such suggestions, however, introduce even bigger questions about whether magistrate judges can or should preemptively prescribe specific search methods in the warrant. Rather than leaving such decisions to the whims of judges, new rules at the federal level would allow MDFTs to help solve the plain-view problem for cellphone searches by sorting, segregating, and deleting non-responsive data. This approach will be discussed further in Parts IV and V.

III. CRITIQUES: CONCERNS ABOUT THE UNCONSTRAINED USE OF MDFTS

Despite the tools’ proliferation across state, local, and federal law enforcement, MDFTs remain almost entirely unregulated—providing advanced capabilities to officers without sufficient oversight, transparency, or democratic

---

103. *E.g.*, if a warrant is limited to searching for evidence of CSAM, does that mean investigators may only look at image files extracted from the phone, or can they look at text communications as well, since those may reveal evidence of coordinating CSAM exchange with others? Similarly, are investigators required to filter and “flag” potential nudity using the image classification features offered by many MDFTs?


105. *Id.* at 17.

106. *E.g.*, photos, emails, text messages, app data, or other class of information accessible to investigators via MDFT extraction.

107. *See, e.g.*, United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1178 (9th Cir. 2010) (Kozinski, J., concurring) (elaborating that if the government refuses to waive plain view doctrine in a digital search, “the magistrate judge should order that the seizable and non-seizable data be separated by an independent third party under the supervision of the court, or deny the warrant altogether”). Concerned by the government’s ability to indefinitely retain heaps of data from digital searches, Judge Kozinski suggested that in addition to (1) waiving reliance on the plain view doctrine, magistrate judges ought to require the government’s affidavit for a warrant to (2) specify that computer personnel or an independent third party will segregate the data and will refrain from disclosing information discovered in the process, (3) disclose the risks of data destruction, (4) contain a procedure to ensure that only the object of the warrant will be seized and reviewed by agents, and (5) require that the government will return or destroy data that is not the object of the warrant. *Id.* at 1180.

accountability. Meanwhile, because MDFTs allow officers to, in many cases, bypass cellphone security features, they erode the public’s reasonable expectation of privacy in their devices. These impacts can generate disparate effects—causing greater harm to on low-income communities, who often rely on their smartphones as their sole means of internet access, and communities of color, who are disproportionately targeted in drug investigations (for which MDFTs are commonly used).

A. Widespread Proliferation with Little-to-No Oversight or Transparency Has Precluded Democratic Debate About the Use of and Risks Associated with These Tools.

Over 2,000 agencies in all fifty states use MDFTs in investigations of both major crimes and mundane cases, including petty theft, graffiti, public intoxication, and marijuana possession. Most large U.S. law enforcement agencies have purchased or used MDFTs, including every one of the fifty largest local police departments, state law enforcement agencies in all fifty states, at least twenty-five of the fifty largest sheriff’s offices and, at least sixteen out of the twenty-five largest district or prosecuting attorneys’ offices. Further, local agencies that lack in-house MDFTs can take advantage of regional partnerships with state or federal authorities. And the supply is as diverse as the demand—U.S. agencies have purchased tools from at least thirteen different providers, more than half of which are foreign companies hailing from Canada, Israel, Russia, and Sweden.

But understanding which agencies are using MDFTs, and how often, is challenging due to the lack of any centralized record or reporting requirement. A mere forty-four of the estimated 2,000 law enforcement agencies who reported using MDFTs responded to Upturn’s request for information. Those forty-four agencies—despite accounting for less than 2.5 percent of those using MDFTs—reported conducting at least 50,000 cellphone data extractions between 2015 and 2019. This is a dramatic undercount because (a) it represents a tiny fraction of

109. Koepke et al., supra note 13. Other offenses agencies reporting using MDFTs for included “prostitution, vandalism, car crashes, parole violations, ... and the full gamut of drug-related offenses.” Id. at 3.
110. Id.
111. See, e.g., Service Offerings, FBI: REG’L. COMPUT. FORENSICS LAB’Y, https://perma.cc/YNE8-PXWJ (archived May 21, 2024). The FBI has seventeen Regional Computer Forensics Labs that offer a range of services including a Cell Phone Investigative Kiosk (CPIK), which provide extractions in as little as thirty minutes. Id.
113. Koepke et al., supra note 13.
114. Id.
115. Id.
the agencies using MDFTs, (b) many departments that responded do not track or collect how often they use their MDFTs, and (c) many of the largest local police departments—including New York City, Chicago, Washington DC, Baltimore, and Boston—either denied or did not respond to Upturn’s requests. Visibility into the costs of these tools is similarly lacking, even though U.S. taxpayer dollars fund their purchase. While no studies to date have attempted to grasp the aggregate costs for MDFTs across agencies, individual reports give insight into the cost of particular tools. For instance, in 2019 Immigration and Customs Enforcement (ICE) planned to pay Cellebrite between $30 and $35 million for universal forensic extraction devices (UFEDs) and associated licenses, training, and support, up from $2.2 million in 2017. ICE also has paid Grayshift $1.2 million for tools.

