Back to the Future: Returning to Reasonableness and Particularity Under the Fourth Amendment

Adam Lamparello
Charles MacLean
Back to the Future: Returning to Reasonableness and Particularity Under the Fourth Amendment

BY ADAM LAMPARELLO AND CHARLES MACLEAN

ABSTRACT

Issuing one-hundred or fewer opinions per year, the United States Supreme Court cannot keep pace with opinions that match technological advancement. As a result, in Riley v. California and United States v. Wurie, the Court needs to announce a broader principle that protects privacy in the digital age. That principle, what we call “seize but don’t search,” recognizes that the constitutional touchstone for all searches is reasonableness.

When do present-day circumstances—the evolution in the Government’s surveillance capabilities, citizens’ phone habits, and the relationship between the NSA and telecom companies—become so thoroughly unlike those considered by the Supreme Court thirty-four years ago that a precedent … simply does not apply? The answer, unfortunately for the Government, is now.

PART I
INTRODUCTION

“Reasonableness is the ‘touchstone’ of Fourth Amendment analysis.”3 Nothing speaks with more constitutional clarity than an unreasonable search. There can be no doubt—in an era of unprecedented technological advances—that individual privacy is under attack by state action that no honest jurist can consider reasonable. In Riley v. California4 and United States v.

1 Assistant Professors of Law, Indiana Tech Law School.
Wurie, the United States Supreme Court will have a golden opportunity to secure privacy rights for the future when it decides whether searches incident to arrest permit law enforcement officers to search, without a warrant, the contents of an arrestee’s cell phone. The answer to that question is no.

And it resides in a place that transcends the past, and has remained fixed and evolved over time: the Fourth Amendment’s “reasonableness” and “particularity” requirement. If a search is not reasonable given the totality of the circumstances, and does not enumerate with particularity the items or “rooms” to be searched, then all evidence resulting therefrom should not be admissible at trial. The one exception, as discussed below, would be where law enforcement officers are faced with an imminent threat to life. In Riley and Wurie, the Court should return to reasonableness, and rescue privacy from an epidemic of unconstitutional searches and intrusive surveillance.

The Court should not, however, engage in hyper-technical legal analysis, or apply stare decisis principles to rely on precedent from an era of black-and-white televisions. The Court should be honest, and say what that Constitution—and Marbury v. Madison—give it the

---

6 See Chimel v. California, 395 U.S. 752 (1969). (holding that a law enforcement officer could search areas within the “immediate control” of a suspect, for the purpose of: (1) protecting the officer’s safety; and (2) preventing the destruction of evidence); see also Preston v. United States, 376 U.S. 364 (1964) (discussing the two justifications that permit searches incident to arrest).
7 U.S. Const. amend. IV. The Fourth Amendment provides as follows:

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

8 United States v. Knights, 534 U.S. 112, 118 (2001)) (stating that the Court examines the “totality of the circumstances” to decide if a search is reasonable within the meaning of the Fourth Amendment”).
10 5 U.S. 137 (1803).
constitutional duty to say: absent an imminent threat to life, warrantless searches of an arrestee’s cell phone memory facially violate the Fourth Amendment.

In so holding, the Court should adopt a “seize but don’t search” doctrine, where officers will be permitted to seize an arrestee’s cell phone to prevent the destruction of evidence, but not to search its contents without probable cause and a warrant. Furthermore, the exigency must be narrowly construed to mean a threat to life, not amorphous notions of safety, that might otherwise threaten to swallow the rule. Put differently, law enforcement cannot search a cell phone’s “rooms” without probable cause, and a warrant setting forth with particularity the “rooms” officers may enter.11

Absent such a ruling, warrantless searches of cell phones, which house the “papers” and “effects” traditionally protected by the Fourth Amendment,12 will become the new general warrants, effectively trumping the Constitution’s written and unwritten guarantee of privacy. Part II explains why the traditional justifications for searches incident to arrest—protecting an officer’s safety and preventing the destruction of evidence13—are inapplicable to cell phone memory searches, and why principles of stare decisis cannot effectively address the complex legal questions that technology poses. Part III examines Riley and Wurie, where the California Court of Appeals and First Circuit, reached opposite conclusions regarding the constitutionality of searching a cell phone incident to arrest. Part IV introduces the “seize but don’t search” doctrine and explains why it is the ideal manifestation of reasonableness under the Fourth

11 See Orin S. Kerr, Applying the Fourth Amendment to the Internet: A General Approach, 62 STAN. L. REV. 1005 (2010) (discussing the particularity requirement in the context of internet searches). When either a search warrant or an exigency allows a law enforcement officer to “search” a cell phone, neither should occur without specifically enumerating the particular parts or “rooms” of the cell phone the officer is authorized to search. Just as an officer cannot constitutionally look inside an envelope when the officer is only authorized by the warrant or exigency to look for a stolen automobile, nor should any computer or cell phone “search” ever authorize a blunderbuss search of the entirety of its memory, that is, a search of all its “rooms.” Both the “particularity” and the “reasonableness” prongs of the Fourth Amendment compel that particularity, without which the search cannot be deemed reasonable.
12 See U.S. Const. amend. IV, supra note 6.
13 See id.
Amendment. Cell phones transcend physical boundaries and finite space, shatter the distinction between public thoroughfares and private homes, and introduce a web of novel legal issues that pre-digital case law cannot solve. One fact, however, has become clear: searching a cell phone’s memory without a warrant and incident to a lawful arrest is not a reasonable search and seizure under the Constitution.

PART II

STARE DECISIS AND THE SEARCH INCIDENT TO ARREST DOCTRINE DO NOT FIT IN THE LAW AND TECHNOLOGY CONTEXT

In *Montejo v. Louisiana*, the Supreme Court held that, “[b]eyond workability, the relevant factors in deciding whether to adhere to the principles of stare decisis include the antiquity of the precedent, the reliance interests at stake, and of course whether the decision was well-reasoned.” In law and technology contexts, slavish adherence to *stare decisis* by stretching analogies beyond reason has led courts to the wrong place—pre-digital era case law that never contemplated the vast technological advances of today. Indeed, courts have tried mightily to force-fit searches of cell phone contents into the decades-old search incident to arrest exception even though a cursory examination shows that the there is no compatibility between the two—and nothing even remotely reasonable.

To begin with, Smartphones, iPads, Facebook, and YouTube did not exist four decades ago when the modern search incident to arrest exception was created. Likewise, phones could not store documents, download movies, take pictures, or record videos when the United States

---

14 556 U.S. 778, ___ (2009)
15 *Id.* (emphasis added).
Supreme Court decided *Smith v. Maryland*,\(^{16}\) which allowed law enforcement to use a pen register to monitor outgoing calls from a suspect’s residence.

Furthermore, the justifications underlying the search incident to arrest exception cannot possibly be construed as authorizing warrantless searches of a cell phone’s contents. As the Supreme Court held in *Arizona v. Gant*,\(^{17}\) “the scope of a search incident to arrest is commensurate with its purposes of protecting arresting officers and safeguarding any evidence of the offense of arrest that an arrestee might conceal or destroy.”\(^{18}\)

A cell phone implicates neither of these concerns. It is not—and cannot—be used as a weapon,\(^{19}\) and “cannot hide weapons.”\(^{20}\) Furthermore, it presents no reasonable threat to safety. The hyper-technical distinctions established in pre-digital era case law, for example, including “wingspan,”\(^{21}\) “immediate[] associat[ion],”\(^{22}\) and “lunging area”\(^{23}\) were designed to protect an officer’s safety.\(^{24}\) In the cell phone context, it does not matter where the arrestee’s cell phone is located. It cannot be used as a knife, just like it cannot be analogized to a cigarette pack.

The only issue that arises relates to the preservation of evidence. Importantly, however, unless an arrestee’s cell phone has minimal storage capacity, an automatic delete function,\(^{25}\) or

\(^{16}\) See *Smith v. Maryland*, 442 U.S. 735 (1979) (holding that law enforcement could use a pen register to track outgoing telephone calls from a suspect’s private residence).

\(^{17}\) 556 U.S. 332 (2009).

\(^{18}\) Id. at 339 (emphasis added).


