**Boston College Law Review**

Volume 56 | Issue 5 Article 7

12-1-2015

# Protecting the Privacies of Digital Life: *Riley v. California*, the Fourth Amendment's Particularity Requirement, and Search Protocols for Cell Phone Search Warrants

William Clark
*Boston College Law School*, william.clark.2@bc.edu

# PROTECTING THE PRIVACIES OF DIGITAL LIFE: *RILEY V. CALIFORNIA*, THE FOURTH AMENDMENT'S PARTICULARITY REQUIREMENT, AND SEARCH PROTOCOLS FOR CELL PHONE SEARCH WARRANTS

**Abstract:** In 2014, in *Riley v. California*, the U.S. Supreme Court held that the police must obtain a warrant before searching a cell phone. Since then, lower courts have struggled to determine what scope limitations judges should place on cell phone warrants in order to ensure that these warrants do not devolve into unconstitutional general searches. This Note argues that the Fourth Amendment's particularity requirement mandates that the government submit search protocols, technical documents that explain the search methods the government will use on the seized device, for cell phone search warrants. This argument is based on the *Riley* decision, as well as a series of decisions from two magistrate judges that have required search protocols for cell phone search warrants. Detailed search protocols will ensure that cell phone search warrants have a particularized scope and thereby protect the privacies of life modern cell phones contain.

## INTRODUCTION

As of January 2014, ninety percent of American adults own a cell phone.[1] In 2013, Americans used their cell phones to send 1.9 trillion text messages, talk for 2.6 trillion minutes, and view 3.2 trillion megabytes worth of data from the Internet.[2] Today, the most popular types of cell phones are smartphones, handheld computers capable of storing massive amounts of information.[3] Most smartphone users rely on their devices for a wide range of daily activities.[4] For

[1] *Mobile Device Ownership Over Time*, PEW RESEARCH CTR., http://www.pewinternet.org/data-trend/mobile/device-ownership/ [http://perma.cc/SWN4-372D] [hereinafter PEW RESEARCH CTR]; *see also* Riley v. California (*Riley II*), 134 S. Ct 2473, 2490 (2014) (noting the prevalence of cell phones in the United States).

[2] *See* CELLULAR TELECOMM. INDUS. ASS'N, WIRELESS INDUSTRY SUMMARY REPORT, YEAR-END 2013 RESULTS 8 (2014), http://www.ctia.org/docs/default-source/Facts-Stats/ctia_survey_ye_2013_graphics-final.pdf?sfvrsn=2 [http://perma.cc/SWN4-372D].

[3] *See Riley II*, 134 S. Ct at 2489 (describing smartphones as "minicomputers that also happen to have the capacity to be used as a telephone"); PEW RESEARCH CTR., *supra* note 1 (stating that 58% of American adults own a smartphone).

[4] *See Riley II*, 134 S. Ct at 2484, 2489 (stating that modern cell phones "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy" and observing that these devices "could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers"); *How Smartphones Are Changing Consumers' Daily Routines Around the Globe*,

seventy-nine percent of smartphone users, the first thing they do when they wake up is check their phones.[5]

With the rising popularity of smartphones, many Americans are placing more and more sensitive and personal information on their mobile devices.[6] Smartphone users can not only make phone calls, write emails, and send text messages, but they can also keep records of credit card and bank statements and input their symptoms for medical diagnoses all at the touch of their phone's screen.[7] As these advanced smartphone functions become more popular, many users are increasingly concerned about privacy and security on their devices.[8]

---

NIELSON (Feb. 24, 2014), http://www.nielsen.com/us/en/insights/news/2014/how-smartphones-are-changing-consumers-daily-routines-around-the-globe.html [http://perma.cc/MT76-HKYK] [hereinafter NIELSON]. Smartphones and other mobile devices have quickly become the most popular way for Americans to access the Internet. *See* James O'Toole, *Mobile Apps Overtake PC Internet Usage in U.S.*, CNN MONEY (Feb. 28, 2014, 11:00 AM), http://money.cnn.com/2014/02/28/technology/mobile/mobile-apps-internet/ [http:// perma.cc/8LLP-KU99] (noting how in January 2014, mobile devices accounted for 55% of Internet usage in the United States, with 47% of Internet usage occurring through applications ("apps") on mobile devices and only 45% of Internet usage occurring through personal computers); Sarah Perez, *Majority of Digital Media Consumption Now Takes Place in Mobile Apps*, TECHCRUNCH (Aug. 21, 2014), http://techcrunch.com/2014/08/21/majority-of-digital-media-consumption-now-takes-place-in-mobile-apps/ [http://perma.cc/45B3-ATVX] (observing that 60% of time spent consuming digital media occurs on mobile devices, leaving 40% of time spent consuming digital media on personal computers).

[5] *See* Allison Stadd, *79% of People 18–44 Have Their Smartphones with Them 22 Hours a Day*, ADWEEK: SOCIAL TIMES (Apr. 2, 2013, 12:00 PM), http://www.adweek.com/socialtimes/smartphones/480485?red=at [http://perma.cc/SBN3-J8LR]. Seventy-nine percent of smartphone users carry their phone with them for all but two hours of the time they are awake. *Id.*

[6] *See* CONSUMER & CMTY. DEV. RESEARCH SECTION, FED. RESERVE BD., CONSUMERS AND MOBILE FINANCIAL SERVICES 2014, at 1 (Mar. 2014), http://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201403.pdf [http://perma.cc/ER59-EP8H] (noting how banking via mobile phones is becoming increasingly popular); *Hacking Health: How Consumers Use Smartphones and Wearable Tech to Track Their Health*, NIELSON (Apr. 16, 2014), http://www.nielsen.com/us/en/insights/news/2014/hacking-health-how-consumers-use-smartphones-and-wearable-tech-to-track-their-health.html [http://perma.cc/NN4B-EDD9] (describing the growing popularity of health and fitness apps for smartphones); *Keep Your Phone Safe: How to Protect Yourself from Wireless Threats*, CONSUMER REPORTS MAG. (June 2013), http://www.consumerreports.org/privacy0613 [http://perma.cc/4C3U-WDEP] (listing examples of the private information many Americans store on their cell phones, including financial information and personal photographs).

[7] *See Bank of America Mobile Banking App on Your iPhone and iPad*, BANK OF AM., https://www.bankofamerica.com/online-banking/iphone-banking-app.go [http://perma.cc/T95T-SYME] (describing the features of Bank of America's mobile apps for smartphones, including account transfers and remote deposits); NIELSON, *supra* note 4 (stating 11% of smartphone time is spent using text message or phone call capabilities); *What We Make*, HEALTHTAP, http://www.healthtap.com/what_we_make/overview [http://perma.cc/S5ES-5J8W] (describing HealthTap, an application that allows users to communicate directly with doctors through their smartphones twenty-four hours a day, including through text, voice, and video chat).

[8] *See Riley II*, 134 S. Ct. at 2490 (noting how American cell phone users "keep on their person a digital record of nearly every aspect of their lives"); Janice C. Sipior et al., *Privacy Concerns Associated with Smartphone Use*, 13 J. INTERNET COMM. 177, 178 (2014) (stating that the increasing popularity of smartphones leads to an increasing risk to user privacy); *Smartphone Users Care More About Privacy Than Screen Size or Brand*, INFOSECURITY MAG. (Sept. 5, 2013), http://www.infosecurity-magazine

Accordingly, most smartphone users want protections to ensure that their sensitive and personal information will remain private and secure.[9]

Recognizing the important role that cell phones play in the lives of many Americans, in 2014, in *Riley v. California*, the U.S. Supreme Court held that the police could not search a cell phone incident to an arrest without first obtaining a warrant.[10] A unanimous Court recognized that to allow the government unfettered access to the deeply sensitive information cell phones often contain would authorize the type of broad and intrusive searches against which the Fourth Amendment protects.[11] Privacy advocates championed the decision as a reaffirmation of the Fourth Amendment's warrant requirement in the digital age.[12]

In the aftermath of *Riley*, however, lower courts have articulated different standards for the scope of cell phone search warrants.[13] A few courts have re-

---

.com/news/smartphone-users-care-more-about-privacy-than/ [http://perma.cc/4Z7H-L7Q9] [hereinafter INFOSECURITY MAG.] (noting how privacy is second only to battery life as smartphone users' most pressing concerns when considering using mobile applications). *But see* Winston Ross, *How Much Is Your Privacy Worth?*, MIT TECH. REV. (Aug. 26, 2014), http://www.technologyreview.com/news/529686/how-much-is-your-privacy-worth/ [http://perma.cc/N899-9FG6] (discussing new companies that are paying smartphone users a monthly fee for access to the users' web browsing and banking data). In 2014, Americans used smartphone applications 76% more than they did in 2013. *See* Simon Khalaf, *Shopping, Productivity and Messaging Give Mobile Another Stunning Growth Year*, FLURRY (Jan. 6, 2015), http://www.flurry.com/blog/flurry-insights/shopping-productivity-and-messaging-give-mobile-another-stunning-growth-year# [http://perma.cc/5KNC-Y668]. They used shopping apps 174% more, messaging apps 103% more, and health apps 89% more than in 2013. *Id.*

[9] *See* Sipior et al., *supra* note 8, at 178 (noting how many smartphone users believe privacy on their devices is an important issue and that they would like more control over their private information); INFOSECURITY MAG., *supra* note 8 (stating that consumers are becoming increasingly concerned with privacy on their mobile devices).

[10] *Riley II*, 134 S. Ct. at 2495.

[11] *Id.* at 2494–95.

[12] *See, e.g.*, Andrew Pincus, *Evolving Technology and the Fourth Amendment: The Implications of* Riley v. California, 2014 CATO SUP. CT. REV. 307, 336 (asserting the importance of *Riley* in charting a new course for Fourth Amendment protections in the digital age); Emily Phelps, *In* Riley*, a Decision Worth Celebrating—Just in Time for Independence Day*, CONST. ACCOUNTABILITY CTR. (June 27, 2014), http://theusconstitution.org/text-history/2749/riley-decision-worth-celebrating—just-time-independence-day [http://perma.cc/7ART-Y4R7] (discussing the Court's recognition of the parallels between writs of assistance and warrantless cell phone searches); Richard Re, *Symposium: Inaugurating the Digital Fourth Amendment*, SCOTUSBLOG (June 26, 2014, 12:37 PM), http://www.scotusblog.com/2014/06/symposium-inaugurating-the-digital-fourth-amendment/ [http://perma.cc/PB2R-UVM9]; Jay Stanley, *How the Supreme Court Could Have Ruled in* Riley, AM. C.L. UNION (June 26 2014, 11:17 AM), https://www.aclu.org/blog/technology-and-liberty-criminal-law-reform/how-supreme-court-could-have-ruled-riley [https://perma.cc/HP7E-3LVV] (noting how privacy scholars have celebrated the *Riley* decision).

[13] *See In re* Nextel Cellular Tel., No. 14-MJ-8005-DJW, 2014 WL 2898262, at *9 (D. Kan. June 26, 2014) (relying on *Riley* to hold a warrant for a cell phone search without a search protocol violates the Fourth Amendment's particularity requirement); Hedgepath v. Commonwealth, 441 S.W.3d 119, 130 (Ky. 2014) (interpreting *Riley* as placing no new particularity limitations on cell phone search warrants); State v. Henderson, 854 N.W.2d 616, 633–34 (Neb. 2014) (stating that, in the wake of *Riley*, courts will have to determine how detailed warrants for cell phones must be); John Wesley Hall,

fused to issue cell phone search warrants unless the government submitted search protocols, technical documents that explain the exact methods the police will use to limit the scope of their search.[14] Other courts have discussed the potential need for search protocols, but have yet to mandate them for cell phone search warrants.[15] Finally, at least one court has upheld broad warrants that allow the government to review the entire contents of cell phones, later inferring scope limitations into the warrants when challenged by defendants.[16]

This Note argues that judges must require detailed search protocols for cell phone search warrants in order to comply with the Fourth Amendment's particularity requirement.[17] As the U.S. Supreme Court held in *Riley*, to allow the police unguided review of the entire contents of a cell phone when executing a search warrant would authorize the exact type of general warrants that the Fourth Amendment forbids.[18] Some earlier U.S. Supreme Court cases have interpreted the particularity requirement to place no limitations on how the police execute warrants.[19] In *Riley*, however, the Court recognized that the fundamental differences between physical and digital searches may require courts to articulate new rules and new interpretations of the Fourth Amendment.[20]

Part I of this Note discusses the principles of the Fourth Amendment's particularity requirement, how those principles have been applied to computer

---

*D.Kan.: Standard Gov't Cell Phone Search Protocol Violates Particularity Requirement and Results in a General Search*, FOURTHAMENDMENT.COM (July 1, 2014), http://fourthamendment.com/?p=12343 [http://perma.cc/9P7K-R2QY] (arguing that the particularity requirement will be a recurring issue in warrants for cell phone searches).

[14] *See, e.g.*, *In re Nextel Cellular Tel.*, 2014 WL 2898262, at *14; *In re* the Search of Apple iPhone, 31 F. Supp. 3d 159, 166 (D.D.C. 2014); *In re* ODYS LOOX Plus Tablet Serial No. 4707213703415 in Custody of U.S. Postal Inspection Serv., 1400 New York Ave. NW, Wash., D.C., 28 F. Supp. 3d 40, 46 (D.D.C. 2014); *In re* the Search of Black iPhone 4, 27 F. Supp. 3d 74, 79 (D.D.C. 2014).

[15] *See* United States v. Lustyik, No. 13-CR-616-VB, 2014 WL 4802911, at *12 n.12 (S.D.N.Y. Sept. 29, 2014) (discussing the *Riley* decision and its possible impact on search protocols for cell phone search warrants); *Henderson*, 854 N.W.2d at 633–34 (recognizing the potential need for search protocols in cell phone search warrants, but deciding the case before it on other grounds).

[16] *See Hedgepath*, 441 S.W.3d at 130.

[17] *See infra* notes 158–221 and accompanying text.

[18] *See* U.S. CONST. amend. IV; *Riley II*, 134 S. Ct. at 2494–95 (requiring the police to get search warrants for cell phone searches in part because of the historical prohibition against general warrants); *infra* notes 32–46 and accompanying text (outlining the foundational principles of the Fourth Amendment).

[19] *See* United States v. Grubbs, 547 U.S. 90, 98 (2006) (holding that the Fourth Amendment's particularity requirement does not require the police to submit in warrant applications how they will execute the search warrant); Dalia v. United States, 441 U.S. 238, 257 (1979) (holding that the police do not need prior authorization before covertly installing electronic listening devices because the police have discretion over how to execute a warrant).