The lack of transparency into MDFT use remains a major barrier for researchers and the public to evaluate the privacy and Fourth Amendment concerns posed by the tools. Even the limited information available suggests cellphone extractions using MDFTs are becoming standard protocol. This is especially concerning considering that many law enforcement agencies have generic, boilerplate policies, or more commonly, no policies at all. And those with policies rarely mention anything about ensuring a device search warrant affidavit is sufficiently particularized to pass Fourth Amendment muster. On the contrary, some encourage seeking broad search warrants from the court, and a judge might approve affidavits without realizing whether and to what extent an MDFT will be used to facilitate the search. Broad warrants paired with an absence of policy guidance for how to handle the discovery of nonresponsive incriminating evidence outside the warrant’s scope increases the risk of general “fishing expeditions.” And even the most savvy and well-resourced defense

116. Id.


118. Brewster, supra note 117.

119. Koepke et al., supra note 13. Departments have noted that “[r]equests for cellphone analysis has become the standard for phones involved in all types of criminal investigation,” MDFTs are “used on a daily basis,” and “[o]ur department relies heavily on Cellebrite . . . tools.” Id.

120. Id. Out of the eighty-one agencies who responded to Upturn’s inquiry, forty said they had no departmental policies in place. Id.


122. See Koepke et al., supra note 13.
attorney will struggle to convince a court to invalidate a warrant given the deference afforded to judges’ probable cause determinations.  

B. MDFTs Undermine Mobile Device Security and the Public’s Reasonable Expectation of Privacy in Their Devices, with Disparate Impacts

MDFTs allow law enforcement to circumvent most security features on most phones. And yet most of the public is likely unaware that MDFTs render their devices vulnerable to police intrusion regardless of the manufacturer’s advertised security features. Similarly, the public is unlikely to anticipate the vast range and depth of data police can extract from their phones—even during investigations of minor infractions.

Also troubling is that, for several reasons, certain sectors of the populace will be more vulnerable to MDFT-enabled searches than others. Because low-income communities are more likely to rely on smartphones as their sole source of internet access, their phones will likely contain an even greater trove of private information. Additionally, because many agencies use their MDFTs primarily for drug investigations, which have historically had disparate effects on black and Latinx communities, we can expect these populations are being disparately impacted by MDFT-enabled searches. Upturn’s study found that drug-related offenses featured prominently in police department extraction logs, which is “especially worrisome given the extreme racial disparities in drug arrests, the disproportionate severity of drug sentences, and the role drug arrests play in deportations.” If MDFTs are being used subject to a consent search or a broad search warrant, and without adequate departmental checks in place, there is a high potential risk of officers using drug infractions as a pretext for a complete, unlimited cellphone search. As will be discussed further in Part V, limiting MDFT use to serious felony investigations rather than minor or misdemeanor offenses could reduce the disparate impact on low-income and minority


124. See supra Part I.A.

125. See Koepke et al., supra note 13 (listing the minor offenses in which police departments are using MDFT-enabled phone searches).

126. Emily A. Vogels, Digital Divide Persists Even as Americans with Lower Incomes Make Gains in Tech Adoption, PEW RECH. CTR. (June 22, 2021), https://perma.cc/SMWY-2TEB (finding that in 2021, “27% of adults living in households earning less than $30,000 a year are smartphone-only internet users—meaning they own a smartphone but do not have broadband internet at home”).

127. See Koepke et al., supra note 13.

128. Id.

129. See, e.g., supra notes 76–79 and accompanying text.
populations.

Worth noting, too, is that MDFTs are proliferating outside the U.S. law enforcement context. At least eight U.S. school districts have purchased MDFTs. Older versions of MDFTs such as Cellebrite’s Universal Forensic Extraction Device (UFED) can be purchased by private individuals through online retailers including eBay for an average price of $1,700. The resale market allows UFEDs and software updates to continue reaching countries with questionable if not abysmal human rights records, including Bangladesh, Belarus, China, Hong Kong, Russia, and Venezuela, despite Cellebrite highlighting that it would no longer do business there. Considering U.S. agencies continue to be a major customer base for MDFT companies, the U.S. is indirectly fueling the proliferation of these technologies—including to authoritarian regimes. This puts an even greater impetus on U.S. lawmakers and courts to reign in the use of MDFTs by domestic law enforcement, to both (a) set a better example for the responsible use of device forensics and spyware tools and (b) pave the way for international cooperation in their unregulated proliferation.

IV. PROONENTS’ POSITIONS: A POWERFUL TOOL, IF WIELDING RESPONSIBLY

As one of the dissenters in Green highlighted, there is rarely if ever an excuse for an exceptionally broad warrant or search of a cellphone because “digital searches, by their nature, permit the use of modern forensic tools to narrow the content to be searched using specific software, dates, file types, hash values, etc., the combination of which avoids the rummaging that the Fourth Amendment and Article I, Section 8 seek to prevent.” Indeed, with the appropriate guardrails in place, MDFTs could facilitate greater particularity in cellphone searches, save agencies vital work hours during investigations, and improve audit records of phone searches to ensure reproducibility—all without infringing the Fourth Amendment rights of device users.

130. Tom McKay & Dhruv Mehrotra, U.S. Schools Are Buying Phone-Hacking Tech That the FBI Uses to Investigate Terrorists, Gizmodo (Dec. 11, 2020), https://perma.cc/N8EY-7CL.

131. Behind the Resale of Cellebrite Technology That Can Hack Your Phone, TEMPEWS (Feb. 20, 2022), https://perma.cc/DHE3-BDUV (noting this price is, according to a Polish forensic specialist, “lower than the average $10,000 someone has to pay for a new UFED Touch with an annual license fee of $3,000 to $4,000”).


