THE POST-*RILEY* SEARCH WARRANT: SEARCH PROTOCOLS AND PARTICULARITY IN CELL PHONE SEARCHES

Adam M. Gershowitz

William & Mary Law School
William & Mary Law School Research Paper No. 09-313
69 VAND. L. REV. ___ (forthcoming 2016)

The Post-*Riley* Search Warrant: Search Protocols and Particularity in Cell Phone Searches

Adam M. Gershowitz•

ABSTRACT

Last year, in Riley v. California*, the Supreme Court required police to procure a warrant before searching a cell phone. Unfortunately, the Court's assumption that requiring search warrants would be "simple" and very protective of privacy was overly optimistic. This article reviews lower court decisions in the year since Riley and finds that the search warrant requirement is far less protective than expected. Rather than restricting search warrants to the narrow evidence being sought, some magistrates have issued expansive warrants authorizing a search of the entire contents of the phone with no restrictions whatsoever. Other courts have authorized searches of applications and data for which no probable cause existed. And even when district and appellate courts have found these overbroad search warrants to be defective, they have almost always turned to the good faith exception to save the searches and allow admission of the evidence.*

This article calls on courts to take the Fourth Amendment's particularity requirement seriously before issuing search warrants for cell phones. Just as magistrates cannot authorize police to search for a fifty-inch television in a microwave, nor should officers be permitted to rummage through all of the files on a cell phone when a narrower search will suffice. In order to effectuate the privacy guarantee in Riley, this Article proposes two approaches to narrow cell phone search warrants. First, I argue that judges should impose search protocols that specify in advance exactly how police should execute warrants and sift through electronic data. Second, this Article challenges the common assumption that all cell phone searches require full forensic analysis. In many cases involving street crimes, magistrates should initially restrict warrants to a manual search of the particular functions or applications for which there is probable cause. These two ex ante restrictions on cell phone searches will protect privacy and prevent over-use of the good faith exception, while still permitting police to examine all data they have probable cause to investigate.

• Kelly Professor of Teaching Excellence and Professor of Law, William & Mary Law School. I am grateful to Elizabeth Rademacher and Louis Mascola for helpful research assistance.

For nearly a decade, scholars[1] called for the Supreme Court to forbid warrantless cell phone searches incident to arrest. The argument was simple: cell phones carry an enormous amount of personal data and searches incident to arrest can be conducted for low-level offenses that have nothing to do with cell phones. Allowing police to search millions of pages of private data simply because a suspect was arrested for driving while intoxicated or some other low-level offense made no sense. The obvious solution was for police to procure a warrant before searching a cell phone.

In June 2014, in *Riley v. California*, the Supreme Court obliged and forbid warrantless searches incident to arrest of cell phones.[2] The decision met with widespread applause. Leading scholars, such as Orin Kerr, commended the Court for recalibrating the balance between privacy and the needs of law enforcement.[3] The public and media reaction to *Riley* was nearly universally positive.[4] With neutral magistrates standing between the police and cell phones, privacy rights would be protected.

Given the sweeping language in *Riley* about the importance of impartial judges and the limitation of police authority to invade privacy, one might expect that judges would take an active role in ensuring that warrants are narrowly tailored to protect privacy rights. Yet, many courts have issued post-*Riley* warrants that authorize an expansive search of the entire cell phone – and the millions of pages of attendant data – with little or no guidance or limitation on what police can search.

For example, in the 2015 case of *United States v. Winn*, police observed a man use his cell phone to photograph teenagers in their bathing suits at a pool.[5] Police and prosecutors believed the suspect should be

---

[1] I was an early proponent of the Supreme Court banning warrantless cell phone searches. *See* Adam M. Gershowitz, *The iPhone Meets the Fourth Amendment*, 56 UCLA L. REV. 27 (2008).

[2] *See* Riley v. California, 134 S. Ct. 2473 (2014).

[3] Prior to the decision Professor Kerr advocated what he calls an equilibrium adjustment theory of the Fourth Amendment. *See* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 478 (2011). Immediately after *Riley*, Professor Kerr posited that the decision effectively adopted that theory. *See* Orin Kerr, *The Significance of Riley*, VOLOKH CONSPIRACY, June 25, 2014, available at http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/06/25/the-significance-of-riley/.

[4] *See, e.g.*, John Cassidy, *The Supreme Court Gets It Right on Cell-Phone Privacy*, THE NEW YORKER, June 25, 2014 (contending that the justices "appear to be on the right side of history"); Linda Greenhouse, Op-Ed., *The Supreme Court Justices Have Cellphones, Too*, N.Y. TIMES, June 25, 2014; Editorial, *The Supreme Court Saves Cellphone Privacy*, N.Y. TIMES, June 25, 2014; Editorial, *A Win for Digital Privacy*, MIAMI HERALD, June 25, 2014.

[5] *See* United States v. Winn, No. 14-CR-30169, 2015 WL 553286 (S.D. Ill. Feb. 9, 2015), at *1.

charged with the misdemeanor of public indecency.[6] Yet, even though the only relevant evidence of public indecency that could be on the phone was photographs and videos, the prosecutors convinced a judge to sign a warrant authorizing a search of "any or all files contained on said cell phone" including the phone's calendar, phonebook, text messages, emails, call logs, GPS information, internet history, Wi-Fi information, and numerous other applications.[7] As a federal district judge later remarked, the warrant "authorized the seizure of virtually every piece of data that could conceivably be found on the phone."[8] Indeed, the officers used a data extraction device[9] to do a "complete phone dump"[10] that eventually turned up evidence of the more serious crime of possessing child pornography.[11]

While a federal judge eventually suppressed the evidence in the *Winn* case, other courts have upheld similarly overbroad search warrants. For instance, in a recent New York case, officers sought a search warrant for a video the suspect was taking on his iPhone when the police arrested him.[12] The officers had seized the phone and personally turned off the video recording during the arrest, thus making it crystal clear that the suspect had no time to hide the video in an unusual place on the phone.[13] Although the probable cause was for a specific video and there was no reason to believe it would be anywhere other than the phone's video library, a judge authorized a search warrant for the *entire* contents of the phone.[14] When the defendant later filed a suppression motion arguing that the search should have been limited to video and photo files, a judge upheld the warrant.[15]

Police have also pushed the envelope for broad warrants in drug cases. Law enforcement has long recognized that drug dealers use cell phone functions – particularly text messages -- to conduct their illegal operations.[16]

---

[6] *See id.*
[7] *See id*. at *2.
[8] *Id*. at *9.
[9] For a description of data extra devices, see Adam M. Gershowitz, *Seizing a Cell Phone Incident to Arrest, Data Extraction Devices, Faraday Bags, or Aluminum Foil as a Solution to the Warrantless Cell Phone Search Problem*, 22 WM. & MARY B. RTS. J. 601, 606-07 (2013).
[10] *Winn*, 2015 WL 553286, at *11.
[11] *See id*. A federal judge overseeing the child pornography charges eventually found the search warrant to be overbroad. Had the case remained in state court or been assigned to a different federal district court the warrant might have survived. *See id*.
[12] *See* People v. Watkins, 994 N.Y.S.2d 816 (N.Y. Supr. Ct. 2014). The search warrant in *Watkins* was issued before *Riley* but upheld after the Court's decision.
[13] *See id*. at 817.
[14] *See id.*
[15] The court confusingly and incorrectly said that "a search warrant that allows an inspection of the entire cellular telephone is appropriate to determine what, if any, applications and files pertain to the subject of the observed criminality." *Id*. at 818.
[16] *See infra* notes 30 and 247 and accompanying text.

In both pre- and post-*Riley* drug cases, it is therefore very common for officers to request cell phone search warrants. In some instances however, police go beyond communications data such as text messages and call logs, and also seek warrants for unrelated applications such as photos and videos.[17] The officers do not specify why they have suspicion that there would be photographic evidence of drug transactions, but magistrates nevertheless issue warrants to search for photographs anyway. Indeed, in some cases, magistrates issue cell phone search warrants for photographs and videos based on nothing other than officers' testimony that in their experience cell phones often hold evidence of drug dealing.[18]

In an alarming number of post-*Riley* cases, search warrants have authorized police with extremely limited suspicion of criminal activity to rummage through reams of unrelated private data.[19] Courts should have found some of these warrants to be overbroad because that they allowed searches of cell phone applications and functions for which there was no probable cause. Other warrants should have failed the Fourth Amendment's particularity requirement because they did not make clear how the search was connected to the crime under investigation.[20]

In other cases, courts have found cell phone search warrants to be defective, but have turned to the good faith exception to admit the evidence.[21] Even though the search warrants were overbroad or failed the particularity requirement, courts concluded that because of the complexity of digital searches, the average police officer would not have understood that the warrants were defective and thus acted in good faith when executing the warrants.[22]

The serious flaws in post-*Riley* search warrants indicate that courts should take a different approach. In standard Fourth Amendment case law, the question of whether a search warrant was properly executed is litigated after the search is conducted. Courts conduct an ex post analysis to see if the

---

[17] *See, e.g.*, United States v. Garcia-Alvarez, No. 14-cr-0621 JM, 2015 WL 777411 (S.D. Cal. Feb. 24, 2015).

[18] *See, e.g.*, United States v. Herevia, No. RDB-13-639, 2014 WL 4784321 (D. Md. Sept. 23, 2014).

[19] *See infra* Parts III.A.1 and III.B.1.

[20] *See infra* notes 100-03 and 139-42 and accompanying text. Of course, many post-*Riley* courts have issued cell phone warrants that are supported by probable cause and satisfy the particularity requirement. Yet, this merely highlights the discrepancy. Even though Fourth Amendment standards as to probable cause, over-breadth, and particularity should be uniform across the nation, there appears to be little consistency between jurisdictions as to the proper scope of cell phone search warrants and how they should be executed.

[21] *See, e.g.*, State v. Henderson, 854 N.W.2d 616, 625 (Neb. 2014).

[22] *See, e.g.*, United States v. Walker, No. 13-64-RGA, 2015 WL 3485647 (D. Del. May 29, 2015).

search was performed reasonably.[23] However because of the sheer amount of data held on cell phones and the clear over-breadth, particularity, and good faith exception problems present in post-*Riley* search warrants, addressing the execution of the warrant *ex post* is extremely problematic. As such, this Article argues that magistrates should impose restrictions on cell phone search warrants at the time the warrants are issued.

There are two plausible approaches courts should take for limiting the scope of post-*Riley* search warrants.[24] First, courts should try to effectuate the Fourth Amendment's particularity requirement by imposing *ex ante* search protocols on cell phone searches. Before issuing a warrant, courts should insist that officers submit the detailed steps they will take to search the cell phone once they have seized it.

The legality and wisdom of search protocols has attracted growing attention over the last decade, particularly after the Ninth Circuit wrestled with them in the BALCO steroid investigation.[25] Since the *Riley* decision, a few federal magistrates have been very vocal about demanding ex ante search protocols, saying that they are the only way to prevent search warrants for electronic data from becoming general warrants.[26] Not surprisingly, the

---

[23] *See* WAYNE R. LAFAVE 2 SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT 565 (5th ed. 2012) (noting narrow role for ex ante regulation).

[24] Legislatures could also take action by imposing statutory restrictions on the scope and execution of search warrants. Legislatures could model restrictions on the federal wiretapping statute, which imposes restrictions beyond the Fourth Amendment. For example, the federal wiretap statute, but not the Fourth Amendment, contains a requirement that the wiretap be truly necessary to the investigation before being issued. And the statute requires minimization such that investigators cannot listen to non-pertinent communications. The Vermont Supreme Court has pointed to such minimization requirements and explained that they should apply "with even more force in the computer context." *See* In Re Appeal of Application for Search Warrant, 71 A.3d 1158, 1170, 1171 (Vt. 2012). However, given that state legislatures took virtually no action to forbid warrantless cell phone searches before *Riley*, a legislative solution seems unlikely. *See* Adam M. Gershowitz, *Password Protected? Can a Password Save Your Cell Phone From a Search Incident to Arrest?* 96 IOWA L. REV. 1125, 1146-47 (2011) (lamenting lack of legislative activity). For instance, while the California legislature passed a bill to restrict warrantless cell phone searches in 2011, but the governor vetoed it. *See* Bob Egelko, *Brown Vetos Bill to Limit Cell Phone Searches*, S.F. CHRON., Oct. 10, 2011.

[25] *See* United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162 (9th Cir. 2010); *see also infra* note 162 (discussing earlier cases).

[26] *See, e.g.*, United States v. Phua, Nos. 2:14-cr-00249-AGP-PAL, 2015 WL 1281603 (D. Nev. Mar. 20, 2015). In the Matter of the Premises Known as Three Cellphones and One Micro-SD Card, No. L4-MJ-8013-DJW, 2014 WL 3845157 (D. Kan. Aug. 4, 2014); In the Matter of the Search of the premises known as a Nextel Cellular Telephone, No. 14-MJ-8005-DJW, 2014 WL 2898262 (D. Kan. June 26, 2014).

Department of Justice has strenuously resisted providing its own search protocols or having judges impose them as part of the warrant.[27] Academic commentators have likewise been critical, suggesting that ex ante protocols have no constitutional basis and are ill advised given judges' lack of computer forensic expertise.[28] Although there are valid objections to search protocols, the concerns are overblown. Properly implemented, search protocols can be an effective tool to reduce the privacy invasion associated with cell phone searches.[29]

A second approach to limiting post-*Riley* warrants would be for courts to restrict *where* on the phone police can search. Not all cell phone searches require a complicated forensic analysis of the phone's data however. In some "simple" cases – particularly certain street crimes -- magistrates can restrict warrants to the particular cell phone application for which there is probable cause. For example, police regularly conduct drug stings by having an informant or undercover officer exchange text messages with a suspected drug dealer.[30] In these cases, the search warrant should limit officers to searching the text messaging application, and not authorize a search of other data such as photographs or videos. As one court colorfully put it, "probable cause to believe drug trafficking communication may be found in [a] phone's mail application will not support the search of the phone's Angry Birds application."[31]

---

[27] *See* U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 79-83 (3rd ed. 2009).

[28] *See* Orin S. Kerr, *Ex Ante Regulation of Computer Search and Seizure*, 96 VA. L. REV. 1241 (2010).

[29] *See* Paul Ohm, *Massive Hard Drives, General Warrants, and the Power of Magistrate Judges*, 97 VA. L. REV. IN BRIEF 1 (2011); *see also infra* notes 196-232 and accompanying text.

[30] For a few recent examples, *see* United States v. Dahl, No. 14-382, 2014 WL 6792676 (Dec. 3, 2014), at * 2 ("[A]n undercover law enforcement officer . . . had been communicating with Dahl through e-mails and text messages."); United States v. Mack, 53 F. Supp. 3d 179 (D. D.C. 2014) (undercover officers arranged purchases of PCP by text message); State v. Carpenter, 158 So.2d 693 (Fla. Ct. App. 1st Dist. 2015) (undercover officer communicated with suspect by email and text messaging); Herrington v. Commonwealth, No. 1083–13–4, 2014 WL 5836895 (Va. Ct. App. Nov. 12, 2014), at *1 ("Using the informant's cell phone, and posing as the informant, [Deputy] McBride exchanged text messages. . . ."); State v. Paster, 15 N.E.2d 1252 (Ohio Ct. App. 2014) (undercover agent from Internet Crimes Against Children task force exchanged emails and text messages with suspect); State v. Hurley, No. 6–13–02, 2014 WL 2859112 (Ohio Ct. App. June 22, 2014) (police detective testifies at trial that informant set up a drug buy with a suspect and that copies of the text messages were not available because **"**we try to help preserve the CI [confidential informant], not getting their phone number out there").