\(^{20}\) Id. at 1389.


\(^{22}\) People v. Diaz, 244 P.3d 501, 505 (Cal. 2011), *cert. denied*, 132 S. Ct. 94 (2011) (holding that a cell phone is “immediately associated” with the arrestee’s person).

\(^{23}\) Id. at 502.

\(^{24}\) See Comment, Constitutional Law—Fourth Amendment—First Circuit Holds That the Search-incident-to-Arrest Exception Does Not Authorize the Warrantless Search of Cell Phone Data—United States v. Wurie, 728 F.3d 1 (1st Cir. 2013), Reh’g en Banc Denied, No. 11-1792, 2013 WL 4080123 (1st Cir. July 29, 2013).

can be remotely deleted by a third party,”

the risk of losing evidence is remote. Modern cell phones “no longer store only a handful of recent text messages and phone calls and greatly expanded digital memories eradicate any real risk of automatic deletion.”

Also, even though remote deletion “pose[s] a real and substantial risk of destroying evidence,”
it depends on factors that law enforcement can mitigate by seizing—but not searching—the phone. As one commentator explains, “for an arrestee to effectively erase evidence … (1) a phone must be enabled with remote wipe capabilities, (2) an accomplice must have access to the remote wipe program, and (3) there must exist some way for the arrestee to contemporaneously alert the accomplice of the arrest.”

Seizing the phone eliminates the risk, while maintaining reasonableness.

Thus, permitting searches incident to arrest based on the preservation of evidence rationale stretches this exception “beyond its breaking point.”

It is predicated on the erroneous assumption that “incoming calls or messages will replace recent calls or messages in a phone’s memory or that an arrestee's accomplice will activate a remote wipe program to erase the phone’s memory entirely.”

In the absence of a “remote wipe threat” or other method of deletion, however, this justification “cannot logically be applied to cell phones.”

Courts that have relied on this justification to permit warrantless fishing expeditions into an arrestee’s cell

---

26 Id.
27 See, e.g., Samuel J. H. Beutler, The New World of Mobile Communication: Redefining the Scope of Warrantless Cell Phone Searches, 15 VAND. J. ENT. & TECH. L. 375, 394 (2013). (explaining that, “for an arrestee to effectively erase evidence … (1) a phone must be enabled with remote wipe capabilities, (2) an accomplice must have access to the remote wipe program, and (3) there must exist some way for the arrestee to contemporaneously alert the accomplice of the arrest”).
28 Id. at 395.
29 Id. (emphasis added).
30 Butterfoss, supra note 21, at 77.
31 Beutler, supra note 27, at 394.
32 Id.; see also 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 BILL RIGHTS J. 601, passim (Dec. 2013).
33 See Joshua Eames, Can You Hear Me Now? Warrantless Cell Phone Searches and the Fourth Amendment; People v. Diaz, 244 P.3d 501 (Cal. 2011), 12 WYO. L. REV. 483, 501 (2012).
phone either misperceive the nature of cell phone use in modern society, or are being dishonest. In both cases, they are being unreasonable.

To be sure, Smartphones—which are now owned and operated by fifty-five percent of the population—transcend the finite physical space that is traditionally subject to searches incident to arrest. Smartphones, for example, bear no relation to a wallet address book, cigarette package, or a container. While some parts are arguably similar, e.g., call logs and contact information, a cell phone’s sheer storage capacity far exceeds the limited space in a Rolodex or an empty suitcase. Furthermore, a Smartphone’s multi-faceted personal uses, e.g., to store confidential documents, download videos, and send private electronic messages, demonstrate its dissimilarity to the other physical objects that courts have held to be searchable incident to arrest. People do not store confidential documents in a Rolodex, and they do not watch YouTube videos in a suitcase.

We now live in a “cell-phone centric” society, where individuals use a compact electronic device as an outlet for self-expression and as storage space for uniquely personal information. In many ways, Smartphones are no longer “phones” at all. They are an extension of the mind, a warehouse for an individual’s intimate thoughts and beliefs, and the modern-day

---

35 United States v. Rodriguez, 995 F.2d 776, 778 (7th Cir. 1993) (“search the search of [defendant’s] wallet and the photocopying of the contents of the address book were permissible as a search incident to arrest”).  
36 Id.  
37 United States v. Robinson, 414 U.S. 218 (1973) (in Robinson, the court permitted the search of a “crumpled up cigarette package,” which many courts have used for the more general proposition that police may search the contents of any container found on a person); see generally New York v. Belton, 453 U.S. 454 (1981); United States v. Cote, No. 03 CR 271, 2005 U.S. Dist. LEXIS 11725 (N.D. Ill. May 25, 2005), at *19, aff’d, 504 F.3d 682 (7th Cir. 2007) (citing United States v. Rodriguez, 995 F.2d 776 (7th Cir. 1993); United States v. Molinaro, 877 F.2d 1341, 1346-47 (7th Cir. 1989)).  
38 See Mark L. Mayakis, Cell Phone – A Weapon of Mass Discretion, 33 CAMPBELL L. REV. 151, 161 (2010) (Even the “more basic models of modern cell phones have the technological capabilities of storing and transmitting exponentially greater amounts of private information than that of a pager or any traditional closed container”) (citation omitted).  
39 See Eames, supra note 33, at 499.  
repository for the private “papers” and “effects” that the Fourth Amendment, from the time of its adoption, safeguarded from arbitrary government intrusion. 41 Relying on case law from an era of rotary phones and black-and-white televisions is the equivalent to putting a square peg in a round hole. A Smartphone is the square peg, and the search incident to arrest doctrine is the round hole. The incompatibility underscores the problems of analogizing cyberspace to finite physical space.

Thus, although cell phones “defy easy categorization,” 42 there can be little doubt that, as technology becomes more advanced, so too must the courts’ conception of privacy—and reasonableness—under the Fourth Amendment. 43 The threat is very real—and uniquely widespread—because cell phones provide law enforcement with an abundant source of potentially incriminating evidence. As the Ohio Supreme Court explained in State v. Smith, “for law enforcement, these devices can be ‘attractive targets for criminal investigators,’ providing a wealth of evidence such as lists of recent incoming and outgoing calls, text messages, and possibly incriminating photographs.” 44 The court furthered explained as follows:

An officer searching a cell phone can at least initially do so fairly easily, by “just ‘thumbing through’ the cell phone.” As Professor Gershowitz has written, searches of pagers and early generation cell phones “do not require in-depth searching to obtain evidence. Police need to push only a limited number of buttons in order to reach pager numbers and only a few additional buttons to retrieve text messages.” 45

This information resides, however, in a place where individuals —both at home and on public thoroughfares—live their private lives. As the First Court noted in Wurie, “allowing the

41 See U.S. Const. amend. IV.
42 State v. Smith, 920 N.E.2d 949, 955 (Ohio 2009).
43 See Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (a search under the Fourth Amendment on whether an individual has “an actual (subjective) expectation of privacy,” and second, whether the individual’s subjective expectation is “one that society is prepared to recognize as ‘reasonable’”) (citation omitted).
44 Id. (citation omitted).
45 Id.
police to search that data without a warrant any time they conduct a lawful arrest would, in our view, create ‘a serious and recurring threat to the privacy of countless individuals’.”

In fact, the damage has already been severe. For example, without a warrant—or any suspicion whatsoever—law enforcement now tracks cellular telephone “meta data,” conducts invasive searches into a cell phone’s contents, and at the border, performs week-long, invasive forensic searches of laptop computers. Incredibly, courts continue to invoke the search incident to arrest doctrine, along with outdated case law from the pre-digital era, to sanction the Government’s unprecedented intrusion into the private lives of ordinary citizens. As a result, law enforcement’s investigatory dragnet has swelled to unprecedented proportions, and privacy rights have begun to drift into the sea of abstraction. Riley and Wurie are the vehicles to create principled changes, and return to reasonableness.