133. Commonwealth v. Green, 265 A.3d 541, 557 (Pa. 2021) (Donohue, J., dissenting). Hash values are unique alphanumeric values that are essentially fingerprints of a file. Hash matching technology can be used to locate certain files at an incredibly high degree of accuracy—all without even opening the file. See Micro Systemation AB, How to Use Rapid Hash Matching in the Battle Against CSAM, FORENSIC FOCUS (July 31, 2023), https://perma.cc/26GS-6S7A/ (describing how law enforcement can use hash matching to detect CSAM).
A. MDFTs Promise to Facilitate More Particularized Phone Searches

Because MDFTs increasingly offer features that help an investigator stay within the limits of a sufficiently particularized warrant, there is little reason for a judge to approve a broad search of a mobile device. For example, MDFT products are incorporating image recognition and categorization technologies that use artificial intelligence and machine learning to detect, sort, and flag images based on faces and objects such as money, weapons, drugs, or CSAM. Such tools could prevent authorities from rummaging through all the images on a device, and instead flag only those relevant to their search.

Similar features are emerging for classifying text and chat conversations, allowing investigators to filter conversations based on keywords. Magnet Forensics’ text classification model, for instance, can “detect potential sexual conversations in addition to child luring,” promising to allow investigators to “better prioritize their time . . . and find potentially relevant evidence faster than they could through manual review.” Judges ought to gain familiarity with and inquire into the law enforcement agency’s MDFT capabilities before approving cellphone search warrants, and require that affidavits describe how automated features in the tools will be used to keep the search narrowly scoped to content or file types relevant to the investigation.

Looking forward, as computer processing speeds and machine learning algorithms continue to improve, so too will the capabilities of MDFTs to auto-detect and flag certain types of imagery, files, and text. These capabilities should be embraced and regulated, rather than banned altogether, because the better MDFTs are at sorting, organizing, labeling, and presenting data in a sanitized manner (i.e., displaying responsive data only), the harder it will be for an investigator to claim the discovery of contraband was inadvertent and admissible under the plain view doctrine. Indeed, as the court reasoned in Mann, if a file is flagged suspect for reasons outside of the crime under investigation, or beyond the scope of a search warrant, police would have no excuse for embarking on a secondary, unrelated search without returning to a judge for a second search warrant. In other words, MDFTs can help label the no-go zones for officers. That

134. Christa Miller, Image Recognition and Categorization, FORENSIC FOCUS (July 8, 2019), https://perma.cc/4FXA-JMMQ. Modern tools build on the FTK technology used by the detective in Mann, which flagged known child pornography images using a “KFF (Known File Filter) Alert.” See United States v. Mann, 592 F.3d 779, 781 (7th Cir. 2010).

135. See, e.g., Ian Martorana, Oxygen Forensics Releases Cutting-Edge Integration to Categorize Images and Unveils TamTam Messenger Cloud Extraction, GLOBENEWswire (Dec. 9, 2019, 9:00 ET), https://perma.cc/T7M8-GJJG. Oxygen Forensics’ flagship software, Forensic Detective, offers “image categorization and grouping, allowing investigators to use AI to sort and categorize images into twelve categories, including drugs, weapons, alcohol, and nudity, to more quickly find pertinent images to an investigation.” Id.


137. Id.

138. See Mann, 592 F.3d at 784-85.
said, if MDFTs are to encourage compliance with narrowly scope warrants, law enforcement must be required to maintain search-step records that are subject to audit by the court and opposing counsel, so an investigator cannot claim they merely stumbled into the nonresponsive evidence in “plain view” among the extracted data.

B. MDFTs Are a Powerful Enabler for Criminal Investigations and Public Safety Efforts

Nearly seventy percent of law enforcement agencies view technology as a “game-changer” in alleviating workloads, providing a force multiplier, and reducing agency costs.139 Considering most criminal cases include digital evidence, the ability to more rapidly extract and parse data is a critical enabler for law enforcement—less manual labor means MDFTs cut the costs of collecting, parsing, and retaining digital evidence.140 Further, MDFTs can reduce the duration of a phone seizure. Faster extractions (including in the field) allow a device to be returned to its user faster, limiting inconvenience and burden on the user. These benefits all suggest that banning MDFTs outright is not the ideal solution. Rather, if their use is appropriately regulated, MDFTs can lead to more effective policing, more efficient use of taxpayer dollars, and less interruption in the lives of witnesses or suspects subject to cellphone searches.

C. MDFTs Can Record Extraction and Search Steps to Improve Auditing

Agencies that use MDFTs currently lack requirements for investigators to sufficiently document their searches, which is the only way anyone outside of law enforcement—like the court, or a defense lawyer—can reproduce the search to ensure it was conducted within its authorized bounds.141 However, manually documenting the steps taken in a manual search can extend an already time-intensive process. MDFTs can help solve this dilemma by facilitating record-keeping and auditing through features that capture an investigator’s search process, including information viewed and queries conducted.142 For example, Cellebrite advertises that its Guardian software now includes an “enhanced Investigator Activity Report” that “creat[es] and maintain[s] a full chain of

141. See Koepke et al., supra note 13. The few departments that require investigators to document searches include only vague direction to take contemporaneous notes during the search or document the procedures and type of software used. Without more detail, already-papework-encumbered law enforcement agents are unlikely to document the search to a degree sufficient for future auditing.
142. See infra Part V.B.
Here again, MDFTs can increase law enforcement accountability by providing investigators with an easy, automated method of “showing their work” to the court and opposing counsel. That said, MDFT providers must be incentivized to continue building and improving search-recording features. Requiring investigators to thoroughly document the steps taken during a cellphone search (including the particular procedures or MDFT features used to scope the search) would drive demand for better search-record software capabilities, enabling future audits both within and outside law enforcement.

