Printed in U.S.A.
Vol. 111, No. 2

RILEY AND ABANDONMENT: EXPANDING FOURTH AMENDMENT PROTECTION OF CELL PHONES

Abigail Hoverman

ABSTRACT—In light of the privacy concerns inherent to personal technological devices, the Supreme Court handed down a unanimous decision in 2014 recognizing the need for categorical heightened protection of cell phones during searches incident to arrest in *Riley v. California*. This Note argues for expansion of heightened protections for cell phones in the context of abandoned evidence because the same privacy concerns apply. This argument matters because state and federal courts have not provided the needed protection to abandoned cell phones pre- or post-*Riley*.

AUTHOR—J.D., Northwestern University School of Law, 2017; B.A., University of Notre Dame, 2014. I would like to thank Professor Tonja Jacobi for sparking my interest in the interplay between the Fourth Amendment and technology, and for her advice in developing this topic. Additional thanks to the members of the *Northwestern University Law Review* who helped me write and edit this Note and added invaluable improvements, especially Brenna Helppie-Schmieder and Andy Rodheim. Any errors herein are my own.

INTRODUCTION 518
I. ABANDONMENT DOCTRINE 520
A. Katz *and the Origins of the Abandonment Exception* 521
B. *Modern Abandonment Doctrine* 523
II. THE CASE OF *RILEY V. CALIFORNIA* 527
A. Riley*'s Reasoning* 529
B. *Scholarly Reaction to* Riley 533
III. CURRENT TREATMENT OF ABANDONED CELL PHONES 535
A. *Federal Cases* 535
B. *State Cases* 539
IV. EXPANSION OF *RILEY*'S CELL PHONE PROTECTIONS TO ABANDONED PHONES 543
A. *The Mismatch Between Abandonment Doctrine and Cell Phones* 543
B. *What* Riley *Revealed About Justifications for Warrantless Searches* 547
C. *Protection for All Types of Cell Phones Including "Burner Phones"* 550
V. EXPANSION OF *RILEY*'S PROTECTIONS TO OTHER PERSONAL DEVICES 552
CONCLUSION 553

*Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans "the privacies of life." The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—**get a warrant**.*

—Chief Justice John Roberts[†]

INTRODUCTION

The majority of Americans keep a cell phone on their persons at all times. In effect, a treasure trove of personal information can be uncovered in minutes, including a person's internet search history, hundreds of text messages and e-mails, photos, GPS and map history, and even bank information, dating back months and even years, creating a serious threat to privacy if these devices are opened without permission.[1] Fourth

[†] Riley v. California, 134 S. Ct. 2473, 2494–95 (2014) (emphasis added) (citation omitted) (quoting Boyd v. United States, 111 U.S. 616, 630 (1886)).

[1] Research suggests that smartphone owners use their phones to access personal information: over the course of a year of smartphone use, 62% of users access health information, 57% do online banking,

Amendment jurisprudence has been slow to adapt to modern technology and to protect the vast amount of data and information people have on their cell phones that an unlawful search or seizure can uncover. In an important step towards the protection of easily accessible personal data, in 2014, the Supreme Court held in *Riley v. California* that officers can no longer search through cell phones during searches incident to arrest.[2] The opinion articulated that cell phones are different from other objects "kept on an arrestee's person" because of the digital data they contain:

> Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse. . . . Prior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day.[3]

While *Riley* took an important step in recognizing the unique privacy threats cell phones pose, based on the same logic, special protections for these devices should be expanded to other areas of criminal procedure. This Note argues that heightened protection for cell phones should expand beyond the context of search incident to arrest to the doctrine of abandoned property. When investigating a crime or following a suspect, courts generally consider any property left behind as unprotected by the Fourth Amendment because the item's former owner lost all expectation of privacy by discarding the object.[4] Just as police cannot search through a person's cell phone incident to an arrest, police should be similarly barred from opening a person's cell phone that has been left behind. Furthermore,

---

44% look up real estate listings, and 40% look up government services. PEW RESEARCH CTR., U.S. SMARTPHONE USE IN 2015 5 (2015), http://www.pewinternet.org/files/2015/03/PI_Smartphones_0401151.pdf [https://perma.cc/SP4K-SMFW]. Smartphone users, especially those between the ages of eighteen and twenty-nine, regularly use their devices for transportation: 80% of these users use their phones for turn-by-turn navigation, 38% use them for public transit information, and 17% use them to reserve taxis or car services. *Id.* at 23. In the course of one week, 97% of smartphone owners send text messages, 92% make voice or video calls, 89% access the internet, 88% send and receive e-mail, and 60% take pictures or videos. *Id.* at 33.

[2] 134 S. Ct. at 2495. Searches incident to arrest represent a well-accepted exception to the warrant requirement, allowing officers to search "the arrestee's person and the area 'within his immediate control'" including "the area from within which he might gain possession of a weapon or destructible evidence." Chimel v. California, 395 U.S. 752, 763 (1969). The Supreme Court construed the appropriate boundaries of a search incident to arrest to allow officers to search inside containers on the arrestee's person (such as cigarette boxes), inside the passenger compartment of an arrestee's vehicle, and inside any containers inside that vehicle, presuming requisite reasonable suspicion that those containers would contain evidence. *See* Arizona v. Gant, 556 U.S. 332, 335 (2009); United States v. Robinson, 414 U.S. 218, 231–36 (1973).

[3] *Riley*, 134 S. Ct. at 2488–90. The majority opinion was joined by eight Justices. *Id.* at 2479. Justice Alito filed a separate opinion concurring in part and concurring in the judgment. *Id.* at 2495 (Alito, J., concurring in part and concurring in the judgment).

[4] *See infra* Section I.B.

the case law establishing the abandonment theory should not apply to cell phones because the nature of the information contained in a phone is completely different than the information that can be gleaned from trash, illegal drugs, or weapons left behind in traditional abandonment cases both in sensitivity and quantity.

This Note begins by examining foundations of the abandonment exception to the Fourth Amendment, including the test for when property should be ruled abandoned. Part II considers *Riley v. California*, examining why the Supreme Court determined cell phones are different and deserve heightened protections through warrants. This Part also explores how scholars have reacted to *Riley*, both by acknowledging the significance of the expansion of Fourth Amendment protection to include digital data and by attempting to expand this protection to other areas of the law beyond searches incident to arrest. This Note follows previous scholars who have advocated for expanded protection of personal digital devices, but unlike other scholarship, argues this protection should apply to abandoned cell phones. Part III examines how state and federal courts have treated left-behind or abandoned cell phones just like any other tossed contraband or container.

Part IV of this Note then analyzes why the holding in *Riley* should expand categorical protection of cell phones to include abandoned phones and explores the implications of forbidding warrantless searches of abandoned cell phones. This Part addresses why this protection should extend to both smartphones and less advanced "flip phones," considers whether passcodes affect the expectation of privacy in the contents of a cell phone, and acknowledges concerns about the possible hindrance of the police's ability to pursue suspects and fight crime. This Note argues apprehensions about police effectiveness can be addressed through *Riley*'s articulation of the "exigent circumstances" exception, allowing officers to search abandoned cell phones in extremely time-sensitive situations.

I. ABANDONMENT DOCTRINE

Under the Fourth Amendment, courts presume searches conducted without prior approval of a judge through a warrant are per se unreasonable.[5] However, Fourth Amendment jurisprudence has recognized a number of exceptions to the warrant requirement, including exceptions for searches incident to arrests and evidence abandoned by its owner.[6] This

[5] *Gant*, 556 U.S. at 338 (citing Katz v. United States, 389 U.S. 347, 357 (1967)).

[6] *Id.* (discussing the search incident to arrest exception); Abel v. United States, 362 U.S. 217, 241 (1960) (discussing the exception for evidence abandoned by its owner).

Part examines the origin and modern applications of the abandonment exception before exploring how courts have specifically treated abandoned cell phones in Part III.

A. Katz *and the Origins of the Abandonment Exception*

The Fourth Amendment protects the public against unreasonable searches and seizures at the hands of the government.[7] However, the courts have deemed only *certain* actions to constitute "searches" within the meaning of the Fourth Amendment. If an intrusion is not a search, any protections requiring a warrant or probable cause to search no longer apply, and the defendant cannot contest the admission of that evidence to be used against him or her at trial.[8]

Courts have established that an officer's search of abandoned property is not a search for Fourth Amendment purposes.[9] To determine which types of police actions are not protected searches, instead of focusing on the definition of a search, early Supreme Court abandonment cases refer to principles of property law that allow police to seize abandoned evidence.[10] As early as 1924 in *Hester v. United States*, the Supreme Court established that no Fourth Amendment search or seizure occurs when evidence is "abandoned" by a "defendant's own acts."[11] In 1960, the Court reaffirmed *Hester* by refusing to suppress a hollowed out pencil and a pad of paper discovered in a trash can in the defendant's hotel room during a federal espionage investigation after the defendant "paid his bill and vacated the room."[12] The Court found these items admissible and lawfully seized because the defendant "had abandoned these articles" and "thrown them away."[13] The Court reasoned, "[s]o far as [the defendant] was concerned, they were *bona vacantia*. There can be nothing unlawful in the Government's appropriation of such abandoned property."[14] Although neither case explored the basis for this reasoning, the Court's reference to "*bona vacantia*," a common law principle allowing ownerless property to

---

[7] U.S. CONST. amend. IV ("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 . . . .").

[8] *See* Edward G. Mascolo, *The Role of Abandonment in the Law of Search and Seizure: An Application of Misdirected Emphasis*, 20 BUFF. L. REV. 399, 400–01 (1971).

[9] *See, e.g.*, *Abel*, 362 U.S. at 241; United States v. Colbert, 474 F.2d 174, 176 (5th Cir. 1973).

[10] *See e.g.*, Hester v. United States, 265 U.S. 57, 58 (1924).

[11] *Id.* at 58 (holding no search or seizure occurred when officers investigating a "moonshine" operation examined a glass jug, jar, and bottle abandoned in an open field).

[12] *Abel*, 362 U.S. at 240–41.

[13] *Id.* at 241.

[14] *Id.* (citing *Hester*, 265 U.S. at 57–58).

be claimed by the finder or taken by the state, suggests reliance on the treatment of abandoned and ownerless property as extinguishing the previous owner's Fourth Amendment rights protecting the property.[15]

The abandonment doctrine shifted from property rights[16] to focus on the definition of a search after the Supreme Court provided the modern test for a search in *Katz v. United States*, requiring both subjective and objective reasonable expectations of privacy.[17] To be a Fourth Amendment search, an intrusion must violate a personal "expectation of privacy . . . that society is prepared to recognize as 'reasonable.'"[18] Generally, behaviors and belongings in the home carry both subjective and objective expectations of privacy, but those same activities and belongings in public in the plain view of outsiders are no longer protected because it would be unreasonable to presume they would be kept private.[19] Accordingly, "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[20]

Following *Katz*, the Supreme Court redefined the abandonment doctrine by applying the reasonable expectation of privacy test to property left in the open in *California v. Greenwood*.[21] Here, the Court considered

---

[15] *See Bona Vacantia*, BLACK'S LAW DICTIONARY (10th ed. 2014) (defining "*bona vacantia*" as (1) "[p]roperty not disposed of by a decedent's will" or (2) "[o]wnerless property; goods without an owner," and noting that "*[b]ona vacantia* often resulted when a deceased person died without an heir willing and able to make a claim" such that "[t]he property either belonged to the finder or escheated to the Crown"); *see also* RESTATEMENT (THIRD) OF PROP.: SERVITUDES § 7.4 (AM. LAW INST. 2000) ("A servitude benefit is extinguished by abandonment when the beneficiary relinquishes the rights created by a servitude.").

[16] *See, e.g.*, United States v. Lewis, 921 F.2d 1294, 1302 (D.C. Cir. 1990) ("Abandonment for purposes of the Fourth Amendment differs from abandonment in property law; here, the analysis examines the individual's reasonable expectation of privacy, not his property interest in the item.").

[17] 389 U.S. 347, 352 (1967) (holding that a conversation held behind closed doors of a telephone booth carries an expectation of privacy because the speaker presumes outsiders cannot hear).

[18] *Id.* at 361 (Harlan, J., concurring).