[31] In the Matter of the Search of the premises known as a Nextel Cellular Telephone, No. 14-MJ-8005-DJW, 2014 WL 2898262 (D. Kan. June 26, 2014), at *13.

Restricting where police can search on a cell phone has a clear parallel in the tangible world. When an informant says that a drug dealer keeps heroin in the trunk of his car, courts have long restricted searches to the area where there is probable clause – the trunk – rather than the entire vehicle.[32] The same logic should apply in the electronic context. Courts could thus narrow search warrants in many simple cases – particularly street-level drug investigations -- by restricting *where* officers can search, rather than focusing on the more difficult protocol question of *how* the officers should organize and carry out their search.[33]

This Article offers a roadmap for effectuating the privacy guarantee announced in *Riley v. California*. Part I reviews the sweeping decision in *Riley* and the Supreme Court's desire to rely on search warrants to protect cell phone privacy. Part II then describes the particularity requirement of the Fourth Amendment. It demonstrates how a fairly straightforward restriction on law enforcement in the tangible world has proven difficult to apply in the electronic age. Part III then reviews post-*Riley* search warrants and explains that many search warrants have been issued (and some upheld on appeal) despite a staggering lack of probable cause and particularity. Part IV then wades into the ongoing debate about the legality and wisdom of search protocols. Here I challenge a number of the criticisms of search protocols made by Professor Orin Kerr. Part V then goes beyond search protocols and argues that in some simple cases (such as street-level drug deals) magistrates should restrict the applications that police can search on cell phones. Part V proposes the straightforward solution (not yet adopted by courts) that if police only have probable cause for data held on a specific cell phone application that the search warrant should only authorize a manual search of that application.

I. The Supreme Court's Desire To Protect Cell Phone Privacy in Riley v. California

[32] *See, e.g.*, United States v. Gastiaburo, 16 F.3d 582, 586 (4th Cir. 1994) ("[P]robable cause to believe that a container placed in the trunk of an automobile contains contraband does not justify a search of the entire car.").

[33] Of course, restricting the search location will not always work. For instance, child pornography can be hidden practically anywhere on a cell phone and law enforcement should not be restricted by a magistrate's guess as to where it is likely to be located. Yet, while child pornography cases represent a substantial number of traditional computer searches, they have been less common in the cell phone context. Instead, at least in the pre-*Riley* era, many cell phone searches were conducted so that law enforcement can look for evidence of drug transactions. *See* Gershowitz, *Password Protected? supra* note 24, at 1136; Bryan Andrew Stillwagon, *Bringing an End to Warrantless Cell Phone Searches*, 41 GA. L. REV. 1165, 1168 (2008).

For many years, the Supreme Court gave law enforcement wide authority to search arrestees incident to arrest.[34] So long as officers made a custodial arrest, the Court authorized a complete search of the arrestee's person and his immediate grabbing space.[35] In the Court's decision in *United States v. Robinson*, it made clear that police could open containers on a person, even if there was no probable cause to believe that the particular container posed a risk to the officer or held evidence that could be destroyed.[36] Although the Court subsequently wavered on the scope of the search incident to arrest doctrine with respect to automobiles,[37] the overall doctrine remained very steady and clear for over four decades. In a swamp of otherwise confusing and contradictory Fourth Amendment law,[38] the search incident to arrest doctrine continued to be a bright-line rule that offered fairly clear guidance to police who make millions of arrests per year.[39]

As technology advanced however the bright-line rule began to pose problems. In the early 1990s, police began to arrest drug dealers and search their pagers incident to arrest to find out who the dealers were communicating with.[40] Thereafter, officers began searching early generation cell phones because drug dealers arranged transactions by cell phones.[41] Most lower courts upheld such searches because pagers and flip phones were technically containers – they simply contained electronic information, rather than physical evidence – and the search incident to arrest doctrine imposed a bright-line rule allowing warrantless searches of all containers on or near an arrestee.[42]

As cell phone technology advanced however and devices began to hold emails, photos, and a huge amount of other personal information, many judges became uncomfortable with applying the search incident to arrest

---

[34] *See* Gershowitz, *The iPhone Meets the Fourth Amendment*, *supra* note 1, at 33-34.
[35] *See id.*
[36] *See* United States v. Robinson, 414 U.S. 218 (1973).
[37] *See* Barbara E. Armacost, *Arizona v. Gant: Does It Matter?* 2009 SUP. CT. REV. 275 (discussing New York v. Belton, 453 U.S. 454 (1981) and Arizona v. Gant, 556 U.S. 332 (2009)).
[38] *See* David A. Sklansky, *The Fourth Amendment and Common Law*, 100 COLUM. L. REV. 1739, 1751 (2000) ("[T]he term most often used to describe Fourth Amendment law is 'mess.'").
[39] *See* Wayne A. Logan, *An Exception Swallows a Rule: Police Authority to Search Incident to Arrest*, 19 YALE L. & POL'Y REV. 381 (2001) (describing the search incident to arrest doctrine as an "oasis of consistency").
[40] *See, e.g.*, United States v. Chan, 830 F. Supp. 531 (N.D. Cal. 1993); Gershowitz, *The iPhone Meets the Fourth Amendment*, *supra* note 1, at 36 (discussing other cases).
[41] For what appears to be the earliest reported case, see United States v. Parada, 289 F. Supp. 2d 1291 (D. Kan. 2003).
[42] *See* Gershowitz, *The iPhone Meets the Fourth Amendment*, *supra* note 1, at 38-39.

doctrine to a device that could hold more information than a warehouse.[43] A few courts pushed the envelope and refused to apply the doctrine to cell phones.[44] By 2013, there was a modest circuit split among the federal courts[45] and a handful of state courts, most prominently the Ohio Supreme Court, had banned warrantless cell phone searches incident to arrest.[46]

In spite of its reluctance to wade into emerging technology issues,[47] the Supreme Court acted fairly briskly and granted certiorari to a California case and a federal case to address the constitutionality of warrantless cell phone searches.[48] Many observers – this author included[49] – predicted that the Court would be fractured and that the justices might get mired in the technological uncertainty, leaving lower courts without much guidance.[50] Those predictions turned out to be (mostly) false.

In *Riley v. California*, the Supreme Court unanimously held that police cannot conduct warrantless cell phone searches incident to arrest.[51]

---

[43] *See* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 542 (2005) (noting that "every computer is akin to a vast warehouse of information" and that those sold in 2005 contained the equivalent of every book on the floor of an academic library).

[44] *See, e.g.*, United States v. Park, No. CR-05-375, 2007 WL 1521573 (N.D. Cal. May 23, 2007).

[45] *See* Evan O'Connor, *The Search for a Limited Search, The First Circuit Denies the Search of Cell Phones Incident to Arrest in* United States v. Wurie, 55 B.C. L. REV. E-SUPPLEMENT 59 (2014).

[46] *See* State v. Smith, 920 N.E.2d 949 (2009).

[47] While the Supreme Court decided a few technology cases in the years just prior to *Riley*, see United States v. Jones, 132 S. Ct 945 (2012); City of Ontario v. Quon, 560 U.S. 746 (2010), the Court's footprint here is, by its own admission, very modest. *See Quon*, 560 U.S. at 759 ("The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."). Over a decade ago, Professor Kerr argued in favor of judicial restraint in dealing with emerging technologies and the Court appears to have listened. *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 802 (2004).

[48] *See* Adam Liptak, *Supreme Court Will Consider Whether Police Need Warrants to Search Cell Phones*, N.Y. TIMES, Jan. 17, 2014.

[49] *See* Adam M. Gershowitz, *Surprising Unanimity, Even More Surprising Clarity*, SCOTUSBLOG, June 27, 2014, available at http://www.scotusblog.com/2014/06/symposium-surprising-unanimity-even-more-surprising-clarity/ (describing the Court's unanimity as "startling").

[50] *See, e.g.*, Robert Barnes, *Supreme Court Considers Cell Phone Searches, Right to Privacy*, WASH. POST Apr. 29, 2014 ("There did not seem to be majority support for the government's position . . . Nor did there seem to be enough votes for the other side's position…."); Adam Liptak, *Justices Appear Divided on Cellphone Warrants*, N.Y. TIMES, Apr. 29, 2014 ("The Supreme Court on Tuesday seemed torn . . . .").

[51] 134 S. Ct. 2473 (2014).

The Court's decision was unanimous and sweeping.[52] Chief Justice Roberts noted that technology had moved fast and that while smart phones were unheard of ten years ago, today a significant majority of Americans have such phones.[53] And smart phones are markedly different than the containers at issue in previous search incident to arrest cases. The Chief Justice noted that comparing a cell phone to an ordinary container "is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together."[54] The Court explained that smart phones can hold millions of pages of text, provide a history of internet usage, and access even more data in the cloud.[55]

Given the massive potential for privacy invasion, the justices concluded that the bright-line rule allowing warrantless searches incident to arrest would not strike the appropriate balance when applied to cell phones.[56] Unlike in the tangible world, in which a container might hold a knife or a gun, cell phones do not pose a risk of harm to the officers.[57] And while there is a risk that electronic evidence can be destroyed, police have solutions to that problem. Police can cut off the network by removing the cell phone's battery or by placing it in an aluminum-lined Faraday bag.[58]

Although the Court carved out an exception to the search incident to arrest doctrine, it certainly did not ban all cell phone searches. Chief Justice Roberts made clear that in ticking-time-bomb cases and other emergencies that police could turn to the exigency exception to search without a warrant.[59] And in cases with no exigency, criminals would not be able to hide behind their cell phones. Rather, the police could do something "simple – get a warrant."[60]

The Court's unanimous opinion in *Riley* has met with nearly uniform praise.[61] Chief Justice Roberts laid out a clear case for treating cell phones differently. And, at least at first glance, requiring police to "get a warrant" before searching a cell phone seems like a sufficient approach for protecting privacy interests. An unexpected problem is beginning to emerge however. While "get a warrant" is a "simple" answer, the scope of a cell phone search

---

[52] Although Justice Alito joined the majority, he wrote a short and fairly tepid concurring opinion. *See id*. at 2495 (Alito, J., concurring in part and concurring in the judgment).
[53] *See id.* at 2484.
[54] *Id*. at 2488.
[55] *See id*. at 2489-91.
[56] *See id*. at 2484-85.
[57] *See id*. at 2486.
[58] *See id*. at 2487.
[59] *See id*. at 2493-94.
[60] *Id*. at 2495.
[61] *See supra* note 4.

warrant and the question of how it should be executed are far from "simple." One might expect that the Fourth Amendment's particularity requirement would solve this problem. As outlined below in Part II however, the particularity requirement has largely proven to be ineffectual in the digital context.

II. An Overview of the Particularity Requirement and Its Application to Electronic Devices

The Fourth Amendment requires not just that searches be based on probable cause and be reasonable, but also that "no Warrants shall issue" unless "particularly describing the place to be searched, and the persons or things to be seized."[62] This so-called particularity requirement was designed to protect against the much-reviled "general warrants."[63] Officers must describe what they are looking for and where they will find it so that magistrates will know they are not "indiscriminate[ly] rummaging through citizens' personal effects."[64]

In the physical world, the particularity requirement is not very complicated. If police approach a magistrate with an informant's testimony that Sally Suspect is involved in narcotics trafficking, the magistrate should not automatically issue a warrant for Sally's house, her office, her car, and her person. As the Second Circuit has explained, "[a]bsent some limitation curtailing the officers' discretion when executing the warrant, the safeguard of having a magistrate determine the scope of the search is lost."[65] As such, the magistrate in Sally's case should demand more information about where the narcotics are likely to be found so that the search warrant can be tailored to a particular location where there is probable cause to believe narcotics will be located. The particularity guarantee applies within structures as well. If police have a search warrant for a stolen fifty-inch television, they cannot look in the microwave. If police only have probable cause for the trunk of an automobile, they cannot search in the car's glove compartment.[66]

In the context of computers, which house millions of pages of data, the particularity requirement should take on greater importance. Officers cannot procure a search warrant simply to engage in a "general search of all

---

[62] U.S. Const. Amend. IV. As one commentator has explained, "probable cause and particularity are closely related in search and seizure law." JOHN WESLEY HALL, JR. SEARCH AND SEIZURE 56.03 (5th ed. 2012).

[63] *See, e.g.*, Ashcroft v. al-Kidd, 131 S. Ct. 2074, 2084 (2011). A few courts have recognized that particularity and overbreadth are "two distinct legal issues." United States v. Zemlyansky, 945 F. Supp. 438, 450 (S.D.N.Y. 2013). Most cases intermingle the two concepts however.

[64] United States v. George, 975 F.2d 72, 75 (2nd Cir. 1992).

[65] *Id*. at 76.

[66] *See infra* notes 32 and 254 and accompanying text.

of the devices, records, files, and data."[67] As the Tenth Circuit explained, "[t]he modern development of the personal computer and its ability to store and intermingle a huge array of one's personal papers in a single place increases law enforcement's ability to conduct a wide-ranging search into a person's private affairs, and accordingly makes the particularity requirement that much more important."[68] As one court explained by way of example, "a warrant to search a computer for evidence of narcotics trafficking cannot be used as a blank check to scour the computer for evidence of pornographic crimes."[69]

Unfortunately, the particularity guarantee has provided little protection to defendants in the digital context. Because electronic data can be hidden anywhere on a computer or cell phone, it is very hard for officers to narrow down in advance the area that should be searched. Instead, courts typically let officers search through enormous amounts of data to find the needle in the haystack. As Professor Orin Kerr has recently explained, a "big problem [in digital searches] is that the particularity requirement does not play the significant role in computer search cases that it can play in digital search cases."[70] Thus, while one might expect that search warrants in computer or cell phone cases would specify in great detail what files or applications police may search, generally speaking that assumption would be wrong.

There are two fairly narrow categories of cases in which courts tend to find particularity violations in computer search warrants.[71] First, courts will sustain particularity challenges when the search warrant does not state on its face what crime the search is being conducted to find evidence of.[72] For instance, in *United States v. Galpin*, police submitted an affidavit indicating that Galpin – who was on parole for prior sex offenses -- was using MySpace to lure young boys to his home for sexual activity.[73] The warrant did not incorporate the application however and instead provided that police could search for evidence that Galpin had violated a sex offender

---

[67] United States v. Juarez, No. 12-CR-59 (RRM), 2013 WL 357570 (S.D.N.Y. Jan. 29, 2013), at *3.
[68] United States v. Otero, 563 F.3d 1127, 1132 (10th Cir. 2009).
[69] United States v. Villar, No. S305CR621KMK, 2007 WL 1075041 (S.D.N.Y. Apr. 4, 2007) at *37.
[70] *See* Orin S. Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 TEX. TECH. L. REV. __ (forthcoming 2016), at *16 (on file with the author).
[71] There is "no settled formula for determining whether a [computer search] warrant lacks particularity." United States v. Zemlyansky, 945 F. Supp.2d 438, 453 (S.D.N.Y. 2013).
[72] *See id*.
[73] 720 F.3d 436, 439-41 (2d. Cir. 2013).

registration statute requiring him to register online profiles.[74] The warrant thus authorized a search for evidence of a registration offense, not the crimes of child pornography or luring minors. The forensic examiner however searched for evidence of the more serious crimes and located computer files containing child pornography.[75] Because the search exceeded the scope of the named offense specified in the warrant, the court found a particularity violation.