V. RECOMMENDATIONS

MDFTs can be powerful law enforcement enablers, but like all law enforcement investigative tactics, they require regulation to reduce the risk of infringing Fourth Amendment protections. While many of the issues related to MDFT-enabled cellphone searches apply to digital forensics more broadly, reforming the law for cellphone searches specifically is a critical and urgent first step. This is because cellphone searches can be uniquely invasive and because the limited data available suggests consent-based cellphone searches are extremely common, especially for lower-level offenses. As discussed above, MDFT-enabled cellphone searches are disparately impacting vulnerable, low-income, minority populations whose single source of internet access is their smartphone. Law enforcement is taking advantage of the lack of public awareness about or accountability for MDFT searches and is continuing to use this advanced technology in the shadows, keeping suspects unaware of just how invasive the cellphone search will be.

At the same time, given the potential and actual benefits of MDFTs discussed in Part IV it would be an overreach to ban the tools altogether. Instead, like any new powerful technology, rules must be enacted to ensure MDFTs are harnessed to protect rather than harm Fourth Amendment rights and privacy interests.

Before delving into specific recommendations for reform, it is important to address which actors are best positioned to implement new requirements for MDFT-enabled cellphone searches. Because law enforcement agencies’ interests in preventing and solving crimes favor broader searches, an appropriate check will need to come from one or more external actors. While municipalities and


144. See Koepke et al., supra note 13 (listing the minor offenses in which police departments are using MDFT-enabled phone searches).
local governments are ripe proving grounds for new initiatives aimed at safeguarding Fourth Amendment protections.\textsuperscript{145} broader systemic change must come from (1) DOJ setting national policy, (2) federal legislation, (3) the Supreme Court, or (4) some combination of all the above. Of these options, the most realistic from a practical perspective is the first—a national-level policy driven out of the executive branch. While a federal statute would be ideal for purposes of continuity across successive administrations, congressional deadlock makes passing a bill—even one that could gain bipartisan support—an uphill battle. Likewise, the Supreme Court has not given any indication that it will weigh in on the scope, particularity, and probable cause requirements for digital search warrants—instead permitting the lower courts to continue with the trend of upholding broad warrants or, if not, then applying the good faith exception to save the evidence from exclusion.

At any rate, when and how U.S. government agencies use MDFTs is fundamentally a policy issue because it requires balancing law enforcement’s legitimate investigative purposes with protecting people from unwarranted intrusions into their personal devices, and by extension, their private lives. This type of complex tradeoff is best handled through political processes, with democratic accountability, rather than law-making by the courts.\textsuperscript{146} The most ideal vehicle for regulating MDFTs would be through a federal statute—the same way wiretaps and law enforcement access to stored electronic information are restricted.\textsuperscript{147}

While federal legislation is a route worth pursuing, a simultaneous and likely more realistic, timely, and efficient approach would be through executive-level policy. The obvious downside of a DOJ-led policy initiative is that policies can be more easily reversed and overwritten when administrations change. Another perhaps more signification drawback is that executive regulations will typically only bind federal law enforcement, but not state or local authorities. Nonetheless,

\textsuperscript{145} See, e.g., Nicole A. Ozer, Santa Clara County Passes Landmark Law to Shut Down Secret Surveillance, ACLU (June 8, 2016). https://perma.cc/5457-R6E3. Santa Clara County’s Surveillance Technology & Community Safety Ordinance was the first in a wave of Community Control Over Police Surveillance (CCOPS) initiatives passed by local jurisdictions to empower residents to decide whether and how police surveillance technologies are used. Community Control Over Police Surveillance (CCOPS), ACLU (updated Apr. 2022). https://perma.cc/R2WH-MARK.

\textsuperscript{146} See, e.g., United States v. Jones, 565 U.S. 400, 429-30 (2012) (Alito, J., concurring) (highlighting that “[i]n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative” because a “legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way”) (citing Orin S. Kerr, The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution, 102 Mich. L. Rev. 801, 805-06 (2004)). Kerr argues that some legal scholars’ enthusiasm for judicial solutions to privacy and technology questions “overlooks significant institutional limitations of judicial rulemaking”—it is inflexible and tends to become quickly outdated as technology changes. Id. at 858-59.

there are mechanisms through which DOJ and other executive agencies can influence state and local policies, like, for instance, controlling their access to the FBI’s Regional Computer Forensics Labs for agencies that lack their own in-house MDFTs.\footnote{See FBI: REG’L. COMPUT. FORENSICS LAB’Y, supra note 111.}

All that being said, parallel efforts are necessary in the legislative and executive branches to implement the following reforms to limit MDFT-enabled cellphone searches: (a) setting bounds for consent searches, eliminating the plain view doctrine, and restricting the tools to use in serious felony offense investigations only; (b) minimum requirements for cellphone search warrants to describe the specific MDFT and search procedures used, and scoping the search by time frame, data type, application, or parties involved depending on the probable cause established; and (c) requiring agencies to maintain in each case file an audit record detailing how an MDFT was used, annually report key statistics on MDFT use, and establish retention and deletion policies.

