What Comes after Get a Warrant: Balancing Particularity and Practicality in Mobile Device Search Warrants Post-Riley

Andrew D. Huynh
NOTE

WHAT COMES AFTER “GET A WARRANT”: BALANCING PARTICULARITY AND PRACTICALITY IN MOBILE DEVICE SEARCH WARRANTS POST-RILEY

Andrew D. Huynh†

INTRODUCTION ........................................... 188
I. RILEY: GROUNDBREAKING AND NOT, ALL AT ONCE ...... 191
   A. Historical Justifications for Warrantless Mobile Phone Searches ......................... 191
   B. Technology and the Fourth Amendment Leading up to Riley .......................... 192
   C. The Contours Take Shape: Riley v. California’s Warrant Requirement ................ 194
II. FINDING A BASELINE FOR WARRANT PARTICULARITY .... 195
   A. Warrants: A Brief Background ................. 195
   B. The Computer Analogy ....................... 198
   C. The Computer Analogy Is Not a Good Fit for Mobile Devices ......................... 204
      1. Distinguishing Mobile Device Forensics from Computer Forensics .................. 204
      2. Mobile Phones Are Functionally Different from Computers ......................... 207
      3. In Short: Mobile Device Searches Are Distinct from Computer Searches ........ 208
III. CURRENT APPROACHES TO PARTICULARITY AND A PATH FORWARD .............................. 208
   A. Conflicts in Particularity Deference Among the Lower Courts ....................... 209
      1. “Reasonableness” Deference and Its Problems ............................................. 210
      2. Approaches to Enhanced Warrant Particularity ...................................... 212
   B. How a Search Protocol Looks ................. 217

† B.A., Wesleyan University, 2011; J.D. Candidate, Cornell Law School, 2016; Senior Notes Editor, Cornell Law Review, Vol. 101. I am grateful to my family and friends for their tireless support and encouragement through this and all of my endeavors. I would also like to thank the members of the Cornell Law Review for all their work editing this Note for publication.
In June 2014, the Supreme Court handed down Riley v. California, a landmark decision in which the Court ruled that search warrants are required whenever law enforcement officers want to search a mobile device. Some commentators hailed the decision as a great expansion of privacy rights in a digital, mobile society. By striking down the application of judge-made exceptions for a “warrantless” search of an individual’s smartphone, the Court drew a line in the sand to protect individual privacy rights. Writing for the Court, Chief Justice John Roberts acknowledged that the decision would “have an impact on the ability of law enforcement to combat crime.”

Riley is notable for two reasons. First, the decision has the rare import of unanimity. This means that the Court’s nine members looked past individual unease about cementing a constitutional search warrant requirement in order to support the ruling. Specifically, both Justices Antonin Scalia and Clarence Thomas have previously opined that the Fourth Amendment does not mandate warrants unless a search is ostensibly “unreasonable.” Although the Riley opinion’s tenor

1 134 S. Ct. 2473 (2014).
2 See id. at 2493.
3 The terms “smartphone,” “mobile phone,” and “mobile device” will be used interchangeably throughout this Note to reflect the significant overlaps in end-user design between smartphones and tablet computers.
5 Riley, 134 S. Ct. at 2493.
7 See California v. Acevedo, 500 U.S. 565, 581 (1991) (Scalia, J., concurring in the judgment) ("The Fourth Amendment does not by its terms require a prior warrant for searches and seizures: it merely prohibits searches and seizures that
suggests that all warrantless mobile device searches are categorically unreasonable," some commentators nevertheless expressed surprise that the Court’s most openly “originalist” and “textualist” Justices signed onto the Riley opinion’s explicit stand on an issue traditionally left to the discretion of the lower courts and law enforcement.⁹

Second, Riley was the Supreme Court’s first computer-search case, and its first at-bat left a large impression on the public. The New York Times proclaimed the result a “sweeping victory for privacy rights in the digital age” on its front page.¹⁰ Prominent scholar Orin S. Kerr asserted that Riley “is a bold opinion . . . and it says we are in a new digital age.”¹¹ The national legal director of the American Civil Liberties Union (ACLU) posited that “the digital revolution has transformed our expectations of privacy, [and] today’s decision [in Riley] is itself revolutionary . . . .”¹² In late-June 2014, it was difficult to find pieces that were not effusive about the Riley decision.¹³

“Revolutionary” is not necessarily colorful hyperbole. Prior to Riley, courts commonly applied a fairly deferential “reasonableness” determination when deciding whether to suppress fruits of a warrantless search. Indeed, courts frequently relied on predigital analogies in order to couch mobile devices in existing search warrant exceptions developed for physical objects.¹⁴ Privacy activists and legal scholars argued that permitting such intrusions would severely undermine any real

---

8 See generally Riley, 134 S. Ct. at 2491–93 (rejecting petitioner’s suggested compromises due to application issues).

9 See Posner, supra note 4.


11 Id.


14 See, e.g., United States v. Finley, 477 F.3d 250, 259–60 (5th Cir. 2007) (rationalizing a mobile phone as a container).
constitutional protections. Therefore, when the Riley Court ordered law enforcement officers to “get a warrant,” it seemed to solve everyone’s privacy concerns.

But if predigital analogues are now legally insufficient, what must go into a warrant—itself based on predigital search methods—to comport with Fourth Amendment protection? The Court’s lengthy discussion about the amount of personal information accessible on a modern mobile device suggests that a search warrant’s particularity may be the next subject for scrutiny. So what do law enforcement officers and prosecutors need to include in a search warrant to balance investigatory interests with privacy considerations? After all, there remains a strong interest for law enforcement in efficient prosecution of criminal offenses. And yet, the Court’s explicit privacy concerns cannot go unheeded.

This Note explores the practical background that underpins the delicate balancing act between state policing and individual privacy interests in state and federal courts. It concludes that incorporating a search-protocol requirement into mobile device search warrants may be the only workable standard. This way, an increasingly tech-savvy corps of magistrate judges may scrutinize how searches are conducted and thereby ensure the target’s privacy rights.

This Note is organized in four Parts. Part I summarizes the road up to and including the Court’s logic in Riley, to mandating warrants when searching mobile devices. Part II discusses the current requirements for valid search warrants and will address the applicability of analogizing computer search warrant jurisprudence to mobile devices. Part III analyzes the current tensions in lower courts over search warrant particularity for mobile devices and discusses why a search protocol requirement is a persuasive method of balancing law enforcement and privacy interests. Part IV provides a conclusion.

---

15 See Steven I. Friedland, Cell Phone Searches in a Digital World: Incorporating Function as well as Form in Fourth Amendment Analysis, 19 TEX. J. C.L. & C.R. 217, 244 (2014) (“Trying to fit the existence of smartphones into an earlier reality that focuses on form provides for a bad fit and, generally, bad results.”); Daniel Zamani, Note, There’s an Amendment for That: A Comprehensive Application of Fourth Amendment Jurisprudence to Smart Phones, 38 HASTINGS CONST. L.Q. 169, 198 (2010).


17 See id. at 2489–91 (discussing the qualitative and quantitative aspects of smartphone content).

18 See id. at 2493 (“Our holding, of course, is not that the information on a cell phone is immune from search; it is instead that a warrant is generally required before such a search . . . .”).
I

RILEY: GROUNDBREAKING AND NOT, ALL AT ONCE

A. Historical Justifications for Warrantless Mobile Phone Searches

Prior to Riley, lower courts justified warrantless mobile phone searches under a variety of preexisting “exceptions.” These exceptions were laid out in a trilogy of cases: Chimel v. California, United States v. Robinson, and Arizona v. Gant. In Chimel, the Court put forth two scenarios in which a warrantless search was valid: first, to protect a police officer by removing any weapons that the arrestee might use to effect an escape, and second, to prevent the destruction of evidence. In United States v. Robinson, the Court applied this framework to the physical search of an arrested individual. Upholding the search of a container found on a suspect during a custodial arrest, the Court held that a search of a container in the immediate vicinity of an arrestee was reasonable in all cases where there was probable cause for the arrest, even where the justifications developed in Chimel did not apply. Finally, in Arizona v. Gant, the Court extended Chimel and Robinson to permit warrantless searches of a suspect’s vehicle when it is seized as an instrumentality of an offense.