[20] *See Riley II*, 134 S. Ct. at 2485 (recognizing the limits of applying rules of physical searches to digital searches); *In re* Search Warrant, 71 A.3d 1158, 1169 n.11 (Vt. 2012) (stating that earlier U.S. Supreme Court cases, such as *Dalia*, do not prevent judges from requiring search protocols for warrants for computer searches), *cert. denied*, 133 S. Ct. 185 (2013).

searches, and the U.S. Supreme Court's decision in *Riley v. California*.[21] Part II of this Note outlines the different approaches to cell phone warrants taken by lower courts, comparing courts that have required search protocols for cell phone search warrants with those that have not.[22] Part III of this Note argues that courts should recognize the fundamental differences between physical and digital searches and require search protocols for cell phone search warrants.[23] Part III then provides four recommendations for requirements judges should place in cell phone search protocols.[24]

## I. The Fourth Amendment's Particularized Warrant Requirement and Its Surprising Resurgence in *Riley v. California*

This Part outlines the Fourth Amendment's particularized warrant requirement and the U.S. Supreme Court's 2014 decision in *Riley v. California*, which applied the warrant requirement to cell phone searches.[25] Section A reviews the foundational principles of the Fourth Amendment.[26] Then, section B discusses how courts have applied the Fourth Amendment's particularity requirement to computer searches.[27] Finally, section C explains the U.S. Supreme Court's decision in *Riley v. California*, including the background of the decision and its broader implications for digital searches.[28]

### *A. The Fourth Amendment's Protections of the "Privacies of Life"*

This section discusses the principles of the Fourth Amendment.[29] Subsection 1 outlines the foundational principles of the Fourth Amendment.[30] Subsection 2 examines the Fourth Amendment's protection against government intrusions into the "privacies of life" and searches of the home.[31]

#### 1. The Foundational Principles of the Fourth Amendment

The Fourth Amendment of the U.S. Constitution protects the right of the people against government intrusions into their private lives and spaces.[32] The

---

[21] *See infra* notes 25–94 and accompanying text.
[22] *See infra* notes 95–157 and accompanying text.
[23] *See infra* notes 158–221 and accompanying text.
[24] *See infra* notes 205–221 and accompanying text.
[25] *See infra* notes 25–94 and accompanying text.
[26] *See infra* notes 29–56 and accompanying text.
[27] *See infra* notes 57–72 and accompanying text.
[28] *See infra* notes 73–94 and accompanying text.
[29] *See infra* notes 29–56 and accompanying text.
[30] *See infra* notes 32–46 and accompanying text.
[31] *See infra* notes 47–56 and accompanying text.
[32] *See* U.S. Const. amend. IV ("The right of the people to be secure . . . against unreasonable searches and seizures, shall not be violated . . . ."); United States v. Jones, 132 S. Ct. 945, 949 (2012)

amendment contains two separate clauses: the reasonableness clause and the warrant clause.[33] The reasonableness clause requires that all government searches and seizures be reasonable.[34] The warrant clause allows courts to issue warrants only if two conditions are met: the warrant is supported by probable cause and it includes particularized descriptions of "the place to be searched" and "the people or things to be seized."[35] This second condition is known as the particularity requirement.[36]

In order to comply with the particularity requirement, the warrant must contain two sets of precise descriptions.[37] First, the warrant must describe the place to be searched with enough detail to allow the police to recognize the location with relative ease.[38] Second, the warrant must describe the persons or

---

(holding the government's physical intrusion onto private property for the purpose of obtaining information was a search under the Fourth Amendment); Katz v. United States, 389 U.S. 347, 353 (1967) (stating the Fourth Amendment's protections extend beyond physical intrusions onto property and protect people from secret government wiretapping); Silverman v. United States, 365 U.S. 505, 511 (1961) (characterizing the core protection of the Fourth Amendment as "the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion").

[33] *See* U.S. CONST. amend. IV; Kentucky v. King, 131 S. Ct. 1849, 1856 (2011) (stating that the Fourth Amendment's text establishes two requirements); RONALD J. ALLEN ET AL., COMPREHENSIVE CRIMINAL PROCEDURE 420–21 (3d ed. 2011) (chronicling the U.S. Supreme Court's shift towards reading the reasonableness requirement and warrant requirement separately).

[34] *See* U.S. CONST. amend. IV ("The right of the people to be secure . . . against unreasonable searches and seizures, shall not be violated . . . ."); *King*, 131 S. Ct. at 1856 (noting how the Fourth Amendment requires all searches and seizures to be reasonable); Brigham City v. Stuart, 547 U.S. 398, 403 (2006) (stating that "[t]he ultimate touchstone of the Fourth Amendment is reasonableness").

[35] *See* U.S. CONST. amend. IV ("[N]o warrants shall issue, but upon probable cause . . . and particularly describing the place to be searched, and the persons or things to be seized."); *King*, 131 S. Ct. at 1856 (stating the Fourth Amendment requires the government to establish probable cause and set out the scope of the search with particularity in order for a court to issue a warrant); Groh v. Ramirez, 540 U.S. 551, 557 (2004) (holding a warrant that failed to particularly describe the items to be seized violated the Fourth Amendment); Illinois v. Gates, 462 U.S. 213, 240 (1983) (characterizing a neutral judge's determination that probable cause has been established as "the essential protection of the warrant requirement"). Probable cause is a malleable concept, requiring a magistrate to weigh the totality of the information presented in the application and decide if there is a fair probability that the search will expose particular evidence of a crime. *See* Ornelas v. United States, 517 U.S. 690, 695–96 (1996) (stating that it is impossible to provide a precise articulation of the meaning of probable cause); *Gates*, 462 U.S. at 232 (describing how probable cause "turn[s] on the assessment of probabilities in particular factual contexts" and how it is "not readily, or even usefully, reduced to a neat set of legal rules").

[36] *See* U.S. CONST. amend. IV; *Groh*, 540 U.S. at 557 (holding the warrant itself, and not the warrant application, must provide a particularized description of the things to be seized); Maryland v. Garrison, 480 U.S. 79, 85 (1986) (stating the warrant's description must be proportionally detailed to the amount of information available to the police at the time they submit the warrant).

[37] *See Grubbs*, 547 U.S. at 97 (stating that the Fourth Amendment requires two particularized descriptions); *Groh*, 540 U.S. at 557 (noting how the Fourth Amendment requires warrants to contain detailed descriptions of both the place the government will search and the items the government wishes to seize); ALLEN, *supra* note 33, at 426.

[38] *See Garrison*, 480 U.S. at 88–89 (holding the police made "reasonable effort to ascertain and identify" the place to be searched); Steele v. United States, 267 U.S. 498, 503 (1925) (stating that the description should allow the police officer executing the warrant to find the place to be searched); ALLEN, *supra* note 33, at 425.

things to be seized in order to limit where the police can look and for how long they can look.[39] These dual demands of particularity ensure that the police establish the proper location for their search and have clear objectives in mind during their search.[40]

The particularity requirement does not, however, mandate that the police include descriptions of how they plan to execute their warrants.[41] The U.S. Supreme Court rejected such a requirement in 1979, in *Dalia v. United States*.[42] In *Dalia*, the Court held the police did not violate the particularity requirement when they covertly entered the defendant's office to install a recording device.[43] The police had a warrant to install the device, but they did not have prior authorization for their covert entry into the defendant's office.[44] The Court held that the police have the discretion to determine how to execute warrants and that the particularity requirement places no limits on this discretion.[45] But, the Court noted that, as a policy matter, prior authorization for covert entry was the "preferable approach" because such entry was an additional intrusion upon the defendant's privacy rights.[46]

---

[39] *See King*, 131 S. Ct. at 1856 (stating the particularity requirement limits the scope of the government's search); Marron v. United States, 275 U.S. 192, 196 (1927) (stating that particularized descriptions of the things to be seized prevent the police from seizing items beyond the scope of the warrant); ALLEN, *supra* note 33, at 426 (describing how the particularity requirement limits searches both spatially and temporally); THOMAS MCINNIS, THE EVOLUTION OF THE FOURTH AMENDMENT 66 (2009) (discussing how requiring particularized descriptions of the items to be seized prevents "fishing expeditions" by the police).

[40] *See Groh*, 540 U.S. at 554–55, 557 (holding that a warrant failed to meet the particularity requirement because it did not identify any of the items intended to be seized); *Garrison*, 480 U.S. at 84 (discussing how the probable cause and particularity requirements work together to limit the scope of government searches); Berger v. State of New York, 388 U.S. 41, 55–56 (1967) (invalidating New York's wiretap statute because it allowed warrants for wiretaps to be issued without specifying the particular crime being investigated); ALLEN, *supra* note 33, at 426 (discussing how the particularity requirement limits both the areas the police can search and how long the police may search an area).

[41] *See Dalia*, 441 U.S. at 257; Orin Kerr, *Ex Ante Regulation of Computer Search and Seizure*, 96 VA. L. REV. 1241, 1266 (2010) (interpreting *Dalia* as rejecting the view that the particularity requirement commands preapproval of how warrants will be executed); Stephen Guzzi, Note, *Digital Searches and the Fourth Amendment: The Interplay Between the Plain View Doctrine and Search–Protocol Warrant Restrictions*, 49 AM. CRIM. L. REV. 301, 310 (2012) (discussing how after *Dalia* the police determine the manner in which warrants are executed, with the only limitation on police discretion being the reasonableness requirement).

[42] *Dalia*, 441 U.S. at 257.

[43] *Id.*

[44] *See id.* at 245 (describing how FBI agents secretly entered the defendant's office at midnight and spent three hours installing recording devices in his ceiling).

[45] *See id.* at 257.

[46] *See id.* at 257, 259 n.22 (accepting that by covertly entering the office, the police impinged on privacy interests "not explicitly considered by the judge who issued the warrant" and discussing how the Department of Justice's policy was to seek prior authorization for covert entries to install listening devices); *see also* Nicole Friess, *When Rummaging Goes Digital: Fourth Amendment Particularity and Stored E-mail Surveillance*, 90 NEB. L. REV. 971, 1015 (2012) (reading *Dalia* to encourage limitations on the execution of warrants); Paul Ohm, *Massive Hard Drives, General Warrants, and the*

2. Home Searches and the "Privacies of Life"

A person's home receives the highest level of protection under the Fourth Amendment.[47] Although deriving in part from traditional property rights, the Fourth Amendment's steadfast protection of the home is primarily founded on the belief that the home is the most private of places.[48] In 1887, in *Boyd v. United States*, the U.S. Supreme Court declared, in an often-quoted line, that the Fourth Amendment protects the sanctity of a person's home and the "privacies of life" therein contained.[49] The "privacies of life" are the intimate and private details of a person's day: from family budgets, to conversations with a partner, to love letters, to evening prayers.[50] Because the home has traditionally has been the vault for this private property and the scene for these private mo-

---

*Power of Magistrate Judges*, 97 VA. L. REV. IN BRIEF 1, 3–4 (2011) http://www.virginialawreview.org/sites/virginialawreview.org/files/ohm.pdf [http://perma.cc/C6LE-MFNY] (interpreting *Dalia* to endorse ex ante restrictions on searches). In 2006, in *United States v. Grubbs*, the U.S. Supreme Court reaffirmed this narrow interpretation of the particularity requirement, stating again that it does not command the police to explain how they plan to execute warrants. *Grubbs*, 547 U.S. at 98; *see* Friess, *supra*, at 1003–04 (reading *Grubbs* to once again reject attempts to expand the particularity requirement's meaning); Kerr, *supra* note 41, at 1268 (characterizing *Grubbs* as reading the particularity requirement narrowly). The Court stated that the Fourth Amendment provides no general requirement of particularity and that courts should be skeptical of efforts expand the particularity clause's meaning. *See Grubbs*, 547 U.S. at 97; Friess, *supra*, at 1003–04 (recognizing *Grubbs*' rejection of a generalized particularity requirement); Kerr, *supra* note 41, at 1268 (reading *Grubbs* to preclude attempts to expand the meaning of the particularity requirement).

[47] *See* Kyllo v. United States, 533 U.S. 27, 40 (2001) (stating "the Fourth Amendment draws 'a firm line at the entrance to the house'" and requiring a warrant for a thermal scan of the area above a house (quoting Payton v. New York, 445 U.S. 573, 590 (1980))); *Silverman*, 365 U.S. at 511 (stating "[a]t the very core [of the Fourth Amendment] stands the right of a man to retreat into his home and there be free from unreasonable governmental intrusion"); Stephanie M. Stern, *The Inviolate Home: Housing Exceptionalism in the Fourth Amendment*, 95 CORNELL L. REV. 905, 912 (2010) (describing how judges provide the highest protection under the Fourth Amendment to homes).

[48] *See* Florida v. Jardines, 133 S. Ct. 1409, 1417 (2013) (holding that the government's use of drug sniffing dogs to investigate defendant's home was a search under Fourth Amendment because of the Fourth Amendment's protection of a homeowner's property rights); *Kyllo*, 533 U.S. at 40 (requiring a warrant for a thermal scan above a house because the Fourth Amendment provides special protection to homes); *see also* Lawrence v. Texas, 539 U.S. 558, 567 (2003) (characterizing the home as "the most private of places").

[49] Boyd v. United States, 116 U.S. 616, 630 (1886); *see, e.g.*, *Riley II*, 134 S. Ct. at 2494–95 (quoting *Boyd* to support requiring a warrant to search cell phones); Payton v. New York, 445 U.S 573, 585 (1980) (quoting *Boyd* to support requiring a warrant to arrest a suspect in his home); *Berger*, 388 U.S. at 58 (quoting *Boyd* and holding that New York's wiretap statute violated the particularity requirement); Griswold v. Connecticut, 381 U.S. 479, 484 (1965) (quoting *Boyd* to support a general right of privacy).

[50] *See Riley II*, 134 S. Ct. at 2490, 2494–95 (stating that cell phones contain the modern "privacies of life" and discussing mobile applications for family budgets, prayers, and dating); *Berger*, 388 U.S. at 58–59 (expressing concern that a wiretap would seize private conversations outside scope of government investigation and thereby invade the "privacies of life"); *Boyd*, 116 U.S. at 630; *see also Kyllo*, 533 U.S. at 38 (stating that the government's use of a heat sensor around a house could expose intimate details such as "at what hour each night the lady of the house takes her daily sauna and bath").

ments, the Fourth Amendment requires the police to obtain a warrant before almost all home searches.[51]

Invoking the home's special status, the U.S. Supreme Court has held that facially broad search warrants for homes violate the particularity requirement.[52] In 2004, in *Groh v. Ramirez*, the U.S. Supreme Court held a search warrant for a home was invalid because it failed to include a particularized description of the evidence sought.[53] The warrant's application included a detailed description of weapons the government wished to seize from the home, but the warrant itself failed to incorporate this description.[54] Citing the heightened privacy protections given to the home, the Court refused to find that the application's detailed descriptions cured the warrant's facially unlimited scope.[55] Instead, the Court considered the warrant so overly broad that, for all intents and purposes, the search was warrantless and therefore violated the Fourth Amendment.[56]

### *B. Particularity in Computer Searches and Search Protocols*

Over the past twenty-five years, lower courts have grappled with how to apply the Fourth Amendment's particularity requirement to warrants authorizing the search of computers.[57] Most circuit courts have imported the funda-

---

[51] *See King*, 131 S. Ct. at 1856 (holding that although warrantless searches of homes are presumed unreasonable, that presumption can be overcome through exigent circumstances); *Groh*, 540 U.S. at 559 (stating "our cases have firmly established the basic principle of Fourth Amendment law that searches and seizures inside a home without a warrant are presumptively unreasonable"(citation omitted)); *Payton*, 445 U.S. at 586.

[52] *See Groh*, 540 U.S. at 559, 563 (discussing the special protections homes receive and holding a search warrant for a home violated the particularity requirement); Stanford v. Texas, 379 U.S 476, 486 (1965) (holding a warrant authorizing the search of a home for literary material violated the particularity requirement).

[53] *Groh*, 540 U.S. at 557.

[54] *Id.* Where the police were supposed to incorporate the detailed list of the weapons sought, they mistakenly provided a description of the defendant's house. *Id.* at 554. The warrant therefore confusingly read: "[T]here is now concealed [on the specified premises] certain person or property, namely [a] single dwelling residence two story in height which is blue in color and has two additions attached to the east. The front entrance to the residence faces in a southerly direction." *Id.* at 554 n.2.

[55] *See id.* at 557, 559; Stern, *supra* note 47, at 913–14 (reading *Groh* as one of several U.S. Supreme Court cases "proclaim[ing] the sanctity of the home and its inviolability").

[56] *Groh*, 540 U.S. at 558. The Court found no exception to the warrant requirement applied, thereby making the search unreasonable. *Id.* at 561.

[57] *See* United States v. Rosa, 626 F.3d 56, 62 (2d Cir. 2010) (holding a warrant for the search of several laptops and USB storage drives that did not provide a description of the specific items for which the police searched violated the Fourth Amendment's particularity requirement); United States v. Riccardi, 405 F.3d 852, 862–63 (10th Cir. 2005) (holding a warrant for the search of a computer violated the Fourth Amendment's particularity requirement because it failed to limit the search to evidence of specific crimes or specific materials); Josh Goldfoot, *The Physical Computer and the Fourth Amendment*, 16 BERKELEY J. CRIM. L. 112, 124 (2011) (discussing how courts have translated Fourth Amendment principles to apply to digital searches over the past twenty years); Orin Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279, 280 (2005) (observing how

mental principles of the particularity requirement to computer searches, demanding warrants provide specific descriptions of the places to be searched and the evidence to be seized.[58] Some judges, however, have placed stricter particularity limitations on computer searches, requiring police to submit separate proposals in their warrant applications that describe the methods the government will use to find that data on the seized computers.[59] These proposals are known as search protocols.[60]

Judges who mandate search protocols do so to ensure that the government's search of the device does not violate the particularity requirement.[61]

---

some courts have begun to develop new Fourth Amendment interpretations for searches of computers); Kerr, *supra* note 41, at 1243–44 (noting how some magistrate judges have begun placing stricter limitations in warrants on searches of computers because of particularity concerns). In order to provide an overview of the existing framework for computer searches and the Fourth Amendment, this section focuses on computer searches rather than cell phone searches. *See infra* notes 57–72 and accompanying text.