A. Establish Threshold Requirements for MDFT-Enabled Cellphone Searches: Limiting Consent Searches, Plain View Doctrine, and Use in Minor Offenses

\textit{Bar MDFT Use in Minor Cases.} As a threshold, MDFTs ought to be limited to use only in certain types of cases, with a line drawn at “violent” crimes or felony-level offenses, for instance.\footnote{See Koepke et al., supra note 13 (listing the minor offenses in which police departments are using MDFT-enabled phone searches); see also Wiretap Act, 18 U.S.C. § 2519 (allowing wiretaps for felony-level criminal investigations only).} Barring police from using MDFTs when investigating lower-level offenses reduces the risk that minor offenses will become pretexts to search a phone for evidence of digital contraband or other criminal activity unrelated to the infraction at issue. If law enforcement has a specific reason to need to use an MDFT to investigate a less serious offense, applying for an option is still an available avenue.

\textit{Mandatory Disclosure Requirements for Consent-Based Cellphone Searches.} Another critical reform would curtail the use of consent-based searches. Some have proposed this come in the form of an outright ban,\footnote{See, e.g., Koepke et al., supra note 13.} but there could be instances where consent searches are appropriate—if adequately informed, truly voluntary, and appropriately limited. The benefits of more tightly restricting consent searches of cellphones would reduce the risk that a suspect or witness gives consent without adequate awareness that an MDFT would be used or the capabilities it provides. A prohibition on cellphone consent searches would also better align with the Supreme Court’s intent in \textit{Riley} and would help address racially disparate impacts of MDFT-aided cellphone searches.\footnote{See Strauss, supra note 43.}

To allow a consent-based cellphone search using an MDFT, authorities
ought to use a standardized, written cellphone search consent form that satisfies five basic requirements: (1) discloses that an MDFT will be used and explains how the tool will be used; (2) indicates that only the specific areas or types of information on the form will be searched and/or retained; (3) specifies that any non-responsive data incidentally collected will be deleted; (4) detailing the department’s timelines and policies for data retention, deletion, and cross-agency sharing of responsive data;\textsuperscript{152} and (5) explicitly states that the suspect is free to refuse consent without penalty.

The explanation of the MDFT can be simple, and fairly generic, but the consenting person should understand that (a) this won’t be a manual search, and (b) the MDFT device has the capability to extract a full copy of their cellphone. The form should stipulate that any nonresponsive data extracted will be deleted, and that the only information retained will be that which is responsive to the agreed-upon list. As an example, the first page of the form will be informative, and the second page will be fillable—ideally by the consenting person, or alternatively, an officer—and stipulate which types of information and/or applications may be searched. This page ought to include a list of examples, so consenting individuals know how they might tailor the cabining of their cellphone search (e.g., text messages with X person between [dates]; photo album between [dates], Gmail messages received from [username]@domain.com, etc.).

Adjust the Plain View Protocol for Cellphone Searches. Some critics have urged that the plain view exception be abolished in the context of cellphone searches.\textsuperscript{153} This is because the plain view doctrine’s rationales collapse in the digital domain.\textsuperscript{154} Unlike a home where closed containers (drawers, closets, etc.) cannot be inadvertently viewed, and require intentional opening, an MDFT extraction and its accompanying software potentially makes all data available to officers with them necessarily “opening” anything.\textsuperscript{155} The leading counterargument in defense of retaining the plain view doctrine for digital searches is that criminals will attempt to obfuscate evidence on their hard drives by creating hidden pathways, file names, and changing dates.\textsuperscript{156} But this argument carries far less weight for cellphones than it does for computers because it is much harder, and sometimes impossible, to change the storage locations of data on a cellphone.\textsuperscript{157} There are simply fewer places to hide information.

However, abolishing the plain view doctrine altogether could be a bridge too far. If, as this Note recommends, reforms are focused on improving the particularity of warrants—appropriately narrowing the scope of cellphone

\textsuperscript{152} See infra Part V.C.
\textsuperscript{153} See, e.g., Koepke et al., supra note 13.
\textsuperscript{154} See supra notes 98-99 and accompanying text.
\textsuperscript{156} See Koepke et al., supra note 13.
\textsuperscript{157} Id.
searches to reflect the probable cause in an investigation—then penalizing officers for seeing contraband or unrelated incriminating evidence does not make sense if and only if the officer is looking where they are authorized to look. Rather than deeming inadvertent discoveries universally inadmissible, a more nuanced approach would limit police’s use of that evidence ex post. In other words, officers should only be able to introduce evidence that is described in and directly responsive to the warrant. Effectuating digital searches, especially of computers, may necessitate seizing and searching through nonresponsive data in order to find the responsive evidence described in the warrant, because “[s]earching through the haystack for the needle inevitably reveals a lot of hay.”

Through its initial seizure may be necessary, the subsequent use of nonresponsive evidence turns

[T]he subsequent use of nonresponsive data transforms the nature and quality of the ongoing seizure of that data. Using nonresponsive data no longer effectuates the warrant. Instead, it takes advantage of the overseizure and subsequent search necessary to carry out the warrant to transform the warrant for specific evidence into the equivalent of a general warrant. In effect, allowing use of nonresponsive data effectively treats that data as if it had been included in the warrant. This eliminates the role of the particularity requirement, making the warrant the equivalent of a general warrant. Subsequent use enables every computer warrant that is narrow in theory to become general in fact.

The unreasonable part, then, is the subsequent use of the nonresponsive evidence—information that was necessarily seized to execute the warrant, but that is not within its bounds.