[19] *Id.*

[20] *Id.* at 351 (majority opinion). For example, the third-party doctrine states that a defendant transmitting information in person or over the phone to a third party, like an undercover agent or company, has no expectation of privacy, even if those conversations occur within a defendant's home. Smith v. Maryland, 442 U.S. 735, 744–45 (1979) (holding that the defendant had no expectation of privacy over phone numbers dialed from a home phone recorded by a pen register because the information is already communicated to the telephone company); United States v. Miller, 425 U.S. 435, 442 (1976) (holding that a bank depositor had no legitimate expectation of privacy in financial information "voluntarily conveyed to the banks and exposed to their employees"); United States v. White, 401 U.S. 745, 751–53 (1971) (plurality opinion) (holding that a defendant's conversations with an undercover agent in his home were unprotected because there was no expectation of privacy when the defendant willingly shared information with another).

[21] 486 U.S. 35 (1988).

whether trash left outside the curtilage[22] of the home receives Fourth Amendment protection.[23] The Court did not dispute that the Greenwoods may have had a subjective expectation of privacy based on the opaque quality of the bags and the family's belief that neither the public nor the police would go through the contents of the bags before the garbage collectors removed them.[24] However, the Court rejected the idea that the expectation of privacy would be accepted by society as "objectively reasonable."[25] Justice White reasoned, "It is common knowledge that plastic garbage bags left on or at the side of a public street are readily accessible to animals, children, scavengers, snoops, and other members of the public," and that people leave trash on the curb "for the express purpose of conveying it to a third party, the trash collector," who could easily sort through the trash.[26] Accordingly, because society would not find it reasonable to expect privacy in garbage left outside as it is obviously vulnerable to "public inspection," the Greenwoods had no reasonable expectation of privacy, and the Fourth Amendment did not protect their trash.[27] This analysis of objectively reasonable expectations of privacy based on societal expectations remains central to abandonment analysis.

B. Modern Abandonment Doctrine

Greenwood continues to offer the most extensive Supreme Court consideration of the abandonment doctrine.[28] As *Greenwood* articulates, the

---

[22] Curtilage is the area surrounding the home, or the "land or yard adjoining a house, usu[ally] within an enclosure." *Curtilage*, BLACK'S LAW DICTIONARY (10th ed. 2014). The outer borders of the curtilage of a home define how far the privacy of the home extends beyond the four walls of a home, which can affect Fourth Amendment expectation of privacy analysis. *See*, *e.g.*, United States v. Dunn, 480 U.S. 294, 301 (1987) ("[C]urtilage questions should be resolved with particular reference to four factors: the proximity of the area claimed to be curtilage to the home, whether the area is included within an enclosure surrounding the home, the nature of the uses to which the area is put, and the steps taken by the resident to protect the area from observation by people passing by.").

[23] *Greenwood*, 486 U.S. at 37. In this case, the defendants moved to suppress evidence of narcotics use found by police in a plastic garbage bag left on the curb outside the defendant's home for collection. *Id.* at 37–38. The search was conducted without a warrant, and no court concluded the officer had probable cause to conduct the search. *Id.* at 45 (Brennan, J., dissenting). The Court applied the following test: a "warrantless search and seizure of the garbage bags left at the curb outside the Greenwood house would violate the Fourth Amendment only if respondents manifested a subjective expectation of privacy in their garbage that society accepts as objectively reasonable." *Id.* at 39 (majority opinion).

[24] *Id.* at 39.

[25] *Id.* at 39–40.

[26] *Id.* (footnote omitted).

[27] *Id.* at 40–41.

[28] *See* Maureen E. Brady, *The Lost "Effects" of the Fourth Amendment: Giving Personal Property Due Protection*, 125 YALE L.J. 946, 962 (2016).

modern abandonment analysis generally focuses on abandonment as "intentional relinquishment of [the privacy] expectation with regard to the property in question."[29] This analysis focuses on an intent to abandon, "to be inferred from the words and actions of the parties and other circumstances" indicating a lack of privacy expectations over a discarded item, instead of focusing on the common law concepts of property abandonment.[30] A general iteration of the abandonment test asks if a person voluntarily and knowingly left an item behind so that he "relinquished his interest in the property in question so that he could no longer retain a reasonable expectation of privacy with regard to it,"[31] a requirement easily met if the property is discarded in a public place.[32]

One of the most common applications of the abandonment doctrine in criminal proceedings occurs when a suspect anticipating interactions with police throws, drops, or discards an "incriminating item" or other contraband.[33] This can occur in a variety of "police-approach" circumstances, but the central thread of these cases involves an attempt to hide illegal or incriminating evidence from police before being questioned or arrested.[34] For example, courts have found abandonment of evidence when defendants threw a gun down an alley while running away from an

[29] John P. Ludington, *Search and Seizure: What Constitutes Abandonment of Personal Property Within Rule That Search and Seizure of Abandoned Property Is Not Unreasonable—Modern Cases*, 40 A.L.R. 4th 381, § 2(a) (1985) (providing an updated, substantial list of federal and state cases across the country involving abandonment of evidence, none of which include abandonment of cell phones). This Note focuses on a general view of abandonment doctrine nationally, as state supreme courts and constitutions often adopt different nuances to their criminal procedure doctrine, affording defendants more or fewer protections against unreasonable searches and seizures.

[30] *Id.* Because of the requirement of voluntary relinquishment, a bad act preceding the relinquishment like theft or police misconduct can render the abandonment involuntary. *See* State v. Dixon, No. 13-09-00445-CR, 2010 WL 3419231, at *7–9 (Tex. App. Aug. 27, 2010) (holding that a cell phone could not be abandoned because the phone was stolen and the owner accordingly did not intentionally relinquish ownership of the device even though he did not try to reclaim his phone for weeks after the theft).

[31] United States v. Colbert, 474 F.2d 174, 176 (5th Cir. 1973) (en banc). Note that any abandonment that "results directly from police misconduct, such as an illegal search or seizure, deceit, or, perhaps, a pattern of harassment" may not be voluntary. United States v. Lewis, 921 F.2d 1294, 1302 (D.C. Cir. 1990).

[32] *See, e.g.*, City of St. Paul v. Vaughn, 237 N.W.2d 365, 371 (Minn. 1975) ("Where the presence of the police is lawful and the discard occurs in a public place where the defendant cannot reasonably have any continued expectancy of privacy in the discarded property, the property will be deemed abandoned for purposes of search and seizure." (footnotes omitted)). Note that the court clarifies that the defendant does not need to intend to relinquish ownership, just abandon a reasonable expectation of privacy. *Id.*

[33] Ludington, *supra* note 29, § 2(a).

[34] *Id.*

officer,[35] dropped a plastic baggie of narcotics on the sidewalk while walking away from police,[36] left credit cards and receipts tucked into the headrest of a police squad car after being arrested,[37] flushed drugs down the toilet in police presence,[38] and threw marijuana or narcotics out of a car window while being followed by police.[39] *Greenwood*-style cases involving trash left outside homes[40] or dropped in the trash can of another person or business[41] also often result in abandoned evidence. The abandonment reasoning has even been extended to consider hair clippings discarded after voluntarily getting a haircut abandoned when the person does not express a desire to keep the dropped pieces of hair.[42] Abandonment has been found in a tremendous variety of circumstances, but this list provides a cross-sampling of these cases to demonstrate that abandonment usually involves attempts to stash or get rid of incriminating items like drugs or weapons, usually in anticipation of contact with police, or at least intentionally throwing something away without intent to maintain ownership over the discarded item.

Finally, it should be noted that the abandonment doctrine extends to the opening and searching of discarded containers, from paper bags[43] to abandoned rented rooms;[44] as long as the possessor voluntarily left the container behind, the container and its contents lose Fourth Amendment protections.[45] This principle applies to small containers like suitcases[46] and

---

[35] People v. Gayden, 4 N.Y.S.3d 806, 806–07 (App. Div. 2015).

[36] State v. Eaton, 707 S.E.2d 642, 647 (N.C. Ct. App. 2011).

[37] United States v. Wai-Keung, 845 F. Supp. 1548, 1559 (S.D. Fla. 1994).

[38] Nelson v. State, 286 S.E.2d 504, 505–06 (Ga. Ct. App. 1981); Clapp v. State, 639 S.W.2d 949, 952–53 (Tex. Crim. App. 1982) (en banc), *overruled by* Comer v. State, 754 S.W.2d 656 (Tex. Crim. App. 1986) (en banc).

[39] United States v. McLaughlin, 525 F.2d 517, 519–20 (9th Cir. 1975) (admitting evidence of marijuana thrown out of car window during a chase); United States v. Morquecho, 474 F. Supp. 1134, 1140–41 (S.D. Tex. 1979) (admitting into evidence a paper bag of cocaine that was thrown out of a window into a ditch during a chase).

[40] United States v. Crowell, 586 F.2d 1020, 1025 (4th Cir. 1978).

[41] People v. Mora, 691 N.Y.S.2d 531, 532 (App. Div. 1999) (finding no legitimate expectation of privacy after defendant threw two loaded guns and cocaine into a dumpster on a construction site).

[42] United States v. Cox, 428 F.2d 683, 687–88 (7th Cir. 1970) (finding no search or seizure when hair clippings from ordinary, voluntary prison haircut were seized without warrant).

[43] *Morquecho*, 474 F. Supp. at 1141.

[44] Feguer v. United States, 302 F.2d 214, 249 (8th Cir. 1962).

[45] Abel v. United States, 362 U.S. 217, 241 (1960) (finding that an occupant of a hotel room abandoned contents of the hotel room and trash can inside the hotel room after having time to pack his suitcases, pay the hotel bill, and vacate the room, allowing officers to seize contents of the room without a search or seizure).

[46] People v. Long, 86 Cal. Rptr. 227, 231–32 (Ct. App. 1970) (allowing police to search inside an abandoned suitcase left behind in a motel for evidence of theft). *But see* United States v. Jackson,

eyeglass cases,[47] allowing the abandoned containers to be searched because once abandoned, the loss of expectation of privacy applies to both the case itself and anything inside. The abandonment of containers also allows police to search the inside of much larger containers, like whole rooms.[48] For example, courts have held it constitutional for police to search a rented room after the lease had expired, deeming the rented room vacated and abandoned once rent payment ceased, and allowing the search and seizure of personal papers and receipts found inside.[49] Courts have also held hotel rooms and their entire contents to be abandoned after an occupant checks out, leaving personal objects behind.[50]

In many ways, Fourth Amendment abandonment doctrine has failed to keep up with technical innovations and needs to be adapted to recognize the vast amount of information small containers can now hold. One such area involves abandoned DNA.[51] Decades of abandonment jurisprudence allow police to seize discarded evidence—like a cigarette butt, spit on a sidewalk, or utensils used at a restaurant—and then test the DNA on those abandoned items against evidence from unsolved crimes.[52] For example, Los Angeles police solved a series of murders after retrieving DNA from a coffee cup of Adolph Laudenberg, a man the police had long suspected of the crimes but against whom the police had no evidence.[53] In this type of case, courts encountering the admissibility of abandoned DNA often use *Greenwood*'s analysis of abandoned property and trash, concluding there is no expectation of privacy in bodily fluids "left behind on a coffee cup or on a smoked cigarette," as the objects and the genetic information are "'knowingly exposed' to the public."[54] Essentially, because abandonment

544 F.2d 407, 410 (9th Cir. 1976) (holding that a suitcase was not abandoned when a defendant took three steps away from the suitcase after setting it on the floor because of lack of intent to abandon).

[47] City of St. Paul v. Vaughn, 237 N.W.2d 365, 370–71 (Minn. 1975) (holding an eyeglass case was abandoned after it was discarded behind the counter of a dry cleaner, and allowing the police to open the case to find a syringe inside).

[48] *See Abel*, 362 U.S. at 241; *Feguer*, 302 F.2d at 249.

[49] *See, e.g.*, *Feguer*, 302 F.2d at 249 (citing Hester v. United States, 265 U.S. 57, 58 (1924)).

[50] *See, e.g.*, *Abel*, 362 U.S. at 241.