[58] *See Rosa*, 626 F.3d at 59, 62; *Riccardi*, 405 F.3d at 862–63; Friess, *supra* note 46, at 993–94 (observing that courts consistently hold warrants in violation of the particularity requirement if the government fails to use available information to particularize its descriptions of the items to be seized); Goldfoot, *supra* note 57, at 136 (discussing how warrants calling for the search and seizure of all the data on a computer have routinely been found overbroad in violation of the particularity requirement).

[59] *See In re* Search of 3817 W. West End, 321 F. Supp. 2d 953, 954 (N.D. Ill. 2004) (describing the search protocol the magistrate judge required before issuing a warrant); Kerr, *supra* note 41, at 1255–56 (describing how judges have begun to use search protocols to limit warrants); *see also* United States v. Richards, 659 F.3d 527, 538 (6th Cir. 2011) (observing that most federal courts do not require search protocols for search warrants for computers); United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1179 (9th Cir. 2010) (en banc) (Kozinski, C.J., concurring) (arguing that warrant applications for computer searches should include search protocols); *In re Search Warrant*, 71 A.3d at 1170 (upholding a judge's power to force police to submit search protocol along with application for search warrant of computer).

[60] *See In re Search of 3817 W. West End*, 321 F. Supp. 2d at 954 (stating how a search protocol describes "(a) the information the government sought to seize from the computer and (b) the methods the government planned to use to locate that information"); Susan W. Brenner, *Requiring Protocols in Computer Search Warrants*, 2 DIGITAL EVIDENCE 180, 182 (2005) (defining search protocols and noting how they derive from the Fourth Amendment's particularity requirement).

[61] *See In re Search of 3817 W. West End*, 321 F. Supp. 2d at 961; *In re Search Warrant*, 71 A.3d at 1162 (discussing how the lower court required the search protocol for the computer search warrant in order to limit the search's scope); Kerr, *supra* note 41, at 1255 (noting how some judges require search protocols in order to keep digital searches narrowly focused). These judges also require search protocols in order to address the knotty issue of the Fourth Amendment's plain view doctrine and digital searches. *See In re Search Warrant*, 71 A.3d at 1162 (noting that the lower court judge explicitly prevented the government from relying on the plain view doctrine in order to seize evidence outside the warrant's scope); Kerr, *supra* note 41, at 1255. The plain view doctrine allows the police to search and seize evidence they find in plain view during a search, even if such evidence falls outside the authorized scope of that initial search. *See* Texas v. Brown, 460 U.S. 730, 738–39 (1983) (noting how plain view doctrine allows police to seize "suspicious objects" immediately so long as their initial search is justified); Coolidge v. New Hampshire, 403 U.S. 443, 465 (1971) (plurality opinion) (discussing the history and policies behind the plain view doctrine); Sam Kamin, *The Private Is Public: The Relevance of Private Actors in Defining the Fourth Amendment*, 46 B.C. L. REV. 83, 104–05 (2004) (noting how the plain view doctrine allows the police to discover evidence without implicating

These judges have noted that, without search protocols, the government could engage in a full scale review of the seized computers and thereby view data not within the warrant's scope.[62] The government cannot name at the outset where relevant data is stored on the seized device; thus, search protocols provide some form of particularized description as how the government will find the items to be seized.[63] Moreover, rather than having courts review the constitutionality of searches afterwards at motions to suppress, search protocols allow judges to establish the constitutional limits on searches before their execution.[64] By following search protocols, the government can search computers without violating the constitutional rights of defendants or risking suppression of any relevant evidence found in the search.[65]

Search protocols can range in technical detail, with some describing general strategies the government might employ in its search and others prescribing the precise methods and technologies the government must use.[66] Some

---

the Fourth Amendment's warrant requirement). For more extensive discussions of the plain view doctrine's application to digital searches, see Orin Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 576–84 (2005); Guzzi, *supra* note 41; James Saylor, Note, *Computers as Castles: Preventing the Plain View Doctrine from Becoming a Vehicle for Overbroad Digital Searches*, 79 FORDHAM L. REV. 2809 (2011).

[62] *See In re Search of 3817 W. West End*, 321 F. Supp. 2d at 962–63 (requiring a search protocol for a computer search because without a search protocol, the government would have "a license to roam through everything in the computer without limitation and without standards"); *In re Search Warrant*, 71 A.3d at 1183–84 (approving of a lower court's search protocol for a computer search because it was a permissible way to limit the scope of the government's search).

[63] *See In re Search Warrant*, 71 A.3d at 1171 (observing how it is difficult to initially describe the place to be searched in computer searches because "particular information is not accessed through corridors and drawers, but through commands and queries"); Athul K. Acharya, Note, *Semantic Searches*, 63 DUKE L.J. 393, 414 n.137 (noting how search protocols aim to describe the place to be searched (citing Ohm, *supra* note 46, at 9–10)).

[64] See *In re Search of 3817 W. West End*, 321 F. Supp. 2d at 962 (stating review at motion to suppress could lead to unnecessary exclusion of evidence); *see also* United States v. Carey, 172 F.3d 1268, 1276 (10th Cir. 1999) (excluding evidence found on defendant's computer because the search performed with a warrant but without a search protocol violated the particularity requirement); United States v. Barbuto, No. 2:00CR197K, 2001 WL 670930, at *5 (D. Utah Apr. 12, 2001) (granting a motion to suppress documents seized from the defendant's computer because the search violated the particularity requirement and stating that the government's "[search] methods or criteria should have been presented to the magistrate before the issuance of the warrants").

[65] *See Carey*, 172 F.3d at 1276 (suppressing evidence from a computer search done without a search protocol because the government's overly broad search violated the defendant's Fourth Amendment rights); *In re Search of 3817 W. West End*, 321 F. Supp. 2d at 962 (requiring a search protocol for a computer search so that relevant evidence would not be suppressed).

[66] *See In re Search of 3817 W. West End*, 321 F. Supp. 2d at 956 (discussing the different ways courts can craft search protocols and noting how courts can limit the search methods the government will use); *In re Search Warrant*, 71 A.3d at 1183–84 (approving of a lower court's search protocol that limited access to documents and files on the computer based on who created the documents and on what date the files were created); Derek Haynes, Note, *Search Protocols: Establishing the Protections Mandated by the Fourth Amendment Against Unreasonable Searches and Seizures in the World of Electronic Evidence*, 40 MCGEORGE L. REV. 757, 771 (2009) (noting that search protocols will

basic search protocols simply limit the search to data created during specific time periods or to certain types of data, for example only text files or image files.[67] Other search protocols place stricter limits on the search, requiring the government to provide the phrases and words it will use in keyword searches of the computer's documents.[68] Finally, the most exacting search protocols may combine all of these limitations and further require the government to name the software that it will use during the search and explain how the software will be used to identify relevant data.[69]

Commentators are divided as to both the efficacy and constitutionality of judicially required search protocols.[70] Professor Orin Kerr, one of the leading scholars on the Fourth Amendment's application to digital media, has argued that search protocols not only are ill-advised but also unconstitutionally infringe the police's power to execute warrants.[71] Others argue that without search protocols, computer search warrants represent a return to general warrants, and that judges who impose search protocols are merely striking an appropriate balance between the demands of the Fourth Amendment's particularity requirement and the needs of police to investigate crimes.[72]

---

ideally set forth precise descriptions of the information sought from the seized device and the techniques the police will use to discover that information).

[67] *See In re Search of 3817 W. West End*, 321 F. Supp. 2d at 956.

[68] *See id.*; Haynes, *supra* note 66, at 771–72. *But see* COMPUTER CRIME & INTELLECTUAL PROP. SECTION, CRIMINAL DIV., DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 79 (2009), http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf [http://perma.cc/ZED4-5LVF] (hereinafter COMPUTER CRIME) (describing the limitations of keyword searches and noting that "keyword searches will fail to find many kinds of files that fall within the scope of a warrant").

[69] *See In re Search Warrant*, 71 A.3d at 1182, 1184 (approving of a search protocol that required the police to obtain judicial preapproval before using certain software in a computer search and placed several other restrictions on how the police could search the computer); Haynes, *supra* note 66, at 765 (listing several common targeted search methods courts require in search protocols for digital searches); *see also In re Search of Apple iPhone*, 31 F. Supp. 3d 159, 166 (D.D.C. 2014) (denying a search warrant for a cell phone that failed to include a precise explanation of all the different tools the government would use to search the device).

[70] *See* Kerr, *supra* note 41, at 1246 (arguing that search protocols are misguided attempts at limiting warrants, and judges should simply consider whether search was reasonable after the warrant has been executed); Ohm, *supra* note 46, at 11–12 (asserting the importance of strategies like search protocols in preventing computer search warrants from becoming general warrants); *see also* Brenner, *supra* note 60, at 186 (recognizing the difficult questions surrounding the effectiveness and constitutionality of search protocols for computer searches).

[71] *See* Kerr, *supra* note 41, at 1246. Kerr believes judges should not, as a policy matter, and cannot, as a constitutional matter, set limits on the execution of warrants beforehand. *Id.* Rather, judges can only evaluate afterwards whether the police's execution of the warrant was reasonable. *Id.*

[72] *See* Friess, *supra* note 46, at 987 (arguing that judicial oversight through search protocols, specifically in search protocols for email searches, is necessary to balance the government's need to investigate crime and the people's Fourth Amendment rights); Ohm, *supra* note 46, at 11; Guzzi, *supra* note 41, at 335 (noting how if courts do not place limits on search warrants in the digital space, these warrants will become general warrants). Furthermore, they assert that earlier U.S. Supreme Court cases upon which Kerr bases his argument, such as *Dalia* and *Grubbs*, do not answer the ques-

### *C.* Riley v. California*: The U.S. Supreme Court Brings the Fourth Amendment to Cell Phones*

This section explains the U.S. Supreme Court's 2014 decision in *Riley v. California*, which applied the Fourth Amendment's warrant requirement to cell phone searches, but did not address what those search warrants must say.[73] Subsection 1 discusses the history of warrantless searches and the circuit split before *Riley* regarding whether the police could search cell phones without a warrant incident to an arrest.[74] Subsection 2 provides an overview of the *Riley* decision and its potential impact on cell phone search warrants.[75]

#### 1. The History of the Search Incident to Arrest Exception to the Warrant Requirement

Although a search performed without a warrant is presumed unreasonable, the U.S. Supreme Court has long recognized the police's right to search an arrestee's person incident to arrest without a warrant.[76] In 1973, in *United States v. Robinson*, the U.S. Supreme Court held that a police officer could open a cigarette pack found on the defendant during a search of his person without obtaining a warrant.[77] The Court reasoned that the officer's safety concerns and the threat of the destruction of evidence justified the warrantless search.[78]

---

tion of how the particularity requirement applies to digital media. *See* Friess, *supra* note 46, at 1015 (reading *Dalia* to potentially support search protocols because *Dalia* identified ex ante restrictions on warrants as the "preferable approach" (quoting *Dalia*, 441 U.S. at 259 n.22)); Ohm, *supra* note 46, at 3, 11.

[73] *See infra* notes 73–94 and accompanying text.

[74] *See infra* notes 76–85 and accompanying text.

[75] *See infra* notes 86–94 and accompanying text.

[76] *See Riley II*, 134 S. Ct. at 2482 (stating "a search is reasonable only if it fails within a specific exception to the warrant requirement"); *id.* at 2495 (Alito, J., concurring) (characterizing the search incident to arrest exception to the warrant requirement as an "ancient rule"); *Stuart*, 547 U.S. at 403 (stating that "[t]he ultimate touchstone of the Fourth Amendment is reasonableness"); Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 653 (1995) (noting how for a search to be reasonable, the government usually must have a warrant); *Payton*, 445 U.S at 590 (holding a warrantless entry into a home to make a felony arrest violated the Fourth Amendment, absent exigent circumstances); United States v. Robinson, 414 U.S. 218, 236 (1973) (holding a warrantless search of an arrestee's person incident to his arrest did not violate the Fourth Amendment); Weeks v. United States, 232 U.S. 383, 392 (1914) (describing how courts have repeatedly affirmed the government's right to search people incident to their arrests).

[77] *See Robinson*, 414 U.S. at 236 (holding that a police officer had right to inspect a cigarette pack and had authority to seize heroin found within the cigarette pack as evidence of criminal conduct).

[78] *See id.* at 234 (stating the justification for a warrantless search incident to arrest of an arrestee's person "rests quite as much on the need to disarm the suspect in order to take him into custody as it does on the need to preserve evidence on his person for later use at trial"); *see also Riley II,* 134 S. Ct. at 2485 (explaining how *Robinson* established the dual justifications for the search incident to arrest exception even when there is no perceived threat to officer safety or of the destruction of evidence); Chimel v. California, 395 U.S. 752, 762–63 (1969) (holding that an arresting officer may search the

In 2013, courts began to split over whether *Robinson* allowed the police to search cell phones incident to arrest without a warrant.[79] Several circuit courts held the police could search cell phones incident to an arrest without first obtaining a warrant.[80] Similarly, in February 2013, in *People v. Riley*, the Court of Appeal for the Fourth District of California affirmed the denial of a motion to suppress evidence obtained from the warrantless search of the defendant's cell phone incident to his arrest.[81] In contrast, in May 2013, in *United States v. Wurie*, a divided panel of the U.S. Court of Appeals for the First Circuit held that the police could not search a cell phone incident to an arrest without a separate search warrant.[82]

---

arrestee for weapons and any evidence on the arrestee's person in order to prevent the destruction of evidence).

[79] *Compare* United States v. Wurie, 728 F.3d 1, 12–13 (1st Cir. 2013) (holding that the search incident to arrest exception to the warrant requirement did not apply to cell phone searches), *aff'd sub nom*. Riley v. California (*Riley II*), 134 S. Ct. 2473, *with* People v. Riley (*Riley I*), No. D059840, 2013 WL 475242, at *6 (Cal. Ct. App. Feb. 8, 2013) (holding that the search incident to arrest exception to the warrant requirement did apply to cell phone searches), *rev'd sub nom*. Riley v. California, 134 S. Ct. 2473.

[80] *See* United States v. Flores-Lopez, 670 F.3d 803, 807 (7th Cir. 2012) (holding the police could search an arrestee's phone to find the phone number linked to the device, but indicating more invasive cell phone searches could require warrants); United States v. Curtis, 635 F.3d 704, 712 (5th Cir. 2011) (recognizing that the Fourth, Fifth, Seventh, and Tenth Circuits all allow warrantless cell phone searches incident to arrest); Silvan W. v. Briggs, 309 Fed. App'x. 216, 225 (10th Cir. 2009) (holding the police can search a person's phone incident to arrest); United States v. Murphy, 552 F.3d 405, 411–12 (4th Cir. 2009) (holding the police could retrieve and read text messages from a cell phone found on an arrestee's person because the need to preserve evidence on the phone justified the warrantless search); *see also* Charles E. MacLean, *But Your Honor, a Cell Phone Is Not a Cigarette Pack: An Immodest Call for a Return to the* Chimel *Justifications for Cell Phone Memory Searches Incident to a Lawful Arrest*, 6 FED. CTS. L. REV. 37, 54 (2012); Sara M. Corradi, Comment, *Be Reasonable! Limit Warrantless Smart Phone Searches to* Gant*'s Justification*, 63 CASE W. RES. L. REV. 943, 948–49 (2013); Evan O'Connor, Comment, *The Search for a Limited Search: The First Circuit Denies the Search of Cell Phones Incident to an Arrest*, 55 B.C. L. REV. E. SUPP. 59, 64 (2013) http://bclawreview.org/files/2014/02/05_OConnor.pdf [http://perma.cc/UGM2-PP6Z] (discussing the circuit split on whether cell phones can be searched incident to arrest without a warrant).

[81] *See Riley I*, 2013 WL 475242, at *6. The defendant was arrested on weapons charges and, during a search of his person, the police seized his cell phone. *See id.* at *1–2. Detectives, who were investigating the defendant's involvement in an attempted murder, examined the phone's contact list, and viewed videos and pictures on the phone, finding evidence that defendant was a member of a gang. *See id.* at *3. As the defendant's case was pending trial, in 2011, in *People v. Diaz*, the California Supreme Court held the police could search cell phones incident to an arrest without a warrant. *Id.*; People v. Diaz, 244 P.3d 501, 505 (Cal. 2011). Therefore, the California Court of Appeal applied *Diaz* to the defendant's case and upheld denial of the motion to suppress the evidence found on the phone. *See Riley I*, 2013 WL 475242, at *6.