However, entirely restricting the use of nonresponsive information may prove similarly excessive as eliminating the plain view doctrine altogether. While this is a smart approach for computer searches, where overseizure and discovery of nonresponsive yet criminal evidence are far more common, it should not be necessary for cellphone searches if those searches are subject to sufficiently particularized authority, either in a warrant or on a consent form. Here is where MDFTs can provide an advantage. First, appropriately scoped

158. Orin Kerr, Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data, 48 TEX. TECH L. REV. 1, 1 (2015). Kerr amends his previous assessment that the plain view doctrine should be eliminated to ex-ante restrictions: “The better path is for courts to rule that the Fourth Amendment imposes use restrictions on nonresponsive data because use transforms the underlying seizure from a justified and modest step needed to execute the warrant to an unjustified and invasive seizure unrelated to the warrant itself. Agents can overseize at the first stage because they must, and they can search through all the data for the responsive files because there is no other way to ensure that they find all the evidence described in the warrant. But when agents use nonresponsive data, the seizure of that data is no longer justified by the warrant and ordinarily is no longer reasonable.” Id.

159. Id. at 18 (arguing that “to make sure computer warrants do not resemble general warrants in their execution, the agents should only be allowed to use the evidence that is actually described in the warrant”).

160. Id. at 25-26.

161. Id.
authorities should, in most cases, not allow a complete cellphone extraction, but rather specify which types of data and timeframes will be downloaded. Second, even where a complete extraction is authorized or otherwise practical, MDFTs allow investigators to conduct tailored searches within that data. Investigators don’t have to dig through the haystack—the software does that for them, and returns, ostensibly, only the “needles” related to probable cause.

Because of these differences, anything discovered in “plain view” during an MDFT-enabled cellphone search ought not be barred outright. Rather, nonresponsive but incriminating evidence ought to be permitted for one single use—as probable cause to return to the court for a warrant for a second unrelated investigation—if and only if officers have remained within the reasonable confines of the initial authority to search, whether granted by warrant or consent.

What might this look like in practice? To illustrate, let’s take the example of Detective Kristin, attempting to the suspect’s consent to search his phone for nude images after another student accused him of taking nonconsensual photos of her. Had the recommended policies been in place, Detective Kristin would have to fully disclose to the suspect that, if he agreed, an MDFT would be used to search his phone for images—and images only. If the suspect was indeed innocent, he may be willing to consent to a search only of the photos on his phone, and he could stipulate “photos from [relevant time period]” on his consent form. Detective Kristin would then extract only the images timestamped within the relevant dates from the suspect’s phone. Because some MDFTs can use machine learning technology to recognize and sort nudity in images, Detective Kristin could use that feature to flag potentially responsive images for her review. Alternatively, if she did not have this capability, Detective Kristin could conduct a manual review. In either instance, Detective Kristin may inadvertently discover unrelated contraband such as nude images of underage individuals (i.e., illegal CSAM).

Those images would not necessarily be related to Detective Kristin’s probable cause, which is scoped to nude images of the alleged victim. A blanket use restriction or abolishing the plain view exception would render the discovered CSAM inadmissible for any purpose. But in this case, that outcome would not serve the interests of justice. Rather, because Detective Kristin was looking where she was authorized to look—at the images within a specific time frame—her “plain view” discovery should be usable, but for only one singular purpose: as probable cause to obtain a second warrant for a separate investigation into the suspect’s possession and/or distribution of CSAM. This approach would neither permit Detective Kristin to extract more data from the phone nor expand her search at that moment. Rather, she would need to return the suspect’s phone, having completed the initial consent-based search.

There is one dilemma with this approach worth discussing. If evidence of a different crime was discovered, the investigator must make a tactical decision about trying to gain consent for a second search or saying nothing to the suspect, returning their phone, and getting a search warrant for the new investigation. Either avenue poses risks, primarily that the suspect could destroy evidence.
Immediately pursuing a second consent-based search would allow police to retain custody of the device, but if the suspect refused, detectives would have shown their hand, and the suspect would be free to leave and destroy evidence by deleting files or wiping the cellphone. Alternatively, the detective could choose not to reveal that she stumbled across contraband or incriminating evidence during her authorized search. Even if she immediately applied for a warrant, the detective would have to track down the suspect’s phone a second time. In the interim, a spooked or conscious suspect might destroy evidence.

One approach to navigating this dilemma is by treating it like a preservation of evidence exigency. Typically, the need to prevent the destruction of evidence creates an exception to the search warrant requirement. Applied in this context, the exigency should operate slightly differently. Rather than the discovery of contraband or incriminating evidence automatically giving an officer authority to conduct a full search—here, the complete extraction of the cellphone—it could instead give law enforcement reason to retain the device until they can get a second search warrant. The cellphone would be placed in airplane mode or in a Faraday container to prevent a remote wipe, essentially embargoing the device until police are able to obtain a warrant.