Taken together, the foregoing cases led lower courts to reject a number of defendant challenges to information obtained from warrantless cell phone searches, albeit under varying rationales. For example, in United States v. Finley, the Fifth Circuit applied the Robinson rationale that a mobile phone was

---

23 See Robinson, 414 U.S. at 235–36; see also New York v. Belton, 453 U.S. 454, 460 & n.4 (1981) (upholding a police officer’s search of any container—“any object capable of holding another object”—that was within a suspect’s reach at the time of arrest). Indeed, the Robinson container rule compelled some courts to permit searches incident to arrest, regardless of any reason to believe that evidence would be found. See Smallwood v. State, 61 So. 3d 448, 460 (Fla. Dist. Ct. App. 2011); Derek A. Scheurer, Are Courts Phoning It In? Resolving Problematic Reasoning in the Debate over Warrantless Searches of Cell Phones Incident to Arrest, 9 WASH. J.L. TECH. & ARTS 287, 303–04 (2014).
24 See Gant, 556 U.S. at 343. The Court permitted searches “only when the arrestee is unsecured and within reaching distance of the passenger compartment at the time of the search.” Id. This comports with the two Chimel concerns for officer safety and preventing destruction of evidence.
26 477 F.3d 250 (5th Cir. 2007).
nothing more than a container. Using that predigital analogue, a police officer had the right to inspect the phone’s contents—namely, the call history and text messages—during a search incident to arrest.27 The California Supreme Court utilized similar logic in People v. Diaz28 by refusing to distinguish between types of “containers” found on an arrestee’s person. The Diaz court thereby rejected a defendant’s motion to suppress text messages obtained from a warrantless search.29 In addition, in United States v. Flores-Lopez,30 the Seventh Circuit analogized a mobile phone to a diary within close proximity to the suspect’s person at the time of arrest. Therefore, the police’s cursory search of the telephone was reasonable and did not spark the need for a search warrant.31

B. Technology and the Fourth Amendment Leading up to Riley

The Riley Court’s eventual break from a long line of search-incident-to-arrest cases did not occur in a vacuum; rather, it followed from a line of cases in which the Supreme Court grappled with the rise of new technologies in light of the Fourth Amendment.32 In Kyllo v. United States,33 the Court ruled that

28 244 P.3d 501 (Cal. 2011).
29 See id. at 507.
30 670 F.3d 803 (7th Cir. 2012).
31 See id. at 807.
32 See Andrew Pincus, Evolving Technology and the Fourth Amendment: The Implications of Riley v. California, 2014 CATO SUP. CT. REV. 307, 311–20 (discussing the impact of three Supreme Court cases—Kyllo v. United States, 533 U.S. 27 (2001), United States v. Jones, 132 S. Ct. 945 (2012), and Maryland v. King, 133 S. Ct. 1958 (2013)—on the contours of the Riley decision). In fact, there were growing signs of resistance from lower courts and commentators over the significant latitude law enforcement officers had to comb through private data in mobile devices without a warrant. See, e.g., Flores-Lopez, 670 F.3d at 807 (noting that a phone may be akin to a “diary,” but that the extent of the police’s intrusion into stored private information may determine whether a warrant should have been issued); Hawkins, 704 S.E.2d at 891 (“Electronic ‘containers’ . . . often will contain the most sensitive kinds of personal information, in which individuals may reasonably have a substantial expectation of privacy and for which the law offers heightened protection.”). Notably, in 2013, the First Circuit categorically refused to permit warrantless smartphone searches due to privacy concerns. See United States v. Wurie, 728 F.3d 1, 13 (1st Cir. 2013). Wurie and the California Supreme Court’s denial of review in Riley v. California led to the Supreme Court’s granting of certiorari in Riley. See People v. Riley, No. D059840, 2013 WL 475242 (Cal. Ct. App. Feb. 8, 2013) cert. granted, 134 S. Ct. 999 (2014).
“[i]t would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology.”34 In finding the use of thermal imaging technology to find marijuana “grow lights” a form of property search, the Court emphasized that “[i]n the home . . . all details are intimate details.”35

In United States v. Jones,36 the Court grappled with police use of GPS tracking devices to locate suspects. Citing the Fourth Amendment’s history and language—the protection of “persons, houses, papers, and effects”37—the Court declared that the use of GPS tracking devices on vehicles constituted a search.38 Specifically, the Court reasoned, GPS tracking is a type of search that reveals detailed information about a target’s movements—a significant penetration into a person’s reasonable expectation of privacy.39 Therefore, a search warrant is required.40

In contrast, in Maryland v. King,41 the Court considered the privacy implications of using DNA technology as part of a routine booking procedure upon a suspect’s arrest. The Court observed that there are certain circumstances where there is a “diminish[ed] . . . need for a warrant,” either because of a heightened public interest42 or when “some reasonable police intrusion on [an individual’s] privacy is to be expected.”43 DNA evidence, like fingerprinting, only provides a more accurate means of identifying a suspect and does not reveal other types of personal information.44 Therefore, a warrant is not required.45

The preceding three cases present a common theme: to the extent that a particular investigative technique could reveal more information about a target than might originally be obtained in a reasonable search, Fourth Amendment warrant issues are triggered.

34 Id. at 33–34.
35 Id. at 37.
37 Id. at 950.
38 See id. at 953–54.
39 See id. at 964 (Alito, J., concurring); Pincus, supra note 32, at 317–18.
40 See Jones, 132 S. Ct. at 954; Pincus, supra note 32, at 316.
42 See id. at 1969 (citing Maryland v. Buie, 494 U.S. 325, 331 (1990)).
43 Id.
45 See King, 133 S. Ct. at 1980 (holding that “analyzing a cheek swab of the arrestee’s DNA is, like fingerprinting and photographing, a legitimate police booking procedure that is reasonable under the Fourth Amendment”).
C. The Contours Take Shape: Riley v. California’s Warrant Requirement

The Riley Court’s decision to strike down search-incident-to-arrest exceptions for smartphones was driven exclusively by concerns of overaccess to personal information. The Court considered, “on the one hand, the degree to which [the warrant exemption] intrudes upon an individual’s privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.”46 Acknowledging the Chimel-Robinson warrant exceptions, the Court refused to extend the physical search exceptions to digital data searches because “harm to officers and destruction of evidence—[factors] present in all custodial arrests”—have “no comparable risks when the search is of digital data.”47 Absent the risks present in a physical search, digital data privacy qualms remained in the balance.

The Court laid out three specific concerns that distinguished smartphones from any other kind of search previously contested before the Court. First, the Court considered how “[c]ell phones differ in both a quantitative and a qualitative sense from other objects” with their immense storage capacity and ability to contain personal data.48 Second, the Court noted that “a cell phone’s capacity allows even just one type of information to convey far more than previously possible” compared to a predigital analogue.49 Finally, the Court acknowledged the pervasiveness of mobile phone usage and how “a digital record of nearly every aspect of [individuals’] lives” is routinely on their person.50 The Court then recognized that such a digital record may include not just the data stored within the phone’s appli-

47 Id. at 2484–85. The Court distinguished the Robinson warrant exception for in-person container searches, noting that the “search of the information on a cell phone bears little resemblance to the type of brief physical search considered in Robinson.” Id. at 2485. The Court also rejected its container rationale in New York v. Belton by arguing that “the analogy crumbles entirely when a cell phone is used to access data located elsewhere, at the tap of a screen.” Id. at 2491 (citing New York v. Belton, 453 U.S. 454, 460 n.4 (1981)). However, the Court still recognized the Chimel concerns, noting that law enforcement officers could still perform a physical inspection of a mobile device to avoid physical harm. See id. at 2485. Nevertheless, the Court reasoned that the loss of digital evidence could be sufficiently precluded by securing the physical device, rendering warrantless data inspections unnecessary. See id. at 2486–87.
48 Riley, 134 S. Ct. at 2489.
49 Id.
50 Id. at 2490.
WHAT COMES AFTER “GET A WARRANT”

Balancing these considerations, the Court declared that “a cell phone search would typically expose to the government far more than the most exhaustive search” of any predigital analogue. The Court then rejected every compromise limitation set forth by the Government and amici to ensure “meaningful constraints” on law enforcement officers. However, despite its exhaustive contemplation of the myriad ways in which privacy interests may be harmed, the Court offered only two paragraphs to articulate its preferred result: obtaining a warrant. Therefore, the lengthy privacy interest discussion suggests the Court’s “simple” solution may not be so simple.

II
FINDING A BASELINE FOR WARRANT PARTICULARITY

A. Warrants: A Brief Background

The American “particularized” search warrant requirement was a response to colonial experiences with British “writs of assistance,” which permitted nearly limitless searches of colonists’ homes. The Fourth Amendment articulated a number of parameters governing search and seizure in an effort to limit

---

51 Id. By contemplating the mere assortment of apps as part of a user’s private information, the Court expanded privacy consideration to any inspection of a mobile phone forthright. Therefore, even viewing the telephone’s apps without accessing any information contained therein no longer would fit within the “plain view” exception for a search warrant. See Horton v. California, 496 U.S. 128, 141–42 (1990) (articulating the “plain view” exception to require that (1) the officer did not violate the Fourth Amendment in arriving at the same location as the evidence; (2) the incriminating character of the evidence is immediately apparent; and (3) the officer had lawful access to the object itself). For mobile devices, the first prong is now foreclosed.

52 Riley, 134 S. Ct. at 2491.

53 Id. at 2491–93. Among the proposals the Court rejected was an extension of Gant, such that the Government would be permitted to conduct a warrantless search of a cell phone when there was reason to believe it was the instrumentality of a criminal offense. See id. at 2492. The Court held that such a standard “would prove no practical limit at all when it comes to cell phone searches.” Id.

54 The Court’s slip opinion devoted seventeen pages to rejecting the search-incident-to-arrest exceptions, followed by eight pages discussing the various ways in which mobile phones contain extensive personal information too sensitive for warrantless review. See Riley v. California, Nos. 13-132 and 13-212, slip op. 17–25 (U.S. June 25, 2014).