PART III

A SPLIT DECISION: THE GOVERNMENT WINS IN RILEY, BUT PRIVACY PREVAILS IN WURIE

The Supreme Court recently granted certiorari in two cell phone search incident to arrest cases that reached opposite results below. In Riley, the California Court of Appeals held that the

---

46 728 U.S. at 14 (quoting Gant, 345 U.S. at 556).
47 See U.S. Const. amend. IV.
48 “Metadata” refers to phone numbers that a person dials from a cell phone. As discussed below, however, technology now allows the Government to identify the location where a cell phone is used, along with other arguably private information.
49 See Hanni M. Fakhoury, Challenging Cell Phone Searches Incident to Arrest, 37-NOV CHAMPION 30, 31 (2013) (“[T]he Fourth, Fifth Seventh and Tenth Circuits, as well as state appellate courts in Alabama, California, Colorado and Kansas, have permitted police to search cell phone or pager with little limitation incident to arrest. A number of federal district courts have reached the same result”).
50 See Abidor v. Napolitano, No. 10-CV-04059 (ERK)(JMA), 2013 WL 6912654 (E.D.N.Y. Dec. 31, 2013) (holding that the “border exemption” doctrine allows law enforcement to search the laptop computers of citizens entering the country, whether the border agents have reasonable suspicion or no suspicion at all).
search incident to arrest doctrine permitted the search of an arrestee’s cell phone contents.\textsuperscript{52} In \textit{Wurie}, the First Circuit reached the opposite result.\textsuperscript{53} By granting \textit{certiorari} for both cases, the Court may be signaling that it intends to adopt a “middle ground” approach that strengthens privacy protections in the digital age, but gives law enforcement sufficient latitude to conduct warrantless search where the facts warrant.

A. \textbf{RILEY V. CALIFORNIA—A MISGUIDED APPLICATION OF THE SEARCH INCIDENT DOCTRINE TO SEARCHES OF A CELL PHONE’S CONTENTS}

David Leon Riley, a member of the Lincoln Park gang, was standing by his car with fellow gang members when a rival gang drove by in another car and sparked a gunfight.\textsuperscript{54} The gangsters near Riley’s car opened fire at the rival’s car.\textsuperscript{55} The shooters then fled the scene in Riley’s car.\textsuperscript{56} Spent shell casings from at least two different handguns, .40 caliber and .45 caliber, were found at the shooting scene.\textsuperscript{57} Almost three weeks later, officers unaware of the shooting, stopped Riley as he was driving his other car.\textsuperscript{58} When they noticed Riley’s driving privileges were suspended, they decided to impound Riley’s car.\textsuperscript{59} Pursuant to departmental policy, the officers conducted an impound inventory of Riley’s car, including, as the policy prescribed, under the car’s hood.\textsuperscript{60} Under the hood, wrapped in a sock, the officer conducting the impound inventory found two handguns, .40 caliber and .45 caliber.\textsuperscript{61}

\textsuperscript{52} 2013 WL 3938997 (Jan. 17, 2014).
\textsuperscript{53} 2013 WL 4402108 (Jan. 17, 2014).
\textsuperscript{54} Riley, 2013 WL 475242, at *1.
\textsuperscript{55} Id.
\textsuperscript{56} Id.
\textsuperscript{57} Id.
\textsuperscript{58} Id.
\textsuperscript{59} Id.
\textsuperscript{60} Id. at *1-2.
\textsuperscript{61} Id. at *1.
After finding the hidden handguns, the officers arrested Riley. At the arrest scene, the officers seized Riley’s cell phone from his person and briefly looked through the phone’s various displays. Visible on Riley’s cell phone at the scene, once the officers paged through the cell phone’s screens, were several indicia of gang involvement; therefore, the arresting officers, upon return to the station, gave Riley’s cell phone to a gang officer. That gang officer found some relevant photographs and video clips on Riley’s cell phone.

At trial, the State admitted gang evidence, photographs, and video clips seized from Riley’s cell phone, along with locational data from Riley’s cell phone records indicating that his cell phone had been near the shooting scene at the time of the shooting. The trial court found that a recent California Court of Appeals case, People v. Diaz, controlled, and held that officers were authorized to search the memory of a cell phone seized from an arrestee’s person incident to a lawful arrest, whether or not any exigency exists at the time the cellphone is searched. The California Court of Appeals affirmed, applying Diaz and reasoning that, “Riley’s cell phone was immediately associated with his person when he was arrested, and therefore the search of his cell phone was lawful whether or not an exigency still existed.”

The California Court of Appeals reached the wrong result. First, the court conflated the words “immediate association” with the purposes underlying a search incident to arrest. Even if the cell phone was immediately associated with Riley’s “person,” it neither threatened the officers’ safety nor presented a risk that evidence would be destroyed. Surprisingly, however,

---

62 Id. at *2.
63 Id. at *3.
64 Id.
65 Id.
66 Id.
68 Riley, 2013 WL 475242, at *3.
69 Id. at *6 (emphasis added).
the Court of Appeals made no attempt to establish a nexus between the *Chimel* justifications and the subsequent search of Riley’s cell phone.

In addition, the California Court of Appeals failed to consider whether the search of Riley’s cell phone should be limited in scope, purpose, or duration. For example, the court could have allowed law enforcement to search only those areas where evidence of the crime of arrest was likely to be found. Moreover, the court could have restricted the search to those areas where Riley had a reduced expectation of privacy, such as the outgoing call log or text messages sent in the past forty-eight hours. For all other, more personal areas of Riley’s cell phone, the court could have mandated that, in the absence of exigent circumstances, probable cause and a warrant were required. It did none of these things.

Instead, the California Court of Appeals permitted an unfettered search of Riley’s cell phone, essentially sanctioning a suspicionless fishing expedition into his personal life. Neither the search incident to arrest doctrine, nor the text of the Fourth Amendment—which requires that searches be “reasonable”—countenances such an unbridled infringement on personal privacy. The court’s decision effectively meant that Riley sacrificed his privacy rights the moment police placed him under arrest. By way of analogy to the Fifth Amendment’s right against self-incrimination, such a result is tantamount to holding that a suspect surrenders his right to silence the moment police place him under arrest. The Constitution, however, does not allow for the forfeiture of fundamental rights, particularly when a suspect needs them the most.

To be sure, even if the California Court of Appeals believed that Riley had no expectation of privacy in his cell phone, it would not necessarily justify a warrantless and unrestricted search of his cell phone.⁷⁰ There is a constitutionally significant distinction between an individual’s

---

⁷⁰ See, e.g., Howard E. Wallin, *Plain View Revisited*, 22 PACE L. REV. 307, 325 (2003) (stating that, where “privacy is not protected by the Constitution,” it garners no protection from the Fourth Amendment). This reasoning,
expectation of privacy in a cell phone as an object, and as the safe keeper of the “papers” and “effects” that the Fourth Amendment has always deemed private. Surely, for example, an individual has at least some expectation of privacy in personal documents stored on a cell phone, videos downloaded from YouTube, or private emails sent from an email account. Of course, this does not immunize the information from a valid search, but it does require law enforcement to have probable cause, and to secure a warrant that delineated with particularity the places to be searched. Otherwise, information historically designated as worthy of the most stringent privacy safeguards would suddenly lose its constitutional protections simply because an individual decided to store it in a cell phone rather than a closet. Such a result cannot qualify as reasonable under the Fourth Amendment, because it would allow an individual’s efficient use of technology to constitute an implicit waiver of basic civil liberties.

It is not surprising, therefore, that neither Chimel nor any other exceptions to the warrant requirement supported the search of Riley’s cell phone. After all, the Court’s Fourth Amendment jurisprudence is based on whether, prior to a search, it would be reasonable to require law enforcement to obtain a warrant. Indeed, where the Court has created exceptions to the warrant requirement, they have been based on: (1) impracticability; and (2) inevitability. Impracticability, for example, exists when procuring a warrant would lead to the destruction of evidence or threaten the life or safety of others. Certainly, no one would argue that it would be unreasonable to proceed without a warrant in this circumstance.