[51] Professor Elizabeth E. Joh defined "abandoned DNA" as "human tissue," including blood, saliva, or hair, "capable of DNA analysis and separated from a targeted individual's person inadvertently or involuntarily." Elizabeth E. Joh, *Reclaiming "Abandoned" DNA: The Fourth Amendment and Genetic Privacy*, 100 NW. U. L. REV. 857, 858–59 (2006).

[52] *Id.* at 860–61.

[53] *Id.* at 861 (first citing Jaxon Van Derbeken, *How Alleged Serial Killer Fell into Trap*, S.F. CHRON., Sept. 21, 2003, at A1; then citing Andrew Blankstein & Richard Winton, *Man Is Charged in 1972 Murder*, L.A. TIMES, Sept. 10, 2003, at B3).

[54] *Id.* at 866; *see also* Laura A. Matejik, *DNA Sampling: Privacy and Police Investigation in a Suspect Society*, 61 ARK. L. REV. 53 (2008) (providing further examples and discussion of police use of abandoned DNA).

law applies to the human cells and tissue left behind, courts have found that the Fourth Amendment does not protect the DNA found inside.[55] Both abandoned genetic material and abandoned cell phones can expose an incredibly expansive and revealing amount of information about their owners, and these types of evidence deserve greater protection than the trash or contraband usually described in cases of abandonment.[56] While this Note does not take on the argument in support of protection for abandoned genetic material, this DNA case law demonstrates what happens when courts are slow to respond to privacy concerns caused by technological advances.

II. THE CASE OF *RILEY V. CALIFORNIA*

In June 2014, in *Riley v. California*, the Supreme Court unanimously prohibited police officers from warrantlessly searching cell phones found during searches incident to arrest.[57] The Court issued a joint ruling for two lower court cases involving searches of cell phones incident to arrest, *People v. Riley*[58] and *United States v. Wurie*,[59] both concerning "whether the police may, without a warrant, search digital information on a cell phone seized from an individual who has been arrested."[60] The

[55] Joh, *supra* note 51, at 868. Scholars such as Joh heavily criticize courts for applying abandonment doctrine to allow for police seizure of discarded items and the testing of "abandoned DNA" because it allows police to avoid "clear restraints" imposed on police search and seizures by the Fourth Amendment's warrant requirements. *See id.* at 861–62. Allowing police to test "detailed genetic information," even when "police have no more than a hunch about the suspect," is a violation of Fourth Amendment protections that has serious implications for all suspects' privacy, especially when those DNA matches lead to convictions. *See id*. For a discussion of applications of abandoned DNA beyond police use, including, for example, employers requiring genetic screening before hiring an employee and relatives hoping to disinherit genetically unrelated descendants, see Elizabeth E. Joh, *DNA Theft: Recognizing the Crime of Nonconsensual Genetic Collection and Testing*, 91 B.U. L. REV. 665 (2011) (arguing that nonconsensual DNA collection and analysis should be considered a criminal offense).

[56] Professor Joh, for example, likens a sample swab for DNA testing to a "microchip containing an entire library's worth of information." Joh, *supra* note 51, at 874. While DNA mapping can link a person to a crime, reveal their parentage, or expose predisposition for diseases, cell phones similarly contain a treasure trove of personal information.

[57] 134 S. Ct. 2473 (2014). Justice Alito wrote a separate opinion concurring in part and concurring in the judgment, agreeing that police "must generally obtain a warrant" to search information on cell phones incident to an arrest. *Id.* at 2495 (Alito, J., concurring in part and concurring in the judgment). He disagreed with the majority that police safety and the preservation of evidence are the only two justifications for the doctrine of search incident to arrest. *Id.* at 2495–96. He argued the search incident to arrest also developed to allow for the discovery of material evidence. *Id.* Justice Alito also argued that state legislatures and Congress should be able to pass their own laws about police searches of information on cell phones. *Id.* at 2497–98.

[58] No. D059840, 2013 WL 475242 (Cal. Ct. App. Feb. 8, 2013).

[59] 728 F.3d 1 (1st Cir. 2013).

[60] *Riley*, 134 S. Ct. at 2480 (majority opinion).

circumstances and reasoning behind the Court's ruling in *Riley* must be understood to justify expansions of the protections of cell phones to circumstances beyond searches incident to arrest.

The first case involved David Riley, who police pulled over for driving with expired registration tags.[61] During the stop, officers learned that Riley drove without a license, so they impounded his vehicle and did an inventory search, resulting in the discovery of two handguns under the hood of the car.[62] Officers then arrested Riley, and during their search of Riley incident to this arrest, they seized a smartphone[63] from his pocket.[64] Officers looked through the phone and found text messages and contacts with the letters "CK," which police believed meant "Crip Killers," linking Riley to the Bloods gang.[65] During a second search of the phone hours later at the police station, officers found incriminating evidence, including a photo of Riley standing in front of a car recently involved in a shooting.[66] After the trial court rejected Riley's motion to suppress the evidence found during the warrantless search of his phone, Riley was convicted for the shooting and attempted murder.[67] The California Court of Appeals affirmed that ruling.[68]

In the second case, police arrested Brima Wurie after witnessing him make a drug transaction from his car.[69] Officers seized two phones from Wurie's person, including a flip phone[70] that repeatedly rang with calls from a caller labeled "my house," causing police to open the phone, view a photograph of a woman and a baby, identify the phone number that had been calling, and then use that number to find an apartment building.[71] Officers went to that building, obtained a search warrant for the apartment number on the mailbox with Wurie's name, and found a firearm and large amount of crack cocaine, marijuana, and cash in the apartment.[72] The district court denied Wurie's motion to suppress evidence found during the

---

[61] *Id.*

[62] *Id.*

[63] The *Riley* Court defined smartphone as "a cell phone with a broad range of other functions based on advanced computing capability, large storage capacity, and Internet connectivity." *Id.*

[64] *Id.*

[65] *Id.*

[66] *Id.* at 2480–81.

[67] *Id.* at 2481.

[68] *Id.*

[69] *Id.*

[70] The *Riley* Court defined flip phone as "a kind of phone that is flipped open for use and that generally has a smaller range of features than a smart phone." *Id.*

[71] *Id.*

[72] *Id.*

search of the apartment as unlawful fruits of the initial search of his cell phone, and Wurie was convicted for distributing crack cocaine.[73] Unlike the California court in *People v. Riley*, the First Circuit reversed and vacated Wurie's conviction, holding that cell phones cannot be searched incident to arrest like other containers "because of the amount of personal data cell phones contain and the negligible threat they pose to law enforcement interests."[74]

A. Riley*'s Reasoning*

In an opinion written by Chief Justice Roberts, the Supreme Court upheld the First Circuit's increased protections for cell phones during searches incident to arrest. Chief Justice Roberts first emphasized the importance of obtaining a warrant before conducting a search.[75] Chief Justice Roberts then described the basis for the search-incident-to-arrest exception to the Fourth Amendment warrant requirement in *Chimel v. California*,[76] outlining the two justifications for search incident to arrest—ensuring officer safety and preventing destruction of evidence.[77] Chief Justice Roberts, quoting the Court's prior decision in *Chimel*, described the Court's rule for conducting a search incident to arrest: officers can conduct this search within the arrestee's "immediate control," meaning the "area from within which he might gain possession of a weapon or destructible evidence."[78] Thus, the Court noted that officers can examine containers discovered during these searches without a warrant or probable cause.[79]

Chief Justice Roberts rejected the search of cell phones incident to arrest because the *Chimel* justifications for searches incident to arrest did not apply to searches of cell phones. First, the Court reasoned that cell phones do not pose a safety risk to police, as "[d]igital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee's escape. . . . [D]ata on the phone can endanger no one."[80] The Court elaborated that destruction of evidence also does not

---

[73] *Id.* at 2482.

[74] *Id.* (citing United States v. Wurie, 728 F.3d 1, 8–11 (1st Cir. 2013)).

[75] *Id.* (holding that obtaining a warrant ensures that the decision to search is "drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime" (quoting Johnson v. United States, 333 U.S. 10, 14 (1948))).

[76] 395 U.S. 752 (1969).

[77] *Riley*, 134 S. Ct. at 2484.

[78] *Id.* at 2483 (quoting *Chimel*, 395 U.S. at 763).

[79] *Id.* at 2483–84 (noting that the Court in *Robinson* allowed the search of a cigarette package found in a pocket during a search after Robinson's arrest).

[80] *Id.* at 2485 (allowing officers to still search the physical aspects of the phone, like examining the inside of the case for a razor blade).

justify the warrantless search of phones during arrest because once officers separate the phone from the arrestee, there is "no longer any risk that the arrestee himself will be able to delete incriminating data from the phone."[81]

The Court also rejected the argument that third-party destruction of evidence through remote wiping[82] or data encryption[83] justifies immediate search of cell phones, as officers rarely encounter encryption because cell phones usually already have passcodes locking them to everyone but their owners.[84] Remote wiping also does not pose a threat to evidence because it can "be fully prevented by disconnecting [the] phone from the network" so it cannot receive a signal to erase data; officers can easily disconnect a phone by turning it off, removing its batteries, or placing the phone in a radio-wave cancelling container like a Faraday bag.[85]

The Court then justified treating cell phones differently than other items found during arrest because the traditional justification of search incident arrest does not apply. While normally a search incident to arrest involves only "minor additional intrusions compared to the substantial" intrusion that already occurs in all arrests, searches of cell phones are fundamentally more invasive than what courts have allowed in searches in the past.[86] As the Court eloquently described, "assert[ing] that a search of all data stored on a cell phone is materially indistinguishable from searches of these sorts of physical items . . . is like saying a ride on horseback is materially indistinguishable from a flight to the moon."[87] Instead, "[m]odern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse."[88]

---

[81] *Id.* at 2486.

[82] Remote wiping occurs when stored data on a phone is erased by a third party sending a remote signal to the phone or by a pre-installed program to erase data if the phone is brought outside set geographical limits. *Id.*

[83] According to the Court, when a phone is encrypted, the phone becomes "unbreakable" to law enforcement without a password. *Id.*

[84] *Id.* at 2486–87. Chief Justice Roberts suggested that officers who find a phone unlocked during a search incident to arrest can lawfully open the phone's settings to disable any "automatic-lock" or encryption features. *Id.* at 2487.

[85] *Id.* at 2487 (describing "Faraday bags" as "sandwich bags made of aluminum foil" that are "cheap, lightweight, and easy to use").

[86] *Id.* at 2488–89.

[87] *Id.* at 2488 (citation and internal quotation marks omitted).

[88] *Id.* at 2488–89. Chief Justice Roberts discussed the newness of the technology earlier in the opinion, stating:

> A smart phone of the sort taken from Riley was unheard of ten years ago; a significant majority of American adults now own such phones. . . . Both [Wurie's and Riley's] phones are based on technology nearly inconceivable just a few decades ago, when *Chimel* and *Robinson* were decided.

Chief Justice Roberts first outlined the "quantitative" differences between cell phones and other items that could be on an arrestee's person.[89] These differences include the huge storage capacity of cell phones, the privacy implications that massive data storage causes, and the pervasiveness of the devices in today's society.[90] The vast storage space on cell phones caused Chief Justice Roberts to call cell phones "minicomputers that also happen to have the capacity to be used as a telephone."[91] Chief Justice Roberts pointed out that "millions of pages of text, thousands of pictures, or hundreds of videos" can be stored on the phone itself.[92] Chief Justice Roberts reasoned:

> Most people cannot lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read . . . . And if they did, they would have to drag behind them a trunk of the sort held to require a search warrant in *Chadwick*, rather than the size of a cigarette package in *Robinson*.[93]

Data storage on cell phones provides a particularly dangerous threat to privacy because phones store many types of data in one place, including bank statements, prescriptions, and videos accumulated over months or even years, allowing an "individual's private life" to be "reconstructed."[94] The final quantitative concern came from the pervasiveness of cell phones, with the Court claiming that 90% of American adults owned a cell phone, and that nearly 75% of smartphone users kept their cell phone within five feet of them most of the time.[95] The Court worried that, while a decade ago it would be extremely rare for police to stumble upon a "highly personal item such as a diary," today virtually every adult stopped by the police will

---

Id. at 2484.

[89] *Id.* at 2489–90.