[82] *Wurie*, 728 F.3d at 13; *see also* Roy K. Altman, *The Case for Incident-to-Arrest Searches of Cell Phones*, 29 CRIM. JUST. 28, 28 (2014) (noting how the First Circuit was the only federal appellate court to deny warrantless searches of cell phones incident to arrest and criticizing the First Circuit's distinction between cell phones and other property that may be searched incident to arrest); O'Connor, *supra* note 80, at 63–64 (discussing how the First Circuit found that the search incident to arrest exception should not apply because there was no immediate need for the police to search the phone). The First Circuit stated that to allow the police to search a cell phone incident to an arrest for even the

In order to resolve this deepening split, on January 17, 2014, the U.S. Supreme Court granted certiorari to both *Riley* and *Wurie*.[83] When the Court heard oral arguments on April 29, 2014, the justices appeared skeptical of California and the United States' position that the police should always be allowed to search cell phones incident to an arrest without a warrant.[84] At the same time, the justices questioned how to limit the scope of cell phone search warrants if the Court were to require them.[85]

---

most minor of traffic infractions would authorize the exact type of unfettered government rummaging the Fourth Amendment was designed to prevent. *See Wurie*, 728 F.3d at 9. The court recognized that most people carry a significant amount of personal and private information in their cell phones, far more information than individuals would have previously carried on their person. *See id.* Furthermore, the court concluded its duty to provide clear guidelines to officers in the field compelled them to craft a bright-line rule: absent exigent circumstances, the police must get a warrant to search a cell phone. *See id.* at 13. The dissent argued that the court should not disregard longstanding Fourth Amendment precedent on searches incident to arrest just because the object searched is a cell phone. *See id.* at 14 (Howard, J., dissenting).

[83] *See* Riley v. California, 134 S. Ct. 999, 999 (2014) (mem.) (granting certiorari); United States v. Wurie, 134 S. Ct. 999, 999 (2014) (mem.) (same); Adam Lamparello & Charles MacLean, *Back to the Future: Returning to Reasonableness and Particularity Under the Fourth Amendment*, 99 IOWA L. REV. BULL. 101, 102 (2014) http://ilr.law.uiowa.edu/files/ilr.law.uiowa.edu/files/ILRB_99_LamparelloMacLean.pdf [http://perma.cc/T8VG-ALUR] (noting the U.S. Supreme Court's grant of certiorari and calling on the Court to require warrants to search cell phones); Lyle Denniston, *Court to Rule on Cellphone Privacy*, SCOTUSBLOG (Jan. 17, 2014, 2:33 PM), http:// www.scotusblog.com/2014/01/court-to-rule-on-cellphone-privacy/ [http://perma.cc/RB8V-V3BP] (observing how the Court's grant of certiorari would pit police power against new privacy interests in technology).

[84] *See* Oral Argument at 0:04, 28:00, *Riley II*, 134 S. Ct. 2473 (No. 13-132), http://www.oyez.org/cases/2010–2019/2013/2013_13_132 [hereinafter *Riley II* Oral Argument]; Amy Howe, *A Whole New World: Today's Oral Arguments in Plain English*, SCOTUSBLOG (Apr. 29, 2014, 5:20 PM), http://www.scotusblog.com/2014/04/a-whole-new-world-todays-oral-arguments-in-plain-english/ [http://perma.cc/LYC2-2CKJ] (describing the justices' criticisms of the government's argument and the justices' search for a more limited approach).

[85] *See Riley II* Oral Argument, *supra* note 84, at 12:08, 16:48. Chief Justice John Roberts wondered how a judge could limit the scope of a warrant when it could often be reasonable to assume that the entirety of the phone could have relevant evidence. *See id*. at 12:30, 14:00. Riley's attorney tried to list applications that would hold no relevant evidence, citing a banking application as having no reasonable connection to a drug offense. *See id.* Chief Justice Roberts responded that a bank transaction could demonstrate when a particular drug deal took place. *See id.* Justice Elena Kagan stated that a magistrate could place whatever limitations on the warrant he or she feels are appropriate. *See id.* at 55:53. Assistant Solicitor General Michael Dreeben disagreed with Justice Kagan's assertion and cited to *Grubbs* and *Dalia* as precluding a magistrate from setting forth limitations on how the police execute the warrant. *See id.* at 56:00. Before the discussion could continue, Dreeben's time expired. *See id*. at 56:30. Professor Kerr noted this exchange at oral argument between Justice Kagan and Dreeben as demonstrative of the future issues involving search protocols and searches of digital media. *See* Orin Kerr, *The Role of Warrants in the Cell Phone Search Cases*, VOLOKH CONSPIRACY (Apr. 29, 2014), http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/04/29/the-role-of-warrants-in-the-cell-phone-search-cases/ [http://perma.cc/83LR-LDW2].

2. *Riley v. California*: The Court Reaffirms the Warrant Requirement

On June 25, 2014, in *Riley v. California*, the U.S. Supreme Court unanimously held that the police must obtain a warrant before searching a cell phone in order to comply with the Fourth Amendment.[86] Writing for the Court, Chief Justice Roberts recognized how modern cell phones have become an essential part of the daily lives of most Americans.[87] To the Court, because cell phones often store massive amounts of personal information, it would be inappropriate to allow officers immediate access to cell phones.[88] The Court compared cell phones to homes, the most protected of spaces under the Fourth Amendment, and noted that the search of a cell phone would in many cases reveal more information than even an extensive search of a home.[89] The Court stated that to allow the search of cell phones incident to arrests would be to allow the exact type of limitless searches the Fourth Amendment was designed to prohibit.[90]

Both the Court's unanimity and its bright-line rule requiring a search warrant for cell phones surprised many Fourth Amendment scholars and sparked debate over the future applications of the decision.[91] In recent years, the Court has often deferred to the Fourth Amendment's reasonableness requirement and, in many contexts, allowed warrantless government searches.[92] To flatly require

---

[86] *See Riley II*, 134 S. Ct. at 2495. The Court did note that the exigent circumstances exception to the warrant requirement would likely still likely apply to cell phone searches. *Id.* at 2494. Justice Samuel Alito joined the court's opinion in part, but wrote a separate concurrence to discuss the history of the search incident to arrest exception and to emphasize that his view on cell phone searches may change if Congress and state legislatures enacted statutes regulating these searches. *See id.* at 2495, 2497 (Alito, J., concurring).

[87] *See id.* at 2484 (majority opinion) (describing how a "proverbial visitor from Mars might conclude [cell phones] were an important feature of human anatomy").

[88] *See id.* at 2485.

[89] *See id.* at 2491.

[90] *See id.* at 2494–95. The Court invoked the historical impetus for the Fourth Amendment, recounting how the British government used general warrants to search invasively through the private lives and materials of American colonists. *Id.*

[91] *See* Ryan Watzel, Riley*'s Implications for Fourth Amendment Protection in the Cloud*, 124 YALE L.J. F. 73 (2014), http://www.yalelawjournal.org/forum/rileys-implications-in-the-cloud [http://perma.cc/63G3-Y7ZF] (noting how the court provided a clear answer to whether a warrant is required to search a phone); Adam Gershowitz, *Symposium: Surprising Unanimity, Even More Surprising Clarity*, SCOTUSBLOG (June 26, 2014, 11:02 AM), http://www.scotusblog.com/2014/06/symposium-surprising-unanimity-even-more-surprising-clarity/ [http://perma.cc/5MMW-QPFE] (asserting that the Court's unanimous holding was "rather startling"); Amy Howe, *Get a Warrant! Today's Cellphone Privacy Decision in Plain English*, SCOTUSBLOG (June 25, 2014, 5:25 PM), http://www.scotusblog.com/2014/06/get-a-warrant-todays-cellphone-privacy-decision-in-plain-english/ [http://perma.cc/7ZP2-Q7XR] (expressing surprise over the Court's unanimity because the Court dealt with such an important privacy issue).

[92] *See, e.g.*, *King*, 131 S. Ct. at 1858 (holding a warrantless entry into home was justified by the exigency of the threat of destruction of evidence); Arizona v. Gant, 556 U.S. 332, 346 (2009) (holding a warrantless search of an arrestee's car is permitted when an arrestee is in reaching distance of the vehicle or when an officer reasonably believes the vehicle contains evidence of the offense of arrest);

a warrant was a major surprise to many observers.[93] Scholars immediately began to speculate about how lower courts would apply *Riley* both when issuing cell phone search warrants and when hearing particularity challenges to cell phone search warrants.[94]

## II. LOWER COURTS ATTEMPT TO CRAFT CELL PHONE SEARCH WARRANTS THAT COMPLY WITH THE FOURTH AMENDMENT'S PARTICULARITY REQUIREMENT

After the U.S. Supreme Court's 2014 decision in *Riley v. California*, the question remained: what must a cell phone search warrant contain to satisfy the Fourth Amendment's particularity requirement?[95] Accordingly, this Part outlines how lower courts have limited the scope of cell phone search warrants.[96] Section A discusses courts that have required detailed search protocols for cell phone search warrants in order to comply with the Fourth Amendment's particularity requirement.[97] Section B examines courts that have not required search protocols for cell phone search warrants.[98]

### *A. Ensuring Particularity with Search Protocols: Courts Requiring Search Protocols for Cell Phone Search Warrants*

In 2014, two magistrate judges in two different federal district courts held that the government must submit search protocols along with their warrant applications for cell phone searches in order to meet the Fourth Amendment's particularity requirement.[99] U.S. Magistrate Judge John M. Facciola of the Dis-

---

*Stuart*, 547 U.S. at 403 (stating that "[t]he ultimate touchstone of the Fourth Amendment is reasonableness").

[93] *See The Supreme Court, 2013 Term—Leading Cases*, 128 HARV. L. REV. 251, 251 (2014) (stating the *Riley* decision represents a break from the U.S. Supreme Court's trend of allowing searches without warrants); Gershowitz, *supra* note 91; Richard Re, *Symposium: Inaugurating the Digital Fourth Amendment*, SCOTUSBLOG (June 26, 2014, 12:37 PM), http://www.scotusblog.com/2014/06/symposium-inaugurating-the-digital-fourth-amendment/ [http://perma.cc/F7YE-4Z33] (seeing *Riley* as founding a new era of Fourth Amendment interpretation and protection in the digital age).

[94] *See* Pincus, *supra* note 12, at 329–36 (discussing the potential applications of *Riley* on email messages, cell phone location information, and border searches of digital information); Hall, *supra* note 13 (arguing that the particularity requirement will be a recurring issue in warrants for cell phone searches); Re, *supra* note 93 (arguing that after *Riley*, more defendants will challenge computer searches, including searches done pursuant to warrants).

[95] *See* Riley v. California (*Riley II*), 134 S. Ct. 2473, 2495 (2014) (holding that the police must obtain a warrant before searching a cell phone); Hall, *supra* note 13 (noting how the Court did not resolve how arguing the particularity requirement applies to cell phone searches).

[96] *See infra* notes 96–157 and accompanying text.

[97] *See infra* notes 99–140 and accompanying text.

[98] *See infra* notes 141–157 and accompanying text.

[99] *See, e.g.*, *In re* Cellular Tels., No. 14-MJ-8017-DJW, 2014 WL 7793690, at *1 (D. Kan. Dec. 30, 2014); *In re* Search of Premises Known as Three Cellphones & One Micro-SD Card, No. L4-MJ-8013-DJW, 2014 WL 3845157, at *1 (D. Kan. Aug. 4, 2014); *In re* Nextel Cellular Tel., No. 14-MJ-

trict Court for the District of Columbia and U.S. Magistrate Judge David Waxse of the District Court for the District of Kansas have both refused to issue search warrants for cell phones without detailed search protocols that clearly explain how the government will avoid searching and seizing material outside the warrant's scope.[100] Both judges reasoned that issuing cell phone search warrants without search protocols would authorize the type of general searches that the Fourth Amendment forbids.[101] Subsection 1 discusses Judge Facciola's opinions requiring search protocols.[102] Subsection 2 discusses Judge Waxse's interpretation of *Riley* as mandating search protocols for cell phone search warrants.[103]

### 1. U.S. Magistrate Judge Facciola of the District Court for the District of Columbia Establishes the Model for Cell Phone Search Protocols

In March 2014, U.S. Magistrate Judge Facciola of the District Court for the District of Columbia issued a series of three opinions denying cell phone search warrant applications because each application failed to include a detailed search protocol and thereby violated the Fourth Amendment's particularity requirement.[104] First, on March 11, 2014, in *In re Search of Black iPhone 4*,

---

8005-DJW, 2014 WL 2898262, at *14 (D. Kan. June 26, 2014); *In re* Search of Apple iPhone, 31 F. Supp. 3d 159, 168 (D.D.C. 2014); *In re* Search of ODYS LOOX Plus Tablet Serial No. 4707213703415 in Custody of U.S. Postal Inspection Serv., 1400 New York Ave. NW, Wash., D.C., 28 F. Supp. 3d 40, 46 (D.D.C. 2014); *In re* Search of Black iPhone 4, 27 F. Supp. 3d 74, 79 (D.D.C. 2014); *see also* Hall, *supra* note 13 (discussing how the District Court for the District of Kansas relied on *Riley* to require search protocols for cell phone search warrants).

[100] *See In re Nextel Cellular Tel.*, 2014 WL 2898262, at *12 (requiring the government to submit a search protocol that precisely explained how the police determine what sections of the smartphone's hard drive are within the scope of the warrant); *In re Search of Apple iPhone*, 31 F. Supp. 3d at 168 (finding deficient the government's proposed search protocol because it failed to provide the method by which the government would decide where on the phone it would search).

[101] *See In re Nextel Cellular Tel.*, 2014 WL 2898262, at *14 (stating how "[i]f the Court were to authorize this warrant, it would be contradicting the manifest purpose of the Fourth Amendment particularity requirement, which is to prevent general searches"); *In re Search of Black iPhone 4*, 27 F. Supp. 3d at 78 (stating the government's proposed warrant would authorize "precisely the type of 'general, exploratory rummaging in a person's belongings' that the Fourth Amendment prohibits" (quoting Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971) (plurality opinion))).

[102] *See infra* notes 104–127 and accompanying text.

[103] *See infra* notes 128–140 and accompanying text.

[104] *See In re Search of Apple iPhone*, 31 F. Supp. 3d at 168; *In re Search of ODYS LOOX Plus Tablet Serial No. 4707213703415*, 28 F. Supp. 3d at 46; *In re Search of Black iPhone 4*, 27 F. Supp. 3d at 79. Judge Facciola has issued several controversial opinions involving the Fourth Amendment's application to digital technology. *See In re* Search of Info. Associated with [Redacted]@mac.com That Is Stored at Premises Controlled by Apple, Inc., 13 F. Supp. 3d 145, 152 (D.D.C.) (denying the government's warrant application for all emails associated with a specific email address because the warrant would authorize the seizure of emails for which probable cause had not been established), *vacated*, 13 F. Supp. 3d 157 (D.D.C. 2014); *In re* Application of the U.S. of Am. for a Search Warrant for a Black Kyocera Corp. Model C5170 Cellular Tel. with FCCC ID: V65V5170, No. 14-231 (JMF), 2014 WL 1089442, at *2 (D.D.C. Mar. 7, 2014) (denying the government's war-

the District Court for the District of Columbia denied a warrant application that sought to search and seize "[a]ll records contained in the cellular phones."[105] Judge Facciola stated that the application failed to specify the information sought and failed to explain how the government would avoid seizing irrelevant information.[106] Judge Facciola explained that a detailed search protocol would address the court's concerns and suggested that future warrant applications for cell phones contain search protocols.[107]

In a warrant application nine days later, the government did submit a search protocol, but it failed to address Judge Facciola's particularity concerns.[108] On March 20, 2014, in *In re Search of ODYS LOOX Plus Tablet Serial Number 4704213703415*, the District Court for the District of Columbia denied a warrant application to search several mobile devices.[109] The application included a search protocol, which set forth in general terms how the government would

---

rant application to search a cell phone the defendant dropped while the police pursued him because no warrant is required to search abandoned property); *In re* Search of Information Associated with the Facebook Account Identified by the Username Aaron.Alexis That Is Stored at Premises Controlled by Facebook, Inc., 21 F. Supp. 3d 1, 7, 10 (D.D.C. 2013) (holding the government lacked probable cause to search and seize Facebook account information from third parties who communicated with a specific Facebook user and requiring minimization procedures to limit data seized from Facebook); Ann E. Marimow & Craig Timberg, *Low-Level Federal Judges Balking at Law Enforcement Requests for Electronic Evidence*, WASH. POST (Apr. 24, 2014), http://www.washingtonpost.com/local/crime/low-level-federal-judges-balking-at-law-enforcement-requests-for-electronic-evidence/2014/04/24/eec81748-c01b-11e3-b195-dd0c1174052c_story.html [http://perma.cc/SFH7-N6XB] (describing Judge Facciola's opinions as some of the "most aggressive" rebukes of law enforcement requests for digital personal data); Joe Palazzolo, *Judges Rebel Against Prosecutors' Bulk Requests for Emails in Probes*, WALL ST. J. (Apr. 4, 2014, 6:56 PM), http://www.wsj.com/articles/SB10001424052702303847804579479513205095706 [http://perma.cc/ME9A-3VL5] (discussing Judge Facciola's repeated denials of broad applications to search email accounts).