While a bit more complicated, inevitability nonetheless reflects the primacy of reasonableness in the constitutional analysis. Inevitability is present when an officer sees an item

---

however, does not apply to searches of a cell phone’s contents, because the contents themselves include items traditionally afforded protection by the Fourth Amendment.}
in plain view in a place where the officer is lawfully present.\(^{71}\) While police officers maintain a lawful presence when securing a valid arrest, and can seize the cell phone to preserve evidence, there is nothing to ‘see’ in plain view unless the officer initiates a second, warrantless search of cell phone memory. This can occur by simply by pushing buttons on the cell phone, which will allow law enforcement to search, among other things, an arrestee’s email, text messages, or applications. In so doing, however, the ‘presence’ becomes unlawful; the officer has entered an ‘area’ where the search for evidence includes objects traditionally afforded Fourth Amendment protection. And it has done so without impracticability, inevitably, or exigency. Law enforcement—and the courts—need another reason. They cannot find one, however, because it does not exist in precedent—or in the Fourth Amendment.

Some courts have relied on the third-party doctrine\(^ {72}\) to hold that a cell phone user’s Google searches constitute a voluntary disclosure (thus surrendering Fourth Amendment protections), because the user knows that the search will be transmitted through a server. Importantly, however, “the Supreme Court decisions that established the third-party doctrine are decades old,”\(^ {73}\) and cell phones, just as they are not containers or address books, are unlike “bank records voluntarily conveyed to banks in the ordinary course of business.”\(^ {74}\) They are also not comparable to “exposing numerical information to the telephone company,”\(^ {75}\) because individuals should not be required to “assum[e] the risk that the company would turn over that information to the government.”\(^ {76}\)

\(^{71}\) See id. (the plain view exception applies only where “an officer has already justifiably intruded into a constitutionally-protected area, spots and then removes incriminating evidence.


\(^{73}\) Id.

\(^{74}\) Id. at 507-08 (discussing United States v. Miller, 425 U.S. 435, 442-43 (1976)).

\(^{75}\) Rothstein, supra note 72, at 507. (discussing Smith v. Maryland, 442 U.S. 735, 743-44 (1979))

\(^{76}\) Rothstein, supra note 72, at 507.
If this reasoning were applied to cell phones, it would, in effect, condition the downloading and storage of traditionally private information, e.g., confidential legal documents, upon the knowing waiver of constitutional rights. No conception of reasonableness can support this view, because it would result in an unconstitutional chill, through a *de facto* prior restraint, on speech and other expressive activity. It would also require the assumption, under *Katz v. United States*,\(^{77}\) that individuals do not have an objectively reasonable expectation of privacy\(^ {78}\) in otherwise-private material simply because they know it may be viewed by an unidentified third party, for whatever reason, and disclosed to the government, for no reason. That logic might work for bank records that are given to tellers, or numbers that are dialed from a home phone. But it goes too far when applied to private information that reveals intimate details about individuals, and embraces a concept of disclosure that is incompatible with the role cell phones play in the digital age. Individuals are not ‘disclosing’ information in the traditional sense; they are capitalizing on the efficiency cell phones offer and the ubiquitous role they play in modern human interaction. Comparing a Google search to the act of handing over bank records to a teller fails to appreciate these differences, and ignores the fact the ‘disclosure’ in this context is not to a single person, but to the entire world. That requires more, not less, protection.

Of course, there is nothing problematic about saying that a cell phone is “immediately associated” with the person, if this term is construed as an association with the person’s thoughts, private “papers,” and personal “effects.”\(^ {79}\) In *Wurie*, the First Circuit did exactly that. It recognized that the Fourth Amendment “protects people, not just areas.”\(^ {80}\)

\(^{77}\) 389 U.S. 347.

\(^{78}\) *Katz* held that the Fourth Amendment is triggered only where an individual can demonstrate both an objective and subjective expectation of privacy. 389 U.S. at 361-62.


\(^{80}\) *Katz*, 389 U.S. at 353.
B. United States v. Wurie—Categorically Drawing the Line on Cell Phone Searches Incident to Arrest, But Leaving an Unanswered Question.

The First Circuit’s decision in Wurie got it right, but the court’s analysis was incomplete. In other words, it drew a better, but not sufficiently brighter, line. In Wurie, a detective on routine patrol saw the defendant pull his Nissan Altima into a convenience store parking lot, pick up a man there, and engage in what appeared to be a hand-to-hand drug sale inside the Altima.\(^81\) The detective followed and stopped the apparent buyer, and found two bags of crack cocaine in his pocket; the man admitted that he had bought the drugs from a man he knew as “B,” a crack seller, who had been driving the Altima.\(^82\) The detective then instructed another officer, who had tailed the Altima, to stop the car and arrest the driver for distributing crack cocaine.\(^83\) Wurie, the driver and lone occupant of the Altima when the officers stopped it, was arrested and transported to the police station, where two cell phones and $1,275 in cash were seized from him.\(^84\)

Officers noticed in plain view on the visible screen of one of Wurie’s cell phones that his phone “was repeatedly receiving calls from a number identified as ‘my house’.”\(^85\) A few minutes later, officers opened Wurie’s cell phone that was receiving the repeated calls, saw that a photo of a Black female was the screensaver, and by pushing two buttons on the phone determined that “my house” had a particular phone number associated with it.\(^86\) Officers then determined the address associated with the “my house” phone number, and drove to that address; upon arrival, officers noted the mailbox indicated “Wurie and Cristal,” and through the front window, officers saw a female matching the screensaver on Wurie’s cell phone.\(^87\) Officers obtained a search warrant for that address, and recovered 215 grams of crack cocaine, a firearm and ammunition,

\(^{81}\) Riley, 2013 WL 475242, at *3.

\(^{82}\) Id. at *1-2.

\(^{83}\) Id. at *2.

\(^{84}\) Id.

\(^{85}\) Id.

\(^{86}\) Id.

\(^{87}\) Id.
among other items. Wurie moved to suppress the warrantless cell phone search and its fruit, but the trial court denied the suppression motion; a jury subsequently found Wurie guilty of all counts, and he was sentenced to over twenty-one years in prison.

The First Circuit suppressed all evidence relating to the search, holding that it violated the original intent of the Fourth Amendment:

Since the time of its framing, “the central concern underlying the Fourth Amendment” has been ensuring that law enforcement officials do not have “unbridled discretion to rummage at will among a person's private effects.” … Today, many Americans store their most personal “papers” and “effects,” U.S. Const. amend. IV, in electronic format on a cell phone, carried on the person. Allowing the police to search that data without a warrant any time they conduct a lawful arrest would, in our view, create “a serious and recurring threat to the privacy of countless individuals.”

Importantly, the First Circuit traced the history of the modern search incident to arrest doctrine from Chimel v. California, through Arizona v. Gant, and found the Supreme Court had repeatedly expressed a preference for bright-line rules in Fourth Amendment cases so law enforcement officers would not have to parse arcane constitutional tests or engage in complicated balancing of interests and circumstances. The First Circuit then provided what it termed, “Our vantage point.” The First Circuit reasoned,

We suspect that the eighty-five percent of Americans who own cell phones and “use the devices to do much more than make phone calls” . . . would have some difficulty with the government’s view that “Wurie’s cell phone was indistinguishable from other kinds of personal possessions, like a cigarette package, wallet, pager, or address book, that fall within the search incident to arrest exception to the Fourth Amendment’s warrant requirement” . . . In reality,

---

88 Id.
89 Id.
90 728 U.S. at 14 (internal citations truncated to remove parallel cites). cf. United States v. Jones, ___ U.S. ___, 132 S. Ct. 945, 950 (“At bottom, we must ‘assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.’ “ (quoting Kyllo v. United States, 533 U.S. 27, 34 (2001))).
91 395 U.S. 752.
93 728 U.S. at 3-6.
94 Id. at 6.
“a modern cell phone is a computer,” and “a computer . . . is not just another purse or address book.”

In part, the First Circuit differentiated the modern-day cell phone by the contents of its memories:

The storage capacity of today’s cell phones is immense. . . . That information [stored on modern cell phones] is, by and large, of a highly personal nature: photographs, videos, written and audio messages (text, email, and voicemail), contacts, calendar appointments, web search and browsing history, purchases, and financial and medical records. . . . It is the type of information one would previously have stored in one’s home and that would have been off-limits to officers performing a search incident to arrest. . . . In short, individuals today store much more personal information on their cell phones than could ever fit in a wallet, address book, briefcase, or any of the other traditional containers that the government has invoked. . . . Just as customs officers in the early colonies could use writs or assistance to rummage through homes and warehouses, without any showing of probable cause linked to a particular place or item sought, the government’s proposed rule [allowing searches of cell phone memories as a bright-line rule] would give law enforcement automatic access to “a virtual warehouse” of an individual’s “most intimate communications and photographs without probable cause” if the individual is subject to a custodial arrest, even for something as minor as a traffic violation.