[90] *Id.*

[91] *Id.* at 2489. Chief Justice Roberts also lists the abilities of modern cell phones to act as "cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers." *Id.*

[92] *Id.*

[93] *Id.* (internal citation omitted). In *United States v. Chadwick*, the Supreme Court held that a 200-pound footlocker could not be searched incident to arrest. 433 U.S. 1, 4, 15 (1977). Note that *Riley* also questioned whether digital data storage devices like cell phones with internet connectivity could be treated like other packages because cell phones use the internet or data stored with "cloud computing" and thereby "access data located elsewhere, at the tap of a screen." 134 S. Ct. at 2491.

[94] *Riley*, 134 S. Ct. at 2489 ("The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. . . . A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a phone.").

[95] *Id.* at 2490 (citations omitted).

have a cell phone, filled with revealing information about its owner, on or near their person.[96]

After outlining the quantitative characteristics of cell phones, Chief Justice Roberts next asserted that cell phones also qualitatively differ from nondigital objects in the detailed personal information they contain, particularly in the internet history,[97] geographic location tracking,[98] and "apps"[99] on most cell phones.[100] Because of the incredible amount and the revealing type of information a cell phone contains, Chief Justice Roberts reasoned that

> a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form.[101]

Accordingly, the Supreme Court held that, in absence of extreme exigent circumstances, police officers must obtain a warrant to search any cell phone found on or near an arrestee's person during a search incident to arrest.[102]

---

[96] *Id.* Scholars have also explored the modern realities of the vast amount of data on mobile devices and the prevalence of these devices, just as Chief Justice Roberts detailed in his opinion. For example, Michael Arnold and Dennis Kiker explored the impact of "device-based data" on litigation in general, compiling much-needed and revealing data on the prevalence of mobile devices. Michael Arnold & Dennis R. Kiker, *The Big Data Collection Problem of Little Mobile Devices*, 21 RICH. J.L. & TECH. 1 (2015). Specifically, they cited to data compiled by the Pew Research Center demonstrating the percentages of American adults who own mobile devices: 90% have a cell phone, 58% have a smartphone, 32% own an e-reader, and 42% own a tablet computer. *Id.* at 2–3. They also recognized the dramatic increase in cell phone ownership: a 37% increase since 2000 and a 23% increase between 2012 and 2015. *Id.* at 3. While their work focuses on the effect of these devices and the data they contain, these studies mirror and support the arguments in *Riley* demonstrating the prevalence of these technologies.

[97] The Court provided an example of a revealing search: a search for "certain symptoms of disease, coupled with frequent visits to WebMD." *Riley*, 134 S. Ct. at 2490.

[98] The Court pointed out that "[h]istoric location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building." *Id.*

[99] The Court observed that the average smart phone user has thirty-three apps on his or her phone. *Id.* (citing Brief for Electronic Privacy Information Center (EPIC) et al. as Amici Curiae Supporting Petitioner at 9, *Riley*, 134 S. Ct. 2473 (No. 13-132)). The Court identified several examples of revealing apps: apps for news for different political parties, addiction, religion, tracking pregnancy symptoms, budget planning, and dating. *Id.*

[100] *Id.*

[101] *Id.* at 2491.

[102] *Id.* at 2495. See *infra* Section IV.B for further discussion of a possible exigent circumstance exception to abandoned cell phone searches.

B. Scholarly Reaction to Riley

This Note is the first to address *Riley*'s impact on the abandonment doctrine with regards to cell phones. Though unique, it falls within a larger framework of scholarship that documents doctrinal gaps that must be filled post-*Riley*. Since *Riley*, scholars studying the Fourth Amendment have explored its implications on privacy protections. Professors Adam Lamparello and Charles MacLean published an article months after *Riley* heralding the case as a significant step towards "the end of the Government's intrusion into the private digital lives of its citizens."[103] Lamparello and MacLean emphasized the significance of the Court abandoning ad hoc analysis of searches in favor of adopting "bright-line rules" protecting cell phone data that better recognize and protect the realities of modern communication and technology, equating digital communication to a new "public forum" deserving particular protection.[104] Calling *Riley* the "*Katz* for the digital age," the authors argue that *Riley* will cause tremendous changes beyond modernizing Fourth Amendment jurisprudence to reflect the value of privacy in the digital age and extend broader protection over this information from the government in general.[105] They argue, "soon the Government's ability to track metadata, record Internet browser history, apply the third-party doctrine to digital data, and peer into other aspects of our private lives will end—just like pre-digital era case law saw its relevance disappear in *Riley*."[106]

As this Note aims to do, other legal scholarship has similarly documented the gaps that need to be filled post-*Riley* to protect cell phone communications. In light of the sensitive and personal information

---

[103] Adam Lamparello & Charles MacLean, Riley v. California: *The New* Katz *or* Chimel*?*, 21 RICH. J.L. & TECH. 1, 8 (2014).

[104] *Id.* at 12, 14 ("[T]he Internet . . . is the digital age equivalent of traditional public and limited purpose public forums (e.g., public sidewalks and town halls), just as cellular telephones are similar to a private home for search and seizure purposes.").

[105] *Id.* at 17–19.

[106] *Id.* at 19. The third-party doctrine refers to an area of Fourth Amendment jurisprudence that holds individuals' expectations of privacy to be lower when individuals "knowingly transmit information through a third party." *Id.* at 16; *see, e.g.*, Smith v. Maryland, 442 U.S. 735, 744–46 (1979) (holding that information about dialed numbers tracked through a pen register do not receive protection because the phone user knew or should have known that information would be shared with the phone company). *Riley* undoubtedly has implications in this area of Fourth Amendment case law because essentially everything individuals transmit through their phones that *Riley* seeks to protect—from text messages to internet searches—relies on phone and internet providers who have access to that data. *See* Laurie Buchan Serafino, *"I Know My Rights, So You Go'n Need a Warrant for That": The Fourth Amendment,* Riley*'s Impact, and Warrantless Searches of Third-Party Clouds*, 19 BERKELEY. J. CRIM. L. 154 (2014) (analyzing the impact of *Riley* on the third-party doctrine considering the sharing of digital data with ISP providers). This would be an incredibly interesting implication of *Riley* to explore, but this discussion is too lengthy to be included in this Note.

contained in text messages, Lauren Harriman has argued, in a student comment, that *Katz*'s expectation of privacy analysis should extend the same protection to text messages as has been extended to phone conversations when police seek warrants for cell phone data.[107] Also in a student comment, Matthew Kugler explored the need to extend protection of digital devices to the context of border-crossing searches, contemplating whether an elevated-suspicion standard would be appropriate.[108] Kugler performed an original empirical study about the perception of the intrusiveness of electronic-device searches, finding people's perception "comparable to [the intrusiveness] of strip searches and body cavity searches," which require "elevated suspicion" of wrongdoing to be conducted during a border search.[109] He argued that in light of *Riley*'s "strong[] protect[ion] of individuals' privacy interests in electronic devices in the context of searches incident to arrest," even though the opinion did not address border searches, "it is extremely likely that the next round of border cases will grapple with the Court's willingness to write special rules for electronic devices in the arrest context."[110] This Note follows this trend of arguing for application of Fourth Amendment special protection for cell phones based on *Riley*.

While other scholars have correctly realized the need to change and adapt Fourth Amendment search and seizure rules to the realities of personal technology and digital communication, the implications of the abandonment doctrine allowing officers to search through lost or dropped cell phones without limits have yet to be explored. As Part III demonstrates, courts across the country actively allow police officers to search abandoned cell phones as if they were any other abandoned container or item of contraband. This Note builds on existing scholarship that has recognized the need to expand protection for cell phones and digital data and the possibility that *Riley* could completely modernize Fourth Amendment law to protect the incredibly sensitive private data on cell phones that a majority of Americans now carry. If the Court's

---

[107] Lauren Harriman, Comment, *Protecting Your Texting: Gaps in Fourth Amendment Protection for Modern Communication*, 19 INTELL. PROP. L. BULL. 79, 83 (2014) (arguing that probable cause needs to be present before officers can obtain text message content under the Stored Communications Act).

[108] Matthew B. Kugler, Comment, *The Perceived Intrusiveness of Searching Electronic Devices at the Border: An Empirical Study*, 81 U. CHI. L. REV. 1165, 1166–67 (2014).

[109] *Id.* ("The results show that people see the intrusiveness of electronic-device searches as comparable to that of strip searches and body cavity searches, which have generally been held to require elevated suspicion. Electronic searches are the *most* revealing of sensitive information and are only slightly less embarrassing than the most intimate searches of the body." (footnote omitted)).

[110] *Id.* at 1188.

reasoning in *Riley* is to be taken seriously, this Note argues that it mandates that police obtain warrants before searching an abandoned cell phone.

III. CURRENT TREATMENT OF ABANDONED CELL PHONES

While the Supreme Court has not ruled on whether or not abandoned cell phones can be searched without a warrant, both federal and state courts generally treat cell phones like any other abandoned item: the person who dropped it lost an expectation of privacy over the item, and the Fourth Amendment allows police to immediately search its contents. This Part provides a sampling[111] of cases denying protection for abandoned cell phones, first in federal courts, and then in state courts. This Part aims to survey how courts treat abandoned cell phones and samples selected cases across the country that have encountered motions to suppress evidence from defendants' cell phones. The Part includes both pre- and post-*Riley* cases to demonstrate the lack of protection for abandoned cell phones that did not change after *Riley*'s June 2014 mandate for special warrant requirements to protect the personal data on cell phones. The cases show that federal and state courts have not afforded abandoned cell phones the heightened protections they deserve, and that the Supreme Court's guidance regarding the privacy implications of cell phone searches in the search incident to arrest context had little impact in rulings on abandoned cell phones.

A. Federal Cases

Federal judges—including magistrates, district court judges, and circuit court judges—treat abandoned cell phones like any other abandoned evidence. In March 2014, a magistrate judge in the District Court for the District of Columbia denied a search warrant request to search the contents of a cell phone presumably thrown shortly after the suspect tossed a firearm while he fled from officers down an alley.[112] The judge called the

[111] There seem to be few cases published explicitly reviewing the constitutionality of searching abandoned cell phones: as of February 9, 2017, only twenty-nine cases are pulled up by a Westlaw search of the terms "'cell phone' /10 abandon." This Part considers all cases resulting from that search that involve suppression of evidence from abandoned cell phones, in addition to the *Black Kyocera Corp Model* case discussed *infra* note 112, found during an internet search of news articles about abandoned cell phones.

[112] *In re* Application of the U.S. for a Search Warrant for a Black Kyocera Corp Model C5170 Cellular Tel. with FCC ID: V65V5170, No. 14-231 (JMF), 2014 WL 1089442, at *1–2 (D.D.C. Mar. 7, 2014). The facts of the case involve a man, Rivers, spotted by officers reaching into his waistband, and when asked to see Rivers' waistband, Rivers fled down an alley. *Id.* at *1. Officers pursuing Rivers observed him throw a semiautomatic weapon before being stopped, and Rivers faces charges for unlawful possession of a handgun. *Id.* During their later investigation of the scene, officers found a Kyocera cell phone, and began looking through the unlocked phone to determine the identity of the

application "moot" because the phone was abandoned, and "a warrantless search of abandoned property does not violate the Fourth Amendment."[113] The court concluded that because the owner of the phone left it outside, the owner clearly revealed an intent to abandon the phone.[114] Beyond just allowing officers to search through everything stored on the phone, including "address books, call logs, phone books, photos, images, text messages, contact information, voice mails, images, video, and any other stored electronic data," the court went so far as to refuse to issue a warrant because of the abandonment rule.[115] Thus, the court in effect discouraged officers from applying for warrants to search abandoned cell phones in the future.

District court judges have similarly allowed abandoned cell phones to be searched without warrants. For example, the District Court for the Western District of Pennsylvania denied a motion to suppress evidence from a cell phone found in an alley near the scene of a murder because the owner had "no reasonable expectation of privacy" in the cell phone.[116] The court especially weighed the fact that the defendant never returned to try to retrieve the phone despite knowing he had dropped it and considered this to be evidence of intent to leave the phone behind.[117] Accordingly, the court held that the defendant had no Fourth Amendment right to challenge any search of that phone by police.[118]

Federal circuit courts have reaffirmed lower courts' practice of not protecting the data on abandoned cell phones. One example comes from the Sixth Circuit, which affirmed a district court's denial of a motion to

owner. *Id.* Officers saw numerous photos of firearms, including the firearm Rivers threw. *Id*. Officers applied for a warrant to search through the digital contents of the phone for evidence of the possession charge. *Id.* at *2.