[105] *See In re Search of Black iPhone 4*, 27 F. Supp. 3d at 75, 80. During an investigation regarding the distribution of child pornography, the government obtained a warrant to search a hotel room. *See id.* at 76. The government seized six computing devices, including an iPhone 4 and two Samsung cell phones. *See id.* The government further stated that it wished to seize: "Any and all list of names, telephone numbers, and addresses stored as contacts to include pictures. . . . Images, pictures, photographs sent or received by user. . . . The content of any and all text messages sent or received by user. . . . The content of any and all voice mail messages. . . . Any and all evidence of passwords needed to access the user cell phone." *Id.*

[106] *See id.* at 78.

[107] *See id.* at 79. The court posed several questions that it hoped future warrant applications would answer, including whether all of the cell phones would be imaged, how long any such images would be stored, what procedures the government would use to avoid viewing material outside the warrant's scope, and what would happen if the government discovered unrelated incriminating evidence during its search. *See id.* at 79–80.

[108] *See In re Search of ODYS LOOX Plus Tablet Serial No. 4707213703415*, 28 F. Supp. 3d at 46.

[109] *See id.* at 43. During a search of the defendant's hotel room as a part of an investigation into the distribution of child pornography, the government seized four electronic devices: a Sony laptop, a Fujifilm digital camera, an LG cell phone, and an ODYS tablet. *See id.* at 41–42. The government's warrant application to search the devices contained three attachments: Attachment A, which described the devices to be searched, Attachment B, which described the information to be seized, and Attachment C, which was titled "Search Protocol." *See id.*

search the mobile devices.[110] The court held that some sections of the government's search protocol failed to provide necessary details on how the search would be executed.[111] At the same time, the court found that other sections of the protocol proposed search methods it would not authorize.[112] For example, as a part of its search, the government sought to "image" each device's internal storage, a process that creates a copy of the device's entire hard drive.[113] Judge Facciola rejected this search method, stating that imaging by its nature would seize data beyond the proper scope of the investigation.[114] Judge Facciola concluded that unless the search protocol provided a technical explanation of how the government would conduct a more limited search of the defendant's phone, the warrant application would fail to meet the Fourth Amendment's particularity requirement.[115]

A week later, Judge Facciola denied another of the government's cell phone search protocol submissions and explained in greater detail why the particularity requirement mandates search protocols for cell phone search warrants.[116] On March 26, 2014, in *In re Search of Apple iPhone, IMEI*

---

[110] *Id.* at 43. In the proposed search protocol in Attachment C, the government noted that it planned to image the seized devices, that it would provide copies of the files it seized upon request, and that if during its search the government found evidence of criminal activity beyond the warrant's scope, it would apply for a new search warrant. *Id.* The government also made clear that it still did not believe a search protocol was required for its search, basing its reasoning on Professor Kerr's view of search protocols. *Id.* (citing Kerr, *supra* note 41, at 1242).

[111] *See id.* at 44–45 (stating Attachment B's list of items to be seized "should serve as a model . . . for future applications," but finding Attachment C's proposed search protocol failed to address the court's concerns on the warrant's scope). The proposed search protocol failed to make clear whether the government would retain electronic copies of all the data contained in the devices and also failed to explain whether the investigating officers would be involved in the search of the devices, a detail the court wished to know in order to better understand who would be involved in the search. *See id.* at 45.

[112] *See id.*

[113] *See id.*; MICHAEL J. HANNON, DIGITAL EVIDENCE: COMPUTER FORENSICS AND LEGAL ISSUES ARISING FROM COMPUTER INVESTIGATIONS 15 (2012) (explaining how computer forensic specialists create images, also called "mirror images" and "bit stream images," when searching and seizing devices). The government would retain this image until the defendant's case, including any appeals, had concluded. *See In re Search of ODYS LOOX Plus Tablet Serial No. 4707213703415*, 28 F. Supp. 3d at 45. The government argued that it needed to retain the complete image of the device's hard drive because a partial image of the device, from which information had been deleted, might present later chain of custody issues. *See id.* at 46. The court disagreed, saying that the same testimony about chain of custody for a complete image of the device's hard drive would suffice for a partial image. *See id.*

[114] *See In re Search of ODYS LOOX Plus Tablet Serial No. 4707213703415*, 28 F. Supp. 3d at 45.

[115] *See id.* at 46.

[116] *See In re Search of Apple iPhone*, 31 F. Supp. 3d at 166, 169 (stating detailed search protocols help satisfy the Fourth Amendment's particularity requirement and denying the government's warrant application for failing to provide enough details in its proposed search protocol); *see also* Tim Cushing, *DC Judge Smacks Down Government for Vague iPhone Search Warrant*, TECHDIRT (Apr. 9, 2014), https://www.techdirt.com/articles/20140404/10040126800/dc-judge-smacks-down-government-vague-iphone-search-warrant.shtml [https://perma.cc/KRB9-2Q9Z] (characterizing the court as fighting for Fourth Amendment rights against the government's expansive view of digital searches); Cyrus Fari-

*013888003738427*, the District Court for the District of Columbia considered the government's warrant application to search a college student's iPhone.[117] The application contained a new section titled "Electronic Storage and Forensic Analysis," which gave some examples of forensic methods the government would use in searching the iPhone.[118] The new section explained that the government would subject the entire phone to "computer-assisted scans" and, relying on those scans, search smaller parts of the phone via "human inspection."[119] Again the court denied the government's application, holding that phrases such as "computer-assisted scans" were too broad and placed insufficient limits on the search.[120] To Judge Facciola, a permissible search protocol must explain with technical language the exact methods the government will use when deciding where on the phone it will search and for what it will search.[121]

---

var, *Judge Denies Gov't Request to Search Suspect's iPhone in Ricin Case*, ARS TECHNICA (Mar. 26, 2014), http://arstechnica.com/tech-policy/2014/03/judge-denies-govt-request-to-search-suspects-iphone-in-ricin-case/ [http://perma.cc/XNZ8-47SA] (discussing the court's desire for specific technical language in future search protocols); Dan Ivers, *Feds Lose Bid to Search Phone in Georgetown Ricin Case*, LAW360 (Mar. 26, 2014), http://www.law360.com/articles/522156/feds-lose-bid-to-search-phone-in-georgetown-ricin-case [http://perma.cc/6DAP-WCWK] (observing that the court "chastised the government" for failing to provide specific details on how the government would conduct its search); Sara Kropf, *Did the Founding Fathers Think the Fourth Amendment Would Protect Our iPhones?*, GRAND JURY TARGET (Apr. 15, 2014), http://grandjurytarget.com/2014/04/15/did-the-founding-fathers-think-the-fourth-amendment-would-protect-our-iphones/ [http://perma.cc/543K-NMQB] (applauding the court for resisting the government's efforts to search beyond the scope of its investigation and considering whether other courts would follow the court's reasoning).

[117] *See In re Search of Apple iPhone*, 31 F. Supp. 3d at 161. The government was investigating the student for manufacturing ricin in his dorm room. *See id.* The student told investigators that he found the formula for ricin searching the Internet on his iPhone. *See* Justin Jouvenal & Ann E. Marimow, *In Georgetown Ricin Case, a Portrait of a Student with a Sharp Mind, Many Troubles*, WASH. POST (Mar. 25, 2014), http://www.washingtonpost.com/local/crime/georgetown-student-alleged-to-have-ricin-may-have-been-a-threat-to-someone/2014/03/25/73ba55d6-b434-11e3-8020-b2d790b3c9e1_story.html [http://perma.cc/4NQM-N72L]. The student later pleaded guilty to unregistered possession of a biological agent or toxin. *See* Keith Alexander, *Georgetown Student Gets 1-Year Term for Possession of Ricin He Said Was for Suicide*, WASH. POST (Nov. 10, 2014), http://www.washingtonpost.com/local/crime/georgetown-university-student-expected-to-be-sentenced-for-possessing-ricin/2014/11/10/318c4466-68d5-11e4-9fb4-a622dae742a2_story.html [http://perma.cc/T3U7-WJ8Y]; Jouvenal & Marimow, *supra*.

[118] *See In re Search of Apple iPhone*, 31 F. Supp. 3d at 162–63. This section stated that the search may involve scans of the entire device in order to determine what data on the device is evidence within the warrant's scope. *Id.* at 163. According to the application, more specific searches, such as targeted keyword searches, could fail to expose certain types of data relevant to the investigation. *Id.* The section also explained how investigators and an FBI technical review team would work together to analyze the iPhone, addressing the concern raised in *In re Black iPhone 4* as to whether investigators would be involved in the search of the devices. *Id.*

[119] *See id.*

[120] *See id.* at 166.

[121] *See id*. The court encouraged the government to use phrases such as "MD5 hash values," "metadata," "registry," "write blocking," and "status marker," and to name specific software used for the search in its future applications. *See id.* at 168.

Judge Facciola found earlier views of the particularity requirement, such as the U.S. Supreme Court's 1979 decision in *Dalia v. United States*, inapplicable to search protocols.[122] According to Judge Facciola, search protocols do not limit how the government executes a warrant.[123] Rather, a detailed search protocol explains to the court how the government will determine the *place* to be searched.[124] In *Dalia*, the government had set forth a particular description of the place to be searched—it described in detail the office in which it would install the listening device.[125] Unlike in *Dalia*, the government could not specify beforehand the exact place in the iPhone's memory it would search, for without some form of initial scan, it could not determine which parts of the phone's internal storage may contain relevant data.[126] To Judge Facciola, because the government could not at the outset provide a particularized description of the place to be searched, it had to provide a detailed search protocol to assure the court that it had a certain location in mind.[127]

### 2. U.S. Magistrate Judge Waxse of the District Court for the District of Kansas Finds *Riley v. California* Mandates Cell Phone Search Protocols

Like Judge Facciola, Judge Waxse has also found that the particularity requirement mandates search protocols for cell phone search warrants.[128] For

---

[122] *See id.* at 167 (citing Dalia v. United States, 441 U.S. 238, 257–58 (1979)).

[123] *See id. But see* Kerr, *supra* note 41, at 1266 (arguing that mandatory search protocols in warrants for computer searches resemble the restrictions on bugging warrants found constitutionally unnecessary in *Dalia*). Most scholars who argue for search protocols in digital searches differ from Judge Facciola's view, asserting that search protocols are limits on how the government executes warrants, but that they are constitutionally permissible. *See* Friess, *supra* note 46, at 1015 (interpreting *Dalia* to encourage limitations on the execution of warrants even if the Fourth Amendment does not require such limitations); Ohm, *supra* note 46, at 3–4 (reading *Dalia* to allow, but not mandate, ex ante restrictions on searches); Guzzi, *supra* note 41, at 310 n.62 (noting *Dalia* does not state that a judge cannot place limitations on how the government will execute warrants).

[124] *See In re Search of Apple iPhone*, 31 F. Supp. 3d at 167.

[125] *See Dalia*, 441 U.S. at 256 (finding the challenged warrant particularly described the office the government sought to bug).

[126] *See In re Search of Apple iPhone*, 31 F. Supp. 3d at 167. The court viewed the place to be searched as the component parts of the phone's flash drive. *See id.* The court explained how the Apple iPhone's NAND flash drive contains a series of blocks, known as NAND Flash blocks, which are the smallest erasable unit of the device. *See id.* Without running some form of computer scan, the government could not possibly determine what type of data each block contains. *See id.*

[127] *See id.* The court relied on the Vermont Supreme Court's opinion in *In re Search Warrant*, which upheld a lower court's power to require search protocols for computer searches. *See* 71 A.3d 1158, 1171 (Vt. 2012) (holding detailed search protocols to be "an acceptable way," but not a constitutionally required method, of particularly describing the place to be searched), *cert. denied*, 133 S. Ct. 185 (2013).

[128] *See In re Cellular Tels.*, 2014 WL 7793690, at *1, *2 (applying *Riley* to hold that cell phone search warrants must contain search protocols); *In re Search of Premises Known as Three Cellphones*, 2014 WL 3845157, at *2 (same); *In re Nextel Cellular Tel.*, 2014 WL 2898262, at *14 (same). Like Judge Facciola, Judge Waxse has also issued several controversial decisions on the Fourth Amendment's application to searches of digital media. *See In re Search of Premises Known as Three Cell-*

example, on June 26, 2014, in *In re Nextel Cellular Telephone*, the District Court for the District of Kansas denied a warrant application for a cell phone search because the application's proposed search protocol was overly broad.[129] The government's warrant application included a search protocol in a section titled "Search Methodology To Be Employed."[130] The protocol gave examples of some general search methods the government might utilize, including examining all of the data stored in the phone in order to determine what information is relevant to its investigation.[131] The court held the proposed search methods violated the particularity requirement because they allowed the government to engage in general rummaging without naming a specific place on the phone it would search or the items it hoped to seize.[132]

Judge Waxse grounded his decision in the U.S. Supreme Court's 2014 decision in *Riley v. California* and in Judge Facciola's series of D.C. District

---

*phones*, 2014 WL 3845157, at *2; *In re Nextel Cellular Tel.*, 2014 WL 2898262, at *14; *In re* Applications for Search Warrants for Info. Associated with Target Email Accounts/Skype Accounts, No. 13-MJ-8163-JPO, 2013 WL 4647554, at *8 (D. Kan. Aug. 27, 2013) (denying a warrant application authorizing search and seizure of all email communications associated with a specific email account because the search would be overly broad); *In re* Applications for Search Warrants for Info. Associated with Target Email Address, No. 12-MJ-8119-DJW, 2012 WL 4383917, at *9 (D. Kan. Sept. 21, 2012) (denying a warrant application because the government failed to show probable cause to search the contents of all emails associated with a specific email address); Julie Bort, *This Judge Blocked the Feds from Reading Emails Stored by Yahoo, Google, Verizon, Skype*, BUS. INSIDER (Sept. 6, 2013), http://www.businessinsider.com/judge-says-no-to-feds-reading-emails-2013-9 [http://perma.cc/6BAF-YHDK] (calling Judge Waxse's denial of a warrant to search email accounts an interesting and meaningful opinion limiting the government's surveillance powers); Hall, *supra* note 13 (stating that Judge Waxse's opinion in *In re Nextel Cellular Telephone* was a fascinating application of the *Riley* decision); Palazzolo, *supra* note 104 (discussing Judge Waxse's rejection or modification of warrant applications involving searches of digital media); Somini Sengupta, *Judge Says Search Warrants for E-mails Must Be 'Limited,'* N. Y. TIMES BITS BLOG (Aug. 30, 2013, 8:01 PM), http://bits.blogs.nytimes.com/2013/08/30/judge-says-search-warrants-for-e-mails-must-be-limited/?_r=0 [http://perma.cc/2NKD-UZJD] (characterizing Judge Waxse's denial of warrants to search email accounts as an important holding in defining unreasonable searches and seizures in the digital age).

[129] *See In re Nextel Cellular Tel.*, 2014 WL 2898262, at *14.

[130] *See id.* at *2. Judge Waxse had previously denied search warrants for emails because the government had not proposed a search protocol. *In re Applications for Search Warrants for Info. Associated with Target Email Accounts/Skype Accounts*, 2013 WL 4647554, at *8. These earlier search warrant applications had not included a similar "Search Methodologies to be Employed" section. *Id.* at *1–2. In *In re Nextel Cellular Telephone*, it appears the government added this new section in order to address these particularity issues. *See* 2014 WL 2898262, at *3 (recognizing the new section in the search warrant but still finding the warrant overbroad).