55 Riley, 134 S. Ct. at 2493–95.

56 Id. at 2495.

the federal government’s ability to intrude into one’s home. Specifically, the Fourth Amendment declares that:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Indeed, the Supreme Court historically expressed a strong preference for law enforcement to err in favor of obtaining a warrant. The Court’s preference is derived from the orderly procedure afforded by the warrant process, whereby a magistrate must make an isolated, deliberate determination to find probable cause. Proceeding via magistrate review would theoretically better protect targets’ property and privacy rights than the hurried approach that law enforcement officers take as they conduct the search.

The warrant application process is comparable at both the federal and state levels. Typically, the Government completes a standard form and attaches an affidavit describing the nature of the Government’s search. The warrant must be “particularly describing the place to be searched, and the persons or things to be seized.”

---

58 See Olmstead v. United States, 277 U.S. 438, 465–66 (1928). The Supreme Court subsequently ruled that the Fourth Amendment applied to states through the incorporation doctrine. See Wolf v. Colorado, 338 U.S. 25, 27–28 (1949). Later, the Supreme Court shifted its property-based analysis to a privacy-based analysis, thus interpreting the Fourth Amendment to protect an individual’s reasonable expectation of privacy. See Katz v. United States, 389 U.S. 347, 353 (1967); Zamani, supra note 15, at 174. United States v. Jones, 132 S. Ct. 945 (2012), is the Court’s most recent reminder that Fourth Amendment privacy rights extend to all reasonable expectations of privacy, whether at home or on one’s person or property. See id. at 953–54.

59 U.S. Const. amend. IV.

60 See United States v. Ventresca, 380 U.S. 102, 106 (1965) (holding that in “doubtful or marginal case[s] a search under a warrant may be sustainable where without one it would fail”).


62 See id. (citing Aguilar, 378 U.S. at 110–11).


64 See, e.g., United States v. Lustyik, 57 F. Supp. 3d 213, 218–19 (S.D.N.Y. 2014) (describing the government’s warrant application, consisting of a form and two attachments); see also Marron v. United States, 275 U.S. 192, 196 (1927) (“The requirement that warrants shall particularly describe the things to be seized

---
larized” in that it identifies (1) the place to be searched (frequently “Attachment A”) and (2) the items to be seized, as well as any probable cause to substantiate the purpose for seizing the requested items (frequently “Attachment B”).65 The “probable cause” requirement is fairly broad, requiring only that the items to be seized must be readily identifiable with a particular criminal endeavor and that, at the time of the warrant’s execution, such objects are at the location identified.66

In 2009, the Judicial Conference of the United States adopted a number of amendments to the warrant application process to account for the rise in forensic computer searches.67 Federal Rule of Criminal Procedure 41 now articulates a “two-stage process,” which allows for the physical seizure of the electronic device and then a subsequent copying and analysis of the data “consistent with the warrant.”68 Nevertheless, the new rule remains broad in deference to the practical difficulties that could arise during forensic analysis.69 Indeed, the Committee Notes concede that “[t]he amended rule does not address the specificity of description that the Fourth Amendment may require in a warrant for electronically stored information, leaving the application of this and other constitutional standards concerning both the seizure and the search to ongoing case law makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another.”).

65 See, e.g., Lustyik 57 F. Supp. 3d at 219; see also Orin S. Kerr, Search Warrants in an Era of Digital Evidence, 75 Miss. L.J. 85, 90 (2005) [hereinafter Kerr, Digital Evidence] (“In physical searches, the investigators seek permission to look through a particular physical space for a particular piece of evidence, and then to take that evidence away.”)

66 See 2 LaFave, supra note 61, § 3.7; see also Illinois v. Gates, 462 U.S. 213, 230–31 (1983) (“This totality-of-the-circumstances approach is far more consistent with [the Court’s] treatment of probable cause than is any rigid demand that specific ‘tests’ be satisfied . . . .”); United States v. Cortez, 449 U.S. 411, 418 (1981) (“The process does not deal with hard certainties, but with probabilities . . . . [T]he evidence thus collected must be seen and weighed not in terms of library analysis by scholars, but as understood by those versed in the field of law enforcement.”).


68 H.R. Doc. No. 111-30 at 44.

69 See id. at 55 (“In light of the enormous quantities of information that are often involved, as well as the difficulties often encountered involving encryption and booby traps, it is impractical to set a definite time period during which the offsite review must be completed. The Committee Note emphasizes, however, that the court may impose a deadline for the return of the medium or access to the electronically stored information.”).
development." As such, enhanced particularity requirements for mobile devices must either be derived by analogy from pre-existing case law or be independently developed.

B. The Computer Analogy

One way to approach warrant particularity for mobile devices is to simply adopt the courts’ approaches to computer search warrants. After all, a number of courts analogize smartphones to computers. Predictably, there are significant parallels between how courts first addressed computer searches in the late 1990s and early 2000s and how they addressed cell phone searches less than ten years later. For example, in People v. Gall, the Colorado Supreme Court held that computers are “reasonably likely to serve as ‘containers’ for writings, or the functional equivalent of ‘written or printed material.’” And yet, as with mobile phones today, courts in the late 1990s and early 2000s increasingly expressed concern about the ubiquity of computers and the breadth of their storage capacity.

Unfortunately, computer search jurisprudence remains an unsettled area of the law. Computer search authorizations are doctrinally and practically difficult because digital evidence

---

70 FED. R. CRIM. P. 41 advisory Committee Notes to 2009 amendment.
71 See, e.g., United States v. Wurie, 728 F.3d 1, 8 (1st Cir. 2013) ("[A] modern cell phone is a computer . . . . " (quoting United States v. Flores-Lopez, 670 F.3d 803, 805 (2012))); United States v. Horton, No. 12-228, 2013 WL 3833250, at *2 (E.D. Pa. July 25, 2013) ("Given the functional similarities between a cell phone and a computer, it may be reasonable to refer to a cell phone’s circuit board and other internal parts as ‘computer’ hardware.").
73 30 P.3d 145 (Colo. 2001).
74 Id. at 153; see also Thomas K. Clancy, The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer, 75 Miss. L.J. 193, 196 (2005) ("One view asserts that a computer is a form of a container and that the data in electronic storage are mere forms of documents. . . . This article concludes that [this] first view is correct; computers are containers.").
75 Compare Riley v. California, 134 S. Ct. 2473, 2489 (2014) ("One of the most notable distinguishing features of modern cell phones is their immense storage capacity."), with United States v. Carey, 172 F.3d 1268, 1275 (10th Cir. 1999) ("[A]nalogy to closed containers or file cabinets may lead courts to ‘oversimplify a complex area of Fourth Amendment doctrines and ignore the realities of massive modern computer storage.’" (quoting Raphael Winick, Searches and Seizures of Computers and Computer Data, 8 HARV. J.L. & TECH. 75, 104 (1994))); see also Trepel, supra note 72, at 130 (describing courts’ reactions to developing technology and growing storage capacity).
76 Interestingly, a significant driving factor in developing computer search jurisprudence has been its application in child pornography cases. See Clancy,
of criminal activity could commonly be mislabeled and hidden, making searches more burdensome than a traditional physical search.\textsuperscript{77} In light of the fact that “criminals can—and often do—hide, mislabel, or manipulate files to conceal criminal activity, a broad, expansive search of the hard drive may be required.”\textsuperscript{78} By the same token, “granting the Government a \textit{carte blanche} to search \textit{every} file on the hard drive” can lead to an impermissibly general search.\textsuperscript{79} Courts have struggled to balance these competing interests.

Courts erring in favor of privacy interests focus on the inherent risk of overly intrusive searches when dealing with the vast storage capacity of modern computers. These courts advocate for tighter controls to limit the extent to which law enforcement can review personal digital data. The Tenth Circuit offered one possible limitation in \textit{United States v. Carey}\textsuperscript{80} by extending the “intermingled document” doctrine to computer searches.\textsuperscript{81} Adapted from a case involving large quantities of physical files,\textsuperscript{82} the intermingled document doctrine requires investigators to “engage in the intermediate step of sorting various types of documents and then only search the ones specified in a warrant.”\textsuperscript{83} If the volume of information is too great to sort on-site, then officers may hold the documents “pending approval by a magistrate of the conditions and limitations on a further search through the documents.”\textsuperscript{84}

\textsuperscript{77} \textit{See}, e.g., \\textit{United States v. Karrer}, 460 F. App’x 157, 162 (3d Cir. 2012) (“\textit{Given the nature of computer files and the tendency of criminal offenders to mislabel, hide, and attempt to delete evidence of their crimes, it would be impossible to identify \textit{ex ante} the precise files, file types, programs and devices that would house the suspected evidence.}”).

\textsuperscript{78} \textit{United States v. Stabile}, 633 F.3d 219, 237 (3d Cir. 2011).

\textsuperscript{79} \textit{Id.} (citing Marron v. \textit{United States}, 275 U.S. 192, 196 (1927)).

\textsuperscript{80} 172 F.3d 1268 (10th Cir. 1999).