[113] *Id.* at *2.

[114] *Id.*

[115] *Id.* (footnote omitted). Note that the court doubted there was probable cause to search through all of these "broad categories of information" as they might relate to the possession of firearms, but that by applying the abandonment rule, the court allowed officers to freely search through anything they could find on the phone. *Id.*

[116] United States v. Hanner, No. 02:05-cr-0385-02, 2007 WL 1437436, at *1, *5 (W.D. Pa. May 14, 2007).

[117] *Id.* at *5.

[118] *Id.; see also* United States v. Gaona-Gomez, No. 2:13-cr-00350, 2013 WL 3243619 at *2, *5 (S.D. Tex. Jun. 26, 2013) (denying the defendant's motion to suppress where the police answered a call from a phone found during an inventory search of a vehicle after arresting its driver for undocumented immigrant status, and as a result, the police intercepted a number of other undocumented aliens and charged Gaona-Gomez for helping smuggle undocumented aliens over the border). Note in this case the court's practice of calling "disclaimed" property abandoned property. *Id.* at *5. In this case, neither the defendant nor other occupants in the car claimed they owned the phone when asked by officers. *Id.*

suppress evidence from an abandoned cell phone.[119] In *United States v. Foster*, officers pulled over and searched the trunk of the defendant's car, finding a large paper sack of cocaine; the defendant fled on foot, leaving behind a cell phone plugged into a charger inside the vehicle.[120] The Sixth Circuit held that the defendant "fled from the scene and had abandoned the vehicle he was driving," actions that "extinguishe[d] any reasonable expectation of privacy the defendant might once have had in the property, together with any accompanying Fourth Amendment protections."[121]

The Tenth Circuit came to a very similar ruling in the case of *United States v. Washington*, where the defendant left a cell phone smashed under the bathroom sink of a hotel room linking him to a suspect arrested earlier with a large amount of marijuana.[122] The court refused to suppress evidence from the phone because the defendant "clearly abandoned the phone" after leaving it smashed under the sink, an action which indicated he intended to leave it in the room after the rental period expired, at which point he would lose any expectation of privacy in the hotel room.[123] The court focused its argument on the defendant's treatment of his phone as trash left in the room "for motel employees to collect and dispose of," evident from smashing his phone's screen and leaving it in a corner of the bathroom, and accordingly affirmed the lower court's denial of the motion to suppress the evidence obtained from the abandoned phone.[124]

United States v. Sparks offers the only post-*Riley* federal case to consider whether evidence from abandoned cell phones must be suppressed.[125] The Eleventh Circuit affirmed the refusal of a district court to suppress evidence of child pornography seized from a phone the defendants lost at a Wal-Mart.[126] The majority ruled that the defendants abandoned the phone after they called the store and learned that an employee had located their phone.[127] The court reasoned that because the defendants knew the name of the employee holding the phone for them, the

---

[119] United States v. Foster, 65 F. App'x 41, 43, 46 (6th Cir. 2003).

[120] *Id.* at 43.

[121] *Id.* at 46. It should be noted that the court recognized the only information police gained by searching the cell phone was the phone number associated with the phone, evidence the police would have discovered during their investigation anyway because they knew the identity of the defendant before he fled, making any error in its admission "harmless beyond a reasonable doubt." *Id.*

[122] 536 F. App'x 810, 810–11 (10th Cir. 2013).

[123] *Id.* at 811 (quoting United States v. Washington, No. 2:10-cr-03160-RB, 2011 WL 13135646, at *9 (D.N.M. Mar. 7, 2011)).

[124] *Id.* at 812.

[125] 806 F.3d 1323 (11th Cir. 2015), *cert. denied*, 136 S. Ct. 2009 (2016).

[126] *Id.* at 1329.

[127] *Id.*

owners voluntarily abandoned the device because they failed to attempt to "recover the phone with reasonable effort" and quickly bought a replacement.[128] By contrast, the dissenting opinion relied on *Riley* to find that the cell phone was not abandoned at all.[129] Judge Martin quoted *Riley* as evidence of the "status cell phones now have as property" in light of the "troves of information" on the lost phone, and concluded that the defendants "demonstrated no intent to abandon the cell phone."[130] Despite the dissent's insightful examination of *Riley*, the majority opinion rejected any heightened protections for abandoned cell phones in light of this Supreme Court ruling.[131]

This lack of protection from multiple influential federal circuit courts provides strong evidence of the need for the Supreme Court to take up this issue in light of *Riley* to better protect cell phones. To give proper respect to Supreme Court precedent, federal courts should begin to treat abandoned cell phones differently in light of the Court's unanimous mandate to protect cell phones.

Interestingly, federal judges have largely declined to publish cases about abandoned cell phones in the Federal Reporter, placing them instead in the Federal Appendix.[132] The choice to not extend precedential weight to

---

[128] *Id.* at 1347.

[129] *Id.* at 1354 (Martin, J., dissenting).

[130] *Id.* at 1353–54 ("When Mr. Johnson and Ms. Sparks lost their cell phone, they lost troves of information necessary for navigating modern life. Buying a replacement phone allowed them to begin reaccumulating this information. But getting a new phone does not mean they abandoned their interest in the unique information contained in the lost phone.").

[131] The majority did refer to *Riley* but only in the context of the private search doctrine. The majority relied on *Riley*'s protection for cell phone contents not viewed by a private searcher even when some contents had been viewed by a private party before law enforcement obtained a warrant. *Id*. at 1336 (majority opinion) ("[T]he Court emphasized that cell phones 'hold for many Americans the privacies of life.' It further observed the tremendous storage capacity of cell phones and the broad range of types of information that cell phones generally contain, suggesting that a search warrant for a cell phone must specify what part or parts of the information contained on it may be searched. While Widner's private search of the cell phone might have removed certain information from the Fourth Amendment's protections, it did not expose every part of the information contained in the cell phone." (quoting and citing Riley v. California, 134 S. Ct. 2473, 2489, 2494–95 (2014))). While the majority's consideration of the uniquely sensitive data on cell phones is an accurate takeaway from *Riley*, the Eleventh Circuit failed to expand this protection to the abandonment analysis in this case.

[132] Although *Black Kyocera Corp Model* came from a magistrate court, none of the remaining district court cases cited in this Part were published in a federal reporter. The Federal Rules of Appellate Procedure were amended in 2006 to allow citation of all opinions issued after January 1, 2007, even those that are "unpublished." FED. R. APP. P. 32.1(a). The committee note on the rule change, however, makes clear the rule change only addresses the *citation* of unpublished cases, and "says nothing about what effect a court must give to one of its unpublished opinions or to the unpublished opinions of another court." FED. R. APP. P. 32.1(a) advisory committee's note to 2006 amendment. Accordingly, the rule change did not increase the precedential value of unpublished opinions.

these rulings may suggest that federal district and circuit courts question rulings allowing officers to have open access to all information on cell phones found by officers, perhaps because federal judges realize that cell phones may indeed be different than other types of abandoned property and that searching these devices may pose a much stronger invasion of privacy to the person who left them behind, a sentiment echoed by this Note.[133]

B. State Cases

Unsurprisingly, state courts have analyzed abandoned cell phones in a similar fashion to that of federal courts. In California, a court of appeals allowed police to examine a cell phone dropped during a robbery of a Walgreens, revealing evidence that the defendant owned the phone, in effect linking him to the scene of the crime.[134] The court decided that even if the defendant accidentally dropped or "lost" the phone, the objective circumstances of the phone being left at the scene of the crime indicated the defendant lost any expectation of privacy in the phone's contents.[135]

In a post-*Riley* opinion, a Texas appellate court ruled that the defendant abandoned a cell phone when he hid it on the floor of a women's dressing room to record women trying on clothes at a department store.[136] Evidence from that phone was used to identify the defendant.[137] The court held the defendant lost a reasonable expectation of privacy in the cell phone because the defendant voluntarily left the changing room and the store, leaving the phone behind, and then failed to report it lost or retrieve it at the store or police station.[138] Despite being decided a year after *Riley*, the court never referred to the case.[139]

---

[133] *See* Karen Swenson, *Federal District Court Judges and the Decision to Publish*, 25 JUST. SYS. J. 121, 123 (2004) (suggesting judges decide to publish or not publish cases based on specific goals based on a "wish to make good law, to advance policy, and more"). Swenson points out that federal circuit and district courts must selectively publish, and analyzes the motivations behind judicial decisions to publish or not publish opinions, including that judges publish opinions that "mesh with their ideology." *Id.* at 121–22, 125.

[134] People v. Daggs, 34 Cal. Rptr. 3d 649, 650–51 (Ct. App. 2005).

[135] *Id.* at 651–52 (noting the defendant realized he might have dropped the phone at the Walgreens but did not attempt to retrieve it out of concern of being identified); *cf.* State v. Dixon, No. 13-09-00445-CR, 2010 WL 3419231, at *7–9 (Tex. App. Aug. 27, 2010) (holding that a cell phone could not be abandoned because the phone was stolen and the owner accordingly did not intentionally relinquish ownership of the device even though the defendant did not try to reclaim his phone for weeks after the theft).

[136] Royson v. State, No. 14-13-00920-CR, 2015 WL 3799698, at *3 (Tex. App. June 18, 2015).

[137] *Id.* at *1.

[138] *Id.* at *1, *4.

[139] In a similar case, another Texas court of appeals failed to consider *Riley* in the context of analyzing the privacy interest in an abandoned cell phone. *See* Wesley v. State, No. 08-14-00121-CR, 2016 WL1730356, at *4 (Tex. App. Apr. 29, 2016). This case is omitted, however, because it involved

Similarly, an Ohio appellate court allowed a warrantless search of a cell phone found in a pocket of a jacket left behind by a man fleeing Wal-Mart employees who attempted to apprehend him for theft.[140] In the *State v. Dailey* opinion, the court explicitly rejected a comparison to a *Riley*-like Ohio Supreme Court ruling that prohibited searches of cell phones during searches incident to arrest, and held the defendant lost all expectation of privacy in his phone when he voluntarily abandoned it with his jacket in the hands of a Wal-Mart employee.[141]

The South Carolina Court of Appeals quoted *Daggs* in similarly refusing to expand *Riley* to abandoned cell phones.[142] Here, the court refused to suppress evidence from a locked cell phone found at the scene of a burglary used to identify the defendant, even though the phone had a lock code.[143] Officers guessed the password and used photos and contact information to locate the defendant.[144] The court reasoned that the volume of a locked container's contents does not determine whether the container had been abandoned; instead, "objective indicia of the owner's intent" determine abandonment.[145] Interestingly, the dissenting opinion relied heavily on *Riley* to argue that the phone was not abandoned, referring to the vast amount of information a cell phone can contain.[146] The dissent rightfully argued that *Riley* should inform warrantless searches of cell phones in contexts other than searches incident to arrest.[147] However, the majority dismissed *Riley* as irrelevant, and found the search permissible because the owner had left the phone behind in the burglarized home and did not attempt to retrieve it from police, thus losing any expectation of privacy in the device.[148]

---

an analysis of an adult's expectations of privacy when that adult gives a child a cell phone to use—in essence, a phone lent to another, not a phone left behind or forgotten. *See id.*

[140] State v. Dailey, No. 8-10-01, 2010 WL 3836204, at *3 (Ohio Ct. App. Oct. 4, 2010).

[141] *Id.* at *4–5 (differentiating from a prior Ohio Supreme Court opinion, which held, like *Riley*, that warrantless searches of a cell phone incident to arrest violated the Fourth Amendment when there was no threat to officer safety and no exigent circumstances, because Dailey abandoned his cell phone (citing State v. Smith, 920 N.E.2d 949 (Ohio 2009))).

[142] State v. Brown, 776 S.E.2d 917, 923–24 (S.C. Ct. App. 2015).