Second, courts will also occasionally find a particularity violation when the search warrant contains overbroad catch-all language.[76] For instance, in a recent Second Circuit case, the court concluded that a warrant to search "computer equipment" and "electronic digital storage media" to lack particularity in violation of the Fourth Amendment.[77] Similarly, the Southern District of New York found a warrant that indiscriminately permitted the search of all "computers," "thumb drives," and various other electronic equipment to violate the particularity requirement.[78] The Tenth Circuit found a poorly drafted warrant that authorized the search of "'any and all information and/or data' stored on a computer" to violate the particularity requirement in a mail fraud case.[79] A few other courts have reached similar conclusions.[80]

Although particularity challenges are often made in computer search warrant cases, they are rarely successful. This is troubling because, as discussed below in Part III, many post-*Riley* search warrants authorize extremely broad searches that resemble general warrants.

III. The Post-*Riley* Warrant: Overbroad Search Warrants That Are Rarely Overturned

The *Riley* decision made it crystal clear that police must procure a warrant to search a cell phone.[81] Given the sweeping language in *Riley*, as

---

[74] *See id.* at 441.
[75] *See id.*
[76] This is true both in the electronic and tangible context. *See* HALL, *supra* note 62, 56.16 ("The particularity requirement has added considerations when documents are the subject of a search because a document warrant can easily become a general warrant.").
[77] United States v. Rosa, 626 F.3d 56, 62-64 (2d. Cir. 2010).
[78] United States v. Zemlyansky, 945 F. Supp.2d 438, 458-59, 464 (S.D.N.Y. 2013).
[79] United States v. Otero, 563 F.3d 1127, 1132-33 (10th Cir. 2009).
[80] *See, e.g.*, In re Applications for Search Warrants, No. 13–MJ–8163, 2013 WL 4647554 (D. Kan. Aug. 27, 2013) (refusing to issue search warrant for email service provider because the breadth of information sought failed the particularity requirement).
[81] Of course, the Court left the door open for police to conduct warrantless searches based on consent or exigent circumstances. Closing the door to searches incident to

well as the Fourth Amendment's particularity requirement, one might expect that judges would be careful to limit the scope of cell phone warrants. Relatedly, one might also expect that judges would provide instructions for how police should execute search warrants for cell phones. Those assumptions would largely be incorrect however. After *Riley*, judges assess whether there is probable cause to issue a warrant, but thereafter they typically do not restrict where on the cell phone police can search or how they should go about conducting the search.

As a result, many post-*Riley* cell phone warrants are far broader in scope than they should be. Some warrants authorize a search of "any and all data" on the phone, leading them to resemble the general warrants the Fourth Amendment was designed to prevent. Other warrants contain a more detailed list of the types of data that can be searched, but that list often contains categories of data and applications that are seemingly unrelated to the crime being investigated. For example, in drug cases, warrants often authorize a search for photographic evidence based on assertions that drug dealers take trophy photos of their drugs.[82] Such assertions are almost always just pure speculation however. This Part explores the different types of overbroad warrants issued since *Riley*.

A. Courts Have Issued Post-*Riley* Warrants That Improperly Authorize a Search of Every Piece of Data on the Phone

Some post-*Riley* cell phone search warrants have authorized the police to comb through "any and all data" on the phone. The propriety of these warrants should depend on the type of evidence the police are seeking. In some cases, this broad language may actually be acceptable. For instance, if police are searching for child pornography that could be hidden anywhere, it is arguably the case, depending on the sophistication of the forensic software, that officers may need to review "all data" to find evidence the suspect has purposefully mislabeled or hidden deep within the phone. Yet, even assuming such broad searches are permissible in *some* cases, they are certainly not justifiable in all cases. If police are searching for a specific type of file or if they have knowledge of exactly where the incriminating evidence would be on the phone, then a search of "any and all data" on the phone should violate the Fourth Amendment. Unfortunately, as described below, in

---

arrest, however, eliminated one of the easiest options for police to search cell phones incident to arrest.

[82] *See, e.g.*, United States v. Burgess, 576 F.3d 1078, 1091 (10th Cir. 2009) (noting briefly that computers could hold "trophy photographs"); Lucas v. State, 698 A.2d 1145, 1153 (Md. Spec. App. 1997) (describing detective's testimony that drug dealers take "trophy photographs" to impress their peers and recruit prospective employees and rejecting defendants' challenge to the testimony).

a number of post-*Riley* cases magistrates have issued "any and all" data warrants that are overbroad and lack particularity.[83]

1. Incorrectly Decided "All Data" Cases

In a recent New York case, *People v. Watkins*, a court upheld a search warrant for "all data" on the phone, even though police were looking for a single specific video the suspect was taking at the time of his arrest.[84] While police were arresting Watkins for wearing a loaded firearm, he was taking a video of the police with his iPhone.[85] The officers shut off the video and later procured a search warrant because they believed the video would support the case that Watkins was in possession of an (apparently illegal) firearm.[86] Watkins maintained that "the search warrant should have been limited only to video and audio files and not as to all data in the cellular telephone."[87] The court rejected Watkins's argument, explaining that such a rationale would enable a suspect to hide files in atypical places to misdirect the police.[88] The court therefore held that "a search warrant that allows an inspection of the entire cellular telephone is appropriate."[89] This explanation made little sense in Watkins's case however as the police only appeared to be searching for the video taken at the time of the arrest and it was the officers (rather than the suspect) who shut off the video. Thus, the police had probable cause for a particular video and knew that the video had not been hidden anywhere. The court authorized a search of the entire contents of the phone, even though their search should have been limited to the video library.

The Mississippi Court of Appeals issued a similarly troubling decision in April 2015. The court upheld a search warrant authorizing an investigator "to search and download any and all electronic data."[90] The only probable cause in the case was testimony that the suspect had taken photographs as he had sexually assaulted the victim. The warrant should accordingly have been limited to a search for photographs. Yet, the warrant authorized a complete download of "any and all data" on the cell phone.

---

[83] These warrants were issued in spite of the fact that law enforcement guides have discouraged such broad language. *See* AARON EDENS, CELL PHONE INVESTIGATIONS: SEARCH WARRANTS, CELL SITES, AND EVIDENCE RECOVERY 10-11 (2014) (listing "any and all" language as a "common search warrant and affidavit error" because of Fourth Amendment particularity concerns).

[84] *See* People v. Watkins, 994 N.Y.S.2d 816 (N.Y. Supr. Ct. 2014).

[85] *See id.* at 817.

[86] *See id.*

[87] *Id*. at 818.

[88] *See id.*

[89] *Id*.

[90] Moore v. State, 160 So.2d 728, 731 (Miss. Ct. App. 2015).

While investigators discovered only the incriminating photographs that they were searching for,[91] there is no way of knowing how much other data – completely unrelated to photographs – that the officers rifled through. Put simply, there was probable cause for a search warrant, but not a general warrant authorizing the police to rummage. The appellate court upheld the search warrant nonetheless.

The same problem arose in *United States v. Romain*, a 2014 case from the Southern District of New York.[92] Following a long investigation, police submitted an affidavit alleging that Romain "used multiple cellular phone numbers in order to carry on the drug-related scheme, including setting up narcotics-related meetings and wire payments."[93] The court issued a search warrant not only for call log information, text messages, emails, and other communications, but also for photographs and "*any and all contents of programs or 'apps'* that are contained in the computerized memory [of the phone]."[94] By authorizing a search of all "apps," the warrant effectively permitted a search of the entire contents of the phone. The federal district judge nevertheless rejected the defendant's claim that the warrant was too broad.[95] Even though the phone could have held numerous apps that could not possibly contain evidence of drug trafficking, the court found no fault with the broad "any and all" language of the warrant.[96]

Other cases do not use the "any and all" language, but instead utilize similarly broad and over-inclusive terminology. For instance, in the 2014 case of *Commonwealth v. Hedgepath*, the defendant was arrested for severely beating, raping, and murdering his girlfriend.[97] Police procured a warrant to seize numerous items "that may have been used to aid in the assault . . . including but not limited to all electronic equipment, computers, and cell phones."[98] Officers found ten "highly incriminating videos" on Hedgepath's cell phone that showed him sexually assaulting the victim.[99] Hedgepath contended that the warrant failed for lack of particularity because

---

[91] *See id.*

[92] No. 13 CR. 724, 2014 WL 6765831 (S.D.N.Y. Dec. 1, 2014).

[93] *Id*. at *2.

[94] *Id*. (emphasis added).

[95] *See id.* at *9.

[96] The court did find the warrant to be insufficiently particular because it did not list the criminal statute that the police had probable cause to believe was violated. The court minimized this error however and easily found it subject to the good faith exception. *See id*. at *5-7. For a more detailed explanation of the role of the good faith exception in salvaging defective cell phone search warrants, *see infra* Parts III.A.2 and III.B.2.

[97] 441 S.W.3d 119 (Ky. 2014).

[98] *Id*. at 130.

[99] *Id*. at 123.

it did not "describe[e] the content of the phone to be searched."[100] The Kentucky Supreme Court's opinion did not explain why police believed incriminating evidence would be found on the cell phone or where such evidence would be found.[101] The court's analysis was limited to a conclusory two-sentence statement that "[t]he police searched for and found evidence of Hedgepath's physical and sexual assault of the victim. They did not find evidence of other crimes, such as drug possession or theft."[102]

The Court's reasoning in *Hedgepath* is deeply problematic. First, the warrant did not specify with particularity the nexus between the crime and the cell phone. Second, the warrant was overbroad. There simply was no probable cause to search certain functions of the cell phone that could not possibly harbor evidence of a physical or sexual assault. Probable cause does not exist simply because an officer claims it exists. And a search is not supported by probable cause or sufficiently particular simply because of the end result that the officers found incriminating evidence. As such, the court's conclusory decision that "[t]he search warrant and affidavit were sufficiently particular" makes little sense.[103]

The Michigan Court of Appeals upheld a search warrant with even vaguer language in May 2015.[104] A judge authorized a warrant to search multiple cell phones for "computer generated data."[105] The police then discovered instructions for making methamphetamine.[106] The defendant contended that "the warrant did not state with particularity that the contents of the cell phone could be searched." The appellate court appeared to misunderstand the particularity doctrine and simply concluded that "the relevant images found on defendant's cell phone would also fall under the heading of computer-generated data."[107] The court cited language from the *Riley* opinion that noted that cell phones hold so much information that they amount to minicomputers.[108] Rather than recognizing that the tremendous storage capacity requires a *limitation* on search warrants, the court reached

---

[100] *Id*. at 130.

[101] The Court's decision explained only that the affidavit in support of the warrant "stated that the officer believes the property constitutes 'property or things used as a means of committing a crime' or 'property of things consisting of evidence which tends to show a crime has been committed or a particular person committed a crime." *Id*. at 131.

[102] *Id*.

[103] *Id*.

[104] *See* People v. Farrsiar, No. 320376, 2015 WL 2329071 (Mich. App. May 14, 2015).

[105] *Id*. at *6.

[106] *Id*. at *1.

[107] *Id*. at *6.

[108] *See id*.

the opposite conclusion and upheld the warrant simply because a phone is equivalent to a computer and thus contains "computer generated data."

A case decided eighteen months before *Riley – United States v. Juarez* – suffered from a similar problem.[109] Police observed Juarez use his cellphone to videotape between the legs of women wearing dresses as they walked in New York City.[110] The phone was in video recording mode when the officers recovered it from Juarez's backpack. Nevertheless, officers convinced a magistrate to issue a search warrant for "any numbers, digits, letters, and symbols stored in the memory of said device, as well as any digital photographs and video recordings taken and stored in the memory" of a "Spring HTC Cellular Telephone, model PC36100, with serial number HT48HL10995." Subsequent searches revealed an image of child pornography and the case was handed over to federal prosecutors.[111]

The search warrant in *Juarez* was flawed because it authorized searches in areas of the phone that could not hold the evidence sought. The officers had probable cause only for videos, but the warrant authorized a search of practically all data on the phone. Juarez filed a particularity challenge to the warrant, but inexplicably, he did "not challenge the warrant's particularity on the grounds that it fails to identify with particularity the place to be searched."[112] The court suggested such a challenge would have failed in any event however, because "the warrant states explicitly the place to be searched: 'Spring HTC Cellular Telephone, model PC36100, with serial number HT48HL10995."[113] This reasoning, of course, is the root of the problem. If the search warrant is for a physical place – a lump of metal formed into a cell phone – then law enforcement has free reign to rummage through millions of pages of data based on probable cause for one isolated piece of evidence. The better approach, at least in cases like *Juarez*, is to think of the phone as an electronic container that can be sub-divided into different areas.[114] In a case like *Juarez*, in which the probable

---

[109] United States v. Juarez, No. 12-CR-59 (RRM), 2013 WL 357570 (S.D.N.Y. Jan. 29, 2013).

[110] *See id*. at *1.

[111] *See id*.

[112] *Id*. at *2.

[113] *Id*.

[114] Even this approach, often referred to as the file cabinet analogy, is hardly protective of privacy. *See* Donald A. Dripps, "*Dearest Property": Digital Evidence and the History of Private "Papers" as Special Objects of Search and Seizure*, 103 J. CRIM. L. & CRIMINOLOGY, 49, 59 (2013) (noting that "the orthodox view of searches of computers and other electronics, which equates digital storage devices with file cabinets" but noting that concern about the lack of privacy protection has created "unquiet among judges"); Thomas K. Clancy, *The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer*, 75 MISS. L.J. 193, 198-205 (2005) (describing how most courts have embraced the file cabinet

cause is only for a single video, and in which the officers know for certain that the suspect had no time to hide the video somewhere atypical in the phone, then the particularity requirement should impose restrictions on the extent of officers' ability to search the phone. Search warrants for "any and all" data or similarly broad language thus fail to effectuate the goal of *Riley* to protect privacy against vast government overreaching.[115]

2. Flawed "Any And All Data" Warrants Saved by the Good Faith Exception

Unfortunately, while a small number of judges have been willing to recognize that "any and all data" cell phone warrants pose particularity problems, even that recognition is typically insufficient to suppress the evidence. The reason is that the good faith exception to the exclusionary rule operates with considerable force for electronic search warrants. [116] Cell

---

analogy but explaining how some courts have concluded that the analogy allows officers to access too much information).