\textsuperscript{81} \textit{See id.} at 1275.

\textsuperscript{82} \textit{See United States v. Tamura}, 694 F.2d 591 (9th Cir. 1982).

\textsuperscript{83} \textit{Carey}, 172 F.3d at 1275.

\textsuperscript{84} \textit{Id.} Of course, investigators rarely sort computer files on-site; instead, they usually seize the entire computer and separate the files in a forensic laboratory. \textit{See Kerr, Digital Evidence, supra note 65, at 87.}
In Carey, law enforcement officers were conducting a computer search for evidence of drug trafficking. Their warrant authorized a search for "files on the computers for names, telephone numbers, ledger receipts, addresses, and other documentary evidence pertaining to the sale and distribution of controlled substances." During the course of their investigation, the examiners discovered images of child pornography. Without obtaining a second warrant, the officers searched for more child pornography files. After extending the intermingled document doctrine, the Tenth Circuit held that the lower court erred in refusing to grant the defendant’s suppression motion for the child porn files retrieved by police after they recovered the first, inadvertently discovered image. The court ruled that the police failed to either employ document segregation methods to limit their search for drug evidence or request magistrate review for an additional warrant for the pornographic images. Instead, the police sorted the documents and then conducted “an unconstitutional general search.”

Chief Judge Alex Kozinski offered an alternative approach to limiting law enforcement’s digital search-and-seizure discretion in United States v. Comprehensive Drug Testing, Inc. (CDT III). In a concurring opinion, Chief Judge Kozinski recommended a number of guidelines to limit police access to private information. Most notable was his preference for “a protocol for preventing agents involved in the investigation from examining or retaining any data other than that for which probable

---

85 See Carey, 172 F.3d at 1270.
86 Id.
87 See id. at 1271.
88 See id. at 1276.
89 See id.
90 Id.
91 621 F.3d 1162 (9th Cir. 2010) (en banc) (per curiam). Chief Judge Kozinski’s opinion actually served as the majority opinion—and was thus binding in the Ninth Circuit—in United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989 (9th Cir. 2009) [hereinafter CDT III] revised and superseded by CDT III, 621 F.3d 1162. However, Chief Judge Kozinski lost his majority in the subsequent CDT III en banc rehearing, relegating his approach to an advisory role. See Paul Ohm, Massive Hard Drives, General Warrants, and the Power of Magistrate Judges, 97 VA. L. REV. BRIEF 1, 3 n.9 (2011).
92 See CDT III, 621 F.3d at 1178 (Kozinski, C.J., concurring). Chief Judge Kozinski’s guidelines acknowledge that overseizure of digital data is inevitable but that the government must concede certain liberties in return, such as forsaking reliance “on any . . . doctrine that would allow retention of data obtained only because the government was required to segregate seizable from non-seizable data.” Id.
cause is shown."93 Having a search protocol in a warrant application would afford magistrate judges an ex ante opportunity to review the police’s intended approach to avoid overzealous of evidence.94

While many courts acknowledge both of the foregoing approaches, most courts have settled for a generally permissive attitude towards computer search warrants.95 Faced with voluminous digital storage and easily masked data files, many judges construe broadly termed search warrants as a practical approach to a complex problem.96 The primary limiting principle is that the search authorization be particularized to a specific offense, with probable cause substantiating the sought-for items’ connections to the alleged offense.97 For example, in United States v. Richards98 the Sixth Circuit addressed a criminal appeal where the defendant alleged that the police executed an overly broad search warrant. The Sixth Circuit affirmed the conviction and approved the investigator’s expanded search, holding that “[t]he degree of specificity required [in a warrant] is flexible and will vary depending on the crime involved and the types of items sought.”99 This flexibility re-

93 Id. at 1179. Under Chief Judge Kozinski’s parameters, the search protocol would be the judicially enforceable outer bounds of the search methods investigators may apply. Any deviations or modifications would require judicial authorization. See id.

94 See id. at 1178.

95 See, e.g., United States v. Schesso, 730 F.3d 1040, 1050 (9th Cir. 2013) ("Although we conclude that the exercise of 'greater vigilance' did not require invoking the CDT III search protocols . . . judges may consider such protocols or a variation on those protocols as appropriate in electronic searches."); United States v. Stabile, 633 F.3d 219, 238–39 (3d Cir. 2011) (acknowledging that search protocols can limit the danger of a general warrant but refusing to require such a search protocol); Ohm, supra note 91, at 11 ("Computer search warrants are the closest things to general warrants we have confronted in the history of the Republic.").

96 See Stabile, 633 F.3d at 239; United States v. Mann, 592 F.3d 779, 783–85 (7th Cir. 2010) (rejecting the suggestion to use CDT III’s “more comprehensive rules regarding computer searches” because of the intricacies of computer searches); Trepel, supra note 72, at 134–36.

97 See, e.g., United States v. Karrer, 460 F. App’x 157, 162 (3d Cir. 2012) (holding a warrant not "overbroad simply because the devices and files it authorized to be searched and seized were likely to include materials unrelated to [the specified offense]"); United States v. Welch, 291 F. App’x 193, 198–99, 201 (10th Cir. 2008) (requiring a “totality of the circumstances” approach to assessing the fair probability that a search would yield evidence pertaining to a specific criminal offense but granting deference to magistrate judges and law enforcement officers to make probable cause determinations even when warrants are poorly drafted (quoting United States v. Tisdale, 248 F.3d 964, 970 (10th Cir. 2001))).

98 659 F.3d 527 (6th Cir. 2011).

99 Id. at 537 (quoting United States v. Greene, 250 F.3d 471, 477 (6th Cir. 2001)).
flects “the unique problem encountered in computer searches, and the practical difficulties inherent in implementing universal search methodologies.”

Adopting the Tenth Circuit’s reasoning in United States v. Burgess, the Sixth Circuit emphasized the unique difficulties of conducting digital searches compared to physical searches. Quoting Burgess, the Sixth Circuit noted that “[a]s the description of such places and things [in a computer search warrant] becomes more general, the method by which the search is executed become[s] more important . . . .” Therefore, the Sixth Circuit held, the focus shifts from ex ante scrutiny of the warrant’s language to an ex post reasonableness assessment of how law enforcement officers executed the search.

Similarly, many courts are sympathetic to the burdens that forensic examiners face in parsing through a large volume of data and are lenient when the physical process an investigator employs reasonably extends beyond the warrant’s scope. In United States v. Stabile, the Third Circuit upheld a forensic examiner’s broad search of the defendant’s hard drive for financial information that revealed a cache of child pornography. In this case, the police executed a computer search warrant looking for evidence of financial crimes. But in the process of conducting the search, the forensic examiner flagged and reviewed a folder marked “Kazvid,” which actually contained child pornography.

---

100 Id. at 538.
101 576 F.3d 1078 (10th Cir. 2009).
102 See Richards, 659 F.3d at 538–39. The concerns outlined by the court—namely, purposefully mislabeled files hidden in a large volume of data—are outlined above.
103 Id. at 539 (third alteration in original) (quoting Burgess, 576 F.3d at 1094).
104 See id. at 540 (“In other words, in general, ‘[s]o long as the computer search is limited to a search for evidence explicitly authorized in the warrant, it is reasonable for the executing officers to open the various types of files located in the computer’s hard drive in order to determine whether they contain such evidence.’” (alteration in original) (quoting United States v. Roberts, No. 3:08-CR-175, 2010 WL 234719, at *15 (E.D. Tenn. Jan. 14, 2010))).
105 633 F.3d 219 (3d Cir. 2011).
106 See id. at 227, 231–32.
107 See id. at 226–27. At trial, the investigator testified that “he highlighted the Kazvid folder not because it necessarily contained child pornography but because—as a suspicious folder—it could harbor evidence of any sort of crime, including a financial crime.” Id. at 227. Here, unlike the detectives in United States v. Carey, 172 F.3d 1268 (10th Cir. 1999), after the Stabile examiners discovered the initial folder containing child pornography, they halted their search for additional folders until they obtained a new warrant. Stabile, 633 F.3d at 227–28.
203 WHAT COMES AFTER “GET A WARRANT”

The Third Circuit acknowledged that the search’s results exceeded the bounds of the warrant, conceding that “it is certain that some innocuous documents will be examined” to determine if they fell within the warrant’s scope.108 But the court decided the search was “objectively reasonable because criminals can easily alter file names and file extensions to conceal contraband.”109 Specifically, the Third Circuit noted that the detective “took steps to ensure that his investigation complied with the state search warrant” and that “he examined suspicious and out-of-place folders” based on his experience that files—including those relating to financial crimes—could be hidden anywhere.110 Therefore, the “procedures demonstrate that [the examiner] engaged in a focused search of the hard drives rather than a general search.”111

The inherent difficulties arising in the foregoing cases are what drive most courts to outright reject the required use of search protocols.112 The oft-quoted passage from United States v. Burgess—that it is “folly for a search warrant to attempt to structure the mechanics of the search” because “imposing such limits would unduly restrict legitimate search objectives”113—underlies the courts’ desire to remain forgiving to law enforcement needs. Therefore, for computer searches, an ex post reasonableness review of the search appears to have the greatest traction in the courts.114