[143] *Id.* at 919 n.1, 925.

[144] *Id.* at 919 & n.1 (explaining that the officer rightly guessed that the passcode was "1–2–3–4").

[145] *Id.* at 924.

[146] *Id.* at 926–27 (Konduros, J., dissenting) (citing Riley v. California, 134 S. Ct. 2473, 2488–91 (2014)).

[147] *Id.* at 926 ("Although *Riley* focused on how the search incident to arrest doctrine applies to modern cell phones, the decision provides guidance on the protection of privacy interests under the Fourth Amendment given substantial advancements in technology." (citing *Riley*, 134 S. Ct. at 2488–91)).

[148] *Id.* at 924–25 (majority opinion) ("Whether a container is locked or unlocked, once a reasonable amount of time in which to claim the container and its contents has passed, an objective assessment of

The passage of *Riley* so far has not influenced state courts' analysis of abandoned cell phones. Two of these cases took place in Texas; neither case cites *Riley*. In *Martinez v. State*, the defendant in a capital murder case in Texas appealed his conviction on the grounds of ineffective assistance of counsel for failure to attempt to suppress evidence from his cell phone found left behind at the victim's home, the scene of the murder.[149] Without referring to *Riley*, the court rejected the defendant's claim because the defendant had no grounds to protest the reasonableness of the search of his phone, which the court considered voluntarily abandoned property.[150] In a similar case, *Edwards v. State*, a Texas appellate court affirmed the denial of a motion to suppress evidence from a cell phone left on top of a stolen vehicle at the scene of an armed robbery.[151] Despite the fact that the defendant fled out of fear of police arriving on the scene, the court still considered the fact that the defendant left the phone on the car voluntarily, and thus held that he abandoned all privacy interests in his phone's contents.[152]

In another case decided in 2016 and post-*Riley*, the Washington Supreme Court echoed *Foster* in allowing police to search a cell phone found in an abandoned stolen vehicle when the driver fled on foot after being stopped by police.[153] Without a warrant, officers identified the driver by calling various contacts stored on the phone, which allowed them to track down the defendant.[154] The defendant made an argument on appeal similar to this Note's argument: "that the abandonment doctrine should not apply to cell phones or that there should be at least a heightened showing of

---

the circumstances leads a law enforcement officer to the inescapable conclusion that the owner of the container has abandoned the container and its contents. . . . [T]he mere use of a passcode does not always lead law enforcement to conclude the owner of the phone retained an expectation of privacy in the phone and its contents when other objective facts to the contrary are available." (citations omitted)).

[149] No. 08-14-00130, 2016 WL 4447660, at *1–2 (Tex. App. Aug. 24, 2016). Here, without a warrant, police made a call from the phone to a detective's phone to obtain the cell phone's number, which was used to identify the defendant. *Id.* at *3. The officers "took no further steps to peruse the contents of the phone." *Id.* at *4.

[150] *Id.* at *4 ("By leaving his cell phone in the Flores' residence, a place he had no right to be in the first place, he lost any legitimate expectation of privacy."); *see also* State v. Granville, 423 S.W.3d 399, 409 (Tex. Crim. App. 2014) ("Although a person may have a reasonable and legitimate expectation of privacy in the contents of his cell phone, he may lose that expectation under some circumstances, such as if he *abandons his cell phone*, lends it to others to use, or gives his consent to its search." (emphasis added) (footnote omitted)).

[151] Nos. 01-15-00416-CR, 01-15-00417-CR, 2016 WL 3401748, at *3, *10 (Tex. App. June 16, 2016).

[152] *Id.* at *9–10.

[153] State v. Samalia, 375 P.3d 1082, 1084 (Wash. 2016) (en banc).

[154] *Id.*

intent to abandon."[155] Although the court cited *Riley* and recognized that "cell phones may contain many intimate details of a person's life," the court ultimately refused to expand *Riley* protections to the cell phone because this phone was not seized during an arrest but was found in the abandoned vehicle; thus, the defendant in effect "abandoned his privacy interest in his cell phone."[156] The Washington Supreme Court noted that Chief Justice Roberts limited the holding in *Riley* to searches incident to arrest based on the underlying justifications for that warrant exception, and found that the same rationale did not apply to abandoned cell phones.[157]

The prevalence of cases across the country in both federal and state[158] courts allowing police to search abandoned cell phones demonstrates the importance and urgency in developing a consistent Fourth Amendment protection for the expansive data available on cell phones beyond searches incident to arrest. State and federal post-*Riley* cases that fail to extend *Riley*'s reasoning to abandoned phones reveal that the *Riley* decision alone might not lead courts to expand privacy protections of cell phones beyond searches incident to arrest to encompass discarded cell phones. An explicit Supreme Court ruling expanding *Riley* may eventually be needed to achieve heightened cell phone protection to all interactions with police. No scholars have actively engaged in analysis of this issue. This Note suggests that federal and state courts should treat cell phones differently from other abandoned evidence, a suggestion that is especially important when judges across the country treat abandoned cell phones as equally searchable as a discarded suitcase or bag of illicit drugs despite the frightening amount of information cell phone searches can reveal.

---

[155] *Id.* at 1087. The defendant relied on *Riley* in this argument as evidence of courts limiting the applicability of warrant exceptions to cell phones. *Id.* at 1088.

[156] *Id.* at 1086–87. In another post-*Riley* case, the Supreme Court of Arizona recognized the inherent privacy in cell phones in dicta, noting, "[c]ell phones are intrinsically private, and the failure to password protect access to them is not an invitation for others to snoop." State v. Peoples, 378 P.3d 421, 426 (Ariz. 2016). The case does not advance the purpose of this Note because the defendant left his cell phone in the defendant's girlfriend's home, and all parties and the court agreed that the defendant "did not abandon his cell phone." *Id.*

[157] *Samalia*, 375 P.3d at 1089 ("[T]he rationale driving the abandonment doctrine fits cell phone searches. When an individual voluntarily abandons an item, not as a facet of modern communication but to elude the police, that individual voluntarily exposes that item—and all information that it may contain—to anyone who may come across it. Cell phones are no different in this respect than for any other item; the abandonment doctrine applies to all personal property equally." (footnote omitted)).

[158] *But see* People v. Schutter, 249 P.3d 1123, 1126 (Colo. 2011) (en banc) (holding that an iPhone accidentally locked in a public restroom that the defendant could not retrieve without a store employee is not abandoned, and therefore "[a]ssuming, without deciding, that the Fourth Amendment could tolerate, under some set of circumstances, some kind of warrantless examination of a cell phone to ascertain how it might be returned to its owner, this case cannot present that set of circumstances").

IV. EXPANSION OF *RILEY*'S CELL PHONE PROTECTIONS TO ABANDONED PHONES

Although not yet practiced by courts, the logic behind the Supreme Court's need to protect cell phones during arrests applies just as convincingly to cell phones left behind by their users. Categorically, the Supreme Court clearly identified that cell phones "implicate privacy concerns far beyond those implicated by the search" of any other nondigital physical item or container because of cell phones' immense storage capacity and variety of detailed information.[159] The same invasion of privacy occurs during a warrantless search of a cell phone, regardless of whether that phone is found during an arrest or left behind by its owner. In light of the modern developments of personal technological devices and the Court's analysis in *Riley*, courts should develop a carve-out for cell phones from the abandonment exception to the Fourth Amendment and require police officers to obtain a search warrant before searching cell phones left behind by their owners. Examining the requirements to determine if an object has been abandoned, the qualities of a cell phone require different treatment whenever a left-behind cell phone is discovered by police.

A. The Mismatch Between Abandonment Doctrine and Cell Phones

In *Riley*, the Supreme Court clearly established the mandate for special protections over cell phones when discovered on the person of an arrestee. The same logic behind what makes a cell phone different than other containers during search incident to arrest—the vast amount of intensely private data each device holds—reveals that cell phones left behind do not fit within the doctrine of abandoned evidence. In light of *Riley*, courts should realize that individuals have both a subjective and objective expectation of privacy over the contents of their cell phones even if their phones were dropped or left behind, and the sensitive information cell phones contain make it highly unlikely someone would voluntarily relinquish any expectation of privacy over its contents.

1. Different Expectations of Privacy for Cell Phones and Contraband.—The uniquely personal contents of a cell phone recognized by the Supreme Court in *Riley* means that owners have a very high expectation of privacy over that data, requiring law enforcement to obtain warrants before searching these phones incident to arrest to ensure the legality of these invasive searches.[160] *Greenwood* demonstrates that the Supreme Court requires both subjective and objective reasonableness of the

[159] Riley v. California, 134 S. Ct. 2473, 2488–89 (2014).
[160] *Id.* at 2494–95.

expectation of privacy over an item before deeming that item protected by the Fourth Amendment.[161] It seems highly likely that people would generally claim a subjective expectation of privacy over their cell phones which society would find objectively reasonable. Considering the "digital record of nearly every aspect of [the owner's] li[fe]" that a cell phone contains, from dating information to GPS locations to long records of personal text messages and e-mails,[162] it becomes highly unlikely anyone would actually expect a stranger who came across their device to explore its contents.

This expectation of privacy becomes more evident and reasonable where a phone is password protected. Beyond subjectively demonstrating that the cell phone's owner took steps to keep the phone's contents private, this protective step would make it less likely that the phone would be subjected to "public inspection" because it requires knowing the code to access the phone's contents.[163] This expectation of privacy also becomes more reasonable as the phone's owner takes increasingly protective steps (i.e., longer passcodes or even fingerprint technology) to prevent strangers from breaking the code.[164]

Arguably when compared to cell phones found on one's person, as was the phone in *Riley*, an owner may have a lower expectation of privacy in an abandoned cell phone because he or she lost physical control of it. One may expect a Good Samaritan finding a lost phone to access the contact list to call a number labeled "home" or "mom" or look at recent calls or text messages to contact a friend or family member to return the phone to its owner. However, one would not expect someone who finds a

---

[161] California v. Greenwood, 486 U.S. 35, 39–40 (1988).

[162] *Riley*, 134 S. Ct. at 2489–90.

[163] *Cf. Greenwood*, 486 U.S. at 40–41 (holding that where individuals place "garbage 'in an area particularly suited for public inspection,'" they did not have a reasonable expectation of privacy over those items (quoting United States v. Reicherter, 647 F.2d 397, 399 (3d Cir. 1981))). Note, however, that courts have held that just because a cell phone has no password lock, it does not indicate the phone's owner has no "legitimate expectation of privacy." *See* State v. Peoples, 378 P.3d 421, 426 (Ariz. 2016) (holding that "personal belongings need not be locked for a legitimate expectation of privacy to exist" and that "[c]ell phones are intrinsically private, and the failure to password protect access to them is not an invitation for others to snoop"). The *Peoples* court cited to *United States v. Davis*, 332 F.3d 1163, 1167–68 (9th Cir. 2003), which held that one has a reasonable expectation of privacy in a closed, but unzipped gym bag, and *State v. LaPonsie*, 664 P.2d 223, 225 (Ariz. Ct. App. 1982), which held that even leaving a door "wide open" does not eliminate the expectation of privacy such that others can enter.

[164] For example, using fingerprint technology or a longer letter code may carry with it a stronger, more reasonable expectation of privacy than a typical four-digit code because these passwords become more difficult to guess. *See* Mike Gikas, *5 Steps to Protect Your Smart Phone from Theft or Loss*, CONSUMER REP. (Apr. 2014), http://www.consumerreports.org/cro/2014/04/5-steps-to-protect-your-smart-phone-against-theft-or-loss/index.htm [https://perma.cc/LZ8F-2N9P].

lost phone to, for example, search through GPS location history, bank account transactions, or months of photos stored on the phone. There remains an expectation of privacy over this more intimate, difficult-to-access data.

2. Unlikelihood of Voluntarily Abandoning a Cell Phone.—Beyond a constant expectation of privacy over cell phones—even those left behind—the *Katz*-based abandonment analysis requires subjective intent of an object's owner to knowingly and voluntarily leave an item behind.[165] The intensely revealing contents of a cell phone make it unlikely any cell phone owner would intentionally allow a stranger to gain free access to its contents.