[131] *See In re Nextel Cellular Tel.*, 2014 WL 2898262, at *2. The government also requested permission to open any files in order to determine their contents and indicated that their search would include at a minimum an examination of the phone's contact lists, calendars, picture and video files, internet history, and text messages. *See id.* The government made clear that it might use other search methods not named in its application. *See id.*

[132] *See id.* at *10 (stating the Fourth Amendment's particularity requirement protects against "general, exploratory rummaging in a person's belongings" (quoting *Coolidge*, 403 U.S. at 467 (plurality opinion)).

Court opinions.[133] Because *Riley* recognized that cell phones contain deeply personal information, Judge Waxse asserted that the court had a duty to protect such information from overly broad searches.[134] Moreover, Judge Waxse found the government's search methodology to be even less detained than the deficient search protocol Judge Facciola rejected in *Apple iPhone*, the case of the college student's iPhone.[135] Following Judge Facciola, Judge Waxse explained that future search protocol submissions must include technical language setting forth precisely how the government would determine what data come within the scope of the warrant.[136]

In two subsequent opinions denying cell phone search warrants, Judge Waxse provided further explanation of why the particularity requirement mandates search protocols.[137] Judge Waxse framed his particularity analysis as a balancing test between the government's need to investigate crime and the people's right of privacy.[138] Citing the U.S Supreme Court's recognition of the heightened privacy interests in cell phones in *Riley*, Judge Waxse concluded that cell phone searches without search protocols would tip the scales too far in favor of the government.[139] Judge Waxse asserted that other lower courts should engage in this balancing test after *Riley* and reconsider Fourth Amendment precedent that may strike an unfair balance when applied to cell phone searches.[140]

---

[133] *See id.* at *9. The court provided detailed summaries of each of Judge Facciola's opinions. *Id.* at *6–9; *see In re Search of Apple iPhone*, 31 F. Supp. 3d at 168 (opinion by Judge Facciola denying cell phone search warrants); *In re Search of ODYS LOOX Plus Tablet Serial No. 4707213703415*, 28 F. Supp. 3d at 46 (same); *In re Search of Black iPhone 4*, 27 F.Supp. 3d at 79 (same). The court also relied on precedent from the Court of Appeals for the Tenth Circuit on the particularity requirement's application to computer searches. *See In re Nextel Cellular Tel.*, 2014 WL 2898262, at *5; *see also* United States v. Otero, 563 F.3d 1127, 1132 (10th Cir. 2009) (discussing the importance of the particularity requirement in searches of digital media); United States v. Carey, 172 F.3d 1268, 1276 (10th Cir. 1999) (applying the particularity requirement to computer searches); United States v. Leary, 846 F.2d 592, 600 (10th Cir. 1988) (stating the particularity requirements commands the government to "describe the items to be seized with as much specificity as the government's knowledge and circumstances allow").

[134] *In re Nextel Cellular Tel.*, 2014 WL 2898262, at *4, *14; *see Riley II*, 134 S. Ct. at 2494–95 (observing that cell phones often store private and personal information).

[135] *In re Nextel Cellular Tel.*, 2014 WL 2898262, at *12; *see In re Search of Apple iPhone*, 31 F. Supp. 3d at 161, 166 (denying an application to search a college student's iPhone because the search protocol did not provide enough detail on the methods the government would use in its search).

[136] *In re Nextel Cellular Tel.*, 2014 WL 2898262, at *12; *see In re Search of Apple iPhone*, 31 F. Supp. 3d at 168 (providing examples of technical language, including "MD5 hash values," "metadata," "registry," "write blocking," and "status marker").

[137] *See In re Cellular Tels.*, 2014 WL 7793690, at *2 (noting how the court would provide a more thorough explanation of why it requires search protocols for cell phone search warrants); *In re Search of Premises Known as Three Cellphones*, 2014 WL 3845157, at *2 (discussing why the particularity requirement and *Riley* mandate search protocols for cell phone search warrants).

[138] *See In re Cellular Tels.*, 2014 WL 7793690, at *3.

[139] *Id.* at *8, *11; *see Riley II*, 134 S. Ct. at 2494–95.

[140] *See In re Cellular Tels.*, 2014 WL 7793690, at *4.

### *B. Inferring Scope Limits or Deferring the Protocol Question: Courts That Do Not Require Search Protocols for Cell Phone Search Warrants*

Other courts, rather than requiring search protocols for cell phone search warrants, have either inferred particularity limits into facially broad warrants or found other ways to resolve particularity challenges to cell phone search warrants.[141] On September 14, 2014, in *Hedgepath v. Kentucky*, the Kentucky Supreme Court upheld two warrants authorizing cell phone searches that were challenged on particularity grounds.[142] The warrants authorized the police to search the defendant's apartment and vehicle and both listed cell phones as property to be seized and searched at those locations.[143] Neither of the warrants, however, placed limitations on parts of the phones the police could search or the type of information the police sought to find on the phones.[144] The court held both warrants provided sufficiently particular descriptions of the evidence sought because the "clear thrust" of the warrants was to authorize only the search and seizure of evidence related to the alleged sexual assault.[145] Therefore, although the warrants placed no explicit limits on the scope of the

---

[141] *See, e.g.*, United States v. Lustyik, No. 13-CR-616-VB, 2014 WL 4802911, at *12 (S.D.N.Y. Sept. 29, 2014) (finding Second Circuit precedent prevented the court from requiring search protocols for cell phone search warrants); Hedgepath v. Commonwealth, 441 S.W.3d 119, 130–31 (Ky. 2014) (reading a facially broad cell phone search warrant narrowly in order to avoid a particularity issue); State v. Henderson, 854 N.W.2d 616, 633 (Neb. 2014) (holding the cell phone search warrant at issue was so broad that the court did not need to decide whether all cell phone search warrants needed search protocols).

[142] *See Hedgepath*, 441 S.W.3d at 130; *see also* Charles D. Weisselberg, *Cell Phones and Everything Else: Criminal Law Cases in the Supreme Court's 2013–2014 Term*, 50 CT. REV. 164, 165 (2014) (discussing the Kentucky Supreme Court's interpretation in *Hedgepath* v. *Commonwealth* of what warrants authorizing the search of a phone need to contain in order to be sufficiently particular); *Search Warrant for Suspect's Mobile Phone Need Not Be Limited to Particular Functions*, CRIM. DEF. NETWORK (Sept. 18, 2014), http://www.criminal-defense-network.com/news/search-warrant-for-suspects-mobile-phone-need-not-be-limited-to-particular-functions/ [http://perma.cc/D9UK-M8CN] (observing how *Hedgepath* provides one solution to the ongoing challenge of how to apply the particularity requirement to cell phone searches).

[143] *See Hedgepath*, 441 S.W.3d at 126–27. The warrants authorized the search and seizure of "all personal property including but not limited to all electronic equipment, computers, and cell phones." *See id.* The warrant application further stated that the police believed the listed property was either used in the commission of a crime or would show that a crime had been committed and listed the crime under investigation as assault. *See id.* After the police discovered the defendant's phone in his vehicle, they searched the phone and found several incriminating videos that appeared to show the defendant sexually assaulting the victim. *See id.* at 123. The trial court, in a decision issued before *Riley*, denied the defendant's motion to suppress because it found the defendant did not have a reasonable expectation of privacy in his phone and therefore no warrant was required to search the phone. *See id.* at 129.

[144] *See id.* at 130.

[145] *See id.* Before the section on cell phones, both warrants called for the search and seizure of any blood, semen, fibers, hairs, or other physical evidence resulting from the sexual assault. *See id.* Because these earlier sections contained detailed descriptions of physical evidence to be seized, the court imputed these specific limitations onto the authorization to search the cell phone. *See id.*

cell phone searches, the court inferred that the searches were limited to evidence of the alleged crime and held the warrants did not violate the particularity requirement.[146]

Other courts have considered the potential need for search protocols for cell phone search warrants in light of *Riley v. California*, but have not held the particularity requirement mandates them.[147] On October 17, 2014, in *State v. Henderson*, the Supreme Court of Nebraska held that two cell phone search warrants violated the particularity requirement because they did not list either the specific crimes or the specific types of information the government sought from the seized phone.[148] Because the government's warrants authorized the police to search and seize "[a]ny and all" information contained in the defendant's phone, the warrants clearly failed to provide sufficient limitations on what places in the phone could be searched and what data in the phone could be seized.[149] The court then discussed search protocols for cell phone searches and how *Riley* will likely lead to changes in how courts apply the Fourth Amendment's particularity requirement to cell phone searches.[150] But because the warrants before the court so clearly violated the traditional demands of particularity, the court concluded that it was unnecessary to decide whether search protocols are mandatory or proper for all cell phone search warrants.[151]

Some federal district courts appear to be awaiting direction from circuit courts on whether *Riley* should be read to mandate search protocols.[152] For in-

---

[146] *See id.* at 131.

[147] *See Lustyik*, 2014 WL 4802911, at *12 n.12; *Henderson*, 854 N.W.2d at 633–34.

[148] *See Henderson*, 854 N.W.2d at 633; *see also* John Wesley Hall, *NE: Cell phone SW Was Overbroad for "[A]ny and All Information" but Still Saved by GFE*, FOURTHAMENDMENT.COM (Oct. 21, 2014), http://fourthamendment.com/?p=13826 [http://perma.cc/K9V9-P6DJ] (discussing the holding in *State v. Henderson* and noting that the case could be appealed to the U.S. Supreme Court to clarify how lower courts should review facially broad cell phone search warrants); *State Courts Are Divided as to How to Apply Particularity Requirement to Search of Phone*, CRIM. DEF. NETWORK (Oct. 20, 2014), http://www.criminal-defense-network.com/news/state-courts-are-divided-as-to-how-to-apply-particularity-requirement-to-search-of-phone/ [http://perma.cc/2733-VT24].

[149] *See Henderson*, 854 N.W.2d at 633. The application provided some examples of areas to be searched, including contacts, call logs, text messages, and voicemails, as well as "any other information that can be gained from the internal components and/or memory Cards." *See id.* at 625. When the defendant challenged the first warrant as being overly broad, the police applied for and received the second warrant. *See id.* at 626. The second warrant added a brief statement describing how suspects in shootings often communicate through cell phones. *See id.*

[150] *See id.* at 633–34. The court observed how other lower courts and scholars are debating the need for search protocols in digital searches. *See id.* at 633 (citing United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1179 (9th Cir. 2010) (en banc) (Kozinski, C.J., concurring)); *In re Search Warrant*, 71 A.3d at 1171; Kerr, *supra* note 41; Ohm, *supra* note 46.

[151] *See Henderson*, 854 N.W.2d at 633–34. The court ended up affirming the lower court's denial of the defendant's motion to suppress under the good faith exception to the exclusionary rule, finding that the police had relied in good faith on the warrants. *See id.* at 634.

[152] *See, e.g.*, *Lustyik*, 2014 WL 4802911, at *12 n.12 (stating that Second Circuit precedent from before *Riley* held that search protocols were not mandatory for digital searches, but observing how *Riley* may require a reexamination of that precedent); United States v. Gatson, No. 13-705, 2014 WL

stance, on September 29, 2014, in *United States v. Lustyik*, the District Court for the Southern District of New York denied a motion to suppress evidence found on the defendant's cell phone.[153] Despite the fact that the warrants failed to include search protocols and authorized the government to review the entirety of the defendant's smartphone, the court held the warrants did not violate the Fourth Amendment.[154] In an extensive footnote, however, the court discussed the implications of *Riley* on earlier precedent and the future of search protocols.[155] To the court, *Riley* showed how longstanding criminal procedure precedent, such as the search incident to arrest exception to the warrant requirement, may have to be reevaluated when applied to cell phone searches.[156] Moreover, the court stated that as people place more and more personal information on cell phones, courts may need to mandate search protocols in order to ensure that cell phone search warrants comport with the particularity requirement.[157]

---

7182275, at *21 (D.N.J. Dec. 16, 2014) (holding a warrant to search a cell phone, tablet, and computer did not need to contain a detailed search protocol to meet the particularity requirement under current Third Circuit precedent); United States v. Romain, No. 13 Cr. 724, 2014 WL 6765831, at *9 (S.D.N.Y. Dec. 1, 2014) (noting how the Second Circuit had not required search protocols for searches of digital media before *Riley*).

[153] *Lustyik*, 2014 WL 4802911, at *12, *16. The FBI was investigating the defendant's involvement in a bribery scheme. *Id.* at *1; *see* Russ Buettner, *Lured by Promises of Wealth, F.B.I. Agent Was Drawn into Fraud Scheme*, N. Y. TIMES (Oct. 2, 2012), http://www.nytimes.com/2012/10/02/nyregion/lured-by-promises-of-wealth-fbi-agent-was-drawn-into-fraud-scheme-prosecutors-say.html [https://perma.cc/manage/vest/8LVJ-LQ8N] (describing how the defendant planned to profit off arraigning military contracts, for which he would receive kickback payments). Earlier in the FBI's investigation, the defendants had challenged other warrants for digital searches on particularity grounds as well. *See Lustyik*, 2014 WL 1494019, at *5, *7 (holding cell phone search warrants met the particularity requirement because they noted that only documents relevant to the crime being investigated could be seized); John Wesley Hall, *D. Utah: No Constitutional Requirement of a Search Protocol in an Email Warrant*, FOURTHAMENDMENT.COM (Mar. 20, 2014), http://fourthamendment.com/?p=10562 [http://perma.cc/X2Q9-ARWP] (noting that the court found that the particularity requirement did not mandate a search protocol for a cell phone search warrant).

[154] *See Lustyik*, 2014 WL 4802911, at *12. The court stated that precedent from the Second Circuit Court of Appeals firmly established that search protocols were not mandatory for searches of digital media. *Id; see* United States v. Galpin, 720 F.3d 436, 451 (2d Cir. 2013); United States v. Rosa, 626 F.3d 56, 62 (2d Cir. 2010). Therefore, even if it found the particularity requirement mandated search protocols for cell phone searches, the court observed that the good faith exception to the exclusionary rule would apply because the FBI had relied on binding appellate precedent when conducting its search. *Lustyik*, 2014 WL 4802911, at *12. Because the exclusionary rule would not apply, the court denied the defendant's motion to suppress. *See id.*

[155] *See Lustyik*, 2014 WL 4802911, at *12 n.12.

[156] *See id.* (discussing how *Riley* refused to extend U.S. Supreme Court precedent on physical searches to digital searches).

[157] *See id.* (stating that "threats to privacy posed by digital searches . . . may eventually make digital search protocols a Fourth Amendment necessity" (citing *Galpin*, 720 F.3d at 447 (describing how digital search warrants could devolve into general warrants if courts fail to remain diligent in applying the particularity requirement))).