The obvious flaw with this process is that a suspect could be stuck without their cellphone for days, at least, potentially depriving that person of their only internet access and leading to downstream harmful consequences. Some might suggest that to expedite the process, police could instead request the suspects’ consent to complete the second search. But this a solution that creates a problem we have already discussed: an already fraught consent process would be made even less voluntary if police were presenting suspects with a choice between two bad options—either consent to a search, or go days if not weeks without your cellphone while we wait to get a warrant that will lead to the same conclusion. Because consent in such a situation is essentially coerced, a warrant requirement for conducting any secondary searches pursuant to an inadvertent plain view discovery trumps the inconvenience posed to suspects should their cellphones be embargoed. The harm to suspects being deprived of their property could be mitigated by providing a voucher for a prepaid smartphone and monthly data plan—which can be purchased for as little as $70, even for a month of unlimited data. Similarly, the retention period ought to be limited to more than thirty days, and a return-to-owner plan should be implemented. Though, at this point, the suspect would not be able to refuse the seizure, they ought to be provided with a reimbursement voucher for a temporary replacement phone and informed that they can pick up their phone no later than thirty days from the point of seizure. Ideally, agencies would go a step further and develop tailored return-to-owner plans that notify the suspect when their cellphone extraction is complete and available for pick-up, and/or arrange return delivery of the device.

Similarly, requiring truly informed consent via a written form will almost

---

162. Supra notes 100-102.
certainly reduce the instances that police can obtain a suspect’s consent to search their cellphone, requiring officers to get a warrant instead. Similarly, limiting the plain view exception to a single use—to support probable cause in an affidavit for a second search warrant—is likely to drive up warrant requests. Dramatic inflation in the number of warrant applications could pose real risks. First, if judges become inundated, the warrant process could turn into a de facto rubber-stamping exercise, with each warrant receiving less scrutiny than it deserves. Second, if judges are reviewing warrants with the same degree of scrutiny, yet are still overwhelmed by the volume of applications, a backlog could develop, delaying investigations and potentially contributing to the destruction of evidence as time passes.

But, while these fears are not unwarranted, they are entirely hypothetical. Until reforms are implemented to constrain ill-informed and involuntary “consent” searches, we cannot know the impact on the volume of search warrants. Perhaps officers will decide, in certain situations, the juice is not worth the squeeze and instead turn to alternative sources of evidence. If a greater reliance on the search warrant process, as the Court in Riley intended, becomes untenable, then the intervention ought to be in streamlining the warrant process and/or creating more magistrate judicial positions—not continuing to deprive suspects of their Fourth Amendment rights through involuntary consent searches and broad application of the plain view doctrine. All that said, increasing the situations where law enforcement must apply for a warrant before searching a cellphone with only help address the potential harms of MDFTs if those warrants are sufficiently particularized.

B. Ex Ante Restrictions: Scoping Search Warrants

Depending on the probable cause in a case, a warrant can be tailored to limit the search by time frame, data type, application, or parties involved. MDFTs can then be used to match the scope of the warrant. Some tools already have features that allow pre-extraction limitations on which data is pulled from the device, and most can filter extracted data by various search criteria (e.g., date ranges). A more specific warrant is more likely to survive challenges of overbreadth in court and will help MDFTs become tools to minimize rather than expand a search’s scope and intrusiveness. Meanwhile, requiring greater specificity in cellphone search warrants would not unduly restrict law enforcement investigations. Limitations on the time range, the phone applications to be searched, or which types of data (e.g., images, text messages,

164. Id.
165. See Richardson v. State, 481 Md. 423, 462 (2022) (explaining that when applying and issuing a warrant, “the affiant and the issuing judge must think about how to effectively limit the discretion of the searching officers so as not to intrude on the phone owner’s privacy interests any more than reasonably necessary to locate the evidence for which there is probable cause to search”).
emails, or photos) can be extracted would all be imposed with the understanding that officers “can later apply for a second, broader warrant if their initial search provides a basis to do so.”

Another measure to consider is restricting cellphone search warrants to data stored locally on the device, rather than in the cloud. If investigators use an MDFT to extract login credentials such as usernames, passwords, pins, or keychain data, they ought to return to the judge for a second search warrant authorizing access to the target account(s). If the device is a gateway to a person’s entire online identity, additional checks are needed to serve as a brake, preventing investigators from bridging the search of data on a cellphone to data stored on the cloud.

The ideal way to implement basic requirements for MDFT-enabled cellphone search warrants would be to require the affidavit to specify, at a minimum, (1) the specific MDFT and search procedures to be used, and (2) how the search will be scoped to the probable cause for the crime under investigation (using criteria such as time frame, data type, application, or parties involved). These two minimum requirements for judges to consider before approving affidavits are far fewer and more manageable than the five requirements put forward by several Ninth Circuit judges in Comprehensive Drug Testing. They would strike a balance between two competing risks: the continued approval of unconstitutional, general search warrants for cellphones, on one hand, and on the other, concerns that ex ante restrictions will prove counterproductive “[b]y transforming litigation of the lawfulness of a warrant’s execution into litigation focusing on compliance with restrictions rather than reasonableness.”

Up-front warrant requirements are necessary because, to date, courts’ ex post reviews for reasonableness have failed to provide any clear standard for digital search warrants of any kind, much less for cellphones specifically. Instead, most courts have applied the good faith doctrine to admit digital evidence even after finding it was obtained via an illegally overbroad warrant. Other courts have dodged the Fourth Amendment question altogether in these cases. As a result, there is no incentive for law enforcement to change its practices when applying