108 Id. at 234 (quoting United States v. Williams, 592 F.3d 511, 519–20 (4th Cir. 2010)).
109 Id. at 239; see also United States v. Banks, 556 F.3d 967, 973 (9th Cir. 2009) (holding that a general seizure of “documents may be justified” if it is demonstrated that “the government could not reasonably segregate...documents on the basis of whether or not they were likely to evidence criminal activity” (quoting United States v. Kow, 58 F.3d 423, 427–28 (9th Cir. 1995))).
110 Stabile, 633 F.3d at 239.
111 Id. at 239–40.
112 See, e.g., id. at 238–39 (rejecting search protocols as “folly” (quoting United States v. Burgess, 576 F.3d 1078, 1094 (10th Cir. 2009))).
113 Burgess, 576 F.3d at 1094; see also Kerr, Searches and Seizures, supra note 27, at 575 (“In light of [computer search] difficulties, magistrate judges are poorly equipped to evaluate whether a particular search protocol is the fastest and most targeted way of locating evidence stored on a hard drive. Given the contingent nature of the process, even a skilled forensic expert cannot predict exactly what techniques will be necessary to find the information sought by the warrant.”).
114 See, e.g., United States v. Gagnis, 755 F.3d 125, 136–37 (2d Cir. 2014) (arguing that “[t]he better approach is to reform rules regulating the admissibility of evidence ex post”).
C. The Computer Analogy Is Not a Good Fit for Mobile Devices

If the courts focus on practical reasons to justify latitude in computer search warrants, then the computer analogy cannot be entirely transposed to mobile devices for two reasons: (1) there are different forensic steps involved with mobile device searches compared to computer searches and (2) mobile phones are functionally different from computers.

1. Distinguishing Mobile Device Forensics from Computer Forensics

The differences in the traditional computer market versus the mobile device market have different implications for forensic examiners charged with searching the devices. Specifically, in PC-based forensics, the norm is to physically remove the hard drive from the computer, make and verify a mirror image of it, then subsequently analyze the mirrored content. The fact that there are two predominant operating systems—Windows and Mac OS—that make software development easy and predictable furthers the norm.

However, with mobile devices, the paradigm is very different for multiple reasons. First, data acquisition methods vary based upon the information sought, the proprietary nature of device hardware, and the device software. Moreover, there are different kinds of forensic software due to the large number of operating systems and different types of mobile phone technology in the market. Indeed, as a subcategory of the different device operating systems, the actual variant of the mobile device’s operating system may be proprietarily modified. As

---

tation/PublicationAttachment/ef4a28ad-f7d-4014-a8e8-80505789b86c/Mobile
cc/YBK6-Y8KL].
116 See id.
117 See id.
119 See id. at 5 (listing Apple’s iOS, Google’s Android, RIM’s BlackBerry OS, and Microsoft’s Windows Mobile as the predominant mobile operating systems currently on the market).
120 See id. at 43 (“Each one of the different versions of the [Android] operating system requires slight modifications for each family of device for full support. This has led to hundreds (if not thousands) of different distributions in the wild.”):
a result, mobile device forensics can be more difficult than searching a traditional computer, with different implications for how data is extracted.

The complications are captured in the National Institute of Standards and Technology’s (NIST) Guidelines on Mobile Device Forensics. The NIST Guidelines note that “examiners typically assemble a collection of both forensic and non-forensic tools for their toolkit.” This “collection” of tools reflects the dynamic nature of the mobile device market—there are constant updates and, therefore, different tools are capable of extracting only certain types of data. The NIST Guidelines proceed to classify various data extraction tools on a scale of Level 1 through Level 5, with each level becoming progressively “more technical, invasive, time consuming, and expensive.” To further add complication, “once a level is used, alternate levels may not be possible. . . . With each methodology, data may be permanently destroyed or modified if a given tool or procedure is not properly utilized.”

Level 1, Manual Extraction, involves essentially reading the information directly off of the device’s screen. It is the least invasive method of analysis. Level 2, Logical Extraction, requires connecting the mobile device to a forensics workstation and then manually extracting certain information by entering computer commands into the workstation. This yields more information but is more invasive than a Manual Extraction. Similar to computers, the most common form of data extraction and analysis for mobile devices involves “imaging”—copying—the device’s contents onto a virtual workspace. The NIST Guidelines categorize imaging at Levels 3 and 4, the two.


NIST is a nonregulatory federal agency within the United States Department of Commerce. It is responsible for “advancing measurement science, standards, and technology in ways that enhance economic security” for the United States. See NIST General Information, NIST: PUB. AFF. OFF., http://www.nist.gov/public_affairs/general_information.cfm [http://perma.cc/Q8VN-W6XU].

121 NIST GUIDELINES, supra note 118, at 15.

See id.

122 Id. However, the NIST Guidelines note that Level 5, a “Micro Read,” is primarily theoretical in nature and is not utilized by any American law enforcement agency. Therefore, there practically are only four different levels of forensic analysis. Id. at 19–20.

123 See id. at 16.

124 See id. at 17.

125 See id.
most practically invasive data extraction levels.\textsuperscript{128} Level 3, Hex Dumping/Joint Test Action Group, is where the forensic analyst would use a “flasher box” to copy the memory contents of a device onto a computer.\textsuperscript{129} Subsequently, the computer would decode and recreate the various data levels of the phone’s memory in the computer for analysis.\textsuperscript{130} There are risks that there may be decoding issues, and it is entirely dependent on the software and hardware the analyst uses.\textsuperscript{131} Level 4 is termed a “Chip-Off.”\textsuperscript{132} This requires physically removing the flash memory, which is then converted into a binary image for analysis. Chip-Offs are the most invasive method of analysis and yield the most information from the device.\textsuperscript{133}

But demonstrative of the variance in mobile device forensic tools, there are no fewer than five available software packages to accomplish each layer of analysis, from Level 1 through 4.\textsuperscript{134} However, each available software package, despite purporting to accomplish different layers of data extraction analysis, has different capabilities. Therefore, what the forensic examiner can actually do (or how tailored the data extraction may be) is likely hamstrung by which software package the laboratory decided to purchase.\textsuperscript{135} Moreover, the Guidelines note that “not all relevant data viewable on a mobile device using the available menus may be acquired and decoded through a logical acquisition.”\textsuperscript{136} This means that a forensic examiner may be forced to manually go through the device for any pertinent information, despite having software-based search capabilities. Finally, because mobile devices have short product cycles, each of the varied-capability forensic software packages runs the risk of quickly being outdated.\textsuperscript{137}

\textsuperscript{128} See id. at 17–19.  
\textsuperscript{129} See id. at 18.  
\textsuperscript{130} See id. at 16.  
\textsuperscript{131} See id. at 18.  
\textsuperscript{132} See id. at 19.  
\textsuperscript{133} See id.  
\textsuperscript{134} See id. at 21–23 tbl.3. The NIST Guidelines identify five available software packages for Level 1, thirty programs capable of a Level 2 analysis, twelve available for Level 3, and seven available for Level 4.  
\textsuperscript{135} See id. at 25.  
\textsuperscript{136} Id. at 41.  
\textsuperscript{137} Even still, the Guidelines acknowledge that, “[on occasion, updates or new versions of a tool were also found to be less capable in some aspects than a previous version was.” Id. at 25 (citation omitted).
2. Mobile Phones Are Functionally Different from Computers

In addition to distinguishable forensic techniques between mobile phones and computers, the burdens associated with computer searches—namely, the ability to mask file names—are qualitatively different on a mobile device. As previously discussed, one of the biggest concerns in a traditional computer search is that potentially incriminating evidence may be masked by an innocuous file name or by modifying the file extension. But file names and extensions are not so easily modified on a mobile device, because mobile operating systems are designed for ease of use and do not emphasize user-directed file organization.

For example, on Apple’s iOS and Google’s Android operating systems, file name modifications require special third-party software that actually display the device’s file directory. And even if that software is installed, the ability to move files from one application to another is limited by the operating system’s design structure. Moreover, a number of forensic examination programs now search for file types based on a file signature database, rather than file extension. In doing so, the

---

138 See, e.g., United States v. Karrer, 460 F. App’x 157, 162 (3d Cir. 2012) (“[G]iven the nature of computer files and the tendency of criminal offenders to mislabel, hide, and attempt to delete evidence of their crimes, it would be impossible to identify ex ante the precise files, file types, programs and devices that would house the suspected evidence.”); Trepel, supra note 72, at 135 (“Not only can [perpetrators] give files innocuous sounding titles (for example ‘Johnny’s Science Fair Project’ lacks the malevolent ring of ‘SexyTeenPics’), but suspects with something to hide can also easily change the extensions under which files are saved.”).

139 See, e.g., Donovan Colbert, Which is the Superior Mobile OS: iOS, Android, or Windows 8?, TECHREPUBLIC (Jan. 11, 2013, 3:06 AM), http://www.techrepublic.com/blog/tablets-in-the-enterprise/which-is-the-superior-mobile-os-ios-android-or-windows-8/ [http://perma.cc/9QZW-USSW] (discussing three prominent mobile operating systems emphasizing simplicity of use). However, the Android operating system is acknowledged to permit greater user-directed organization but still not to the extent of a traditional computer. See id.