In its prototypical application (i.e., the attempted disassociation from illegal contraband to prevent discovery by police), the abandonment doctrine risks exposing very little personal information—if any—and also presents a situation where it logically follows that the person holding the item wanted to abandon their claim over the item. Unlike contraband, it is quite likely that the phone's owner accidentally left their device behind. In the case of *People v. Daggs* discussed in Part III, for example, the court misapplied the abandonment doctrine to allow the search of a phone left behind at the scene of a crime because it acknowledged the phone's owner might have unintentionally dropped the phone;[166] if the defendant inadvertently dropped the phone, he by definition did not *intentionally or voluntarily* leave it behind. In this situation, the court should have realized that the owner accidently dropped his or her phone and feared returning to the crime scene to retrieve his device; instead of voluntarily leaving the phone behind for anyone who wanted to search it, the defendant was put in a situation where he had to leave his phone behind to avoid implicating himself in the robbery that had occurred there.[167] As the Fifth Circuit case of *United States v. Colbert* suggests, an item is not abandoned if the owner did not intentionally give up his or her privacy over it.[168]

While a person holding drugs would logically want to abandon them before encountering a police officer, it would be much less likely that same person would try to disassociate themselves from his or her phone, especially considering the treasure trove of identifying information on the

[165] United States v. Colbert, 474 F.2d 174, 176 (5th Cir. 1973) (implying that evidence is not abandoned if it occurs against the will of its owner).

[166] 34 Cal. Rptr. 3d 649, 651–52 (Ct. App. 2005).

[167] For a case mirroring this situation, see *id.* at 650.

[168] *See Colbert*, 474 F.2d at 176.

phone that would easily lead officers to the phone's owner.[169] While a person may want to voluntarily lose his or her expectation of privacy over drugs or a firearm that police are usually unable to connect to him or her, a cell phone often can be easily linked to its owner through photos, phone numbers, text messages, and accounts stored on the phone. Combined with the serious amount of personal data that would be exposed, the futility of the act of abandoning a cell phone makes it less likely that the owner intended to leave their device behind. Kugler's surveys of American adults revealed that the overwhelming majority of people consider a search through the contents of their cell phone to be both intrusive and embarrassing.[170] American adults would therefore be unlikely to voluntarily subject themselves to this intrusion and embarrassment.

The possibility of accidentally dropping a cell phone should also be carefully considered because of the pervasiveness of cell phone and smartphone use, and the fact that three-quarters of smartphone users keep their device within five feet of them at all times.[171] With the majority of device owners almost always having their phones on them, the likelihood that an unaccompanied phone was unintentionally left behind is quite high. Admittedly, when a police officer finds a cell phone unattended, it may be impossible to determine from the circumstances if its owner intended to lose the device or if it was accidentally dropped. In this situation, presuming an owner unintentionally left the device behind better protects the personal data on a cell phone, especially in light of the unlikelihood that its owner intended to allow a stranger to dig through its entire contents.

Beyond the benefit of protecting privacy in situations where it is unclear whether the owner intended to relinquish privacy over their cell phone, requiring officers to obtain a warrant before searching through an abandoned cell phone decreases the likelihood of police abuse after *Riley*. Now that officers need a warrant to search through a cell phone found during a search incident to arrest, it would be easy for officers to claim the

---

[169] Beyond identifying data in a cell phone, most cellular devices contain a serial number or International Mobile Station Equipment Identity (IMEI) code identifying the device with a unique engraved number identifying the phone's registered owner. *See, e.g.*, *Find the Serial Number or IMEI on Your iPhone, iPad or iPod Touch*, APPLE SUPPORT, https://support.apple.com/en-us/HT204073 [https://perma.cc/X7LL-P2CM] (describing the location of IMEI codes on different iPhone models).

[170] Kugler asked participants to rate, on a scale of 0 to 100, with 0 being "not at all" and 100 being "very," both how embarrassing and how intrusive they believed searches of various aspects of their cell phones would be. *See* Kugler, *supra* note 108, at 1194. Kugler found that for searches through text messages, the mean embarrassing rating was 81.94 and the mean intrusiveness rating was 92.91. *Id.* at 1198. For searches through e-mails, the mean embarrassing rating was 80.60 and the mean intrusiveness rating was 93.10. *Id.* Finally, for searches through photos, the mean embarrassing rating was 79.23 and the mean intrusiveness rating was 90.39. *Id.*

[171] Riley v. California, 134 S. Ct. 2473, 2490 (2014).

phone was found on the scene unattended by its owner or that they had witnessed the owner attempt to toss the phone before officers approached. This interpretation of the abandonment doctrine gives officers an easy way around the protections that the Supreme Court intended to give arrestees over the contents of their phones.[172] A bright-line rule requiring officers to obtain a warrant before searching an abandoned cell phone provides an effective tool to discourage police misconduct in handling these devices' sensitive information.[173]

B. What Riley *Revealed About Justifications for Warrantless Searches*

A carve-out from the abandonment doctrine could lead police and prosecutors to assert that they need to immediately access cell phones discovered in the pursuit of a criminal to aid in that pursuit or to locate co-conspirators. They might argue that applying a warrant requirement to abandoned cell phones could interrupt a pursuit, causing police to lose that person. In *United States v. Foster*, for example, officers used information found on a cell phone left in an abandoned vehicle to help identify a suspect who had fled on foot from a traffic stop.[174] California made similar arguments in defense of police searches of cell phones incident to arrest in *Riley*, arguing that police need to search cell phones after an arrest to "alert[] officers that confederates of the arrestee are headed to the scene."[175]

However, preventing police from being able to search through an abandoned cell phone without a warrant should not seriously hamper crime-fighting efforts. The Supreme Court rejected these concerns because of the lack of evidence demonstrating that this situation occurs often, and more importantly, the Court reasoned that this police interest "does not justify dispensing with the warrant requirement across the board."[176] This same reasoning applies to abandoned cell phones: the possibility that police need to immediately identify a dangerous, fleeing suspect by looking

---

[172] A Chicago Police report, for example, reveals numerous instances of police lying on the stand about the discovery of evidence, which are rarely discovered by judges or prosecutors. Steve Mills & Todd Lighty, *Cops Rarely Punished When Judges Find Testimony False, Questionable*, CHI. TRIB. (May 6, 2016, 10:24 AM), http://www.chicagotribune.com/news/local/breaking/ct-chicago-police-testimony-met-20160506-story.html [https://perma.cc/NWY4-RDJS].

[173] Note that the exclusionary rule allows defendants to have evidence obtained against them in violation of the Fourth Amendment suppressed and barred from use in their prosecutions, a procedure necessary to deter police from violating citizens' constitutional rights. *See* Mapp v. Ohio, 367 U.S. 643, 648 (1961) (explaining that the exclusionary rule is a "constitutionally required . . . deterrent safeguard" needed to prevent the Fourth Amendment from being "reduced to 'a form of words'" (quoting Silverthorne Lumber Co. v. United States, 251 U.S. 385, 392 (1920))).

[174] 65 F. App'x 41, 43 (6th Cir. 2003).

[175] *Riley*, 134 S. Ct. at 2485.

[176] *Id.* at 2485–86.

through a cell phone would be a rare occasion and does not justify removing categorical protections of abandoned cell phones. Furthermore, the Court allowed "case-specific exceptions to the warrant requirement" like "exigent circumstances"[177] to address these emergency situations with cell phones discovered during arrests;[178] these same exceptions and considerations could equally be considered in situations with abandoned cell phones. Accordingly, if police found a phone that they could prove in court contained information needed to protect themselves or others from imminent, serious danger, their crime-fighting efforts would not be hindered, as the exigent circumstances exception would apply. In extreme circumstances, if police were to find an abandoned cell phone they knew belonged to a fleeing suspect who was armed and dangerous, threatened to detonate a bomb, or knew the location of a kidnapped child, the exigent circumstances warrant exception would apply;[179] otherwise a warrant would be needed. In light of the privacy concerns the Court outlined in *Riley*, even if courts allowed exigent circumstances exceptions, it would be preferable to protect abandoned cell phones with this carve-out than to always allow warrantless searches.

Police advocates could alternatively argue that the delay in searching an abandoned cell phone to obtain a warrant puts valuable evidence on that phone at risk because of the chance for the phone's owner or a confederate to remotely wipe[180] or encrypt[181] data from the phone.[182] Again, the exigent circumstances exception could apply if officers know an abandoned cell

[177] *Id*. at 2486. The Fourth Amendment warrant exception for exigent circumstances applies when the arrestee poses a grave danger to the lives of others, while officers are in hot pursuit of a dangerous felon, or if there is an imminent threat of destruction of evidence. Minnesota v. Olson, 495 U.S. 91, 100–01 (1990) (holding no exigent circumstances justified officers in entering a home without a warrant when there was no suspicion the getaway driver for a murder inside was violent or posed a threat to others inside the home).

[178] *Riley*, 134 S. Ct. at 2486 ("The Fourth Amendment does not require police officers to delay in the course of an investigation if to do so would gravely endanger their lives or the lives of others." (quoting Warden v. Hayden, 387 U.S. 294, 298–99 (1967))); *id.* at 2494 (listing the common exigent circumstance justifications that could allow for warrantless cell phone searches, including protecting police safety, preventing evidence destruction, and aiding injured or at risk individuals).

[179] *Id.* at 2494.

[180] Wiping a phone can occur when a party sends a remote signal or when the phone is programmed to delete its data; wiping can also occur when the phone enters or leaves a programmed geographic area. *Id.* at 2486.

[181] Encryption renders a phone's data "unbreakable" by police unless they know the owner's password. *Id.*

[182] In *Riley*, the United States and California argued that the warrant requirement risks the "destruction of evidence." *Id.*; *see supra* Section II.A.

phone had data whose destruction was imminent.[183] The Court also doubted the prevalence of encryption and remote wiping of cell phones as a significant argument against a warrant requirement.[184] As discussed above, the Court in *Riley* outlined multiple steps police could take to prevent wiping or encryption, including Faraday bags and powering the phones off when discovered, that could also be used to preserve the data on an abandoned phone until a warrant is obtained.[185] Alternatively, police attempting to get data from a phone could also obtain the data through a warrant even after a phone is encrypted or locked. For example, a suspect's bank records or social media accounts could be later examined by logging into the accounts on a different device; call records, text messages, and photos and notes stored on the phone could also be accessed by going to the cell phone's service provider and asking for access to the "cloud" backing up the device remotely.[186]

It should also be noted that the Supreme Court rejected any arguments against a warrant requirement based on concerns that the requirement would "have an impact on the ability of law enforcement to combat crime" because "[c]ell phones have become important tools in facilitating coordination and communication among members of criminal

---

[183] *See, e.g.*, Kentucky v. King, 563 U.S. 452, 471–72 (2011) (allowing exigent circumstances to justify police entering an apartment without a warrant after hearing the sounds of destruction of illegal drugs outside the door). Note that to use this justification for a warrantless search, officers cannot threaten a search that violates the Fourth Amendment, in effect manufacturing the exigency themselves. *See id.* at 461–62 & 462 n.4. An exigent circumstance justification based on destruction of evidence may be almost impossible to argue in the case of a warrantless abandoned cell phone search unless officers knew the identity of the phone's owner and that the phone's owner imminently intended to wipe the phone.

[184] *Riley*, 134 S. Ct. at 2486–87. A Consumer Reports survey in 2014 suggested that only 8% of cell phone users have installed any type of software that can erase their phone's data, while only 7% of cell phone owners used encryption-like security features. Donna Tapellini, *Smart Phone Thefts Rose to 3.1 Million in 2013*, CONSUMER REPORTS (May 28, 2014, 4:00 PM), http://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm [https://perma.cc/HV8R-DLCN].

[185] *Riley*, 134 S. Ct. at 2487.