## III. Courts Must Mandate Search Protocols for Cell Phone Search Warrants in Order to Comply with the Fourth Amendment's Particularity Requirement

In order to resolve the differing standards for cell phone search warrants, this Part argues that courts must mandate detailed search protocols for cell phone search warrants.[158] Section A asserts that search protocols are necessary based on the Fourth Amendment's particularity requirement and the U.S. Supreme Court's steadfast protection of the people's "privacies of life."[159] Section B argues that even if appellate courts find that the particularity requirement does not mandate search protocols, lower courts should be granted the discretion to impose cell phone search protocols when they find them necessary.[160] Finally, section C proposes a model for search protocols in cell phone search warrants, listing four components that courts should require for such search protocols.[161]

### *A. The Fourth Amendment's Particularity Requirement Mandates Search Protocols for Cell Phone Searches*

This section argues that the particularity requirement mandates search protocols for cell phone search warrants.[162] Subsection 1 explains how search protocols for cell phone search warrants are necessary to ensure that *Riley* truly protects the "privacies of life" from general searches.[163] Subsection 2 argues that longstanding rules on physical searches may be inapplicable to searches of digital media, and thus *Dalia*'s interpretation of the particularity requirement should not preclude courts from requiring search protocols.[164]

#### 1. *Riley v. California* Protects the "Privacies of Life" from General Searches

In *Riley v. California*, the U.S. Supreme Court recognized the unique threat to privacy that cell phone searches pose and therefore held that the police must obtain search warrants before searching cell phones.[165] The Court

---

[158] *See infra* notes 158–221 and accompanying text.
[159] *See infra* notes 162–195 and accompanying text.
[160] *See infra* notes 196–204 and accompanying text.
[161] *See infra* notes 205–221 and accompanying text.
[162] *See infra* notes 162–195 and accompanying text.
[163] *See infra* notes 165–183 and accompanying text.
[164] *See infra* notes 184–195 and accompanying text.
[165] *See* Riley v. California (*Riley II*), 134 S. Ct 2473, 2489 (2014) (stating that "[t]he sum of an individual's private life can be reconstructed" through the data on cell phones in a way inconceivable to previous generations); United States v. Lustyik, No. 13-CR-616-VB, 2014 WL 4802911, at *12 n.12 (S.D.N.Y. Sept. 29, 2014); (noting how, after the *Riley* decision, courts need to recognize the threat to privacy digital searches present); *In re* Nextel Cellular Tel., No. 14–MJ–8005–DJW, 2014

affirmed that, in today's America, cell phones hold "the privacies of life" that were stored in homes in past generations.[166] Because most smartphone users now carry intimate conversations, photographs, and effects in their pockets, the Court held that the government must obtain a warrant before searching a person's cell phone.[167] By requiring the police to establish probable cause and provide particularized descriptions in order to obtain cell phone search warrants, the Court placed essential constitutional limitations on the scope of cell phone searches.[168]

Just as the U.S. Supreme Court has rejected broad warrants for home searches, lower courts should reject facially broad cell phone warrants authorizing the review of the entirety of a cell phone's data.[169] Otherwise, cell phone search warrants will authorize the police to indiscriminately review the "privacies of life" modern cell phones often contain.[170] In 2014, in *Hedgepath v. Kentucky*, the Kentucky Supreme Court upheld the validity of such an overly broad warrant.[171] Although the warrant, on its face, placed no limits on what information the police could review, the court inferred that the intended scope of the warrant was more narrow.[172]

---

WL 2898262, at *14 (D. Kan. June 26, 2014) (using *Riley*'s recognition of the threat to privacy posed by cell phone searches to require search protocol for cell phone search warrant).

[166] *See Riley II*, 134 S. Ct. at 2494–95 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)). The amount of information stored on cell phones will only increase as Americans move away from traditional laptops and desktop computers and rely almost entirely on mobile devices for their technological needs. *See* O'Toole, *supra* note 4 (noting how the majority of Internet usage in the United States occurs through mobile devices); Perez, *supra* note 4 (observing how many Americans are now consuming digital media on mobile devices rather than personal computers).

[167] *See Riley II*, 134 S. Ct. at 2494–95 (discussing the history of general searches and writs of assistance and stating that personal information should retain the same Fourth Amendment protections for which the founders fought); Donald Dripps, *"Dearest Property": Digital Evidence and the History of Private "Papers" as Special Objects of Search and Seizure*, 103 J. CRIM. L. & CRIMINOLOGY 49, 53 (2013) (arguing that digital information should be considered "papers" and should be given protection superior to "effects" under the Fourth Amendment).

[168] *See Riley II*, 134 S. Ct. at 2491 (refusing to apply the search incident to arrest exception because of concerns about the scope of the search); State v. Henderson, 854 N.W.2d 616, 633 (Neb. 2014) (reading *Riley* as attempting to limit the scope of cell phone searches).

[169] *See Riley II*, 134 S. Ct. at 2494–95 (comparing the protections cell phones should receive to the protections homes receive); Groh v. Ramirez, 540 U.S. 551, 557 (2004) (holding a facially broad search warrant for a home violated the particularity requirement); *In re Nextel Cellular Tel.*, 2014 WL 2898262, at *14 (refusing to issue a cell phone search warrant without a detailed search protocol); *In re* Search of Apple iPhone, 31 F. Supp. 3d 159, 168 (D.D.C. 2014) (same).

[170] *Riley II*, 134 S. Ct. at 2494–95; *see Boyd*, 116 U.S. at 630 (observing how the Fourth Amendment protects against invasions into "the privacies of life"); *In re Nextel Cellular Tel.*, 2014 WL 2898262, at *14 (requiring search protocols for cell phone search warrants to ensure cell phone searches do not become general searches); *see In re Search of Apple iPhone*, 31 F. Supp. 3d at 168 (refusing to authorize a search warrant that proposed to examine all the information contained in a cell phone).

[171] Hedgepath v. Commonwealth, 441 S.W.3d 119, 130–31 (Ky. 2014).

[172] *Id. But see Henderson*, 854 N.W.2d at 633–34 (refusing to read limits into an overly broad cell phone search warrant).

When dealing with warrants to search homes, however, the U.S. Supreme Court has rejected similar efforts to infer scope limitations back into facially broad warrants.[173] In 2004, in *Groh v. Ramirez*, the U.S. Supreme Court held that a warrant to search a home violated the Fourth Amendment's particularity requirement because it failed to incorporate the particularized description of a home included in the warrant application.[174] To the Court, the intended scope of the warrant was irrelevant; if the warrant as issued was facially overbroad, then it violated the Fourth Amendment's particularity requirement.[175] If people's most private and intimate of information is to receive the same protections in the digital age, the same strict standards for home search warrants must apply to cell phone search warrants.[176] Therefore, courts cannot be permitted to create post hoc limits on the scope of cell phone search warrants.[177]

Accordingly, lower courts should follow Judge Waxse's and Judge Facciola's interpretation of the particularity requirement and mandate that the government submit technical search protocols for cell phone search warrants.[178] Although the U.S. Supreme Court has not yet defined what particularity means for cell phones searches, the Fourth Amendment at a minimum requires detailed descriptions of "the place to be searched" and "the persons or things to be seized."[179] As Judge Facciola discussed, search protocols address both of

---

[173] *See Groh*, 540 U.S. at 557, 559 (holding a search warrant violated the particularity requirement, even though the warrant application included a detailed list of the items to be seized, because the detailed list was not incorporated into the warrant itself); Stern, *supra* note 47, at 912 (noting how the U.S. Supreme Court has afforded homes the "apex of protection" under the Fourth Amendment).

[174] *See Groh*, 540 U.S. at 557, 559.

[175] *See id.* at 558–59 (recognizing the government's argument that "the search did not exceed the limits intended by the Magistrate" but still holding the warrant violated the Fourth Amendment's particularity requirement because it placed no explicit limits on the search's scope).

[176] *See Riley II*, 134 S. Ct. at 2494–95 (noting how cell phones contain the people's most private information and providing full Fourth Amendment protection to such sensitive information); *Groh*, 540 U.S. at 559 (observing that homes receive the highest level of protection under the Fourth Amendment); *In re Nextel Cellular Tel.*, 2014 WL 2898262, at *14 (requiring a search protocol for a cell phone search warrant in order to protect the deeply personal information stored on cell phones from general searches); *In re Search of Apple iPhone*, 31 F. Supp. 3d at 168–69 (denying the government's warrant application because it failed to articulate necessary scope limitations on the search).

[177] *See Riley II*, 134 S. Ct. at 2494–95 (affording cell phones the same warrant protections given to homes); *Groh*, 540 U.S. at 557, 559 (refusing to infer scope limits into a search warrant for a home). *But see Hedgepath*, 441 S.W.3d at 130 (upholding a facially broad warrant authorizing a cell phone search because the "clear thrust" of the warrant was more limited in scope).

[178] *See In re* Cellular Tels., No. 14-MJ-8017-DJW, 2014 WL 7793690, at *1 (D. Kan. Dec. 30, 2014); *In re* Search of Premises Known as Three Cellphones & One Micro-SD Card, No. L4-MJ-8013-DJW, 2014 WL 3845157, at *2 (D. Kan. Aug. 4, 2014); *In re Nextel Cellular Tel.*, 2014 WL 2898262, at *14; *In re Search of Apple iPhone*, 31 F. Supp. 3d at 166; *In re* Search of ODYS LOOX Plus Tablet Serial No. 4707213703415 in Custody of U.S. Postal Inspection Serv., 1400 New York Ave. NW, Wash., D.C., 28 F. Supp. 3d 40, 46 (D.D.C. 2014); *In re* Black iPhone 4, 27 F. Supp. 3d 74, 78 (D.D.C. 2014).

[179] *See* U.S. CONST. amend. IV; *Riley II*, 134 S. Ct. at 2493 (requiring a warrant for cell phone searches but not mentioning how probable cause and particularity should be applied); *In re Nextel*

these particularity concerns.[180] First, because it is impossible at a search's outset to identify the exact part of a cell phone's internal storage containing relevant data, search protocols provide a particularized description of how the government will identify the place on the phone to be searched.[181] Second, search protocols provide particularized descriptions of the information to be seized by setting forth guidelines for identifying the data the government seeks.[182] Unless lower courts demand such detailed search protocols, cell phone search warrants will authorize broad, unfettered searches, thereby diminishing the reinvigorated protections *Riley* sought to give the "privacies of life" in the modern digital world.[183]

### 2. *Dalia* Strikes an Unfair Balance When Applied to Cell Phone Searches

*Riley* demonstrates that well-established Fourth Amendment rules governing physical searches may be inapplicable to digital searches; therefore lower courts should disregard earlier precedent holding that particularity does not limit how the police execute warrants.[184] Although the search incident to arrest exception to the warrant requirement had been recognized for centuries, the *Riley* court unanimously refused to apply it to cell phone searches.[185] Because

---

*Cellular Tel.*, 2014 WL 2898262, at *4, *6 (observing that neither the U.S. Supreme Court nor the Tenth Circuit had yet to explain what probable cause and particularity mean when applied to cell phone search warrants); *Henderson*, 854 N.W.2d at 633–34 (stating that "[t]he parameters of how specific the scope of a warrant to search the contents of a cell phone must be will surely develop in the wake of *Riley v. California*").

[180] *See In re Search of Apple iPhone*, 31 F. Supp. 3d at 167; *In re* Search Warrant, 71 A.3d 1158, 1171 (Vt. 2012), *cert. denied*, 133 S. Ct. 185 (2013).

[181] *See In re Search of Apple iPhone*, 31 F. Supp. 3d at 167; *In re Search Warrant*, 71 A.3d at 1171 (stating that "the only feasible way to specify a particular 'region' of the computer will be by specifying how to search").

[182] *See In re Nextel Cellular Tel.*, 2014 WL 2898262, at *12 (stating that "sufficiently specific guidelines for identifying the documents sought" must accompany search warrant application (quoting United States v. Tamura, 694 F.2d 591, 595 (9th Cir. 1982))).

[183] *See Riley II*, 134 S. Ct. at 2494–95 (stating that the Court must protect the "privacies of life" cell phones contain from general searches); *Lustyik*, 2014 WL 4802911, at *12 n.12 (recognizing that search protocols may become necessary to ensure the Fourth Amendment remains relevant in digital searches); *In re Nextel Cellular Tel.*, 2014 WL 2898262, at *14 (interpreting *Riley* to mandate search protocols for cell phone search warrants); *Henderson*, 854 N.W.2d at 633 (finding a warrant violated the particularity requirement and leaving open the question of whether search protocols should be mandatory to comport with *Riley*).

[184] *See Riley II*, 134 S. Ct. at 2484 (concluding that the search incident to arrest exception does not strike the proper balance between privacy and government interests for cell phone searches); United States v. Robinson, 414 U.S. 218, 236 (1973) (holding a warrantless search of a cigarette pack found on the arrestee's body during a search incident to arrest was reasonable); Weeks v. United States, 232 U.S. 383, 392 (1914) (recognizing "the right on the part of the Government, always recognized under English and American law, to search the person of the accused when legally arrested to discover and seize the fruits or evidences of crime").

[185] *See Riley II*, 134 S. Ct. at 2482, 2485 (quoting *Weeks*'s observation of the historic right to search an arrestee incident to arrest but declining to apply the search incident to arrest exception to

the Court found one of the fundamental Fourth Amendment principles governing physical searches inapplicable to digital searches, lower courts should pause before applying interpretations of the particularity requirement from physical searches to digital searches.[186]

Earlier views of the particularity requirement provide inadequate privacy protections when applied to cell phone search warrants.[187] In 1979, in *Dalia v. United States*, the U.S. Supreme Court held that the particularity requirement did not limit how the police chose to execute a search warrant for the defendant's office.[188] But, in light of the Court's recognition in *Riley* that longstanding Fourth Amendment precedent may not apply to cell phone searches, some lower courts have refused to read the particularity requirement so narrowly.[189]

Before applying *Dalia*'s view of the particularity requirement to cell phone search warrants, judges should critically examine the balance struck in such earlier cases between the government's need to investigate crime and the people's right of privacy.[190] When U.S. District Court Magistrate Judges Facciola and Waxse considered this balance, they found that rigidly applying traditional views of the particularity requirement would unfairly favor the government at the expense of individual privacy.[191] Although limits on the police's discretion in executing warrants were not necessary for searches of physical spaces, such limitations are necessary to ensure that searches of digital media do not devolve into general rummaging.[192]

---

cell phone searches); *id.* at 2495 (Alito, J., concurring) (characterizing the search incident to arrest exception as an "ancient rule").

[186] *See id.* at 2484 (majority opinion) (stating the search incident to arrest exception provides inadequate privacy protections when applied to searches of digital media on cell phones).

[187] *See Riley II*, 134 S. Ct. at 2484 (refusing to apply a rule on physical searches to digital searches because of privacy concerns); United States v. Grubbs, 547 U.S. 90, 97 (2006); Dalia v. United States, 441 U.S. 238, 257 (1979); *see also In re Search of Apple iPhone*, 31 F. Supp. 3d at 167 (holding *Dalia* does not preclude courts from interpreting the particularity requirement to mandate search protocols).

[188] *See Dalia*, 441 U.S. at 257 (holding that covert entry to execute the warrant was within the police's discretion and the warrant did not violate the particularity requirement for failing to authorize covert entry). The Court reaffirmed this view of the particularity requirement in 2006 in *United States v. Grubbs*. *See* 547 U.S. at 97–98 (relying on *Dalia*'s interpretation of the particularity requirement to find anticipatory warrants constitutional).

[189] *See Riley II*, 134 S. Ct. at 2484 (refusing to apply the search incident arrest exception to the warrant requirement to cell phone searches); *In re Cellular Tels.*, 2014 WL 7793690, at *6; *In re Search of Apple iPhone*, 31 F. Supp. 3d at 167.

[190] *See Riley II*, 134 S. Ct. at 2484 (stating that "while *Robinson*'s categorical rule strikes the appropriate balance in the context of physical objects, neither of its rationales has much force with respect to digital content on cell phones"); *In re Cellular Tels.*, 2014 WL 7793690, at *6; *In re Apple iPhone*, 31 F. Supp. 3d at 167.

[191] *See In re Cellular Tels.*, 2014 WL 7793690, at *3, *4; *In re Search of Apple iPhone*, 31 F. Supp. 3d at 167.

[192] *See In re Cellular Tels.*, 2014 WL 7793690, at *8; *In re Search of Apple iPhone*, 31 F. Supp. 3d at 167. Despite Judge Facciola's attempts to find that search protocols do not limit how the police execute warrants, search protocols are limitations on how the police may search a device.

With *Dalia* inapplicable to cell phone search warrants, courts should mandate limitations on the police's power to execute cell phone search warrants by requiring search protocols.[193] As the Kentucky Supreme Court demonstrated in *Hedgepath*, when courts do not require search protocols, the government will conduct exhaustive and unlimited reviews of every document contained in seized cell phones.[194] By requiring the government to submit detailed search protocols explaining the methods it will use to find relevant data, courts will ensure that the Fourth Amendment's protections remain in full effect in the digital age.[195]

### *B. Courts Should Allow Magistrate Judges to Require Search Protocols*

Even if appellate courts find that the particularity requirement does not mandate search protocols for cell phone search warrants, lower courts must have the power to impose search protocols when necessary.[196] A bright-line rule requiring search protocols would provide clearer guidelines to the police

---

*Compare In re Search of Apple iPhone*, 31 F. Supp. 3d at 167 (holding *Dalia* does not preclude courts from interpreting the particularity requirement to mandate search protocols), *with* Friess, *supra* note 46, at 1015 (citing Marron v. United States, 275 U.S. 192, 196 (1927)) (stating that search protocols do limit the police's discretion, but that judges possess the power to limit the police's discretion in this way). As discussed above, however, these limitations on police discretion are necessary to provide a particularized scope to cell phone searches. *See In re Nextel Cellular Tel.*, 2014 WL 2898262, at *14 (stating that without a search protocol, the court would authorize a general search of the defendant's cell phone in violation of the Fourth Amendment); Friess, *supra* note 46, at 1015 (noting how judges have a duty to limit the scope of digital search warrants to ensure they comply with the particularity requirement).