142 See NIST GUIDELINES, supra note 118, at 52.
software “eliminates the possibility of missing data because of an inconsistent [e.g., user-modified,] file name extension.”\footnote{143} Indeed, the same software may “find and gather images automatically into a common graphics library for examination,” thus eliminating the possibility of files being hidden.\footnote{144} Therefore, the same kind of flexibility afforded for computer searches because of hidden or mislabeled files is not directly applicable to mobile phone searches.

3. In Short: Mobile Device Searches Are Distinct from Computer Searches

The takeaway is that mobile devices have greater data extraction volatility and limitations but have fewer actual data locations and content variables than traditional computer searches. Because of the perpetual changes in mobile product offerings, forensic software is slow to catch up and the actual capabilities of the available forensic software vary greatly. Practically speaking, what a forensic laboratory can do is constrained by its software budget. Therefore, the lab’s precision in extracting data likely requires greater planning in order to ensure no pertinent data is lost, within the constraints of the warrant. Even still, the software limitations may necessitate overseizing data simply because the tools available provide no other recourse.

By the same token, once the data is actually extracted, there are fewer mysteries in terms of file labeling or extracting certain types of files. As an added bonus, the storage volume on a mobile device is generally less than that of a computer. Therefore, with sufficient experience, it is conceivable that law enforcement officers can articulate a process by which they intend to search a device. However, imposing or predetermining constraints on \textit{where} forensic examiners may search could prove overly limiting, given the data extraction capabilities that they may have.

III
CURRENT APPROACHES TO PARTICULARITY AND A PATH FORWARD

Mobile devices’ distinguishing characteristics bring the discussion back to the original problem: What standard of particularity should apply to mobile phone search warrants? For

\footnote{143}{\textit{id.}}\footnote{144}{\textit{id.}}
now, judges and academics answer this question in conflicting ways. Nevertheless, in light of the Supreme Court’s extended discussion over privacy interests, it seems inevitable that the law will trend toward greater rigor in digital search warrant particularity. The question is what form that increased particularity requirement will take.

Currently, the particularity debate appears to occur on two different planes. The first plane deals with the level of particularity that lower courts appear to demand. Some courts gloss over defectively broad search warrants in order to preserve the fruits of the search.\textsuperscript{145} Others reject search warrant applications for technical flaws and require substantial information prior to authorizing a search.\textsuperscript{146} The second plane addresses how search warrant particularity is achieved. There are currently two approaches to doing so: the first is a search protocol that emphasizes how a search will be conducted; the second focuses on a protocol identifying where on a device incriminating data will be sought.

The varied approaches across different jurisdictions will likely require reconciliation post-\textit{Riley}. As such, this Note argues that an ex ante search protocol detailing the Government’s search methodology is beneficial for all parties involved. Such a requirement is easily reconcilable with the limited resources available to forensic examiners while also protecting individuals’ Fourth Amendment privacy rights. However, such a search protocol cannot practically specify where on a device incriminating evidence will be found, and to require that information before the search is even conducted would unduly hamper law enforcement officials.

A. Conflicts in Particularity Deference Among the Lower Courts

Following \textit{Riley}, all courts require search warrants prior to the police searching a mobile device, but the stringency of the warrant language varies. Lower courts are currently divided between affording police “reasonableness” deference versus mandating comprehensive search protocols in mobile device

\textsuperscript{145} See, e.g., \textit{United States v. Horton}, No. 12-228, 2013 WL 3833250, at *3 (E.D. Pa. July 25, 2013) (noting that the "language of the warrant used to seize Horton’s cell phone, though less clear, sufficiently permitted that seizure").

\textsuperscript{146} See, e.g., \textit{In re Search of Black iPhone 4}, 27 F. Supp. 3d 74, 78–80 (D.D.C. 2014) (rejecting a search warrant application for not clearly articulating an intended search procedure, but noting the absence of a search protocol requirement in the case law and "concerns about hamstringing a valid criminal investigation by binding the government to a strict search protocol ex ante").
search warrants. This debate reflects the same tensions arising from computer search cases. But unlike in computer search cases, a number of courts appear willing to preemptively restrict law enforcement access to data rather than wait for a suppression hearing.

1. “Reasonableness” Deference and Its Problems

Courts generally adopting “reasonableness” deference employ similar logic as that used in computer search cases. They do so by granting significant leeway in warrant terminology in order to preserve the fruits of the search. For example, in United States v. Horton, the court read the term “computer” in a search warrant application to include a Motorola smartphone when denying the defendant’s motion to suppress evidence of child pornography. In Horton, the defendant was served with a warrant permitting officers to search for and seize “[a]ll computer hardware, including, but not limited to, any equipment which can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical or similar computer impulses or data.” The warrant also authorized officers to seize any “internal and peripheral storage devices” associated with the computer. Denying the motion, the court opined that “the warrant could have more clearly articulated that it covered cell phones” by identifying them as additional items subject to search and seizure. Nevertheless, the court ruled that the “language of the warrant used to seize Horton’s cell phone, though less clear, sufficiently permitted that seizure.”

Similarly, in Hedgepath v. Commonwealth, the defendant challenged the particularity of a warrant used to search his phone. The defendant was called to the local police station for questioning after the assault and death of his girlfriend. He was arrested, and the police searched his car the following day, under a search warrant that authorized the

---

148 Id. at *1 [alteration in original].
149 Id.
150 Id. at *3. The court cited the Third Circuit’s opinion in United States v. Karrer, 460 F. App’x 157 (3d Cir. 2012), as an example of a more detailed search warrant.
151 Id.
152 441 S.W.3d 119 (Ky. 2014).
153 See id. at 130.
154 See id. at 122.
seizure of “any and all items that may have been used to aid in the assault” without additional particularity. The police seized his smartphone, and although the warrant did not specify a search for any digital content, they searched the phone for evidence of the victim’s assault. The search revealed ten graphic, incriminating videos of the defendant sexually assaulting and abusing the victim.

The Kentucky Supreme Court rejected the defendant’s motion to suppress the digital evidence. The court acknowledged that “the warrant did not limit the parts of the cell phone that could be searched, or the types of files or data that were to be sought.” But it held that the “clear thrust of the warrant” governed the police’s search. For this court, it was sufficient that the warrant identified the cell phone itself, and not any of the phone’s content.

What is striking about Horton and Hedgepath is that each court acknowledges defects in the mobile device search warrants but makes a concerted effort to gloss over the flaws in order to uphold the collected data. This is where the risk of an ex post review of the warrant becomes problematic: the evidence collected may prove too crucial to uphold the conviction of a dangerous defendant. In contrast, had there been a more stringent review mechanism prior to the data collection, then the courts’ strained arguments would prove unnecessary. Indeed, even though the evidence against the defendants in Horton and Hedgepath was collected pursuant to warrants, it is

---

155 Id. at 126–27, 130. The warrant authorized seizure of “any and all items that may have been used to aid in the assault . . . [and a search of] any and all places in size where any of the above described personal property may be stored, hidden, and/or concealed. Also all personal property including but not limited to all electronic equipment, computers, and cell phones.” See id. at 130.
156 See id. at 122–23, 130–31.
157 See id. at 122–23.
158 See id. at 131.
159 Id. at 130.
160 Id.
161 See id. (“And the simple fact is that the police in this case had a search warrant that specifically included Hedgepath’s cell phone as an item to be seized in a search of his apartment and vehicle. This was not a warrantless search of the sort condemned in Riley.” (citations omitted)).
162 Indeed, the facts of both Horton and Hedgepath suggest that courts may hesitate to condemn defective search warrants in light of the evidence obtained to convict particularly egregious perpetrators. Cf. Trepel, supra note 72, at 136 (“Unfortunately, the particularly distasteful nature of [the cases in question] may unconsciously influence decision makers . . . to believe that stronger protections against general computer searches are unnecessary.”).
doubtful that the warrants’ broad language would pass muster under the privacy concerns articulated in *Riley*.163

2. Approaches to Enhanced Warrant Particularity

In contrast, a number of courts now demand greater search warrant particularity at the outset in order to control police searches. For example, in *State v. Henderson*,164 the Nebraska Supreme Court held that a warrant “satisfies the particularity requirement if it leaves nothing about its scope to the discretion of the officer serving it.”165 In *Henderson*, the Nebraska Supreme Court declined to comment upon whether “a court issuing a warrant has the authority to—or should—set forth a protocol specifying how the search of digital data should be conducted.”166

But a mandatory search-protocol regime has its advocates. One of the most notable proponents is U.S. Magistrate Judge John Facciola, sitting in the United States District Court for the District of Columbia. In a series of three decisions—*In re Search of Black iPhone 4*,167 *In re Search of ODYS LOOX Plus Tablet*,168 and *In re Search of Apple iPhone, IMEI 013888003738427*169 (collectively, the “D.C. Opinions”)—Judge Facciola laid out a number of particularity concerns and a rectifying protocol framework that a number of other judges have cited.170 Considering the genesis of the D.C. Opinions’ protocol framework helps elucidate a workable process that the Government can use to increase warrant particularity and reduce the risk of losing valuable evidence at a later suppression hearing.