[186] *See* Serafino, *supra* note 106, at 162 (providing an overview of cloud storage for personal devices like cell phones and data accessible to internet service providers (ISPs), including Apple's privacy policy that allows Apple to disclose account information and content with law enforcement). Note that if Serafino's concerns that the third-party doctrine may make all data shared with an ISP outside Fourth Amendment protections is accurate, officers may not even need a warrant to look through this information. *See id.* at 155–56. In the recent high-profile case involving the San Bernardino shooter's iPhone, for example, the FBI admitted they could have accessed the phone through the shooter's iCloud account had the FBI not mistakenly ordered the account's password be reset. Cecilia Kang & Eric Lichtblau, *F.B.I. Error Locked San Bernardino Attacker's iPhone*, N.Y. TIMES (Mar. 1, 2016), http://www.nytimes.com/2016/03/02/technology/apple-and-fbi-face-off-before-house-judiciary-committee.html [https://perma.cc/59KW-T2EL].

enterprises."[187] Chief Justice Roberts pointed out that "technological advances" now allow officers to e-mail warrant requests to judges and obtain these warrants within fifteen minutes, making any concerns about delays less persuasive.[188] The Court has made it clear that the very cell phones that need increased protection have made delays in obtaining a search warrant negligible, an argument especially justifiable in light of the significant privacy interest protected by imposing warrant requirements for cell phones.

C. Protection for All Types of Cell Phones Including "Burner Phones"

If *Riley* is to be properly interpreted, heightened warrant requirements for abandoned cell phones would apply equally to all models of cellular phones, regardless of their technological capacities. Although some of *Riley*'s analysis focused on the privacy concerns of data only found on smartphones with more advanced capabilities, only some cell phones used today contain data from internet search history, location history, and app software.[189] Simpler models of cell phones contain less storage capacity and fewer technical functions with which personal information may be recorded.[190]

These distinctions should be irrelevant when applying *Riley* to abandoned cell phones, just as the Court comprehensively applied a warrant requirement to all cell phones discovered during an arrest regardless of the features of each individual phone. The Court may have been influenced by a desire to provide a bright-line rule for all cellular devices for ease of application; the Court also may have recognized that cell phone technology continues to advance, making simple flip phones increasingly scarce. Whatever the motivation, simple models of cell phones gained protection in *Riley* because even practically obsolete devices hold a relatively vast amount of personal information compared to

---

[187] *Riley*, 134 S. Ct. at 2493.

[188] *Id.* (citing Missouri v. McNeely, 133 S. Ct. 1552, 1573 (2013) (Roberts, C.J., concurring in part and dissenting in part)); *see id.* ("Recent technological advances similar to those discussed here have, in addition, made the process of obtaining a warrant itself more efficient." (citing *McNeely*, 133 S. Ct. at 1561–63)).

[189] *Id.* at 2490 (discussing the personal nature of data stored in internet search history and apps).

[190] Phone provider Cricket currently sells simple flip phones like the LG True, whose features include a camera and basic call, text, and photo message capabilities; the LG True also only has 256 MB of internal memory storage. *LG True*, CRICKET, https://www.cricketwireless.com/cell-phones/basic/lg-true.html [https://perma.cc/K5D7-EXD9]. While the phone does have some internet capabilities, it does not allow for app download. *Id.* By contrast, an iPhone 6S Plus offers the ability to download thousands of apps, video calling, internet connectivity over phone carriers and WiFi connections, and 32 to 128 GB of memory. *Compare iPhone Models*, APPLE, http://www.apple.com/iphone/compare/ [https://perma.cc/WK5J-ULJ7].

nontechnological devices. As the Court described, "[e]ven the most basic phones that sell for less than $20 might hold photographs, picture messages, text messages, Internet browsing history, a calendar, a thousand-entry phone book, and so on."[191] Significantly, the Court's ruling also combined two cases, including *Wurie* which involved a flip phone; the Court reasoned that its exception to the search incident to arrest doctrine needed to protect this device because of the personal information it still had capacity to contain—a phone directory, photos, and a call record.[192] According to this logic, an expansion of *Riley* to require warrants for abandoned cell phones should not differentiate protections based on the technology of each phone.

This blanket protection should also apply to a cell phone that police believe to be a "burner phone," a prepaid, inexpensive cell phone intended for temporary use to communicate criminal activities while evading police detection.[193] Law enforcement interests may argue that burner phones have a lower expectation of privacy because people use them specifically to commit crime, switching phones so often police cannot establish wiretaps before a new phone number is obtained and paying for prepaid phones in cash to avoid providing identifying information to service providers. After a short period, individuals involved in criminal activity could often intentionally abandon these phones to get rid of incriminating evidence.[194] It could be argued that people intentionally abandon the expectation of privacy over burner phones when they dispose of them, perhaps even expecting someone else to eventually access the data on the phone, and

---

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

[192] *See id.* at 2481–82, 2492–93.

[193] *See* Thomas Holt, *'Burner' Phones, Social Media, and Online Magazines: Understanding the Technology of Terrorism*, THE CONVERSATION (Apr. 28, 2016, 6:08 AM), http://theconversation.com/burner-phones-social-media-and-online-magazines-understanding-the-technology-of-terrorism-56727 [https://perma.cc/Y49W-DV34] (noting that terrorists, "[d]rug dealers, street prostitutes and other criminal groups in the U.S. regularly use [burner phones] for communication: they are cheap, plentiful and difficult to link to a real identity"). For example, Times Square car bombing suspect Faisal Shahzad used a prepaid Verizon cell phone for twelve days in 2010 to make calls to Pakistan and gather tools for his planned attack. Nate Anderson, *Times Square Bombing Suspect Used a "Burner" Phone*, ARS TECHNICA (May 5, 2010, 4:04 PM), http://arstechnica.com/tech-policy/2010/05/times-square-bombing-suspect-used-a-burner-phone/ [https://perma.cc/23WY-VX22].

[194] Politicians have noted the use of unregistered burner phones to commit criminal activity, and a bill has been introduced in Congress to close the "'burner phone' loophole" used by "terrorists, human traffickers, and narcotics dealers" to avoid law enforcement. *See* Press Release, Representative Jackie Speier, Speier Introduces Bill to Require ID When Purchasing "Burner Phones" and Other Pre-Paid Mobile Devices (Mar. 23, 2016), http://speier.house.gov/media-center/press-releases/speier-introduces-bill-require-id-when-purchasing-burner-phones-and [https://perma.cc/J4KW-MBFP] (describing H.R. 4886, the Closing the Pre-Paid Mobile Device Security Gap Act of 2016, which would require identification at the time of purchase of all cellular devices).

police should be able to treat burners differently than other cell phones. In theory, burner phones better fit the type of illegal contraband intentionally left behind in abandonment cases. However, in application, this reasoning is flawed.

First, even the simplest, most inexpensive models of phones contain information that the Court has deemed as private and invasive, including phone call records, text messages, photos, and digital contact books; this data is intensely private and can be revealing.[195] Second, and more importantly, when an abandoned, inexpensive flip phone is discovered, there is no way to know if the unknown person who left it behind used the phone as a burner or instead used it for personal, noncriminal activities. Many of these unadvanced models can be used in a prepaid capacity or under a contract, and using a prepaid phone does not necessarily implicate a person in criminal activity.[196] Police who come across these phones therefore cannot make assumptions about the phone's owner that have huge implications for whether the phone can be searched without a warrant. Requiring warrants for all models of abandoned cell phones best interprets *Riley*'s reasoning for increased cell phone protection and best protects privacy considering officers cannot know a person's intention in leaving the phone behind.

V. EXPANSION OF *RILEY*'S PROTECTIONS TO OTHER PERSONAL DEVICES

While not the focus of this Note, *Riley* could also be interpreted to apply to tablets and personal laptops that could conceivably be left behind by their owners. These devices hold much of the same tools as cell phones with an even larger storage capacity, and their search could result in a similar if not greater invasion of privacy. An iPad, for example, can be synced to an iPhone to receive text messages and phone calls,[197] contains a contact book, has a camera to record photos and videos, and also can contain applications logged into bank accounts and social media profiles.[198] However, the application of *Riley*'s reasoning to these devices could be limited because while they are commonly used, tablets may be less

---

[195] *See supra* note 192 and accompanying text.

[196] Even in light of the popularity of smartphones, because of their inexpensive rates, many advocate using an inexpensive "burner" phone as a second number. *See, e.g.*, Eric Griffith, *Burner Accounts 101: How to Get Extra Numbers for Your Smartphone*, PCMAG.COM (Jan. 18, 2016), http://www.pcmag.com/article2/0,2817,2497669,00.asp [https://perma.cc/H4J9-PBUU] (advocating the use of a prepaid phone for coordinating sales on Craigslist, managing Airbnb listings, or online dating).

[197] *See Add or Remove Your Phone Number in iMessage or FaceTime on Your iPad, iPod Touch, or Mac*, APPLE SUPPORT, https://support.apple.com/en-ca/HT201349 [https://perma.cc/2AMW-WNY3].

[198] *See iPad Pro*, APPLE, http://www.apple.com/ipad-pro/specs/ [https://perma.cc/G5AP-RZNQ].

pervasive and less frequently used in everyday life than cell phones.[199] The Court specifically based its reasoning for warrant protections of cell phones not only on the private data in cell phones, but also because such a tremendous portion of the population uses cell phones, making them a pervasive part of everyday life; the Court cited one study that stated that almost 75% of smartphone owners are always within five feet of their phone.[200] Unlike cell phones, most people do not always have a tablet or laptop nearby and do not constantly carry them around; in effect, it becomes less of a concern for courts to protect these devices during a search incident to arrest. Similar logic applies to the abandonment of these devices. Because the devices are less common, it becomes less common that a tablet or laptop would be abandoned, which perhaps challenges *Riley*'s application to these devices.

In terms of abandonment theory, however, individuals are even less likely to voluntarily relinquish their expectation of privacy over tablets and personal laptops than they might with cell phones. Because of the higher cost of these devices, it becomes less likely someone would use a device temporarily with the intent to eventually discard it. Their increased physical size also makes accidentally dropping a tablet or laptop less likely. Regardless, just as *Riley* reveals that the private data contained on a cell phone makes it unlikely an owner would ever voluntarily allow strangers to rummage through it, left-behind tablets and laptops would rarely meet the requirements of intent needed for abandoned evidence, and further research would likely conclude that a warrant should be required for their search as well.

CONCLUSION

The application of heightened Fourth Amendment protections for cell phones demonstrates just one way *Riley v. California* should be expanded to address modern privacy concerns. *Riley* recognized the need for protection of personal technology, a need that grows more dire as technology advances and people carry around more information. The more cell phones can do, the more the data on these devices can reveal about a person's private information, and the more they need to be shielded by the Fourth Amendment. Beyond abandoned cell phones, *Riley* could be expanded to protect all personal devices when discovered by police in

[199] *See* Ben Taylor, *5 Ways the Smartphone Is Conquering the Tablet*, PCWORLD (Feb. 26, 2015, 3:30 AM), http://www.pcworld.com/article/2889275/phones/5-ways-the-smartphone-is-conquering-the-tablet.html [https://perma.cc/72J7-J5YU].

[200] Riley v. California, 134 S. Ct. 2473, 2490 (2014); *see supra* notes 94–95.

multiple instances; this Note explores only one possible expansion.[201] While *Riley* marks an important advancement in personal privacy, search and seizure jurisprudence, especially in the realm of abandonment and personal technology, needs to continue to expand to better reflect the modern realities of the vast amount of data Americans generate and carry with them every day.

[201] Eventually, cell phones may need exemption from all warrantless searches based on the vast amount of private information they contain. Fourth Amendment doctrine has adapted in the past to recognize blanket exceptions for other categories to protect privacy of citizens, including heightened protections for the home. For examples of categorical protections of the home, see *Kyllo v. United States*, 533 U.S. 27, 33, 40 (2001), which required a warrant for sense-enhancing technology that gains information about the interior of the home because of the special right to privacy in the home under the Constitution, and *Payton v. New York*, 445 U.S. 573, 576 (1980), which required an arrest warrant to enter a suspect's home without consent and make a felony arrest. Significantly, *Riley* seems to foreshadow this eventual expansion:

> a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information *never found in a home in any form*.

Riley, 134 S. Ct. at 2490–91 (second emphasis added) (referring to Judge Learned Hand's statement that the Constitution protects a citizen from police "ransacking his house for everything which may incriminate him" (quoting United States v. Kirschenblatt, 16 F.2d 202, 203 (2d Cir. 1926))); *see also* Lamparello & MacLean, *supra* note 103, at 14 ("[C]ellular telephones are similar to a private home for search and seizure purposes.").