[115] A few courts have recognized the particularity problem posed by "any and all data" search warrants in the aftermath of *Riley*. For instance, in *United States v. Winn*, No. 14-CR-30169, 2015 WL 553286 (S.D. Ill. Feb. 9, 2015), police had probable cause that a suspect was guilty of public indecency because he was photographing teenagers at the pool. Rather than issue a warrant for photos or perhaps videos, the judge authorized a search of practically the entire contents of Winn's cell phone, including emails, call logs, internet history, and GPS information. *See id*. at *2. A state judge failed to notice that the search warrant application named the offense of disorderly conduct, while the supporting documents signed by law enforcement named the offense of public indecency. *See id*. After the officers used a data extraction device to do a "complete dump" of the phone, they discovered child pornography and referred the case to federal prosecutors. A federal judge later found that the warrant was overbroad and failed the particularity requirement. *See id*. at *11. With respect to particularity, the judge explained that the warrant failed to specify a relevant time frame of data to search and that it was flawed because it only set forth categories of data (such as photos and videos) rather than a more specific description of the types of photos. *See id.* Had the case remained in state court, it is quite possible a challenge to the warrant would have been rejected.

[116] Prior to *Riley*, courts regularly turned to the good faith exception to approve of questionable computer searches. For example, in United States v. Rosa, 626 F.3d 56 (2d. Cir. 2010) state police procured a warrant for child pornography that authorized broad-based searches of an enormous amount of computer equipment. The court agreed with Rosa that the search warrant "lacked the requisite specificity to allow for a tailored search of his electronic media." *Id*. at 62. Because the warrant did not link the items to be searched and seized to particularized criminal activity it "lacked meaningful parameters on an otherwise limitless search of Rosa's electronic media." *Id*. Nevertheless, the court refused to suppress the evidence because "the officers acted reasonably" and thus in good faith. *Id*. at 65. The court concluded that the

phone warrants are lengthy and complicated and it would be hard for ordinary officers to recognize in advance that the warrant failed under complicated particularity jurisprudence.[117] As such, if a lower court judge or federal magistrate issues a cell phone search warrant for "any or all data" (or some comparably vague and overbroad language) and officers execute that warrant, the execution would likely be found to be in good faith.

As a federal judge in Delaware noted in May 2015 in upholding a defective cell phone search warrant:

> [W]hile I have concluded that the subject warrant is a general warrant . . . I do not think that most federal "street agents" would know on their own whether the warrant was general. Thus, I do not think the officer's reliance upon the warrant was so unreasonable as to conclude that there was a lack of good faith in so relying.[118]

Only a few months after the *Riley* decision, courts began to rely on the good faith exception to allow the admission of evidence seized from "any and all data" cell phone warrants. For example, in *State v. Henderson*, the police seized the cell phone of a murder suspect and requested a warrant to search "[a]ny and all information contained on the cell phone."[119] After a judge issued the warrant, police downloaded various types of data and found

---

warrant was drafted hastily and that the investigative team relied on their knowledge of the ongoing investigation, and the search limitations implicit in documents they submitted to procure the warrant, rather than the warrant itself. *See id*. at 66. Similarly, in United States v. Riccardi, 405 F.3d 852 (10th Cir. 2005) the court did not suppress evidence from a computer search warrant that failed the particularity requirement. Relying on the good faith exception, the court focused on the fact that the affidavit supporting the warrant limited the search to the crime for which there was probable cause and that the officers who executed the warrant were involved throughout the investigation. *See id*. at 863. In other cases, courts have refused to suppress electronic evidence because even though the face of the warrant indicated a particularity requirement, the executing officers could reasonably have read the warrant to be more limited. *See, e.g*., United States v. Otero, 563 F.3d 1127 (10th Cir. 2009) (applying good faith exception because the officers "had reason to believe the warrant was valid, considered themselves authorized to search only for evidence of crimes for which they had probable cause, and conducted their search accordingly").

[117] For instance, one redacted warrant and application provided to the author was 19 pages long. *See* In the Matter of the Search of Cellular Phone Utilizing T-Mobile phone number (757)--- ---- and ISMI No. (Redacted) (E.D.Va. 2013) (on file with the author).

[118] United States v. Walker, No. 13-64-RGA, 2015 WL 3485647 (D. Del. May 29, 2015), at *5.

[119] State v. Henderson, 854 N.W.2d 616, 625 (Neb. 2014).

incriminating text messages.[120] On appeal, the Supreme Court of Nebraska found that the warrant failed to comply with the particularity requirement because it "did not sufficiently limit the search of the contents of the cell phone."[121] The Court then turned to the good faith exception and explained that "there is no indication in this case that the officers would reasonably have known of the defects in the warrant[]. . . ."[122] The court therefore declined to suppress the search.[123]

In a more recent 2015 case – *United States v. Russian* -- a federal court also relied on the good faith exception to admit evidence from a problematic search warrant.[124] Following a drug arrest, officers sought and received a warrant to search for "text messages, phone numbers, phone calls, sent and received, *any data* contained within the phone or on any removable media device within the phone."[125] The court described it as a "close call regarding whether the warrant and its application meets the particularity requirement" but never analyzed that question.[126] Instead, the court simply upheld the search under the good faith exception.[127]

* * *

To be sure, there may be cases in which a search warrant for "any and all data" on a cell phone could arguably be legitimate. If police are searching for electronic evidence that could be hidden anywhere on the phone, and if the suspect had time to hide that evidence in an atypical file location, then law enforcement legitimately may have to look through the entire contents of the cell phone to be sure they have not missed evidence. But in cases where the police know the exact type of file they are looking for, or in cases in which police know for certain the type of application that could hold the incriminating evidence, then searching "any and all" data should violate the particularity requirement. Accordingly, the cases outlined in this Part should have been decided differently. Until appellate courts signal a more robust particularity guarantee for post-*Riley* cell phone search warrants however, confusion and erroneous rulings are likely to continue in numerous other cases.

B. Warrants Authorizing Searches of Data for Which There is No Probable Cause

---

[120] *See id.*
[121] *Id*. at 633.
[122] *Id*. at 634.
[123] *See id*. at 634-35.
[124] United States v. Russian, No. 14-10018-01-EFM, 2015 WL 1863333 (D. Kan. Apr. 23, 2015).
[125] *Id*. at *2 (emphasis added).
[126] *Id*. at *7.
[127] *See id*. at *7-8.

Some cell phone search warrants are more carefully drawn and do not request "any and all data." Instead, these warrants contain long lists of functions and applications on the cell phone that the police may search. For instance, police often have probable cause that cell phones contain evidence of text and voiced-based communication that was used to arrange narcotics distribution. A search warrant might therefore authorize a search of the phone's address book, call history, voicemail, text-messages, email, and other text functions. Unfortunately, post-*Riley* search warrants often go far beyond the logical list of applications that could possibly harbor evidence of criminal activity. In drug cases, the best example is cell phone search warrants that authorize searches for photos and videos, which are unrelated functions for which there is typically no probable cause. And even when courts recognize the warrants are overbroad, they once again turn to the good faith exception.

1. Incorrectly Decided "Laundry List" Search Warrant Cases

In the 2015 case of *United States v. Garcia-Alvarez*, police discovered three cell phones when they arrested the defendant for possession of a large quantity of methamphetamine.[128] Because drug dealers often communicate by text message, it was logical for the officers to seek a warrant for cell phone communications. A logical warrant would therefore authorize a search of text messages, call history, and possibly even emails. Yet, the warrant went further however and authorized a search for "photographs, audio files, videos, or location data" "tending to indicate efforts to deliver controlled substances from Mexico to the United States."[129] However, there was no particular reason to believe photographs and videos would hold evidence that Garcia-Alvarez was involved in drug trafficking. Of course, it is *possible* that photographs and videos could contain evidence of drug trafficking. But many things are possible. To use a clever turn of phrase that courts sometimes invoke, it is possible that a person could hide a lawnmower in a bedroom.[130] Yet, the ordinary search warrant for a lawnmower does not extend to bedrooms because while a "lawnmower could be in the bedroom, [] there is no probable cause to believe that it is there."[131]

---

[128] *See* United States v. Garcia-Alvarez, No. 14-cr-0621 JM, 2015 WL 777411 (S.D. Cal. Feb. 24, 2015).
[129] *Id*. at *1.
[130] *See* Long v. State, 132 S.W.3d 443, 453 (Tex. Crim. App. 2004); *see also* United States v. Ross, 456 U.S. 798 (1982) ("Just as probable cause to believe that a stolen lawnmower may be found in a garage will not support a warrant to search an upstairs bedroom, probable cause to believe that undocumented aliens are being transported in a van will not justify a warrantless search of a suitcase.").
[131] *Long*, 132 S.W.3d at 453.

In short, the possibility that photographic or video evidence *could* possibly exist does not mean that there is probable cause that it actually exists however. Thus, the search warrant in *Garcia-Alvarez* was overbroad and insufficiently particular. The federal court upheld the warrant however.[132]

Shortly after *Riley* was decided, a federal court in Maryland upheld an even more troubling cell phone search warrant.[133] In *United States v. Herevia*, a cooperating defendant informed officers that she was buying cocaine from a Mexican supplier.[134] Following detailed surveillance, the officers eventually arrested multiple defendants and found more than 18 kilograms of cocaine and $30,000 in currency in a vehicle.[135] The officers seized a cell phone from the person of each defendant.[136] Once the cell phones were seized, the officers applied for a warrant before searching them.[137] The supporting affidavit recounted the surveillance that led to the arrests and that the defendants were arrested in possession of cocaine. Only a single conclusory paragraph set forth a rationale for believing evidence would be found on the cell phone however:

> Based on my training, knowledge, and experience, I know that suspected criminals often communicate via wireless telephone regarding their illegal activities. I therefore submit that there is probable cause to believe that SUBJECT TELEPHONES A and B contain additional information relating to the drug trafficking activities of [Defendants], including, but not limited to: (i) communications with co-conspirators and/or sources of supply regarding the transportation and distribution of cocaine, (ii) communications regarding the 18 kilograms seized by law enforcement officers on June 3, 2013.[138]

---

[132] *See Garcia-Alvarez*, 2015 WL 777411, at *5.

[133] The warrant in *Herevia* was issued prior to *Riley*. Because the case was pending on direct review when *Riley* was decided, the Supreme Court's decision would potentially apply so long as the government is unable to invoke the good faith exception of Davis v. United States, 131 S. Ct. 2419 (2011), which can save a defective search if police were relying on binding appellate court precedent.

[134] *See* United States v. Herevia, No. RDB-13-639, 2014 WL 4784321 (D. Md. Sept. 23, 2014), at *1.

[135] *See id*. at *3.

[136] *See* In the Matter of the Search of LG Wireless Telephone (Subject Telephone A), Model No. LG 430G, Serial No. 207CYCV456331, Case No. 1:13-mj-01466 CBA at *5 (D. Md. July 15, 2014), at 5 (search warrant application on file with the author).

[137] *See id*.

[138] *Id*. at 6.

Based on the officers' testimony, a magistrate issued a warrant authorizing a search for telephone numbers, emails, text messages, call logs, voicemails, location information, photos and videos.[139] The defendant challenged the search warrant for the cell phones on the grounds of lack of probable cause and lack of specificity in the warrant itself.[140] In less than a paragraph, the court summarily dismissed the challenge because "law enforcement training, knowledge, and experience with the drug trade [indicates that] drug traffickers often communicate about their business through cell phones."[141]

The court's brief reasoning was flawed. While it is true that drug dealers use cell phones, the warrant application in no way explained why there was probable cause to believe that these particular phones were linked to drugs. Nor did the officers specify what information they expected to find in the phones. And the court utterly failed to place any limitation on what data that officers could and could not search. Indeed, neither the affidavit, the search warrant, the government's opposition to the motion to suppress, nor the federal district court opinion explained why there was probable cause that cell phone communications would contain evidence of drug trafficking in this case.[142] In short, it seems that there was no probable cause that these particular cell phones contained evidence of drug activity.

But even if we accept the proposition (often advocated by law enforcement and prosecutors) that expert testimony can provide probable cause that a drug dealer's cell phone likely harbors evidence of illicit communications,[143] that would only authorize a search for telephone numbers, emails, text messages, call logs, and voicemails. The search warrant in *Herevia* also authorized a search for "location information, photos

---

[139] *See id.* Attachment B.

[140] *See Herevia*, 2014 WL 4784321, at *7.

[141] *Id*. at *8.

[142] *See id*.; United States v. Payne et al., No. RDB-13-0639, Government's Response to Defendants' Motion to Suppress Evidence Recovered From Their Cellular Telephones (D. Md. July 15, 2014) (on file with the author).

[143] Not all courts are willing to accept unsupported assertions from experts that a phone is likely to harbor evidence based on the type of crime committed. For instance, in United States v. Phua, No. 2:14-cd-00249-APG-PAL, 2015 WL 1281603 (D. Nev. Mar. 20, 2015), the government sought to search six cell phones for evidence of illegal gambling during the defendants' stay at Caesars Palace. The court refused to issue the warrant because the federal agents failed to explain why the cell phones "were used to commit the enumerated offenses, or what facts law enforcement has come to believe the devices may contain evidence of the enumerated offenses." *Id*. at *5. Put differently, the judge refused to accept law enforcement's blanket assertion that the cell phones would contain evidence simply because the defendants were charged with an offense that, generally speaking, might leave evidence on a cell phone.

and videos."[144] Yet, there would be no reason to believe those types of files would contain evidence of drug communications.[145]

The search warrants in *Garcia-Alvarez* and *Herevia*, authorized police to search too wide of an area of cell phone data given the limited probable cause in the cases. An apt analogy might be one in which the police had probable cause that a suspect had stolen a car and driven it home. The garage might harbor the car. Perhaps even the shed or barn in the back of the house could hold the car. But there is simply no way that the bedrooms on the second floor could hold a full-sized vehicle. A warrant should therefore issue for the garage, shed, and barn, but not the house itself. Yet, in the cases above, by issuing a warrant for photos or videos when there was probable cause only for different types of communication, the courts upheld searches that should have failed the particularity guarantee.

2. Flawed "Laundry List" Search Warrants Saved by the Good Faith Exception

Even when judges do recognize a cell phone search warrant includes categories of applications that should not be searched, the good faith exception prevents the suppression of evidence. Indeed, even more so than "any and all data" warrants, when police execute a warrant with a long laundry list of applications to be searched, it is very easy for courts to turn to the good faith exception.

For example, in the 2015 case of *United States v. Walker*, a federal district judge found that a post-*Riley* cell phone search warrant failed to satisfy the particularity requirement.[146] The warrant authorized a search of the cell phones for firearms evidence and listed a dozen categories of data that the police could search through, including calendar entries, financial records, and more typical data such as phone numbers, voicemails, and photos. The court found that the warrant was so broad that it effectively "authorize[d] a search of the entire contents of the cell phone."[147] Moreover, while the warrant listed some appropriate categories of evidence for officers to search for, it simply listed the types of applications without any reference to how specific evidence connected to the alleged firearms offense could be

---

[144] *Herevia*, 2014 WL 4784321, at Attachment B.