The First Circuit then applied the Chimel justifications to cell phone memory searches, which authorizes searches incident to lawful arrest only to protect officer safety or preserve evidence, and found:

[W]arrantless cell phone data searches are categorically unlawful under the search-incident-to-arrest exception, given the government’s failure to demonstrate that they are ever necessary to promote officer safety or prevent the destruction of evidence. . . . Instead, warrantless cell phone data searches strike us as a convenient way for the police to obtain information related to a defendant’s crime of arrest – or other, as yet undiscovered crimes – without having to secure a

\[95\] Id. at 8 (internal citations omitted).

\[96\] Id. at 8-9 (internal citations omitted).

\[97\] The First Circuit found that cell phone memories virtually never pose a threat to officer safety. See id. at 10.

\[98\] As the First Circuit found, evidence on cell phone memories can be easily and inexpensively safeguarded from destruction by (1) turning off the cell phone; (2) removing its battery; (3) placing the cell phone in a Faraday enclosure; or (4) copying the entire contents to preserve them for later search pursuant to a validly issued search warrant. Id. at 11 (citing among others, see also Charles E. MacLean, But Your Honor, A Cell Phone is Not a Cigarette Pack: An Immodest Call for a Return to the Chimel Justifications for Cell Phone Memory Searches Incident to Lawful Arrest, 6 FED. CTS. L. REV. 37 (2012).
warrant. We find nothing in the Supreme Court’s search-incident-to-arrest jurisprudence that sanctions such a “general evidence-gathering search.”

The First Circuit in *Wurie* reached the correct conclusion, but neither court has it quite right. As the Supreme Court prepares to hear arguments in both cases, this article proposes a four-pronged, “seize but don’t search” exception to help guide its constitutional analysis. It is the middle ground where privacy meets security.

**PART IV**

**RETURNING TO REASONABLENESS: THE SEIZE BUT DON’T SEARCH DOCTRINE**

The failure of *Chimel* and its progeny to provide workable solutions for the digital age has resulted in a jurisprudential void and an unprecedented assault on privacy rights. Whether through the secret collection of metadata or the warrantless searches of cell phone memory, individual citizens continue to suffer grave constitutional harms without any cognizable remedy. In *Riley* and *Wurie*, the Court must restore the constitutional balance and provide a blueprint for future jurisprudence. One recent case has already begun to return privacy to its rightful resting place: the text and original meaning of the Fourth Amendment.

**A. KLAYMAN v. OBAMA—CELL PHONES ARE NOT PEN REGISTERS**

In *Klayman v. Obama*, the court held that the National Security Agency’s (“NSA”) surveillance program, which consisted of the indiscriminate, suspicionless collection of cell-phone metadata, likely constituted a search under the Fourth Amendment. The court reasoned that, because “people in 2013 have an entirely different relationship with phones than they did

---

100 728 U.S. at 14.
101 See e.g., Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (London), June 5, 2013. The public became aware of the NSA program from leaks of classified material by Edward Snowden, a former employee. Initial media reports suggested that, on April 15, 2013, the Foreign Intelligence Surveillance Court (“FISC”) issued an order, dated April 25, 2013, ordering Verizon Business Services to produce to the NSA all call detail records for telephone metadata.
102 *Klayman*, 2013 WL 6571596, at *22.
thirty-four years ago,\textsuperscript{103} the Government “metadata collection and analysis almost certainly does violate a reasonable expectation of privacy.”\textsuperscript{104}

In so holding, the court rejected the pen register analogy made in \textit{Smith v. Maryland},\textsuperscript{105} stating that a “citizens’ phone habits”\textsuperscript{106} have become “so unlike those considered by the Supreme Court thirty-four years ago [in \textit{Smith}].”\textsuperscript{107} Indeed, the Government’s “almost-Orwellian technology”\textsuperscript{108} was “unlike anything that could have been conceived in 1979,”\textsuperscript{109} when \textit{Smith} was decided. That is precisely the point. Times have changed, and so must the courts. As explained below, \textit{Klayman} embraced a view of privacy—and particularity under the Fourth Amendment—that pre-digital age precedent could not have foreseen, and that the Supreme Court should adopt. And just like \textit{Smith} does not support the indiscriminate collection of cell phone metadata, \textit{Chimel} does not support the search of an arrestee’s cell phone.

In its opinion, the \textit{Klayman} court rejected the Government’s argument that \textit{Smith} “squarely control[s].”\textsuperscript{110} In \textit{Smith}, the Court held that law enforcement could install a pen register to track the numbers dialed from a suspect’s phone.\textsuperscript{111} There was no reasonable expectation of privacy in the dialed numbers because they were “voluntarily transmitted…to his phone company,”\textsuperscript{112} and because “it is generally known that phone companies keep such information in their business records.”\textsuperscript{113}

\textsuperscript{103} Id.
\textsuperscript{104} Id.
\textsuperscript{105} 442 U.S. 735 (1979).
\textsuperscript{106} \textit{Klayman}, 2013 WL 6571596, *17.
\textsuperscript{107} Id.
\textsuperscript{108} Id. at *19.
\textsuperscript{109} Id.
\textsuperscript{110} 2013 WL 475242, at *17.
\textsuperscript{111} Id.
\textsuperscript{112} Id.
\textsuperscript{113} Id.
The collection of cell phone metadata, however, involves novel issues that could not have been contemplated by courts decades ago. To begin with, the Government’s surveillance capabilities, coupled with “citizens’ phone habits, and the relationship between the NSA and telecom companies,”\textsuperscript{114} have become “so unlike those considered by the Supreme Court thirty-four years ago [in \textit{Smith}].”\textsuperscript{115} Indeed, “the Court in \textit{Smith} was not confronted with the NSA’s Bulk Telephony Metadata program,”\textsuperscript{116} and could not “have ever imagined [in 1979] how the citizens of 2013 would interact with their phones.”\textsuperscript{117}

For example, unlike a pen register, which was “operational for only a matter of days,” the “NSA telephony metadata program … involves the creation and maintenance of a historical database for five years’ worth of data.”\textsuperscript{118} Furthermore, in \textit{Smith}, law enforcement installed a pen register to “record the numbers dialed from the [suspect’s] telephone,”\textsuperscript{119} whereas the NSA program collects, “\textit{on a daily basis} [from telecommunications service providers] electronic copies of call detail records, or telephony metadata.”\textsuperscript{120} In other words, \textit{Smith} involved the targeting of an individual suspect, which “in no way resembles the daily, all-encompassing, indiscriminate dump of cell phone metadata that the NSA now receives as part of its … Metadata Program.”\textsuperscript{121} As the court explained, it is “one thing to say that people expect phone companies to occasionally provide information to law enforcement,”\textsuperscript{122} but “quite another to suggest that

\textsuperscript{114} \textit{Id.}
\textsuperscript{115} \textit{Id.}
\textsuperscript{116} \textit{Id.} at *19.
\textsuperscript{117} \textit{Id.}
\textsuperscript{118} \textit{Id.} (emphasis in original).
\textsuperscript{119} \textit{Id.}
\textsuperscript{120} \textit{Id.} (emphasis in original).
\textsuperscript{121} \textit{Id.}
\textsuperscript{122} \textit{Id.}
our citizens expect all phone companies to operate … a joint intelligence gathering operation with the government.”

To be sure, the “almost-Orwellian technology that enables the Government to store and analyze the phone metadata of every telephone user in the United States is unlike anything that could have been conceived in 1979.”

As the court recognized, “[t]he notion that the Government could collect similar data on hundreds of millions of people … for a five year period … was at best, in 1979, the stuff of science fiction.” To make matters worse, the Government uses “the most advanced twenty-first century tools,” to “proceed surreptitiously,” thus circumventing the “ordinary checks that constrain abusive law enforcement practices.”