[193] *See In re Cellular Tels.*, 2014 WL 7793690, at *1; *In re Search of Premises Known as Three Cellphones*, 2014 WL 3845157, at *2; *In re Nextel Cellular Tel.*, 2014 WL 2898262, at *14; *In re Search of Apple iPhone*, 31 F. Supp. 3d at 168; *In re Search of ODYS LOOX Plus Tablet Serial No. 4707213703415*, 28 F. Supp. 3d at 46.

[194] *See In re Search of Apple iPhone*, 31 F. Supp. 3d at 168 (noting how the government's proposed search protocol would authorize the government to examine all the information contained in the device); *Hedgepath*, 441 S.W.3d at 130–31 (upholding a warrant that authorized search and seizure of all data contained in phone). Even in *United States v. Lustyik*, where the District Court for the Southern District of New York recognized the potential need for search protocols, the court still upheld an unlimited search of all the information contained in the defendant's cell phone. *See Lustyik*, 2014 WL 4802911, at *12.

[195] *See In re Nextel Cellular Tel.*, 2014 WL 2898262, at *12; *In re Search of Apple iPhone*, 31 F. Supp. 3d at 167–68.

[196] *See Lustyik*, 2014 WL 4802911, at *12 n.12 (recognizing that search protocols for cell phone warrants may become necessary in certain circumstances to protect against general searches); *Henderson*, 854 N.W.2d at 633–34 (considering the need for search protocols but not yet mandating them for cell phone search warrants); *see also* United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1179 (9th Cir. 2010) (en banc) (Kozinski, C.J., concurring) (stating that the warrant application for computer search warrants "should normally include, or the issuing judicial officer should insert, a protocol for preventing agents involved in the investigation from examining or retaining any data other than that for which probable cause is shown"); *In re Search Warrant*, 71 A.3d at 1171 (allowing judges to impose search protocols on computer searches but not finding search protocols constitutionally mandatory).

and would be easier for courts to enforce.[197] But, if an appellate court is uncomfortable with articulating rigid procedures beyond the plain language of the Fourth Amendment, it can simply defer to the judge issuing the search warrant.[198] As the person first evaluating the warrant application and the facts of the case, the issuing judge is in the best position to determine what limits are needed to ensure a particularized search.[199] If the issuing judge finds a search protocol necessary to limit the cell phone search warrant's scope, a reviewing court should support the judge's evaluation of the warrant application.[200]

Appellate courts could also follow the U.S. Supreme Court's approach in *Dalia* and declare that search protocols are the "preferable approach" for cell phone search warrants.[201] In *Dalia*, the Court found that although the particularity requirement did not mandate that the government obtain prior authorization before covertly installing a listening device, prior authorization was still the "preferable approach."[202] The Court recognized that covert entries further

---

[197] *See Riley II*, 134 S. Ct. at 2491 (stating that, when interpreting the Fourth Amendment, the Court's "general preference [is] to provide clear guidance to law enforcement through categorical rules"); Michigan v. Summers, 452 U.S. 692, 705 n.19 (1981) (noting that "if police are to have workable rules, the balancing of the competing interests . . . must in large part be done on a categorical basis"); *In re Nextel Cellular Tel.*, 2014 WL 2898262, at *12; *In re Search of Apple iPhone*, 31 F. Supp. 3d at 168.

[198] *See Grubbs*, 547 U.S. at 97–98; *Dalia*, 441 U.S. at 258 n.22; *Comprehensive Drug Testing, Inc.*, 621 F.3d at 1177 (allowing judges to impose search protocols for computer searches but not mandating them); *id.* at 1179 (Kozinski, C.J., concurring) (encouraging lower courts to use search protocols for computer searches); *Henderson*, 854 N.W.2d at 633–34 (leaving the question to lower courts of whether to mandate search protocols for cell phone searches); *In re Search Warrant*, 71 A.3d at 1171 (upholding the lower court's power to impose a search protocol for a computer search). Although the U.S. Supreme Court in *Riley* recognized that rules on physical searches may not apply fairly to digital searches, lower courts may hesitate revisiting the longstanding view that the particularity requirement does not limit how the police may execute warrants. *See Riley II*, 134 S. Ct. at 2484 (holding that the search incident to arrest exception does not apply to cell phone searches); *Grubbs*, 547 U.S. at 97–98 (reading the Fourth Amendment's particularity clause very narrowly); *Dalia*, 441 U.S. at 258 (holding that the particularity requirement does not limit how the police execute warrants); *Lustyik*, 2014 WL 4802911, at *12 (reading *Dalia* to find the particularity requirement does not mandate search protocols for cell phone searches). Furthermore, the Court has resisted reading technical procedures into the particularity requirement. *See Grubbs*, 547 U.S. at 99 (holding that anticipatory warrants did not violate the particularity requirement); *Dalia*, 441 U.S. at 258 (refusing to find that the particularity requirement mandated prior authorization for covert entries to execute search warrants).

[199] *See Comprehensive Drug Testing, Inc.*, 621 F.3d at 1179 (Kozinski, C.J., concurring) (discussing the power the issuing judge possesses to limit search methods based on the privacy interests at stake in the search); *In re Search Warrant*, 71 A.3d at 1184 (finding that issuing judges have the power to place limits on the government's search of a computer).

[200] *See Comprehensive Drug Testing, Inc.*, 621 F.3d at 1177 (upholding the power of lower courts to impose search protocols in digital searches); *In re Search Warrant*, 71 A.3d at 1184 (same).

[201] *See Dalia*, 441 U.S. at 259 n.22 (stating prior authorization for covert entry to install a recording device is the "preferable approach); *Comprehensive Drug Testing, Inc.*, 621 F.3d at 1179 (Kozinski, C.J., concurring) (stating that computer search warrants "should normally include" search protocols)**;** *Lustyik*, 2014 WL 4802911, at *12 n.12 (recognizing the growing need in digital searches for protections like search protocols).

[202] *Dalia*, 441 U.S. at 257, 259 n.22.

impinge upon a defendant's privacy and therefore the government, as a policy matter, should seek judicial approval before utilizing this search method.[203] In the same way, appellate courts could express a preference for search protocols while sidestepping the potentially contentious issue of whether search protocols are mandatory under the particularity requirement.[204]

### *C. A Model for Search Protocols for Cell Phone Search Warrants*

Courts should follow Judge Facciola's approach for search protocols in cell phone search warrants and demand a list of the exact methods and tools the government will use both to set the scope of the search and to execute the search.[205] As such, this section makes four recommendations for cell phone search protocols to comply with the particularity requirement.[206]

First, if the government wishes to "image" a cell phone, a process by which the government makes a complete digital copy of the device's contents, it should be required to explain why imaging is necessary and how it will handle information not relevant to its investigation copied in the image.[207] Imaging is a commonly used tool in digital searches and may often be an essential first step in an in-depth forensic review.[208] But because the technique is inherently overbroad, the government must justify its use in each case and explain how it

---

[203] *See id.* (noting how covert entry may impinge on privacy interests "not explicitly considered by the judge who issued the warrant" and therefore expressing a preference for prior authorization).

[204] *See id.* at 259 n.22; *Lustyik*, 2014 WL 4802911, at *12 n.12 (discussing the constitutional questions surrounding mandatory search protocols for cell phone search warrants); Friess, *supra* note 46, at 1015 (recommending that courts rely on *Dalia* to find that search protocols for digital search warrants are the "preferable approach"(quoting *Dalia*, 441 U.S. at 259 n.22)).

[205] *See In re Nextel Cellular Tel.*, 2014 WL 2898262, at *13 (stating that a cell phone search protocol "educates (1) the Court as to what the government is doing when it searches a cell, and (2) the executing officer as to what places and things may or may not be searched and/or seized"); *In re Search of Apple iPhone*, 31 F. Supp. 3d at 168 (stating that cell phone search protocols should be "a sophisticated technical explanation of how the government intends to conduct the search"); *see also In re Search Warrant*, 71 A.3d at 1162, 1184 (upholding a search protocol for a computer search warrant that prevented the police from using specific search tools without prior judicial approval).

[206] *See infra* notes 207–221 and accompanying text.

[207] *See In re Search of Apple iPhone*, 31 F. Supp. 3d at 166 (requiring that the government delete any data beyond the investigation's scope from the image it created of the cell phone); *In re Search of ODYS LOOX Plus Tablet Serial No. 4707213703415*, 28 F. Supp. 3d at 45 (rejecting a proposed search protocol that sought to image all seized devices because imaging would allow the government to search and seize data beyond the scope of its investigation); *In re Search of Black iPhone 4*, 27 F. Supp. 3d at 79–80 (expressing concern over whether all of the seized cell phones would be imaged and, if so, whether the government planned to keep such images indefinitely).

[208] *See* Goldfoot, *supra* note 57, at 115–16 (describing imaging as a commonly used search technique that allows the government to review data at off-site locations); Kerr, *supra* note 61, at 540 (stating that the first step in nearly all forensic computer searches is imaging the device).

will avoid viewing and retaining information beyond the investigation's scope.[209]

Second, cell phone search protocols should include a list of the keywords the government will use in its keyword search.[210] Keyword searches narrow the scope of a search to files containing specific terms, making them a helpful but blunt search tool.[211] Despite their limitations, police commonly use keyword searches, at least as a starting point for a search.[212] By requiring a list of keywords in search protocols, courts can place common sense and nontechnical particularity limitations on at least one aspect of the government's search.[213]

Third, search protocols should list the software the government will use to search the phone.[214] Because the government uses software to automatically perform many aspects of the digital search, courts must know what software the government plans to use in order to ensure that the search is limited in scope.[215] The government can submit a search protocol that authorizes all of

---

[209] *See In re Nextel Cellular Tel.*, 2014 WL 2898262, at *10 (denying a cell phone search warrant because the application failed to specify whether the government would or would not use imaging); *In re Search of Apple iPhone*, 31 F. Supp. 3d at 166 (stating that the court would not approve the warrant until the government made clear whether it would image the seized cell phones and, if so, whether it would delete irrelevant information from the produced image); Kerr, *supra* note 61, at 562 (noting how imaging can result in overbroad seizures of computer files).

[210] *See In re Nextel Cellular Tel.*, 2014 WL 2898262, at *12 & n.92 (observing that the government's proposal to "perform [] keyword searches" without further explanation "may pose problems" (alteration in original)); *In re Search of Apple iPhone*, 31 F. Supp. 3d at 168 (noting how the warrant application stated that the government may employ "keyword searches for related terms"); Haynes, *supra* note 66, at 771–72 (describing keyword searches as a "particularly useful method" for digital searches).

[211] *See* COMPUTER CRIME, *supra* note 68, at 79 (noting that forensic investigators may start with keyword searches, "but a properly performed forensic analysis will rarely end there" because keyword searches often miss relevant information); Goldfoot, *supra* note 57, at 138 (noting how keyword searches can be "imperfect" because they can fail to "catch unanticipated wording, an egregious misspelling, an unexpected foreign language, recently invented slang, or pictures of documents"); Haynes, *supra* note 66, at 771–72.

[212] COMPUTER CRIME, *supra* note 68, at 79; Haynes, *supra* note 66, at 771–72.

[213] *See In re Nextel Cellular Tel.*, 2014 WL 2898262, at *12 (discussing how the government's warrant application failed to provide adequate detail on how it planned to use keyword searches); *In re Search of Apple iPhone*, 31 F. Supp. 3d at 168 (seeking more detail on how the government would execute keyword searches); Haynes, *supra* note 66, at 771–72 (observing how keyword searches easily allow the police to conduct a precise digital search with a narrow scope).

[214] *See In re Search of Apple iPhone*, 31 F. Supp. 3d at 168 (stating that the government should explain what software it will use and how it plans to use that software to search the cell phone); *In re Search Warrant*, 71 A.3d at 1162, 1184 (upholding a search protocol that required the police to receive judicial approval before using specific software).

[215] *See Comprehensive Drug Testing, Inc.*, 621 F.3d at 1176 (recognizing how "specialized forensic software" allows police to determine the contents of digital files); *In re Search of Apple iPhone*, 31 F. Supp. 3d at 168 (stating that the government should explain what software it will use so that the court can evaluate whether the government's search is particularized); Kerr, *supra* note 61, at 544–45 (describing how computer forensic analysts can use software to automatically bring together certain file types for examination).

the software the government usually uses in such searches.[216] If, however, the government decides it needs to use software not previously authorized in its search protocol, it can simply ask the court for permission to use these new techniques.[217]

Finally, in cases where imaging is used, search protocols should set a specific date by which the image must be permanently destroyed.[218] These images must be deleted because the government cannot be permitted to retain indefinitely information beyond the investigation's scope.[219] As Judge Facciola discussed in *In re Search of ODYS LOOX Plus Tablet Serial Number 4704213703415*, subsequent testimony can address any chain of custody or other evidentiary concerns.[220] This testimony can explain that the device's image is a complete record of all relevant files contained on the device and all files beyond the investigation's scope were deleted to comply with a court order.[221]

## CONCLUSION

In 2014, in *Riley v. California*, the U.S. Supreme Court recognized that in today's America, cell phones contain the "privacies of life" and therefore re-

---

[216] *See In re Search of Apple iPhone*, 31 F. Supp. 3d at 168 (explaining that the government can use whatever software or other search methods it believes it needs to conduct its investigation, so long as it demonstrates to the court that it is "making a genuine effort to limit itself to a particularized search"); *In re Search Warrant*, 71 A.3d at 1162, 1184 (noting that the government can present the software it wishes to use so that the judge can make an informed judgment as to whether such software is necessary for a search).

[217] *See In re Search of Apple iPhone*, 31 F. Supp. 3d at 168; *In re Search Warrant*, 71 A.3d at 1162, 1184 (stating that judges can be quickly respond to government requests for additional searching tools as the investigation proceeds).

[218] *See In re Nextel Cellular Tel.*, 2014 WL 2898262, at *10 (finding the government's failure to propose a specific date by which the device's image would be destroyed "fatal" to its warrant application); *In re Search of ODYS LOOX Plus Tablet Serial No. 4707213703415*, 28 F. Supp. 3d at 45–46 (denying the government's request to retain cell phone's image "indefinitely pending appeal"); *see also In re Search Warrant*, 71 A.3d at 1185 (upholding a warrant that banned the indefinite storage of all digital information from the seized device during the defendant's appeals).

[219] *See In re Nextel Cellular Tel.*, 2014 WL 2898262, at *11 (finding that the government must explicitly state the date by which it will destroy or return irrelevant data in order to comply with the Fourth Amendment); *In re Search of ODYS LOOX Plus Tablet Serial No. 4707213703415*, 28 F. Supp. 3d at 45 (stating that if the court failed to require a specific date by which all irrelevant data must be destroyed, it would "allow the government to maintain data that it—and this Court—knows to be outside the scope of the warrant"); *see also In re Search Warrant*, 71 A.3d at 1185 (upholding a lower court's requirement that all irrelevant data be destroyed).

[220] *In re Search of ODYS LOOX Plus Tablet Serial No. 4707213703415*, 28 F. Supp. 3d at 46 (noting how testimony explaining the search protocol's requirements would allay the government's concern over future chain of custody problems); *see also In re Nextel Cellular Tel.*, 2014 WL 2898262, at *8 (discussing Judge Facciola's solution to potential chain of custody problem).

[221] *In re Search of ODYS LOOX Plus Tablet Serial No. 4707213703415*, 28 F. Supp. 3d at 46 (describing the potential testimony that could explain why the device's image is not complete); *see also In re Nextel Cellular Tel.*, 2014 WL 2898262, at *8 (recounting Judge Facciola's discussion of testimony regarding incomplete device images).

quired the police to obtain warrants before searching cell phones. But in order to ensure cell phone searches do not devolve into generalized rummaging in violation of the Fourth Amendment, lower courts must require search protocols when issuing cell phone search warrants. Without search protocols, cell phone search warrants will violate the Fourth Amendment's particularity requirement, for they will fail to set any limitations on where the police can search within the device and what information the police can seize from the device. Although earlier precedent interpreting the particularity requirement in physical searches may preclude mandatory search protocols, lower courts should follow *Riley* and recognize that rules and interpretations for physical searches may not apply to digital searches. The people's "privacies of life" deserve the highest protection under the Fourth Amendment. Only detailed search protocols will provide such protection to the trove of intimate information stored on cell phones.

WILLIAM CLARK