[145] Search warrants in pre-*Riley* cases have also authorized searches for photos and video evidence based on conclusory statements from officers that drug dealers sometimes photograph contraband. *See, e.g.*, United States v. Gorney, No. 13-70, 2014 WL 2860637 (W.D. Pa. June 23, 2014), at *2 (authorizing search warrant for, inter alia, "any photos or videos" based on officers' testimony that "[y]our affiants have seen incidents where individuals involved with illegal narcotics have taken cell phone photographs and videos of illegal narcotics.").

[146] No. 13-64-RGA, 2015 WL 3485647 (D. Del. May 29, 2015).

[147] *Id*. at *4.

found in those applications. The warrant therefore in no way guided or limited the discretion of the officer who executed it.[148] The district judge thus found it to be an invalid general warrant.[149] Even though the warrant was invalid, the court declined to suppress an incriminating text message found on the phone because the officers acted in good faith.[150] The court explained that "I do not think that most federal 'street agents' would know on their own whether the warrant was general. Thus, I do not think the officer's reliance upon the warrant was so unreasonable as to conclude that there was a lack of good faith in so relying.[151] Put differently, the district judge recognized that electronic search warrants can be exceedingly broad and authorize law enforcement officers to search far more expansively than the Fourth Amendment should authorize. At the same time, because electronic warrants are complicated, almost all searches will be upheld because the complexity of proper drafting means that most law enforcement officers would not understand any particularity problems and would act in good faith.

Not surprisingly, a sizeable number of post-*Riley* courts have turned to the good faith exception in upholding cell phone search warrants.[152]

*** * ***

Although a unanimous Supreme Court said in *Riley* that the approach to cell phone privacy was "simple – get a warrant"[153] the cases in Parts III.A and III.B above demonstrate how the warrant process is not simple at all. In the cases described above, police procured a warrant, but they were still able to rummage through mountains of unrelated data that magistrates should have foreclosed by enforcing the particularity requirement. There are undoubtedly many more cases than those outlined

---

[148] *See id.*

[149] *See id*. at *5.

[150] *See id*.

[151] *Id*.

[152] *See* People v. Rackley, No. VCR 213747, 2015 WL 1862880 (Cal. Super. Ct. Apr. 29, 2015) (upholding pre-*Riley* search warrant to search cell phone for evidence of robbery and noting that even if warrant were defective, police relied on it in good faith); Moore v. State, 160 So. 3d 728, 733-34 (Miss. Ct. App. 2015) (finding investigator acted reasonably); United States v. Jefferson, No. 14-20119, 2015 WL 3576035 (E.D. Mich. June 5, 2015), at *6 (finding enough evidence linking cell phone to criminal activity for the agent "to rely in good faith on it."); United States v. Brewer, No. 1:13-CR-13-03, 2015 WL 2250150 (M.D. Pa. May 12, 2015), at *5 (concluding that "even if the nexus is insufficient, a reasonably well trained officer would not have known that the warrant was illegal"); United States v. Willis, No. 13-CR-6013G, 2014 WL 6791386 (W.D.N.Y. Nov. 5, 2014), at *18 (finding no evidence that the searching officers did not rely on the warrant in good faith); *see also infra* notes 119-27 and accompanying text (discussing *State v. Henderson* and United States v. Russian).

[153] *Riley*, 134 S. Ct. at 2495.

above. Reported decisions about cell phone searches are likely only a fraction of the total number of search warrants. Many cell phone search warrants are sealed[154] and never see the light of day. In other cases, police execute search warrants but find no evidence, giving the suspect no reason to file a suppression motion. And while some defendants may enter conditional guilty pleas that enable them to subsequently challenge the cell phone search on appeal, other cases are likely resolved completely by quiet plea bargains that leave no paper trail of judicial decisions. In short, the flawed post-*Riley* search warrants in Parts III.A and III.B are probably only the tip of the iceberg.[155]

In light of the significant problems with post-*Riley* search warrants, Parts IV and V below propose two solutions.

IV. Ex Ante Search Protocols Can Help to Effectuate the Particularity Guarantee

Over the last few years, courts and scholars have begun debating whether search protocols – ex ante regulations and restrictions on how police should execute search warrants – should be imposed in computer and cell phone search warrants. Although the law and policy questions are complicated, they largely boil down to whether magistrates should impose tight restrictions up front so that officers will be guided from the outset, rather than litigating the reasonableness of an electronic search after it has already happened.

The Supreme Court made a passing reference to search protocols in *Riley*,[156] but in no way advanced, no less settled, the debate about the

---

[154] I am grateful to federal magistrate Judge Tommy Miller for making this point to me.

[155] Of course, there are some very well drafted post-*Riley* search warrants. Such decisions unfortunately reinforce the flaws in the decisions highlighted in Parts III.A and III.B above. For example, in Commonwealth v. Dougalewicz, Nos. 247 WDA 2014, 248 WDA, 2015 WL 1431922 (Pa. Super. Mar. 30, 2015), police had probable cause to believe a coach was having a sexual relationship with a thirteen-year-old member of the team. Because the evidence indicated that the coach and victim, texted, called, and exchanged pictures by cell phone, the warrant authorized a search of "[a]ny and all text messages, picture mail and phone calls . . . in regards to alleged sexual misconduct with a 14 year old female by Dougalewicz." *Id*. at *2. This warrant appears sufficiently narrow and particular. It identifies the items for which there are probable cause, authorizes a search of those items only, and instructs the police about how the items link to the specific offense of sexual misconduct with a minor.

[156] In response to the government's assertion that it could develop protocols if the Court allowed warrantless searches incident to arrest, the Court remarked: "Probably a good idea, but the Founders did not fight a revolution to gain the right to government agency protocols." *Riley*, 134 S. Ct. 2491.

wisdom and constitutionality of ex ante restrictions. Thus, as defendants in post-*Riley* cases increasingly move to suppress evidence because of the absence of ex ante search protocols, magistrates find themselves struggling with whether to require ex ante restrictions of electronic searches. This Part explains courts' reluctance to impose search protocols and the Department of Justice's fierce opposition to them. It then assesses whether they are constitutional, and their increasing use by magistrate judges. Finally, this Part challenges the conventional wisdom that ex ante search protocols are unwise and impractical.

A. Courts Are Typically Reluctant To Impose Search Protocols

When magistrates issue a warrant, they specify the places to be searched and the items to be seized. For the most part however, courts have not imposed restrictions on *how* the warrant is to be executed however. As the Supreme Court explained in *Dalia v. United States*, "it is generally left to the discretion of the executing officers to determine the details of how best to proceed with the performance of a search authorized by a warrant."[157] Or, as the First Circuit put it more succinctly, "[t]he warrant process is primarily concerned with identifying what may be searched or seized – not how."[158]

Defendants who have had their computers searched have argued that the rules should be different in electronic search cases. These defendants maintain that because of the sheer amount of information computers hold that is unrelated to the crime being investigated, that the warrants should include search protocols specifying what steps the officers should take in executing the warrant. For example, a magistrate might restrict how long police can view electronic data. Or the judge might specify the particular steps an officer may take in examining the data.

Not surprisingly, the Department of Justice has strongly resisted the introduction of search protocols that would limit how police search computers in executing a warrant.[159] The Justice Department describes such restrictions as "burdensome," "unnecessary," and "inconsistent with Supreme Court precedent."[160] In particular, the Justice Department has long argued against any restriction that limits officers to searching for particular keywords in files because not all types of files -- PDF's are a good example -- are searchable by keyword.[161]

---

[157] 441 U.S. 238, 257 (1979).
[158] United States v. Upham, 168 F.3d 532, 537 (1st Cir. 1999).
[159] *See* U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 79-83 (2009).
[160] *Id*. at 79, 80.
[161] *See id*. at 79.

For the most part, courts have agreed with the Department of Justice and have declined to impose protocols specifying how a search warrant for a computer should be executed.[162] For instance, in *United States v. Burgess* a judge issued a warrant to search a laptop computer and two external hard drives for, *inter alia* "photographs of coconspirators or photographs of illegal narcotics."[163] When the subsequent search revealed child pornography, Burgess moved to suppress. The Tenth Circuit rejected any suggestion of a search protocol, explaining that "this Court has never required warrants to contain a particularized computer search strategy."[164] The court explained that:

> It is unrealistic to expect a warrant to prospectively restrict the scope of a search by directory, filename or extension or attempt to structure search methods – that process must remain dynamic . . . [I]t is folly for a search warrant to attempt to structure the mechanics of the search and a warrant imposing such limits would unduly restrict legitimate search objectives. One would not ordinarily

---

[162] *See, e.g.*, United States v. Khanani, 502 F.3d 1281, 1290 (11th Cir. 2007) (rejecting suppression motion highlighting lack of search protocols); United States v. Brooks, 427 F.3d 1246, 1251 (10th Cir. 2005) ("This court has never required warrants to contain a particularized computer search strategy."); United States v. Upham, 168 F.3d 532, 537 (1st Cir. 1999) (explaining that "[t]he warrant process is primarily concerned with identifying *what* may be searched or seized—not how . . . ."); United States v. Jackson, No. 3:14-CR-1 CAR, 2015 WL 2236400 (M.D. Ga. May 12, 2015), at *14 ("an electronic search strategy [for a cell phone] is not necessarily required to be included in the affidavit"); (United States v. Lustyik, 57 F. Supp. 3d 213, 229 (S.D.N.Y. 2014) (noting in computer and cell phone search case that the Second Circuit does not require search protocols); United States v. Villar, No. S305CR621KMK, 2007 WL 1075041 (S.D.N.Y. Apr. 4, 2007) at *37 ("[W]hile the warrant must state with particularity the materials to be seized from a computer, the warrant need not specify *how* the computers will be searched."); United States v. Cartier, No. 2:06-cr-73, 2007 WL 319648, at *3 (D.N.D. Jan. 30, 2007) ("[T]he warrant is not defective because it did not include a computer search methodology."); United States v. Shinderman, No. CRIM. 05-67-P-H, 2006 WL 522105, at *19 (D. Maine Mar. 2, 2006) (explaining that "there is no Fourth Amendment requirement that search warrants spell out the parameters of computer searches where the warrant provides particularity as to what is being searched for.").

[163] 576 F.3d 1078, 1091 (10th Cir. 2009). The officer's affidavit stated that "Based upon training and experience, your Affiant [Schmitt] knows that persons involved in trafficking or the use of narcotics often keep photographs of coconspirators or photographs of illegal narcotics in their vehicle." The judge and appeals court accepted this seemingly questionable statement in the abstract and without any indication of why it would be true in this particular case.

[164] *Id*. at 1092.

> expect a warrant to search filing cabinets for evidence of drug activity to prospectively restrict the search to "file cabinets in the basement" or to file folders labeled "Meth Lab" or "Customers." And there is no reason to so limit computer searches.[165]

Some pre-*Riley* cases imposed search protocols,[166] yet for the most part courts have been very wary. As Part IV.B explains however, that dynamic is slowly changing in post-*Riley* cell phone cases.

B. Ex Ante Search Protocols After *Riley*

Since *Riley*, most courts have continued to reject the idea that search protocols are required. For instance, in a 2015 case in San Diego, the suspect contended that a search warrant for his cell phone failed the particularity requirement and was overbroad because it "did not identify why a full-blown forensic search was justified, did not limit the search to newer data, did not provide a method for segregating unreviewable data, [and] did not provide specific guidance on how to determine which data had a nexus to the crime."[167] The federal court rejected this claim however because "[a]lthough it may have been better if the warrant had included a search protocol that minimized unnecessary intrusion into Defendant's personal data," precedent did not require such protocols.[168] Other post-*Riley* courts have reached the same conclusion and refused to require search protocols.[169]

There are exceptions however, and the number of cases allowing such protocols is growing. The strongest voice for search protocols has been magistrate Judge David Waxse of the United States District Court for the District of Kansas. In a series of recent opinions,[170] Judge Waxse has denied

---

[165] *Id*. at 1093-94.

[166] The most high profile decision was the Ninth Circuit's initial en banc decision in United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989 (9th Cir. 2009) (en banc). For an overview of the complicated procedural history and the main decisions in *Comprehensive Drug Testing*, see Thomas J. Plumridge, Note, *The Fourth Amendment in a Digital World Decoding United States v. Comprehensive Drug Testing, Inc*., 29 QUINNIPIAC L. REV. 197 (2011).

[167] United States v. Garcia-Alvarez, No. 14-cr-0621, JM, 2015 WL 777411 (S.D. Cal. Feb. 24, 2015), at *4.

[168] *Id*. at *5.

[169] *See, e.g*., United States v. Gatson, No. 13-705, 2014 WL 7182275 (D.N.J. Dec. 16, 2014), at *21; United States v. Jefferson, No. 14-20119, 2015 WL 3576035 (E.D. Mich. June 5, 2015), at *6.

[170] For an extremely thorough overview of the search protocol rulings by Judge Waxse and another prominent federal judge, see William Clark, Note, *Protecting the Privacies of Life: Riley v. California, the Fourth Amendment's Particularity*

federal agents' requests for cell phone search warrants because the agents either did not provide a search protocol[171] or provided one that was insufficiently general.[172]

In the most prominent decision – *In Re the Matter of Cellular Telephones Within Evidence Facility Drug Enforcement Administration* – Judge Waxse declined to grant the DEA a search warrant for "names, addresses, telephone numbers, text messages, digital images, video depictions, or other identification data" on a group of cell phones.[173] Stressing the Court's language in *Riley*, Judge Waxse focused on how digital searches are different than those in the tangible world because of the sheer amount of data held on electronic devices. He maintained that requiring the government to submit a search protocol is "squarely aimed at satisfying the particularity requirement of the Fourth Amendment."[174] A search protocol, in Judge Waxse's view, "helps the court to determine if the proposed warrant satisfies the requirements of the Fourth Amendment" by ensuring that the warrant imposes sufficient "boundaries and limits."[175] The protocol balances "an individual's right to privacy and the government's ability to efficiently and effectively investigate crimes."[176] Judge Waxse recognized that ordinarily judges evaluate the execution of warrants after the fact, rather than imposing restrictions ex ante. Nevertheless, he argued that neither the text of the Constitution nor prior Supreme Court precedent "precludes a magistrate from imposing ex ante warrant conditions to further constitutional objectives such as particularity in a warrant."[177]

Although Judge Waxse has been the most vocal proponent of search protocols, a number of other courts have also demanded that law enforcement submit proposed search protocols in computer and cell phone cases. In the Ninth Circuit, the protocol cases stem from the appellate court's well-known decision in *United States v. Comprehensive Drug Testing, Inc*., which involved a search of computer files for evidence of steroid use in major league baseball.[178] In an early iteration of the case, the Ninth Circuit

---

Requirement and Search Protocols for Cell Phone Search Warrants, 57 B.C. L. REV. ___ (forthcoming 2016) (on file with the author).

[171] *See* In re Search of Three Cellphones and One Micro-SD Card, No. 14-MJ-8013-DJW, 2014 WL 3845157 (D. Kan. Aug. 4, 2014).

[172] *See* In Re Search of Nextel Cellular Telephone, No. 14-MJ-8005-DJW, 2014 WL 2898262 (D. Kan. June 26, 2014).

[173] No. 14-MJ-8017-DJW, 2014 WL 7793690 (D. Kan. Dec. 30, 2014), at *1.