In *In re Search of Black iPhone 4*, the Government submitted six search-and-seizure applications for various devices for

---

163 See *Riley v. California*, 134 S. Ct. 2473, 2489 (2014) (cautioning that a “phone’s capacity allows even just one type of information to convey far more than previously possible”).

164 854 N.W.2d 616 (Neb. 2014).

165 Id. at 633 (citing *United States v. Clark*, 754 F.3d 401, 410 (7th Cir. 2014)).

166 Id. at 633.


2015] WHAT COMES AFTER “GET A WARRANT” 213

evidence of child pornography. The warrant applications incorporated the traditional Attachment A, which describes the device to be searched, and Attachment B, which lists the files or data to be seized. In this case, Attachment A identified three mobile phones and three hard drives. However, a generalized Attachment B was used to describe the types of files sought from all the devices. Put differently, each application’s Attachment B identified files specific to mobile phones and not hard drives.

The court denied the warrant applications for several reasons. But beyond the “wrong” Attachment Bs, the court’s primary concern was that the Government sought data for which there was no probable cause. Indeed, the court charged that the government apparently seeks to seize the entirety of these phones, including all communications, regardless of whether they bear any relevance whatsoever to this investigation. If this were not the intention, then Attachment B would not begin by saying that the government wishes to seize “[a]ll records . . . including . . .”; by using the term “including,” the Applications make the seizure list broader than the categories that are specifically listed.

The court concluded that the only way for the government to rectify the risk of overseizure was by “explaining in a revised application its intended search protocol.” Specifically, the court sought guidance for how the search would limit review of the target’s private information.

---

171 See In re Search of Black iPhone 4, 27 F. Supp. 3d at 75–76.
172 See id. at 76. For a brief review of standard warrant terminology and the warrant application process, see supra notes 63–66 and accompanying text.
173 See In re Search of Black iPhone 4, 27 F. Supp. 3d at 76.
174 See id. at 76–77.
175 See id. at 77 (quipping that the government must have “clearly submitted the wrong Attachment B” because the “government has once again used formulaic language without careful review”).
176 See id. at 77–78. The warrant requested authority to seize all stored contacts, text messages, calls, sent and received images, and voicemails. See id. at 76. The court found that the application failed to articulate sufficient probable cause to necessitate seizing all of this information. See id. at 78.
177 Id. at 78 (alterations in original).
178 Id. at 79.
179 See id. The court asked for the protocol to answer the following questions: “[1] Will all of [the] devices be imaged? [2] For how long will these images be stored? [3] Will a dedicated computer forensics team perform the search based on specific criteria from the investigating officers of what they are looking for, or will the investigating officers be directly involved? [4] What procedures will be used to avoid viewing material that is not within the scope of the warrant? [5] If the government discovers unrelated incriminating evidence, will it return for a separate search and seizure warrant?” Id. at 79–80.
Nine days later, in *In re Search of ODYS LOOX Plus Tablet*, the court issued a new opinion denying another set of government search warrant applications. Like in *In re Search of Black iPhone 4*, the government applied for search warrants seeking evidence of child pornography on a tablet, a digital camera, a cell phone, and a laptop. This time, the government included an “Attachment C,” which incorporated a formal search protocol. However, the court still rejected the warrant applications because the proposed Attachment C “fail[ed] to adequately detail the proposed search protocol and thus fail[ed] to adequately address the [c]ourt’s concerns.”

In this case, the proposed search protocol attempted to directly address the questions posed in *In re Search of Black iPhone 4*. First, it stated that the United States would make available to interested persons any copies of the data collected, “[t]o the extent practical.” It then provided that the government would create mirror images of the devices, and perform any searches based off of the copies. The government then stated that “after inspecting the device[s] or computer system[s] . . . the computer specialist conducting the forensic examination” would determine whether the devices contain evidence of the crimes outlined in Attachment B. If the devices do not contain such evidence, they would be returned. The search protocol concluded that the government would hold any seized data until all appeals are exhausted.

Nevertheless, the court ruled that the government’s protocol was insufficient. The court judged that “Attachment C is far from a paragon of clarity” and that it failed to address “the Court’s concerns by explaining how the search will occur and how the government will avoid overseizure by avoiding keeping documents and other information outside the scope of Attachment B.” Beyond data retention concerns, the court also

---

181 See id. at 41–42.
182 Id. at 42–43.
183 Id. at 41.
184 See id. at 42–44. Judge Facciola’s questions in *In re Search of Black iPhone 4* are outlined *supra*, in note 179.
185 *In re Search of ODYS LOOX Plus Tablet*, 28 F. Supp. 3d at 43.
186 See id.
187 Id.
188 See id.
189 See id. at 44.
190 Id.
191 See id. at 45 (“[T]he government intends to wholly image these devices and store them ‘until the target/defendant’s appeals and habeas proceedings are concluded.’ . . . This is unacceptable.”).
2015] WHAT COMES AFTER “GET A WARRANT” 215

asserted that the search protocol “provides no actual search protocol.”\textsuperscript{192} Instead, the court demanded that “the government needs to provide a sophisticated technical overview of how it plans to conduct the search.”\textsuperscript{193}

Subsequently, in \textit{In re Search of Apple iPhone, IMEI 013888003738427},\textsuperscript{194} the government submitted its third attempt to comply with the court’s specifications. This time, the government replaced the Attachment C search protocol with an FBI forensic scientist’s affidavit. In the affidavit, the forensic scientist detailed his experience with searching mobile devices and his intended use of “[t]raditionally used forensic methods” such as keyword searches and “computer-assisted scans of the entire medium,” with a plan to destroy any discovered information that fell outside the warrant.\textsuperscript{195}

Once again, the court rejected the warrant application.\textsuperscript{196} However, the court noted that its “remaining quibble is that, unlike in \textit{In re Search of Odys Loox}, the government does not specify here that the iPhone will be imaged.”\textsuperscript{197} The court emphasized that explaining whether the imaging process occurs is important because “there will be a complete copy of all [of the device’s] data . . . that must be accounted for.”\textsuperscript{198} Any data accessed without probable cause would need to be filtered out and purged from the government systems.\textsuperscript{199}

The court then explicitly detailed its vision for an appropriate search protocol that would comport with the Fourth Amendment’s probable cause and particularity requirements. In addition to accounting for and destroying any collected data for which the government lacks probable cause, the court sought a technical explanation for how the search would be conducted.\textsuperscript{200} The court reasoned:

\textit{[A]n explanation of the scientific methodology the government will use to separate what is permitted to be seized from what is not, will explain to the Court how the government will decide where it is going to search—and it is thus squarely aimed at satisfying the particularity requirement of the Fourth Amendment.}\textsuperscript{201}

\textsuperscript{192} Id. at 46.
\textsuperscript{193} Id.
\textsuperscript{194} 31 F. Supp. 3d 159 (D.D.C. 2014).
\textsuperscript{195} Id. at 163.
\textsuperscript{196} See id. at 165–66.
\textsuperscript{197} Id.
\textsuperscript{198} Id. at 166.
\textsuperscript{199} See id.
\textsuperscript{200} See id. at 166–67.
\textsuperscript{201} Id. at 166.
Specifically, the court urged that the government ought not shy away from using technical language such as “MD5 hash values,” “metadata,” “registry,” “write blocking,” and “status marker,” or from detailing the software programs the government intended to use.\(^202\) This would enable the court to understand “how [the government] will determine which blocks should be searched for data within the scope of the warrant.”\(^203\) The goal, the court concluded, is to constrain the government to running searches that “minimize the risk that files outside the scope of the warrant will be discovered.”\(^204\)

The D.C. Opinions proved divisive but influential among a number of lower courts.\(^205\) However, the D.C. Opinions’ emphasis on search methodology is not the only approach used by courts. A different search protocol variant is exemplified in \textit{In re Search of a Nextel Cellular Telephone}.\(^206\) Here, the Nextel court’s approach differs from the D.C. Opinions’ approach by demanding ex ante determinations as to \textit{where} the searches would be conducted.\(^207\)

In \textit{Nextel}, the warrant’s search protocol was similar in text to the application in \textit{In re Search of Black iPhone 4}. It generally provided for an “examination of all of the data contained in such cellular telephone hardware,” executed by “surveying various file directories and the individual files they contain.”\(^208\) In this case, the court rejected the warrant application because, “as written, [it] will result in the overseizure of data and indefinite storage of data that it lacks probable cause to seize.”\(^209\) The court then surveyed the D.C. Opinions, noting that they were persuasive in formulating its own holding.\(^210\)

\(^{202}\) See \textit{id.} at 168.

\(^{203}\) \textit{Id.} at 167.

\(^{204}\) \textit{Id.} at 168.


\(^{207}\) Indeed, it is notable that the \textit{Nextel} court approvingly cites to \textit{In re Search of Apple iPhone} and its predecessors for what should be incorporated in a search protocol. \textit{See In re Nextel,} 2014 WL 2898262, at *9, *12. However, it fails to cite to any of the D.C. Opinions when discussing a search protocol requirement articulating \textit{where} evidence would be sought on a device. \textit{See id.} at *13.