---

166. Id.
167. See supra notes 27-28 and accompanying text.
168. See supra notes 102, 166.
169. This is especially true considering that once the login credentials are in hand, an investigator could then monitor, impersonate, or otherwise tamper with a person’s account. The risk of abuse is immense. Further, any ongoing collection of evidence beyond the point in time of the warrant execution should require a Title III wiretap order.
170. See Electronic Communications Privacy Act, supra note 147. The “super warrant” requirement in the federal Wiretap Act may serve as a useful model for imposing additional requirements for MDFT-enabled searches. 18 U.S.C. § 2518.
171. Supra note 107.
172. See Kerr, supra note 108.
173. See supra notes 75-82 and accompanying text.
174. See supra note 81 and accompanying text.
for a cellphone search warrant. Officers can continue to conduct full cellphone extractions and searches knowing courts are almost certain to give them refuge from the exclusionary rule by a finding of good faith reliance on the warrant. Given the courts’ track record on this issue, interrupting this status quo will likely require action outside of the courts—demonstrating the necessity of executive-level policy reform and/or congressional intervention via federal law. That said, the Supreme Court could, at any point, more clearly define the particularity requirements for digital search warrants or for cellphone searches specifically. Should any court be willing to intervene, they ought to interpret the Fourth Amendment’s probable cause and particularity requirements more stringently in the digital domain, while being careful to account for the advanced search and seizure capabilities offered by MDFTs and similar technologies.

C. Improving Transparency and Accountability: Reporting and Recording Requirements

To facilitate future auditing, law enforcement agencies should be required to record which MDFT software, hardware, and procedures were used to conduct a cellphone extraction. This information ought to be (1) a mandatory component of any case file where an MDFT is used, and (2) made available to the court and discoverable to defense counsel as a check against overbroad searches. If an audit log is not produced, or is not sufficient to allow an external party to replicate the search, the statute could stipulate a suppression remedy—barring the information obtained from that search from being used in a criminal trial. While such a remedy may seem drastic, it would help restore the balance of incentives for law enforcement to follow procedures necessary to protect defendants’ Fourth Amendment rights.

Additionally, all agencies using MDFTs should be required to report on how often these tools are being used, for which offenses, and pursuant to what legal authority (consent or warrant). These records, which do not exist today, will allow greater transparency and public accountability while giving legal scholars and policymakers alike the information necessary to assess the impact of reforms and consider future adjustments that will better protect privacy interests while balancing law enforcement and public safety imperatives.

Finally, whether in a federal policy or statute, there ought to be universal minimum time periods—no more than six months—for the retention and

---

175. Id.
176. Id.
177. See Koepke et al., supra note 13. State or federal laws requiring “detailed audit logs and automatic screen recording . . . would incentivize MDFT vendors to build this functionality.” Without sufficient records, judges and defenders will have no reliable way of verifying whether investigators went beyond a warrant’s scope when searching a phone.
178. Id. Additional relevant details for reporting could include how often extractions succeeded, explanations for any failed extractions, which tools were used, and demographic data to track whether these tools are being used in racially disparate ways.
deletion of responsive data from a cellphone extraction.\textsuperscript{179} Similarly, agencies should be required to permanently delete any nonresponsive data they have extracted. A few states have already taken such measures. New Mexico, for instance, 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.”\textsuperscript{180}

Limiting retention periods for nonresponsive data extracted from a cellphone would prevent investigators from using the information in subsequent, unrelated investigations. They would also restrict law enforcement from using data obtained in cellphone extractions to feed general criminal intelligence databases like the “gang databases” common in many jurisdictions.\textsuperscript{181}

\textbf{CONCLUSION}

Although they pose major challenges to constitutional searches, like all powerful tools, MDFTs can be harnessed to help rather than hinder law enforcement efforts so long as they are implemented with appropriate checks, oversight, and public accountability. Especially considering courts’ scattered approach to digital search warrants has left the legal space so uncertain, a federal statute and/or executive-enacted policies establishing the aforementioned baseline requirements for MDFT use would go leaps and bounds in the way of reigning in this powerful capability. While efforts initiated by local governments and proactive judges may be useful at a limited scale, systemic change demands federal regulations that restore an appropriate balance between public safety interests, privacy rights, and Fourth Amendment freedoms.

As surveillance technologies rapidly improve, the time could not be more

\textsuperscript{179} See United States v. Ganias, 755 F.3d 125 (2d Cir. 2014) (holding that the government may not indefinitely retain mirrored hard drives for use in future criminal investigations without an independent basis for retention).

\textsuperscript{180} N.M. STAT. ANN. § 10-16F-3 (West 2021). 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.” CAL. PEN. CODE § 1546.1 (West 2017).

\textsuperscript{181} See Koepke et al., supra note 13. Upturn’s study notes that cellphone data like contacts, photos, videos, messages, and location history would be “of immediate interest” to gang task forces. Currently, most jurisdictions have no restrictions about what information can be fed into these databases, both making them unreliable, and permitting long-term retention of cellphone data from unrelated or decades-old investigations: “Factors can include things like ‘pictures of the individual displaying perceived gang signals on social media,’ ‘association with known gang members,’ ‘frequenting gang areas,’ and other indicators fabricated by law enforcement. This discretion has led to extreme racial disparities in gang databases. 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.’” Id. (citations omitted).
ripe for implementing restrictions on law enforcement’s use of MDFTs. Fourth Amendment doctrine has historically lagged behind technological advancements. But as we wait for courts to catch up to the times, creating a more just criminal legal system requires fast-adapting laws and policies that regulate law enforcement’s use of high-tech capabilities. Implementing the recommended regulations for MDFT-enabled cellphone searches can serve as a model for regulating digital searches more broadly and for integrating future police technologies. More broadly, policies that establish reasonable limitations for MDFT use will provide decision-makers—whether at the federal, state, or local level—with a blueprint of guiding principles for balancing public safety and law enforcement with privacy interests and Fourth Amendment protections.