[174] *Id*. at *8 (citations omitted).

[175] *Id*. at *7.

[176] *Id*. at *8.

[177] *Id*. at *6.

[178] 621 F.3d 1162 (9th Cir. 2010) (en banc).

majority imposed search protocols for the execution of computer warrants.[179] However, about a year later the opinion was withdrawn and replaced with a new opinion. This time, the search protocols were not in the majority opinion but instead were relegated to "guidance" in Chief Judge Kozinski's concurring opinion.[180] Subsequent Ninth Circuit precedent has continued to recognize the utility of search protocols. The court has recommended that "judges may consider such protocols or a variation on those protocols as appropriate in electronic searches" – but the court has declined to mandate them.[181]

Ninth Circuit precedent clearly seems to make search protocols optional. Yet, at least one magistrate in a post-*Riley* cell phone case has relied on the circuit court's *Comprehensive Drug Testing* opinion to require a search protocol before issuing a search warrant.[182] After explaining the *Comprehensive Drug Testing* opinion and the importance of the Fourth Amendment's particularity requirement, Magistrate Judge Peggy Leen stated that:

> The court will not approve a search warrant for electronically stored information that does not contain an appropriate protocol delineating what procedures will be followed to address these Fourth Amendment issues. A protocol for forensic review of a device that stores data electronically must make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, or other electronically stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged, or confidential files to the extent reasonably practicable.[183]

A federal magistrate in Washington, D.C. took a nearly identical position only a few months before the *Riley* decision. Judge John Facciola demanded a search protocol before issuing a warrant to search multiple electronic devices, including a cell phone.[184] When the government

---

[179] *See* United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989, 1006 (9th Cir. 2009) (en banc).
[180] United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162 (9th Cir. 2010) (en banc); *id*. at 1179-80 (Kozinski, C.J. concurring).
[181] United States v. Schesso, 730 F.3d 1040, 1050 (9th Cir. 2013).
[182] *See* United States v. Phua, No. 2:14-cr-00249-APG-PAL, 2015 WL 1281603 (D. Nev. Mar. 20, 2015).
[183] *Id*. at *7.
[184] In the Matter of Search of ODYS LOOX Plus Tablet Serial Number 4707213703415, 28 F. Supp. 3d 40 (D.D.C. 2014).

responded with an affidavit indicating simply that a computer forensic specialist would image the files and search them, Judge Facciola again denied the warrant. He explained that "[n]o sophisticated search should occur without a detailed explanation of the methods that will be used, even if the explanation is a technical one, and no search protocol will be deemed adequate without such an explanation."[185]

Unlike many judicial officers, Judge Facciola showed no fear of understanding complicated electronic search methodology. In denying a search warrant in a subsequent opinion he noted that the "government should not be afraid to use terms like 'MD5 hash values,' 'metadata,' 'registry,' 'write blocking' and 'status marker,' nor should it shy away from explaining what kinds of third party software are used and how they are used to search for particular data."[186] Judge Facciola was clear that he was "*not* dictating that particular terms or search methods should be used" but rather that the government must offer its own search methodology in detail so that the court can "conclude that the government is making a genuine effort to limit itself to a particularized search."[187]

The Vermont Supreme Court – although not delving into the same level of technological sophistication as Judge Facciola – went further in a computer search warrant case and upheld search protocols established by the court itself. In the case, police detectives requested a warrant to search an address and seize any evidence, including "any computers or other electronic medium" for evidence of identity theft.[188] A judge granted the warrant but imposed ten conditions, including that the government forego use of the plain view doctrine, that different officers search the computer files than those handling the case, that the executing officers forego use of hashing tools without specific authorization, and limiting the search protocol to methods designed to uncover only information for which the government had probable cause.[189] The State maintained that the judge lacked the authority to impose such ex ante limitations on how law enforcement will conduct its search, and it requested that the Vermont Supreme Court strike them from the warrant.[190] Although the Vermont Supreme Court did strike the clause forbidding officers from relying on the plain view doctrine,[191] it otherwise

---

[185] *Id*. at 46.

[186] In the Matter of Search of Apple iPhone, IMEI 013888003738427, 31 F. Supp. 3d 159, 168 (D. D.C. 2014).

[187] *Id*.

[188] In re Application for Search Warrant, 71 A.3d 1158, 1161 (Vt. 2012).

[189] *See id*. at 1162-63.

[190] *See id*. at 1163-65.

[191] In an effort to limit the privacy intrusion on electronic data, some academic commentators have suggested eliminating prosecutors' ability to rely on the plain view doctrine in digital searches. *See* Eric Yeager, Note, *Looking for Trouble: An Exploration of How To Regulate Digital Searches*, 66 VAND. L. REV. 685 (2013)

completely rejected the State's challenge to ex ante search protocols.[192] The Court held that, in the abstract, an ex ante search protocol is acceptable as a way to ensure the Fourth Amendment's particularity guarantee.[193] The court drew analogies to the minimization requirement in wiretapping cases and limits on body cavity searches, and found that ex ante restrictions could not be categorically prohibited.[194] Indeed, even the dissenting justices (who objected to certain of the protocols as going too far) began their opinion by noting that "[n]othing in the Fourth Amendment precludes a magistrate from imposing ex ante warrant conditions to further constitutional objectives such as particularity in a warrant."[195]

In sum, while most courts have declined to impose *ex ante* search protocols, a small number of courts have turned to protocols to enforce the Fourth Amendment's particularity requirement. The number of cases seems to be growing (albeit slowly) since the *Riley* decision.

C. Objections to Using Search Protocols as a Solution

There are a few objections to relying on search protocols to cabin search warrants for cell phones. First, ex ante regulations on cell phone searches would be a different approach than courts take with tangible evidence. The Supreme Court has been very reluctant to impose ex ante limits on the execution of warrants for physical evidence and, as noted above, most lower courts have declined to alter that approach for computer searches. Second, and related, there is an argument that magistrates lack

---

(suggesting eliminating the doctrine for digital searches); 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) (arguing that plain view doctrine should be limited to cases in which the evidence was reasonably related to what was originally sought by law enforcement). Recently, Professor Kerr has advocated a modified approach to banning the plain view doctrine. *See* Kerr, *Executing Warrants for Digital Evidence*, *supra* note 70. Unfortunately, while limiting or abolishing the plain view doctrine for digital searches may result in suppression of evidence, it does not solve the root problem of privacy invasion. Millions of cell phones likely contain private but non-incriminating data – naked photographs or sexually explicit personal videos are the most graphic examples -- that individuals would like to prevent government actors from observing. Limiting the plain view doctrine does nothing to the government from viewing this data. Restricting the plain view doctrine does not prevent privacy invasion; it only prevents data from being admitted into evidence.

[192] *See* In re Search Warrant, 71 A.3d at 1170 ("We conclude that ex ante instructions are sometimes acceptable mechanisms for ensuring the particularity of a search.").

[193] *See id*.

[194] *See id*. at 1170-71.

[195] *See id*. at 1186 (Burgess, J., concurring and dissenting).

constitutional authority to impose protocols. Third, relying on ex ante protocols would stunt the growth of reasonableness doctrine because courts would not be called on to flesh out in judicial decisions, after the fact, whether cell phone warrants were executed properly. Fourth, and perhaps most importantly, imposing search protocols on cell phones would be quite complicated and beyond the expertise of most judges.

The first three objections to search protocols can be dispensed with fairly easily. The fourth objection – judicial competence – is more compelling but ultimately should fail as well. I take the four objections in turn.

First, while it is true that ex ante restrictions on search warrants have been rare in the universe of tangible searches, we are not operating in the tangible world for cell phone searches. The Court's decision in *Riley* signaled that electronic searches are different and that courts must occasionally apply different doctrinal approaches to electronic equipment.[196] (If it were otherwise, the Supreme Court would not have forbidden warrantless searches incident to arrest of cell phones in *Riley*.)

Second, and relatedly, while Professor Orin Kerr has argued that magistrates lack constitutional authority to impose ex ante search protocols, his argument (unlike his other excellent work in this area) is not compelling. Professor Kerr maintains that four Supreme Court decisions – *LoJi Sales v. New York*, *Dalia v. United States*, *United States v. Grubbs*, and *Richards v. Wisconsin* tie together to foreclose ex ante search protocols.[197] Yet, as Professor Paul Ohm noted in response to Professor Kerr, none of those cases directly addresses magistrates' authority to impose ex ante conditions on electronic searches.[198]

The *LoJi* case involved a magistrate who actually sat at the scene of a physical evidence search nearly forty years ago and was considerably more involved in execution of the warrant than simply specifying some execution instructions on a piece of paper.[199] In *Dalia*, the Court dealt only with whether a restriction on executing a physical evidence warrant was required, not whether it was permitted.[200] The *Richards* decision – about the knock and announce rule – implicated the reasonableness clause, not the particularity requirement that would be at issue in search protocols.[201] Finally, the *Grubbs*

---

[196] Professor Kerr has recently suggested that there will be "*Riley* moments" in which the Supreme Court will have to recognize that "the facts of computer searches differ so greatly from the facts of physical searches that new rules are required." Kerr, *Executing Warrants for Digital Evidence*, *supra* note 70 at 12. The rules governing search warrants could be such a moment.

[197] *See* Kerr, *Ex Ante Regulation*, *supra* note 28 at 1261-71.

[198] *See* Ohm, *supra* note 29, at *2-4.

[199] 442 U.S. 319 (1979).

[200] 441 U.S. 238 (1979).

[201] 520 U.S. 385 (1997).

case involved an anticipatory search warrant for a tangible package (video tapes of child pornography), not an electronic device.[202] And while *Grubbs* does contain some language about the particularity requirement, the case really only concerned whether the police should have left a copy of the affidavit with persons present at the location of the search.[203] As Professor Ohm concisely explained, *Grubbs* is a "short, terse decision which we should try to avoid reading too much into."[204] In short, while it is possible that the Court may one day squarely address judicial authority to impose search protocols, at present there does not appear to be any kind of precedent that would foreclose them. Thus, there seems little evidence for claiming ex ante search protocols are unconstitutional.

The third objection to search protocols is that ex ante restrictions on the execution of search warrants would stifle the natural development of common law reasonableness doctrine in computer cases. Professor Kerr argued in 2010 that "ex ante restrictions impair the ability of appellate courts and the Supreme Court to develop the law of unreasonable searches and seizures in the usual case-by-case fashion."[205] But it is not clear why this should be so. Search protocols will not stop law enforcement from executing warrants and finding evidence. In the face of incriminating evidence, defendants will question whether forensic examiners complied with those search protocols. These suppression motions will result in written district court opinions and those decisions will be appealed to state and federal appellate courts. As such, a body of law will surely develop.

Additionally, even if it is apparent that the law enforcement complied with the protocols, that will simply incentivize defendants to argue that the Fourth Amendment's probable cause, particularity, and reasonableness provisions guarantee *more* protection than the ex ante search protocols provided. Thus, appellate courts will still be called on to assess the reasonableness of law enforcement's execution of electronic searches.[206]

The final objection to search protocols – that judges simply are not equipped to impose them – is the most persuasive. Every cell phone search will seek slightly different evidence. And there are many different types of

---

[202] 547 U.S. 90 (2006).
[203] *See id*. at 94.
[204] Ohm, *supra* note 29, at 9.
[205] Kerr, *Ex Ante Regulation*, *supra* note 28, at 1278.
[206] By way of comparison, a few magistrate judges have rejected the government's proposed search protocols because they were insufficiently detailed. *See* In the Matter of Search of Apple iPhone, IMEI 013888003738427, 31 F. Supp. 3d 159, 168 (D. D.C. 2014); In Re Search of Nextel Cellular Telephone, No. 14-MJ-8005-DJW, 2014 WL 2898262 (D. Kan. June 26, 2014). Appellate courts could just as easily find the search protocols imposed by lower court judges to be inadequate.

cell phones.[207] At the same time, judges are not the most technically savvy group.[208] As one court has noted, computer searches "can be as much an art as a science."[209] Preordaining in advance the exact steps that forensic examiners will have to take is a tall order and one that may end badly. As Professor Kerr has explained:

> Judges are smart people, but they do not have crystal balls that let them predict the number and type of computers a suspect may have, the law enforcement priority of the particular case, the forensic expertise and toolkit of the examiner who will work on that case, whether the suspect has tried to hide evidence, and if so, how well, and what evidence or contraband the seized computers may contain.[210]

All of this is true, of course, yet Professor Kerr's concerns – first articulated a decade ago – seem less significant with each passing year.

First, some judges – like Judge Facciola – appear quite technologically savvy and capable of dealing with sophisticated search protocols.[211] Moreover, even if judges do lack technological sophistication, many will have young law clerks who do possess that knowledge.[212]

Second, judges who lack the necessary knowledge can simply require that law enforcement officers and prosecutors submit proposed search protocols.[213] For instance, Judge David Waxse has required federal agents to submit proposed protocols in multiple cases.[214] The Justice Department is fully capable of proposing such

---

[207] *See* Andrew Cunningham, *The State of Smartphones in 2014: Ars Technica's Ultimate Guide*, ARS TECHNICA, Dec. 21, 2014, available at http://arstechnica.com/gadgets/2014/12/the-state-of-smartphones-in-2014-ars-technicas-ultimate-guide/ (describing two dozen of the leading phones).

[208] *See* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 575 (2005) ("[M]agistrate judges are poorly equipped to evaluate whether a particular search protocol is the fastest and most targeted way of locating evidence stored on a hard drive.").

[209] United States v. Brooks, 427 F.3d 1246, 1252 (10th Cir. 2005).

[210] Kerr, *Ex Ante Regulation*, *supra* note 28, at 1282.

[211] *See supra* notes 184-87 and accompanying text.

[212] *See* Albert Yoon, *Law Clerks and the Institutional Design of the Federal Judiciary*, 98 MARQ. L. REV. 131, 138 (2014) (discussing data indicating that more than 70% of federal law clerks are under the age of 30).

[213] Lawyers, of course, regularly draft documents from warrants to discovery orders that they ask judges to sign.

[214] *See supra* notes 172 and accompanying text.

protocols. As Professor Ohm explained, "[t]he FBI and other law enforcement agencies are resourceful organizations full of industrious, creative, intelligent, and hard-working agents, who are dedicated to finding evidence of crime."[215] Experts in the Department of Justice will surely identify a series of standard practices for cell phone searches to satisfy magistrates like Judge Waxse who request protocol submissions. And while it may be harder for state judges and local law enforcement agencies to identify the proper search protocols, they can simply piggyback off of federal efforts. By point of comparison, the Justice Department produces an invaluable manual -- *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* – that keeps readers updated on digital issues in Fourth Amendment law. Just as the Justice Department shares this manual with the public, it could also share its cell phone search protocols with state and local law enforcement agencies.

Third, and following directly from the first two points above, judges are in the business of learning about new and complicated matters. Setting aside polyglots like Judge Richard Posner, few judges are experts on everything from CERCLA to tax law to regulatory takings. Yet, they do not simply turn away cases because they have little background in certain doctrinal areas. If judges can learn complicated legal doctrine on the job, they can learn how to impose search protocols.