\(^{208}\) \textit{Id.} at *2; see also \textit{In re Search of Black iPhone 4,} 27 F. Supp. 3d 74, 76–77 (D.D.C. 2014) [utilizing similarly general language in its \textit{Attachment B: Specific Items To Be Seized}].

\(^{209}\) \textit{In re Nextel,} 2014 WL 2898262, at *10.

\(^{210}\) \textit{See id.} at *6–9.
However, the Nextel court went further than the D.C. Opinions’ search protocols by demanding specific information about where in the device’s memory the government intended to search for evidence of criminal activity.\textsuperscript{211} To support this development, the court relied on a single line of \textit{In re Search of Apple iPhone}, which questioned “where [the government] will search (which ‘parts’—or blocks—of the iPhone’s NAND flash drive).”\textsuperscript{212} But it appears that the query in \textit{In re Search of Apple iPhone} sought a description of the general process, rather than a list of each application and block of memory in which the government would conduct its search.\textsuperscript{213} Indeed, \textit{In re Search of Apple iPhone} actually asked “how the government intends to determine where it will search . . . and how those decisions with respect to how the search will be conducted” would limit exploratory rummaging.\textsuperscript{214}

Nevertheless, the Nextel court insisted that “an acceptable search protocol educates (1) the [c]ourt as to what the government is doing when it searches a cell phone, \textit{and} (2) the executing officer as to what places and things may or may not be searched and/or seized.”\textsuperscript{215} As the Nextel court quipped, “probable cause to believe drug trafficking communication may be found in phone’s the [sic] mail application will not support the search of the phone’s Angry Birds application.”\textsuperscript{216} In essence, the Nextel opinion demands \textit{more} than a search protocol; it requires a predetermined list of where incriminating evidence is believed to reside.

B. How a Search Protocol Looks

The foregoing cases provide compelling rationales for the concerns warranting a mandatory search protocol regime. Yet the actual effort of incorporating such a search protocol into a warrant application need not be burdensome. Take, as a model, the process-based search-protocol format proposed in the D.C. Opinions. Putting together the D.C. Opinions, an ex ante search protocol requires a technical explanation of the search procedure, drawn upon experience and current

\begin{footnotes}
\item[211] See \textit{id.} at *11–13.
\item[212] \textit{id.} at *9 (quoting \textit{In re Search of Apple iPhone, IMEI 013888003738427}, 31 F. Supp. 3d 159, 167 (D.D.C. 2014)).
\item[213] See \textit{In re Search of Apple iPhone,} 31 F. Supp. 3d at 168 (“The Court is not dictating that particular terms or search methods should be used.”).
\item[214] \textit{id.} at 167 (emphasis added).
\item[215] \textit{In re Nextel Cellular Telephone,} 2014 WL 2898262, at *13 (emphasis added).
\item[216] \textit{id.}
\end{footnotes}
software offerings.\textsuperscript{217} To some extent, the forensic examiners must be equipped to explain what data is sought and, therefore, the extent of the search process that they wish to employ.\textsuperscript{218} Moreover, the government must be prepared to articulate its process for copying the device’s contents for analysis, how examiners will identify and isolate information outside the scope of the search warrant, and its plans to purge the information as efficiently as possible.\textsuperscript{219} Finally, the government must account for the participants in the search process, presumably to control for who has access to a target’s personal information.\textsuperscript{220}

This information can take the form of a simple document attachment, as described in \textit{In re Search of ODYS LOOX Plus Tablet}.\textsuperscript{221} Indeed, the D.C. Opinions already suggest that all “the government [needs] to do is explain how it is going to conduct this search” with requests modeled on rote processes already employed by the forensic labs.\textsuperscript{222} Such an explanation would likely incorporate, either directly or by reference, the standard-form operating procedures employed by forensic scientists, which are then tailored to the offense based on the investigators’ guidance.\textsuperscript{223} The content simply needs to be transposed into a workable document attachment that can be reviewed in conjunction with the rest of the warrant application.

\textbf{C. Why a Process-Based Search Protocol Makes Sense}

Nevertheless, imposing a search protocol requirement only makes sense if its focus remains on process rather than data
WHAT COMES AFTER “GET A WARRANT”

location. A process-based focus yields two notable benefits: First, it enhances the particularity within a search warrant, which increases the target’s privacy protection and comports with the Fourth Amendment. Moreover, frontloading clarification of the government’s search process can limit the number of successful suppression challenges. Second, the enhanced particularity comes at little to no cost to the government, since the current state of forensic technology requires clearly identifying in advance the search goals to prevent data loss. The protocol drafting process need not be daunting, since it reflects the government’s common experience with searching mobile devices.

The rising trend of the “post-PC” era means that mobile devices contain vast quantities of personal information exceeding even that of traditional computers. As the Riley Court noted, mobile phones may now provide “a digital record of nearly every aspect of [individuals’] lives.” So while broadly drafted warrants have efficiency benefits, broad language can result in data extraction previously unsupported with probable cause. This runs afoul of the very privacy concerns the Riley Court articulated.

Moreover, an unduly broad search creates a real risk of having valuable evidence suppressed by a pretrial motion or, worse, having a conviction overturned. But by having a search protocol that articulates the forensic examiner’s procedure, an impartial magistrate would have the opportunity to thoroughly review the scope of the search. Magistrate review of a detailed search protocol could better protect the viability of any evidence the police recovered. A search protocol would

---

227 See Riley, 134 S. Ct. at 2491 (“[A] cell phone search would typically expose to the government far more than the most exhaustive search of a house . . . .”).
228 Cf. United States v. Carey, 172 F.3d 1268, 1276 (10th Cir. 1999) (suppressing evidence of child pornography because investigators went beyond the scope of their search warrant).
also align with the warrant process’s deliberative benefits so favored by the Supreme Court.230

And as discussed at several points throughout this Note, the very nature of the mobile device forensic process already supports incorporating search protocols into warrant applications. The short product cycles inherent in consumer mobile technology create limitations on forensic software usability.231 Therefore, careful deliberation is required in order to ensure that any pertinent data is not lost.232 By simply transcribing the technical procedure the forensic examiner intends to undertake to recover data from the mobile device, the government’s work is already accomplished. The only wrinkle in the process is that investigators should provide specific input about how such a search would be tailored to the offense at hand.233

But an explanation of how a search is conducted is significantly different from where the search process will take place on the device. The Nextel opinion’s divergence from the D.C. Opinions to require an ex ante determination of where the forensic search would be conducted likely would result in overly burdening and directing the government’s search process.234 First, forensic examiners may have limited data-extraction capabilities resulting purely from which software the government body procured.235 This means that identifying a specific file location for extraction and review may simply be infeasible.236 The Fourth Amendment’s “place to be searched” generally cannot be narrower than identifying the device. Second, just because end users cannot as flexibly mask file names, locations, or extensions on mobile devices compared to traditional computers does not mean that investigators know, ex ante, where the evidence may lie.237 Instead, a detailed and approved search methodology, rather than a list of data locations, realis-


231 See Gonzalez & Hung, supra note 115, at 1.

232 See supra notes 115–144 and accompanying text.

233 See In re Search of Black iPhone 4, 27 F. Supp. 3d 74, 78 (D.D.C. 2014) (requiring probable cause for data extracted from the mobile device). The probable cause would necessarily come from law enforcement officers who are directly involved in the criminal investigation.

234 Cf. In re Search of Apple iPhone, 31 F. Supp. 3d at 168 (“The Court is not dictating that particular terms or search methods should be used.”).

235 See supra notes 115–123 tbl.3 (comparing the capabilities of a variety of forensic software packages).

236 See supra notes 139–144 and accompanying text.
2015] WHAT COMES AFTER “GET A WARRANT” 221
tically guides criminal investigations while providing more pri-

CONCLUSION

Riley drew a line in the sand in favor of individual privacy

rights. The Court took a step forward in adapting modern tech-

nology to traditional Fourth Amendment protections. However,
the Riley privacy rights discussion left open the glaring ques-

tion of how much latitude law enforcement officers have when
searching a device with a warrant. As discussed, courts, in-
cluding the Riley Court, considered the practical burdens on
law enforcement in light of an individual’s reasonable expecta-
tion of privacy. With such attention to practical—not doctri-
nal—considerations, it is evident that considering the factual

circumstances underlying forensic searches is crucial before
announcing a new doctrine in Fourth Amendment jurisprudence.

Ultimately, this Note concludes that mobile devices are
currently so unique in both technological development and
daily use that an intermediate standard is required for search
warrant particularity. Therefore, law enforcement officers
should be afforded practical deference when conducting their
search, but they also must bear the burden to articulate their
methodology in an ex ante search protocol. This approach pre-
serves the disciplined, moderated review by an impartial mag-
istrate judge, in line with Fourth Amendment jurisprudence,
while recognizing that some flexibility is required when search-
ing for evidence in a vast, virtual space.
222

CORNELL LAW REVIEW

[Vol. 101:187]