Lastly, “not only is the Government’s ability to collect, store, and analyze phone data greater now than it was in 1979,” but the nature and quantity of the information contained in … metadata is much greater.”

The court held as follows:

Cell phones have also morphed into multi-purpose devices. They are now maps and music players … They are cameras … They are even lighters that people hold up at rock concerts … They are ubiquitous as well. Count the phones at the bus stop, in a restaurant, or around the table at a work meeting or any given occasion. Thirty-four years ago [when Smith was decided], none of those phones would have been there … [instead], city streets were lined with pay phones … when people wanted to send “text messages,” they wrote letters and attached postage stamps.

123 Id.
124 Id.
125 Id. at *20; see also United States v. Jones, 132 S. Ct. 945 (2012) (holding, in a multi-faceted opinion, that law enforcement’s use of a GPS device to track a vehicle’s movements for twenty-eight days violated the suspect’s reasonable expectation of privacy or was a trespass).
127 Id.
128 Id.
129 Id.
130 Id.
131 Id. at *20.
Of course, while metadata itself has not changed substantially over time, it can, unlike thirty-four years ago, “reveal the user’s location.”

Also, the “ubiquity of [cell] phones has dramatically altered the quantity of information that is now available and … what the information can tell the Government about people’s lives.” For example, people “send text messages now that they would not (really could not) have made or sent back when Smith was decided.” In fact, text messaging has become “so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification.” This reflects a “rapid and monumental shift towards a cell-centric culture,” where metadata from each person’s phone reveals “a wealth of detail about her familial, political, professional, religious, and sexual associations.” As the Supreme Court held in City of Ontario v. Quon, “[t]hat might strengthen the case for an expectation of privacy.”

These realities have therefore “resulted in a greater expectation of privacy and recognition that society views that expectation as reasonable.” That expectation is compromised when “the Government, without any basis whatsoever to suspect them of any wrongdoing, collects and stores for five years their telephony metadata for purposes of subjecting it to high-tech querying and analysis without case-by-case judicial approval.”

---

132 Id. at *21.
133 Id. at *21 n.57.
134 Id. at *21.
135 Id.
136 Id. (quoting City of Ontario v. Quon, 560 U.S. ___, ___, 130 S. Ct. 2619, 2630 (2010)).
138 Id. (quoting Jones, 132 S. Ct. at 955-56 (Sotomayor, J., concurring)).
139 130 S. Ct. at 2630.
140 Id.
141 Klayman, 2013 WL 6571596, at *21 (emphasis in original).
142 Id. at *22.
Klayman’s analysis is significant, in part, because the individual’s expectation of privacy was predicated on the scope and breadth of the Government’s intrusion, not whether the place itself was public or private. In United States v. Jones, at least three members of the Supreme Court adopted a similar view, holding that law enforcement’s use of a “GPS device to track a suspect’s movement for nearly a month violated Jones’s reasonable expectation of privacy.” The plurality explained that, while “relatively short-term monitoring of a person’s movements on public streets” is permissible, “the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.” Likewise, in United States v. Maynard, the District of Columbia Circuit held that, while a person “traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another,” it does not mean that “such a person has no reasonable expectation of privacy in his movements whatsoever, without end, as the Government would have it.”

As stated above, while individuals transmit personal information via a cell phone knowing that it can be shared with third parties, they do so because of the phone’s ubiquity, affordability, and efficiency. Few would doubt that, if any of the documents stored on cell phones were located in a private home or other physical space, they would not be searchable without probable cause and a warrant describing with particularity the places to be searched.

143 132 S. Ct. 945.
144 Klayman, 2013 WL 6571596, at *17 (citing Jones, 132 S. Ct. at 955-56 (Sotomayor, concurring)); cf. 132 S. Ct. at 962 (Alito, J., concurring) (advances in technology may require individuals to “reconcile themselves” to the “inevitable diminution of privacy that new technology entails”).
145 132 S. Ct. at 964 (Alito, J., concurring).
146 Id. Of course, the plurality in Jones was rather cobbled together with different but substantial subsets of the Justices favoring, alternatively, a “reasonable expectation of privacy” theory, or a trespass theory. FOOTNOTE NEEDED HERE. In that sense, at least a substantial subset of the Justices in Jones cleaved to a place-based Fourth Amendment construct.
147 615 F.3d 544 (D.C. Cir. 2001).
148 Id. at 557.
149 Id. (distinguishing United States v. Knotts, 460 U.S. 276 (1983)) (holding that the use of a tracking beeper did not constitute a search where an individual was traveling from one place to another on a public thoroughfare).
150 See Kerr, supra note 11, at 1005 (discussing the particularity requirement in the context of internet searches).
The result should not change because data is stored in a cellphone, not a closet. Otherwise, courts would be penalizing individuals for using modern technology to enhance their lives, while allowing the government to use it as a tool to dissolve privacy rights.

*Klayman* stands for a proposition that should have been evident long ago: the Government’s asserted justifications for indiscriminately collecting cell-phone metadata (comparing it to a pen register), and searching cell phone content (based on the “search incident to a lawful arrest” doctrine), are not justifications at all because they are not analogous to the relevant precedent. They are unreasonable searches under the Fourth Amendment. A pen register is analogous to the bank teller, and wholly dissimilar to Government’s surveillance program, which collects data from millions of people. The question now becomes: what is a cell phone?

**B. AN EXTENSION OF THE MIND, A VEHICLE FOR SELF EXPRESSION, AND A REPOSITORY FOR “PAPERS” AND “EFFECTS”**

A cell phone cannot be analogized to a crumpled up cigarette package, address book, wallet, or container. Even though parts of a cellphone, e.g., call logs and outgoing text messages, which are the primary functions of older, more basic cell phones, are somewhat

---

151 *Klayman*, 2013 WL 6571596 at *17 (the Government argued that the Supreme Court’s decision in *Smith v. Maryland*, which allowed the use of a pen register to track a suspect’s phone calls, “squarely control[ed],” its metadata collection program).

152 See *e.g.*, United States v. Murphy, 552 F.3d 405, 411 (4th Cir. 2009); United States v. Finley, 477 F.3d 250, (5th Cir. 2007); see also Adam M. Gershowitz, *Password Protected? Can a Password Save Your Cell Phone from a Search Incident to Arrest?*, 96 IOWA L. REV. 1125, 1136 (2011).

153 *Robinson*, 414 U.S. 218; see also MacLean, *supra* note 97, at 50.

154 *Rodriguez*, 995 F.2d at 778.

155 *Id.*

156 See *Eames, supra* note 32, at 99.
similar, the storage capacities\textsuperscript{157} the technological capabilities of modern-day devices such as Smartphones make them entirely dissimilar to traditional physical objects.

Unlike a container, for example, a cell phone is not an object capable of holding another object.”\textsuperscript{158} Cell phone contents by contrast are “limited to digital data, the intangible nature of which renders it unavailable for use as a weapon or as evidence that can be physically destroyed.”\textsuperscript{159} In addition, “modern cell phones are capable of accessing almost limitless amounts of data,”\textsuperscript{160} and “cloud technology means that to a growing extent cell phone contents are only available by linking wirelessly to a remote cellular relay tower.”\textsuperscript{161} In fact, “[e]ven the more basic models of modern cell phones are capable of storing a wealth of digitized information wholly unlike any physical object found within a closed container.”\textsuperscript{162}

Additionally, cell phones are not merely objects capable of storing massive amounts of private data, and are not analogous to a car, an office, or even a house. Instead, they are a modern extension of the mind, and vehicle for free speech. A cell phone’s contents often contain intimate and highly personal information, such as confidential documents, private messages, videos, data from internet searches, and \textit{thoughts}.\textsuperscript{163}

\begin{quote}
Modern cellular phones have the capacity for storing immense amounts of private information. Unlike pagers or address books, modern cell phones record incoming and outgoing calls, and can also contain address books, calendars, voice and text messages, email, video and pictures. Individuals can store highly personal information on their cell phones, and can record their most private
\end{quote}