Indeed, trial judges in civil cases are already regularly confronted with the same type of complicated questions about electronic evidence that arise in criminal cases. For instance, before federal magistrate Judge John Facciola decided that search protocols were necessary for a cell phone search warrant in 2014,[216] he addressed the very same issue in a civil discovery dispute in 2008.[217] Not surprisingly, over the last few decades, electronic discovery in civil cases has exploded.[218] Large litigations often involve Fortune 500 companies with massive databases and an incredible array of electronic records.[219] When trial judges enter pre-trial discovery

---

[215] *Ohm*, supra note 29, at *12.

[216] *See supra* notes 184-87 and accompanying text.

[217] *See* Equity Analytics, LLC v. Lundin, 248 F.R.D. 331 (D.D.C. 2008)

[218] *See* George L. Paul & Jason R. Baron, *Information Inflation: Can the Legal System Adapt?* 13 RICH. J.L. & TECH. 10 (2007).

[219] *See* Nicholas Barry, Note, *Man Versus Machine Review: The Showdown Between Hordes of Discovery Lawyers and a Computer-Utilizing Predictive Coding Technology*, 15 VAND. J. ENT. & TECH. L. 343, 348 (2013) (noting that "e-discovery has grown exponentially and now includes, inter alia, emails, word-processing files, spreadsheets, databases, video files, MP3 files, and virtually every other file now

orders they certainly confront the question of what types of data and documents will have to be disclosed during the discovery process. The judges do not simply throw up their hands and say it is impossible to separate responsive information from that which is irrelevant and non-discoverable.[220] To the contrary, the Federal Rules of Civil Procedure specifically call on judges to rule on motions to compel the production of electronically stored information that parties have failed to produce.[221] Put simply, judges in civil cases do not order enormous companies such as Microsoft or Pfizer to turn over all of their electronic files and tell them that all discovery disputes will be worked out ex post. Rather, based on information from the parties, trial judges decide many discovery matters – such as motions to compel[222] and wide-ranging discovery plans[223] -- early in the case. The comparison to ex ante search protocols under the Fourth Amendment is therefore quite apt.

Fourth, to the extent that a judge initially imposes a search protocol that is too narrow,[224] law enforcement officers are free to

---

stored on computers and other electronic devices (such as PDAs, cell phones, flash drives, DVDs, etc.").

[220] Indeed, the 2006 e-discovery amendments to the Federal Rules of Civil Procedure specifically required judges to engage with electronically stored information during the discovery process. *See* Rachel K. Alexander, *E-Discovery Practice, Theory, and Precedent: Finding the Right Pond, Lure, and Lines Without Going on a Fishing Expedition*, 56 S.D. L. REV. 25, 30 (2011).

[221] *See* Jason Fliegel & Robert Entwisle, *Electronic Discovery in Large Organizations*, 15 RICH. J.L. & TECH. 7, *7 (2009) ("The non-producing party may move to compel production of information from sources designated as "not reasonably accessible," and if it does so, "the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C).").

[222] *See, e.g.*, Victor Stanley, Inc. v. Creative Pipe, Inc. 250 F.R.D. 251 (D. Md. 2008) (deciding motion to compel electronically stored documents).

[223] *See* Millberg Hausfeld, *E-Discovery Today: The Fault Lies Not in Our Rules*, 4 FED. CTS. L. REV. 131, 157 (2011) ("A survey of recent cases illustrates the myriad of approaches available to judges under the current Rules to control the scope of e-discovery while permitting the parties to obtain relevant evidence. Courts can parse and, if necessary, alter e-discovery requests to strike a fair balance.").

[224] To be sure, some search protocols can be too restrictive. As one expert explained "[c]locks can be wrong, dates can be changed, filenames intentionally misnamed. Keyword searches are an important tool, but they are imperfect." Josh Goldfoot, *The Physical Container and the Fourth Amendment*, 16 BERKELEY J. CRIM. L. 112, 138 (2011); *see also* United States v. Burgess, 576 F.3d 1078, 1093 (10th Cir. 2009) ("[I]llegal activity may not be advertised even in the privacy of one's personal computer—it could well be coded or otherwise disguised.").

return to the judge to request a revised warrant or protocol.[225] Because law enforcement is free to seize cell phones under the *Riley* decision, they will already have the phone in their possession. Accordingly, time is not of the essence. Indeed, law enforcement officers are already taking weeks or even months to execute cell phone search warrants.[226] It simply will not be burdensome if officers occasionally have to return to magistrates to ask them to alter the search protocol.[227]

Fifth and related, to the extent magistrates or district judges impose unduly restrictive protocols and later refuse to alter them, prosecutors can turn to higher level courts for search warrants.[228] Double jeopardy, of course, does not prevent prosecutors from approaching another judge after a search warrant was denied because jeopardy will not have attached.[229]

Over three years ago, one writer observed that "the widespread use of search-protocol restrictions is inevitable."[230] Since then, magistrates have increasingly considered the wisdom of search protocols and the Department of Justice has begun submitting protocols in response to magistrate demands. While Professor Kerr is correct to note that magistrates may not be tech savvy,[231] it is also true that the more people engage in challenging tasks the better they

---

[225] *See* Athul K. Acharya, Note, *Semantic Searches*, 63 DUKE L.J. 393, 425 (2013) (noting that officers are always free to seek a second warrant).

[226] *See* United States v. Phua, Nos. 2:14-cr-00249APG-PAL, 2015 WL 1281603 (D. Nev. Mar. 20, 2015), at *2 (explaining that officials needed assistance from Apple to extract data from cell phones and that "Apple advised it would take approximately nine months to extract data from the devices").

[227] Additionally, although this is nothing to applaud, in large jurisdictions law enforcement officers can simply go magistrate shopping. If a judge imposes flawed, overly restrictive protocols, the officers will stop approaching that judge and will turn to another judge. *See* Abraham S. Goldstein, *The Search Warrant, the Magistrate, and Judicial Review*, 62 N.Y.U. L. REV. 1173, 1183 (1987) (explaining that "the police often engaged in 'magistrate shopping' for judges who would give only minimal scrutiny to the application").

[228] *See, e.g.*, Tex. Code Crim. Pro. 18.01 (explaining that a search warrant can be issued by not only municipal, county, and district judges but also by "a judge of the Court of Criminal Appeals, including the presiding judge [or] a justice of the Supreme Court of Texas, including the chief justice").

[229] Jeopardy attaches much later: in jury trials, when the jury is sworn; in bench trials when the first witness is sworn. *See* WAYNE R. LAFAVE ET AL., CRIMINAL PROCEDURE 25.1(d) (5th ed. 2009).

[230] 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, 329 (2012).

[231] *See supra* notes 207-10 and accompanying text.

become at them. Some federal magistrates sign dozens of cell phone and computer search warrants.[232] Over time, electronic search protocols may become as routine for these magistrates as dealing with complicated areas of tax, administrative, and bankruptcy law.

D. Search Protocols Limit Overuse of the Good Faith Exception

In addition to protecting privacy, a key attribute of ex ante search protocols is that they would limit prosecutors' use of the good faith exception. At present, when officers have a search warrant for digital evidence it is all too easy for them to turn to the good faith exception to save an otherwise unreasonable search.

In the absence of search protocols, police typically receive no guidance on how to execute search warrants. Following execution, the defendant might move to suppress on the grounds that the search proceeded too far and was thus unreasonable. The prosecutor would then argue that even if the search was improper, the police were relying on a valid search warrant and because electronic searching is complicated, they executed the warrant in good faith.

Of course, in the world of physical evidence, prosecutors often successfully invoke the good faith exception to overcome police error and admit unlawfully seized evidence.[233] Yet, there are limits in the physical world. It would be quite hard indeed for prosecutors to convince a court that officers acted in good faith when they opened a microwave while executing a warrant for a stolen fifty-inch television.[234]

By contrast, it is quite plausible for the government to invoke the good faith exception in digital searches when police open the wrong file or application. As noted above, courts have regularly applied the good faith exception to save invalid cell phone search warrants for digital evidence.[235]

Moreover the good faith exception is particularly troublesome when applied to cell phones as opposed to traditional computers. Officers who suspect a cell phone contains incriminating evidence do not always download the contents of the phone and conduct a forensic analysis in a laboratory. Sometimes, the officers simply search the phone manually. In doing so, an officer might accidentally tap the wrong icon, open the wrong

---

[232] I am grateful to federal magistrate Judge Tommy Miller for this point.

[233] Indeed, courts sometimes "duck" underlying substantive Fourth Amendment inquiries by simply turning to the good faith exception first. *See* Zack Bray, Comment, *Appellate Review and the Exclusionary Rule*, 113 Yale L.J. 1143, 1144 (2004).

[234] *See, e.g.*, Miles v. State, 742 P.2d 1150, 1151-52 (Okla. Crim. App. 1987) (finding it "patently unreasonable" for police to search envelopes, medicine bottles, and other small containers while executing a warrant for a 9 millimeter handgun).

[235] *See supra* Parts III.A.2 and III.B.2.

application, and come across an incriminating photo or text message. Worse yet, officers could simply lie and falsely say that they "accidentally" tapped the wrong icon and stumbled upon incriminating evidence. By contrast, it is very hard for police to plausibly say that they accidentally opened a microwave when looking for a fifty-inch television.

Ex ante search protocols would make it much harder for prosecutors to rely on the good faith exception.[236] If a magistrate judge specifies in advance that certain forensic tools are off limits or certain types of data or files cannot be searched, it will take prosecutors a considerable amount of gymnastics to convince a judge that law enforcement should be excused from doing what was flatly prohibited by the warrant.

V. Re-Framing the Inquiry in "Simple" Cell Phone Cases: Limitations on *Where*, as Opposed to *How*, to Search

While search protocols can be beneficial when officers are downloading and forensically analyzing the contents of a cell phone, not all cases are so complicated. In some simple cases, police only need to conduct a straightforward manual search of the cell phone for a particular piece of evidence. For instance, police might be looking for a particular video that had just been filmed on the street or they might be searching for an incriminating text message that a drug dealer had just sent to an informant. These cases do not require a full forensic analysis of the phone.[237] To offer a medical analogy, not all chest pain has to be treated by open-heart surgery. If an angioplasty will clear a heart blockage, doctors do not need to perform a quadruple bypass operation. In simple cases, police only need to manually search the phones. Magistrates can therefore restrict search warrants by simply dictating which applications on the phone police can manually look through. Ex ante specification of *where* on the phone the police can search, rather than *how* the officers must execute the search, would be a simple and effective way to protect privacy while allowing law enforcement to conduct a legitimate investigation.

This Part explains how criminals often use cell phones for different and simpler types of street crimes than they commit with traditional computers. Although there are certainly exceptions, criminals often turn to traditional computers for child pornography and financial misconduct offenses, while using cell phones for drug dealing and other street-level

---

[236] As one commentator explained, "[o]f all the ways in which courts might attempt to limit the scope of digital searches, ex ante regulations that prescribe particular search protocols are likely to be the clearest and most enforceable options." Yeager, *supra* note 191 at 711.

[237] *See* EDENS, *supra* note 83, at 163 (noting the possibility of manual or "fat fingered" investigation of cell phone contents).

offenses. Because evidence of certain street crimes is less likely to be hidden or mislabeled on cell phones, Part V.B below argues that it is appropriate for judges in some instances to limit cell phone warrants to particular applications on the phones.

A. Although Cell Phones Are Mini-Computers, They Are Often Used To Commit Different and Simpler Types of Offenses Than Crimes Committed With Traditional Computers

In *Riley*, the Supreme Court forbid warrantless cell phone searches because modern smart phones are like mini-computers. As Chief Justice Roberts explained:

> The term "cell phone" is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.[238]

This, of course, is true. A smart phone can do most of the complex tasks that computers do. The Court's instinct to think of cell phones and computers synonymously therefore makes sense.[239]

Yet, when it comes to searching for evidence, there are reasons to think of computers and cell phones slightly differently. To over-generalize somewhat, it is more common to see traditional computers involved in child pornography and financial misconduct cases – crimes where it is easy for suspects to mislabel files or bury evidence deep in the confines of the computer.[240] The obvious reason for this is that criminals are more likely to commit these crimes at home behind closed doors and to use a larger screen to do so.

By contrast, drug dealers are much more likely to transact business with cell phones than traditional computers. Drug distribution is typically a street crime and drug dealers utilize the mobility of phones and the instant

---

[238] *Riley*, 134 S. Ct. at 2489.

[239] Indeed, commentators have begun calling for courts to extend the *Riley* cell phone decision to other devices. *See* Tristan M. Ellis, Note, *Reading Riley Broadly: A Call for a Clear Rule Excluding All Warrantless Searches of Mobile Digital Devices Incident to Arrest*, 80 BROOKLYN L. REV. 463 (2015).

[240] *See, e.g.*, United States v. Fumo, 565 F. Supp.2d 638 (E.D. Pa. 2008) (noting in fraud case that "because of the nature of computer files, the government may legally open and briefly examine each file when searching a computer pursuant to a valid warrant" because "few people keep documents of their criminal transactions in a folder marked crime records").

communication of text messages to arrange sales of their products.[241] There are many reported decisions in which law enforcement officials convinced courts that cell phones are recognized tools of the drug trade.[242] Indeed, prior to *Riley*, the Drug Enforcement Administration specifically trained its agents to search cell phones incident to arrest without a warrant.[243] Conversely, it is practically impossible to find courts claiming that traditional computers are used for drug transactions.[244]

Of course, it would be a vast overstatement to say that police only find evidence of drug dealing on cell phones and that child pornography and financial fraud are always located on computers.[245] But looking at the big picture, it is apparent that criminals tend to turn to different devices for different types of crimes.[246]

Why does this matter? In some cell phone cases the distinction between cell phones and traditional home computers matters because there is no reason to think the suspect hid evidence in an unusual location that would

---

[241] *See* EDENS, supra note 83, at 9 ("Some crimes inherently require using mobile communication devices. For example, it is almost impossible to be a successful narcotics dealer without using a mobile phone.").

[242] *See, e.g.*, United States v. Schesso, 730 F.3d 1040, 1046 (9th Cir. 2013) (rejecting overbreadth challenge in child pornography case because the "government had no way of knowing which or how many illicit files there might be or where they might be stored"); United States v. Farlow, 681 F.3d 15 (1st Cir. 2012) (explaining in child pornography case that "computer files are highly manipulable. A file can be mislabeled; its extension . . . can be changed; it can actually be converted to a different filetype . . ."); United States v. Fisher, No. RDB-14-413, 2015 WL 1862329 (D. Md. Apr. 22, 2015), at *2 (quoting a narcotics task force agent testifying that "through his law enforcement training, knowledge, and experience with the drug trade, drug traffickers often communicate about their business through cell phones").

[243] *See, e.g.*, United States v. Wall, No. 08-60016-CR, 2008 WL 5381412 (S.D. Fla. Dec. 22, 2008), at *3 (discussing cell phone searches and citing DEA agent that "it is standard practice of the DEA and is authorized by the DEA Legal Department").

[244] A Westlaw search for "cell phone /10 drug /10 tool" yields dozens of cases explaining that cell phones are used by drug dealers to conduct business. A search of "computer /10 drug /10 tool" yields no such cases however.

[245] There are obviously exceptions to the general trend. *See, e.g.*, United States v. Bass, No. 14-1387, 2015 WL 1727290 (6th Cir. Apr. 15, 2015) (upholding cell phone warrant for financial fraud); In re XXX, Inc., No. 14 Mag. 2258, 2014 WL 5510865 (S.D.N.Y. Oct. 31, 2014) (describing warrant to search for credit card fraud evidence on cell phone); In the Matter of the Search of Black iPhone 4, 27 F. Supp.2d 74 (D. D.C. 2014) (rejecting search warrant for cell phones (and hard drives) to search for child pornography).

[246] Of course, if police have probable cause to believe a cell phone contains evidence of child pornography or financial crimes, it should be very easy for police to explain that to a magistrate and seek to have that cell phone warrant treated differently than the standard approach I outline below.

require sophisticated forensic analysis to uncover. For example, if the suspect arranged drug deals exclusively via text message with an undercover officer – a very common scenario[247] -- the police can find the evidence by having an officer manually scroll through text messages to identify incriminating information by sight. A complete download of the phone's contents and a subsequent detailed forensic analysis is simply unnecessary.

Or imagine that police were searching for a very specific video or photograph that was recently recorded on the street. For instance, in a post-*Riley* case, a suspect was using his cell phone to record a video when he was arrested.[248] The officers seized the phone and shut off the video recorder.[249] The video apparently contained incriminating information, but the suspect had no opportunity to hide it before the police seized the phone.[250] The officers therefore knew exactly what they were looking for and that it would be in the video library. The officers could therefore find the evidence by manually searching through the contents of the phone and then handing the device to a forensic examiner to download it. There would be no need to rummage through many gigabytes of the phone's data.

Put simply, the way that cell phones are used makes them different than traditional computers. Because many criminals – particularly in drug cases and other street crimes – leave evidence in places that are easy to access, the police can recover the data without completely downloading the phone's contents and reviewing millions of pages of data.

When magistrates know that officers could recover the evidence with less invasive searches, there would be no need to authorize a search of "any and all data" on the phone. Nor would there be a need for magistrates to trouble themselves with the search protocols discussed above in Part IV. Rather, in cases in which probable cause is limited to certain applications – for instance when undercover agents communicated with suspects exclusively by text message – magistrates should restrict searches in an easier way. As explained in Part V.B below, in this subset of cases, magistrates should simply restrict *where* the police can search (i.e. which applications), rather than trying to dictate *how* the search should be conducted.

B. Restricting *Where* on the Phone Police Can Search Cell Phones

As explained in Part IV, ex ante search protocols for electronic evidence are controversial because courts have rarely imposed restrictions on

---

[247] For examples, *see supra* note 30 and accompanying text.
[248] *See* People v. Watkins, 994 N.Y.S.2d 816 (N.Y. Supr. Ct. 2014).
[249] *See id.* at 817.
[250] *See id.*

how police are to execute warrants. But what if magistrates could narrow cell phone search warrants by specifying *where* police can search rather than *how* they should carry out the search. Courts have long relied on the Fourth Amendment's probable cause and particularity guarantees to specify where police can search for evidence. To use a simple example, when police have probable cause a suspect is selling drugs out of his car, the magistrate should issue a warrant for the suspect's vehicle, but not for his house or office.[251] The same approach could be applied to the different applications on a cell phone. If there is probable cause for incriminating text messages, but not for photos, videos, or any other data on the phone, then magistrates should limit the search warrant to the text messaging application, rather than the whole phone. We might think of this as a geographic restriction on cell phone searches.

Of course, a restriction on *where* police may search on a cell phone will not always be proper. In some types of cases, it is apparent that a suspect could have hidden evidence in unusual places on a cell phone.[252] In these cases, a full-scale forensic analysis of the phone may be necessary. For example, if police have probable cause that a cell phone contains child pornography, the incriminating files could be mislabeled and hidden anywhere. Police therefore should not be restricted to searching the iPhoto application. In these cases – what I would call "complicated" search cases -- magistrates should impose the search protocols described in Part IV above. Magistrates might set in place ex ante regulations on how files should be separated and filtered after being downloaded. But magistrates should not restrict the search warrant to particular applications on the phone.[253]

Yet, while many cell phone search warrants might involve "complicated" cases in which the evidence could be mislabeled and hidden, a substantial number of cases do not fall into that category. Rather, some cases are, for lack of a better word, "simple" searches. For instance, police may have set up drug deals simply by exchanging text messages with a suspect.

---

[251] Of course, a warrant can lawfully authorize the search of more than one location, but there must be adequate probable cause for each location. *See* WAYNE R. LAFAVE, SEARCH & SEIZURE: A TREATISE ON THE FOURTH AMENDMENT 4.5(c) (5th ed. 2012); People v. Russell, 360 N.E.2d 515 (Ill. App. 3d 1977) (assessing search warrant for person and car and finding probable cause for the former, but not the latter).

[252] Child pornography and financial misconduct cases are the obvious examples.

[253] For instance, in a post-*Riley* financial fraud case federal agents procured a warrant for "any records of communication, indicia of use, ownership, or possession, including electronic calendars, address books, e-mails, and chat logs." United States v. Bass, No. 14-1387, 2015 WL 1727290 (6th Cir. Apr. 15, 2015), at *4. The Sixth Circuit properly concluded that because financial documents could be hidden anywhere, a warrant authorizing a full search of a cell phone to look for a circumscribed list of data was not overbroad. *See id*.

Or law enforcement officers may know for a fact that a suspect just took an incriminating video or photograph with his phone. In these "simple" cases, the officers know the type of evidence they are looking for and they know which application will hold that evidence. A search warrant should therefore be issued *only* for that application – a specific location on the phone – rather than the entire phone. Restricting police to only selecting certain locations is a restriction on *where* the police can search, not a restriction on *how* they can execute a warrant.[254]

The approach I am suggesting – limiting search warrants to particular applications in "simple" cases – would be unique to cell phones. Because of the nature of traditional computer investigations, there are unlikely to be "simple" cases in which officers know that incriminating evidence is in a particular file folder. In a traditional computer, evidence could be buried anywhere. Thus, allowing police to make brief examination of *all* files on a computer when executing a warrant, as some courts do, makes sense and could be applied in all traditional computer searches.[255] Cell phones, however, are different. Because cell phones are mobile, and have unique applications such as text messaging for communications, there will be some "simple" cases in which magistrates can restrict *where* police may search. The proposal for limited search warrants in simple cell phone cases is thus extremely limited.

Even though the proposal is narrow, there is one obvious objection: if magistrates issue warrants restricting *where* police can search on the phone it is possible that those restrictions might be erroneous. For instance, undercover drug officers might have believed all incriminating evidence would be in the suspect's text messages, but they could be wrong. Perhaps the suspect was using a different application to send the messages. Or perhaps incriminating messages had been deleted and could only be recovered through a detailed forensic analysis of the phone.[256] In those instances, a search warrant restricting police to manually searching the text

---

[254] By way of analogy, think of a large university that has many buildings – a campus library, a biology lab, and a law school, to name just a few. If there were probable cause to believe a professor at the law school were engaged in drug dealing or securities fraud, a magistrate would never issue a warrant for "the university." It would simply make no sense that the law professor – who has likely never set foot in the biology building – would have left evidence in the biology department. Accordingly, the warrant -- at its broadest -- should be limited to the law school building.

[255] *See, e.g.*, DEPARTMENT OF JUSTICE, SEARCHING AND SEIZING COMPUTERS, *supra* note 159, at 88; United States v. Potts, 559 F. Supp. 2d 1162, 1175 (D. Kan. 2008) (approving investigators "opening or cursorily reviewing the first few 'pages' of such files in order to determine precise content").

[256] Unfortunately, once a text message is deleted it is sometimes impossible to retrieve it. *See* EDENS, *supra* note 83, at 160.

message application would fail to uncover the evidence for which the police have probable cause.

While true, this objection should not be of much concern however because no evidence will be lost and police can simply request a broader search warrant. Once police have seized a cell phone, they routinely disconnect it from the network – either by removing the battery, placing it in airplane mode, or storing it in a faraday bag[257] -- to prevent the destruction of evidence. Officers also have the ability to download the contents of the phone using a data extraction device[258] or to make a mirror copy of the phone's memory card.[259] A key prerequisite of the Supreme Court banning warrantless cell phone searches incident to arrest in *Riley* was that there was no risk of evidence being destroyed while police take the time to procure a warrant.[260] Thus, if the police execute a limited warrant – for example, only for text messages -- and do not find the incriminating evidence, the officers can simply return to the magistrate and ask for a broader search warrant. Because the police are in control of the cell phone, there is no chance evidence will be lost or destroyed in the meantime.[261] The only cost to the officers is the time it takes to return to the magistrate.[262]

There is nothing revolutionary about suggesting that officers return to the magistrate to request a broader search warrant. Some states have statutes setting forth rules for subsequent warrants.[263] And even in the absence of statutes, it is common for judges to issue second search warrants for the same location.[264] Subsequent warrants are already used with some

---

[257] For a discussion of these and other techniques, see id. at 143-47.

[258] *See* Gershowitz, *Seizing a Cell Phone Incident to Arrest*, *supra* note 9, at 606-07.

[259] *See* EDENS, *supra* note 83, at 169 ("Standard forensic process is to make an exact duplicate of the device to be examined and to use forensic tools to examine the copy, not the original.").

[260] *See Riley*, 134 S. Ct. at 2487 ("Remote wiping can be fully prevented by disconnecting a phone from the network.").

[261] This, of course, is very different than a case involving a home, office, or other tangible location. In those cases, if police do not find the evidence under the first warrant they either have to station an officer at the location and prevent people from entering while awaiting a new warrant, see Illinois v. MacArthur, 531 U.S. 326 (2001), or risk evidence destruction while they are off the premises.

[262] Time is obviously not costless. But here the cost is offset by the added privacy protection to the suspect.

[263] *See, e.g.*, Tex. Code Crim. Proc. 18.01(d) ("A subsequent search warrant may be issued pursuant to Subdivision (10) of Article 18.02 of this code to search the same person, place, or thing subjected to a prior search under Subdivision (10) of Article 18.02 of this code only if the subsequent search warrant is issued by a judge of a district court, a court of appeals, the court of criminal appeals, or the supreme court.").

[264] *See, e.g.*, Marshall v. State, 614 S.E.2d 169 (Ga. 2005) (upholding a subsequent search warrant).

frequency in traditional computer searches. When officers execute a warrant for computer fraud or financial misconduct they sometimes come across evidence of child pornography.[265] If agents are following proper protocol, they immediately stop searching and apply for a second, broader warrant that authorizes a search for child pornography.[266]

There have already been cell phone search warrant decisions in which it would have been far preferable for magistrates to issue narrow search warrants restricting where on the phone investigators could search. For instance, in the post-*Riley* case of *State v. Moore*, police had probable cause to believe Moore had used his cell phone to take photographs as he perpetrated a sexual assault.[267] Police, however, convinced a magistrate to issue a search warrant for the entire contents of the phone.[268] A better approach would have been for the magistrate to issue a warrant for the photo application only. If that search failed to turn up the incriminating evidence, the officers could then have applied for a broader warrant requesting a complete forensic analysis of the phone.

An even better example is *United States v. Juarez*, which was decided the year before *Riley*.[269] In *Juarez*, police observed the suspect using his cell phone to videotape between the legs of women wearing dresses as they walked down the street.[270] The phone was still in recording mode when the police seized it.[271] Therefore the odds were extremely low that incriminating evidence of Juarez's crime would be located anywhere other than the phone's video application. Nevertheless, police convinced a magistrate to issue an extremely broad warrant for the entire contents of the cell phone.[272] A better approach would have been to issue a search warrant restricted only to the phone's video application. If that search failed to turn up the incriminating street video, the officers should have then returned to the magistrate and sought a broader warrant. And a magistrate properly assessing probable cause may very well have rejected the request for the

---

[265] *See, e.g.*, United States v. Loera, 59 F. Supp. 3d 1089 (D.N.M. 2014).
[266] *See, e.g.*, United States v. Wolfe, No. 00-5045, 2000 WL 1862667 (10th Cir. Dec. 20, 2000) (seeking second search warrant for child pornography after finding suspicious images during warranted search for counterfeiting); United States v. Gray, 78 F. Supp.2d 524 (E.D. Va. 1999) (approving second search warrant for child pornography after finding suspicious files during warranted search for computer hacking evidence); Rosa v. Commonwealth, 628 S.E.2d 92 (Va. Ct. App. 2006) (procuring second warrant for child pornography after finding suspicious files during warranted search for drug distribution).
[267] 160 So.2d 728 (Miss. Ct. App. 2015).
[268] *See id.* at 731.
[269] No. 12-CR-59 (RRM), 2013 WL 357570 (S.D.N.Y. Jan. 29, 2013).
[270] *See id.* at *1.
[271] *See id.*
[272] *See id.*

broader warrant. Depending on the officer's testimony, a judge might have concluded that Juarez lacked the time to hide the evidence elsewhere on the phone. And given that the police had no independent probable cause for the other functions on the cell phone – there was no suspicion, for instance, that his text messages or call history contained incriminating information -- a magistrate might properly conclude that the officers were mistaken in their belief that Juarez was improperly videotaping women.

* * *

While cell phones are mini-computers, in some "simple" search cases – particularly when police are searching for drug communications or other street crimes -- it makes sense to treat cell phones differently than traditional computers. In these cases, search warrants should initially authorize law enforcement officers to conduct only a manual analysis of the particular applications the police have probable cause to search. In these straightforward cases where evidence is unlikely to be hidden in unusual places, magistrates should not authorize a complete download and forensic analysis of millions of pages of data. If the initial manual search turns up empty, officers would be free to return to the magistrate and apply for a broader warrant.

CONCLUSION

While the Supreme Court's decision in *Riley v. California* was a strong step toward protecting digital privacy, it was incomplete. In the year since *Riley*, it has become apparent that the "simple" solution of "get a warrant" is far more complicated than the Court realized. Lower courts have issued search warrants for "any and all data" on the cell phone when far narrower warrants would have sufficed. Just as magistrates should not authorize police to search in a microwave to look for a fifty-inch television, nor should they authorize police to download and comb through millions of pages of data that is unrelated to the crime being investigated. For the *Riley* decision to be effective, the Fourth Amendment's particularity guarantee must apply with equal force to cell phone searches as it does to searches of physical spaces. In complex cases – those where incriminating evidence could be buried among millions of pages of data – magistrates should turn to ex ante search protocols to minimize officers' review of lawful data that should remain private. And in simple cases – those where police know that evidence will be found on a particular application, such as text messages – magistrates should restrict a search warrant to that particular application and only allow more expansive searches if the officers return to the judge and make a convincing case for a subsequent warrant. As the amount of data held on cell phones continues to grow, the need for nuanced search warrants will

become even more important. Imposing restrictions on search warrants – in the form of ex ante search protocols and geographic restrictions on the applications police can search – is the best way to ensure that cell phone warrants do not become the reviled general warrants the Fourth Amendment's particularity requirement was designed to prevent.