\textsuperscript{157} See Mayakis, \textit{supra} note 38, at 161 (even the “more basic models of modern cell phones have the technological capabilities of storing and transmitting exponentially greater amounts of private information than that of a pager or any traditional closed container”) (citation omitted).
\textsuperscript{158} Belton, 453 U.S. at 460 n.4.
\textsuperscript{159} Eames, \textit{supra} note 33, at 499.
\textsuperscript{160} Id.
\textsuperscript{161} Id.
\textsuperscript{162} Knott, 460 U.S. at 457.
\textsuperscript{163} See United States v. Park, No. CR 05–375 SI, 2007 WL 1521573, at *9 (N.D. Cal. May 23, 2007); see also Eames, \textit{supra} note 33, at 499 (“cell phone searches potentially expose to public scrutiny almost limitless information of the most private nature”).
thoughts and conversations on their cell phones through email and text, voice and instant messages.\(^{164}\)

As a result, “cell phones have quickly become a storehouse of sorts for holding such information as private correspondence, photographs, personal thoughts, and in some cases even the personal information of others.”\(^{165}\) This, in turn “increases the likelihood that highly personal information, irrelevant to the subject of the lawful investigation, will also be searched or seized.”\(^{166}\)

Thus, “[a]lthough information of this nature can now be stored electronically, in the past such information has traditionally been stored in one's home office or desk and given protection by the Fourth Amendment.”\(^{167}\) In his dissent in *United States v. Seljan*, Judge Alex Kozinski acknowledged as follows:

> The reference to papers [in the Fourth Amendment] is not an accident; it's not a scrivener's error. It reflects the Founders' deep concern with safeguarding the privacy of thoughts and ideas--what we might call freedom of conscience--from invasion by the government. . . .
> 
> . . . [T]he Founders were as concerned with invasions of the mind as with those of the body, the home or personal property--which is why they gave papers equal rank in the Fourth Amendment litany. . . . Papers contain people's most personal information . . . “sealed up in silence, not to be broke, but with their own heart-strings,” so that “some men would rather die” than submit to having their papers searched.\(^{168}\)

Moreover, “categorizing the contents of a cell phone as ‘papers’ not only implicates the Fourth Amendment but could also raise serious First Amendment concerns.”\(^{169}\) In *Seljan*, Judge Kozinski further stated:

---

165 Knott, *supra* note 149, at 452 (emphasis added).
167 Knott, *supra* note 149, at 452 (explaining that “the Fourth Amendment not only guarantees that people will be secure in their ‘persons,’ ‘houses,’ and ‘effects,’ but also expressly ensures that people will be secure in their ‘papers’”).
168 *Id.* at 456 (quoting *United States v. Seljan*, 547 F.3d 993, 1014 (9th Cir. 2008)) (Kozinski, J., dissenting) (emphasis added), *cert. denied*, 129 S. Ct. 1368 (2009)
The Founding generation recognized that the seizure of private papers . . . undermines freedom of speech. . . . [T]he chill on speech that would result from failing to protect personal correspondence . . . would . . . “compel everyone in self-defense to write even to his dearest friends with the cold and formal severity with which he would write to his wariest opponents or his most implacable enemies.”

If, for example, law enforcement were allowed to search in any “room” of a cell phone, an individual might think twice before sending a text message or downloading a video about terrorism. Such a “chilling effect” on free speech cannot be tolerated under the First Amendment or more broadly accepted notions of liberty. For these reasons, a cell phone cannot be categorized as a mere physical object.

In many ways, cell “phones” are not phones at all. They are an amalgamation of so many things that have historically been considered essential to free expression, and accorded the highest degree of constitutional protection. Searching cell phone’s memory is, in essence, searching persons and their “papers.” It gives law enforcement license to forage through an individual’s private life—and mind.

C. THE “SEIZE BUT DON’T SEARCH” DOCTRINE—PROTECTING AGAINST THE DESTRUCTION OF EVIDENCE WHILE SAFEGUARDING PRIVACY.

The “seize but don’t search” doctrine is the logical outcome of digital era rulings where the Court hinted that the search incident to arrest doctrine had been stretched “beyond its breaking point,” The approach would: (1) allow law enforcement to seize an arrestee’s cell

---

170 Id. at 457 (quoting Seljan, 547 F.3d at 1018 (Kozinski, J., dissenting) (quoting 2 JOSPEH STORY, COMMENTARIES ON EQUITY JURISPRUDENCE 251 (13th ed., Boston: Little, Brown and Co. 1886)); see also Charles E. MacLean and Adam Lamparello, Abidor v. Napolitano: Suspicionless Cell Phone and Laptop “Strip Searches” At the Border Compromise the Fourth and First Amendments, 108 NORTHWESTERN UNIV. L. REV. COLLOQUIY (forthcoming Spring 2014).
171 See, e.g., Conor M. Reardon, Cell Phones, Police Recording, and the Intersection of the First and Fourth Amendments, 63 DUKE L.J. 735, 776-77 (2013).
172 Butterfoss, supra note 21, at 77.
phone; (2) require a warrant and probable cause to search the phone’s contents; and (3) provide a narrow exception for imminent exigencies that threaten life or safety.

The Supreme Court has already inched in this direction. In *Gant*, for example, police arrested the defendant for driving with a suspended license.\(^\text{173}\) While the defendant was handcuffed and in the back of a police car, law enforcement searched his car and found a jacket containing cocaine.\(^\text{174}\) The Court held that the search was improper because the officers’ safety was not at risk,\(^\text{175}\) and, because they had no reason “to believe evidence relevant to the crime of arrest might be found in the vehicle.”\(^\text{176}\) In so holding, the Court narrowed its prior decision in *New York v. Belton*,\(^\text{177}\) which had endorsed a bright-line rule permitting law enforcement to search the entire interior of automobiles (except the trunk) following a valid arrest. The majority recognized that, where neither of the *Chimel* justifications is present, law enforcement may not search a vehicle’s interior without probable cause.\(^\text{178}\)

Under the “seize but don’t search” paradigm, the Court should first recognize that individuals have an objectively reasonable expectation of privacy in the contents of their cell phones.\(^\text{179}\) Seizing the phone is permissible because it would prevent an arrestee from destroying evidence or coordinating with third parties to remotely delete the cell phone’s memory. Searching it, however, without a warrant and probable cause “would give authorities an open door into the most private details of an arrestee’s life.”\(^\text{180}\)

\(^{173}\) 129 S. Ct. at 1714.

\(^{174}\) Id.

\(^{175}\) Id. at 1719 (a search of the passenger compartment would only be permissible if “the arrestee is unsecured and within reaching distance of the passenger compartment at the time of the search”).

\(^{176}\) Id. (quoting Thornton v. United States, 541 U.S. 615, 632 (2004)) (Scalia, J., concurring in the judgment).

\(^{177}\) 453 U.S. 454 (1981); see also Gershowitz, *supra* note 152, at 1133. (discussing *Belton*).

\(^{178}\) See Gershowitz, *supra* note 152, at 1133

\(^{179}\) Casenote, Criminal Procedure – Fourth Amendment – Florida Supreme Court Holds that Cell Phone Data is Not Subject to the Search-Incident-to-Arrest Exception – Smallwood v. State 113 So. 3d 724 (Fla. 2013), 127 HARV. L. REV. 1059, 1064-65 (2014).

\(^{180}\) Id. at 1064.
1. IMMINENT EXIGENCIES: THE NARROW EXCEPTION

Wurie mentioned, but did not resolve, the issue of when warrantless searches of a cell phone’s memory might be permissible. The answer to this question, and the one exception to a “seize but don’t search” approach, is the narrow situation where exigent circumstances exist. Exigencies are likely to arise where law enforcement officers have an objectively reasonable belief that: (1) a cell phone’s memory will be remotely deleted; and (2) a crime is ongoing, and imminent threats to persons exist.

a. REMOTE DELETION

With respect to the remote deletion problem, “[m]any courts have reasoned that a search of a cell phone or personal electronic device incident to arrest is lawful because it is a situation where an officer needs to preserve evidence from destruction.” As discussed in Part II, however, “[r]apid improvements in technology … have obviated the … concern[]” that “incoming calls or messages will replace recent calls or messages in a phone’s memory.” Indeed, modern cell phones “no longer store only a handful of recent text messages and phone calls and greatly expanded digital memories eradicate any real risk of automatic deletion.” Furthermore, since the possibility of remote deletion is unlikely—particularly if police seize the cell phone—law enforcement should be required to demonstrate an actual and objectively

---

181 See Dee, supra note 24, at 1160 (a court deciding whether a particular warrantless cell phone search was lawful should engage in only one colloquy--whether there were exigent circumstances justifying the search, specifically, whether information on the cell phone was actually subject to remote deletion at the moment of the search”); see also Beutler, supra note 27, at 393 (the exigent circumstances exception “requires the reasonable belief by a law enforcement officer that evidence is in imminent danger of being removed or destroyed”).

182 Beutler, supra note 27, at 394.

183 Id.

184 Id. at 394 (citing United States v. Gomez, 807 F. Supp. 2d 1134, 1150 n.17 (S.D. Fla. 2011)), which stated as follows:

We tend to agree with this position and recognize the ever-weakening argument that a modern cell phone, with its continually advancing technology, is at any risk of deleting its call history or text messages folder to make space for incoming calls or text messages--the memory capacity of a cell phone is far, far greater than that of an analogized two-decade older pager.
reasonable belief that such a risk was present.\textsuperscript{185} Without this standard, law enforcement could base warrantless cell phone searches on broad and unsubstantiated concerns that would not otherwise be covered under a recognized exception.

b. **ONGOING CRIMINAL CONDUCT—IMMINENT THREATS TO LIFE OR SAFETY**

Where law enforcement officers have an objectively reasonable belief that an “immediate threat to life or safety”\textsuperscript{186} exists, they should be entitled to search a cell phone without a warrant.

One scholar explains the exigent circumstances exception as follows:

> [P]olice may enter premises and conduct a search without a warrant “to provide emergency assistance to an occupant,” or to “enter a burning building to put out a fire and investigate its cause.” In such cases, the law not only dismisses the warrant requirement—in appropriate circumstances, the police may act even in the absence of probable cause.\textsuperscript{187}

Of course, to invoke this exception, an officer “must have had probable cause for the intrusion,”\textsuperscript{188} or, as applied to the cell phone context, the valid arrest.

Furthermore, to prevent the exception from swallowing the rule, law enforcement must demonstrate that the exigency presented an imminent threat to the life or physical safety of

\textsuperscript{185} Beutler, \textit{supra} note 9, at 394 (citing United States v. Rodriguez-Gomez, No. 1:10-CR-103-2-CAP, 2010 WL 5524891, at *3 (N.D. Ga. Nov. 15, 2010)), and Gomez, 807 F. Supp. 2d at 1150, n. 17) (in Rodriguez-Gomez, the court found that the law enforcement officer had provide sufficient evidence of remotely deletion, “thus implicating the need to preserve evidence”). In Gomez, however, the court held that law enforcement had not made the requisite showing:

> [T]he agents never proffered evidence to support an objective belief that the cell phone's call log history was ever at risk of being lost or destroyed. In fact, while agents testified to their speculation that a cell phone could theoretically be ‘wiped’ remotely by an unknown third party, each agent testified that they had no reason to believe that Defendant's specific cell phone was capable of remote deletion.

\textsuperscript{186} Clifford S. Fishman, \textit{Searching Cell Phones After Arrest: Exceptions to the Warrant and Probable Cause Requirements}, 65 \textit{Rutgers L. Rev.} 995, 1002 (2013); see also Eunice Park, \textit{Traffic Ticket Reasonable, Cell Phone Search Not: Applying the Search-Incident-To-Arrest-Exception to the Cellphone as Hybrid}, 60 \textit{Drake L. Rev.} 429, 488 (2012) (“Exigent circumstances arise when the inevitable delay incident to obtaining a warrant must give way to a need for immediate action”) (quoting United States v. Forker, 928 F.2d 365, 368 (11th Cir. 1991)).

\textsuperscript{187} Id., at 1003.

\textsuperscript{188} Id. at 1003-04.
others. Otherwise, law enforcement might interpret “safety” in a manner that encompasses any threat, no matter how attenuated or speculative. This exception would apply in situations where law enforcement has an objectively reasonable belief that: (1) criminal behavior is ongoing; (2) a specific intent to harm others is present; and (3) the harm, including loss of life, is likely to occur; and (4) the search is limited to areas that are likely to uncover evidence relating to the exigency. In some situations, this may include initiating or responding to a call or text message, or reviewing the arrestee’s recent phone calls or emails. It will not ordinarily (and perhaps never), include a search of, for example, the arrestee’s Google search history or purchases on Amazon.com. Additionally, the search must cease when the exigency dissipates, or when officers discover evidence—in the cell phone or elsewhere—that allows them to effectively address the problem. Simply stated, law enforcement officers must act reasonably. If a search exceeds the narrow parameters delineated above, any resulting evidence should be suppressed at trial.

2. THE “REASONABLE RELATIONSHIP” DOCTRINE IS UNWORKABLE

Searches should not be allowed simply because the cell phone may contain evidence related to the crime of arrest. The risk that officers will simply rummage through all “rooms” of the cell phone in an unfettered search for evidence far outweighs the convenience to law enforcement. Furthermore, given the minimal, even non-existent, risk that a cell phone’s memory will be destroyed, there exists no reason whatsoever that could justify such a search.

---

189 Id. at 1004-05 (discussing the scope of cell phone searches when officers are faced with exigent circumstances).
190 United States v. Knights, 534 U.S. 112, 118 (2001) (stating that the Court examines the “totality of the circumstances” to decide if a search is reasonable within the meaning of the Fourth Amendment”).
The second problem relates to the nexus between the crime of arrest and a search of the cell phone’s memory. An individual arrested for possessing images of child pornography, for example, may certainly have images stored in the cell phone. A warrantless search of the cell phone’s memory, however, cannot be considered reasonable under the Fourth Amendment because it leads to more questions—and potential violations of privacy—than answers. For example, would law enforcement be limited to searching the suspect’s incoming and outgoing calls, along with documents that have been downloaded, or can they search the suspect’s Facebook page, Twitter account, and purchases on Amazon.com?

Likewise, if an individual is arrested for possessing marijuana, can law enforcement examine that individual’s Google searches, make a record of that individual’s Facebook friends, and analyze every text message that individual sent for the last six months? These questions highlight the temporal and spatial problems raised by vesting law enforcement with this kind of discretion. The resulting uncertainty would increase the likelihood of unnecessarily invasive and arbitrary searches, without any countervailing interest to justify dispensing with the warrant requirement. Procuring a warrant will allow a magistrate judge to confine the scope of every search, and describe with particularity the areas of a cell phone that are properly subject to a search.\textsuperscript{192}

For similar reasons, courts should not embroil themselves in a hyper-technical parsing of the specific areas within a cell phone where an individual enjoys an objective expectation of privacy and is thus entitled to Fourth Amendment protection. Given the rapid pace at which technology advances, this approach would invite the same problems as those found in pre-digital case law: courts would create rules without knowing the extent to which cell phones may evolve

\textsuperscript{192} See Fabio Arcila, Jr., The Death of Suspicion, 51 WM. & MARY L. REV. 1275, 1294 (2010) (quoting the Fourth Amendment’s requirement that “no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized”) (emphasis added).
C
ONCLUSION

The text and original meaning of the Fourth Amendment give individuals a reasonable expectation of privacy in their papers and effects, regardless of whether they are locked in a safe or stored on a cell phone. Technological advances do not give law enforcement the right to breach the constitutional separation between privacy and state action. The divide is there for a reason: to give individuals the freedom to engage in self-expression without the unnerving fear that the government may eavesdrop if they are arrested for, say, a misdemeanor traffic offense. Up to this point, however, the lower courts have largely relied on decades-old case law and principles of *stare decisis* to tear down the privacy wall. Decisions such as *Riley* have threatened to make privacy as obsolete as pre-digital era case law, and transform the privacy epidemic into a virulent cancer.

For that reason, much depends on the Court overturning *Riley*, and embracing *Wurie’s* reasoning. The Court’s decision will have ramifications that extend far beyond cell phones and containers, influencing the Government’s approach to border searches and surveillance. Ironically, the path to the future sits at the beginning, in a place where one words speaks for millions: reasonableness.